Benutzerhandbuch für Integrated Dell Remote Access Controller 9

Juni 2021
Rev. A01

Hinweise, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und zeigt, wie diese vermieden werden können.

WARNUNG: Mit WARNUNG wird auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen kann.

© 2021 Dell Inc. oder ihre Tochtergesellschaften. Alle Rechte vorbehalten. Dell, EMC und andere Marken sind Marken von Dell Inc. oder entsprechenden Tochtergesellschaften. Andere Marken können Marken ihrer jeweiligen Inhaber sein.

Inhaltsverzeichnis

Kapitel 1: Übersicht über den iDRAC....16
Vorteile der iDRAC-Verwendung....16
Wichtige Funktionen....17
Neue Funktionen hinzugefügt....19
Firmware version 5.00.00.00....19
Verwendung dieses Benutzerhandbuchs....20
Unterstützte Webbrowser....20
Unterstützte Betriebssysteme und Hypervisoren....20
iDRAC-Lizenzen....20
Types of licenses....21
Methoden zum Erwerb von Lizenzen....21
Erwerben von Lizenzschlüssel vom Dell digitalen Schließfach....22
Lizenzvorgänge....22
Lizenzierte Funktionen in iDRAC9....23
Schnittstellen und Protokoll für den Zugriff auf iDRAC....29
iDRAC-Schnittstelleninformationen....32
Weitere nützliche Dokumente....33
Kontaktaufnahme mit Dell....33
Zugriff auf Dokumente der Dell Support-Website....34
Zugriff auf Redfish API-Handbuch....34

Kapitel 2: Anmelden bei iDRAC....35
Kennwortänderung erzwingen (FCP)....36
Anmeldung bei iDRAC mit OpenID Connect....36
Logging in to iDRAC as local user, Active Directory user, or LDAP user....36
Bei iDRAC über eine Smartcard als lokaler Nutzer anmelden....37
Bei iDRAC über eine Smart Card als Active Directory-Benutzer anmelden....38
Bei iDRAC über die einmalige Anmeldung anmelden....38
Bei iDRAC SSO über die iDRAC-Webschnittstelle anmelden....38
Bei iDRAC SSO über die CMC-Webschnittstelle anmelden....39
Über Remote-RACADM auf iDRAC zugreifen....39
Zertifizierungsstellenzertifikat für die Verwendung von Remote-RACADM auf Linux validieren....39
Über lokalen RACADM auf iDRAC zugreifen....39
Über Firmware-RACADM auf iDRAC zugreifen....40
Einfache Zwei-Faktor-Authentifizierung (einfache 2FA)....40
RSA SecurID 2FA....40
Systemzustand anzeigen....41
Anmeldung beim iDRAC mit Authentifizierung mit öffentlichem Schlüssel....42
Mehrere iDRAC-Sitzungen....42
Standardkennwort sichern....43
Lokales Zurücksetzen des standardmäßigen iDRAC-Kennworts....43
Wiederherstellen des iDRAC-Standardkennworts im Remote-Zugriff....44
Ändern des standardmäßigen Anmeldekennworts....45
Ändern des standardmäßigen Anmeldekennworts unter Verwendung der Webschnittstelle....45

Ändern des in den Standardeinstellungen festgelegten Anmeldungskennworts unter Verwendung von RACADM....45
Ändern des standardmäßigen Anmeldekennworts unter Verwendung des Dienstprogramms für iDRAC-Einstellungen....45
Aktivieren oder Deaktivieren der standardmäßigen Kennwortwarnungsmeldung....46
Richtlinie zur Kennwortsicherheit....46
IP-Blockierung....46
Aktivieren und Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung der Web-Schnittstelle....47
Warnungen über RACADM aktivieren oder deaktivieren....48

Kapitel 3: Managed System einrichten....49
iDRAC-IP-Adresse einrichten....49
iDRAC-IP-Adresse über das Dienstprogramm für die iDRAC-Einstellungen einrichten....50
iDRAC-IP-Adresse über die CMC-Webschnittstelle einrichten....53
Auto-discovery....54
Konfigurieren von Servern und Serverkomponenten mithilfe der automatischen Konfiguration....56
Verwenden von Hash-Kennwörtern für mehr Sicherheit....62
Einstellungen für lokales Administratorkonto ändern....63
Standort für das Managed System einrichten....63
Standort des Managed System über die Web-Schnittstelle einrichten....64
Standort für Managed System über RACADM einrichten....64
Standort für Managed System über das Dienstprogramm für die iDRAC-Einstellungen einrichten....64
Systemleistung und Stromverbrauch optimieren....64
Thermische Einstellungen über die iDRAC-Webschnittstelle ändern....65
Thermische Einstellungen unter Verwendung von RACADM ändern....66
Thermische Einstellungen unter Verwendung vom Dienstprogramm für die iDRAC-Einstellungen ändern....70
Ändern von PCIe Airflow-Einstellungen über die iDRAC-Webschnittstelle....71
Management Station einrichten....71
Per Remote auf iDRAC zugreifen....71
Konfigurieren von unterstützten Webbrowsern....72
Internet Explorer konfigurieren....72
Konfiguration von Mozilla Firefox....73
Web-Browser für die Verwendung der virtuellen Konsole konfigurieren....74
Lokalisierte Versionen der Webschnittstelle anzeigen....77
Updating device firmware....78
Firmware über die iDRAC-Webschnittstelle aktualisieren....81
Planung automatischer Firmware-Aktualisierungen....82
Aktualisieren der Gerätefirmware über RACADM....83
Firmware über die CMC-Web-Schnittstelle aktualisieren....84
Firmware über DUP aktualisieren....84
Firmware über Remote-RACADM aktualisieren....85
Firmware über die Lifecycle-Controller-Remote-Dienste aktualisieren....85
Aktualisieren der CMC-Firmware über iDRAC....85
Anzeigen und Verwalten von gestuften Aktualisierungen....86
Anzeigen und Verwalten gestufter Aktualisierungen unter Verwendung der iDRAC Webschnittstelle....86
Anzeigen und Verwalten gestufter Aktualisierungen unter Verwendung von RACADM....86
Rollback der Geräte-Firmware durchführen....86
Rollback für die Firmware über die iDRAC-Webschnittstelle durchführen....87
Rollback der Firmware über die CMC-Web-Schnittstelle durchführen....87

Rollback der Firmware über RACADM durchführen....88
Rollback der Firmware über Lifecycle-Controller durchführen....88
Rollback der Firmware über die Remote-Dienste für den Lifecycle Controller durchführen....88
iDRAC wiederherstellen....88
Easy Restore (Einfache Wiederherstellung)....88
iDRAC über andere Systemverwaltungs-Tools überwachen....89
Unterstützung des Serverkonfigurationsprofils – Import und Export....89
Importieren des Server-Konfigurationsprofils mithilfe der iDRAC-Webschnittstelle....90
Exportieren des Server-Konfigurationsprofils mithilfe der iDRAC-Webschnittstelle....90
Sichere Startfunktion-Konfiguration über BIOS-Einstellungen oder F2....91
BIOS recovery....92

Kapitel 4: Plugin Management....93

Kapitel 5: iDRAC konfigurieren....94
iDRAC-Informationen anzeigen....95
iDRAC-Informationen über die Webschnittstelle anzeigen....95
iDRAC-Informationen über RACADM anzeigen....96
Netzwerkeinstellungen ändern....96
Netzwerkeinstellungen über die Weboberfläche ändern....96
Netzwerkeinstellungen über einen lokalen RACADM ändern....96
IP-Filterung konfigurieren....97
Chiffresammlungs-Auswahl....98
Chiffresammlungs-Auswahl über die iDRAC-Webschnittstelle konfigurieren....98
Chiffresammlungs-Auswahl mithilfe von RACADM konfigurieren....99
Modus FIPS (Konfiguration)....100
FIPS-Modus aktivieren....100
Deaktivieren des FIPS-Modus....100
Dienste konfigurieren....101
Services unter Verwendung der Weboberfläche konfigurieren....101
Dienste über RACADM konfigurieren....102
SEKM-Funktionen....102
Aktivieren oder Deaktivieren der HTTPS-Umleitung....103
Using VNC client to manage remote server....103
Konfigurieren von VNC-Server unter Verwendung der iDRAC-Webschnittstelle....104
VNC-Server unter Verwendung von RACADM konfigurieren....104
Einrichten von VNC Viewer mit SSL-Verschlüsselung....104
Einrichten von VNC Viewer ohne SSL-Verschlüsselung....104
Anzeige auf der Frontblende konfigurieren....105
LCD-Einstellung konfigurieren....105
LED-Einstellung für die System-ID konfigurieren....106
Das Konfigurieren von Zeitzone und NTP....106
Konfigurieren von Zeitzone und NTP unter Verwendung der iDRAC- Web-Schnittstelle....106
Konfigurieren von Zeitzone und NTP unter Verwendung von RACADM....107
Erstes Startlaufwerk einstellen....107
Erstes Startgerät über die Web-Schnittstelle einrichten....107
Erstes Startgerät über RACADM festlegen....108
Einstellen des ersten Startgeräts unter Verwendung der virtuellen Konsole....108
Bildschirm „Letzter Absturz“ aktivieren....108

Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough....108
Unterstützte Karten für Betriebssystem-zu-iDRAC-Passthrough....109
Unterstützte Betriebssysteme für USB-NIC....109
Aktivieren und Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung der Web-Schnittstelle....110
Aktivieren und Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung von RACADM....111
Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung des Dienstprogramms für iDRAC-Einstellungen....111
Zertifikate abrufen....112
SSL-Serverzertifikate....113
Neue Zertifikatsignierungsanforderung erstellen....113
Automatische Zertifikatregistrierung....114
Serverzertifikat hochladen....114
Serverzertifikat anzeigen....115
Hochladen eines benutzerdefinierten Signaturzertifikats....116
Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat herunterladen....116
Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat löschen....117
Mehrere iDRACs über RACADM konfigurieren....117
Zugriff zum Ändern der iDRAC-Konfigurationseinstellungen auf einem Host-System deaktivieren....118

Kapitel 6: Delegierte Autorisierung mithilfe von OAuth 2.0....119

Kapitel 7: Anzeigen von Informationen zu iDRAC und zum Managed System....120
Zustand und Eigenschaften des Managed System anzeigen....120
Konfigurieren der Assetnachverfolgung....120
Viewing system inventory....121
Sensorinformationen anzeigen....122
Überwachen des Leistungsindex für CPU, Arbeitsspeicher und Eingabe-/Ausgabemodule....123
Überwachen des Leistungsindex von CPU, Speicher und E/A-Modulen über die Webschnittstelle....124
Überwachen des Leistungsindex für CPU-, Speicher- und E/A-Module über RACADM....125
Erkennung inaktiver Server....125
GPU-Verwaltung (Beschleuniger)....126
Das System auf Frischlufttauglichkeit überprüfen....127
Temperaturverlaufsdaten anzeigen....127
Anzeigen der Temperaturverlaufsdaten über die iDRAC-Webschnittstelle....128
Temperaturverlaufsdaten über RACADM anzeigen....128
Konfigurieren des Warnungsschwellenwerts für die Einlasstemperatur....128
Anzeigen der auf dem Host-Betriebssystem verfügbaren Netzwerkschnittstellen....129
Anzeigen von verfügbaren Netzwerkschnittstellen auf dem Host-Betriebssystem über die Webschnittstelle....129
Anzeigen der auf dem Host-Betriebssystem verfügbaren Netzwerke über RACADM....130
Verbindungen der FlexAddress-Mezzanine-Kartenarchitektur anzeigen....130
Anzeigen und Beenden von iDRAC-Sitzungen....130
Beenden der iDRAC-Sitzungen über die Webschnittstelle....130

Kapitel 8: Einrichten der iDRAC-Kommunikation....132
Mit iDRAC über eine serielle Verbindung über ein DB9-Kabel kommunizieren....133
BIOS für serielle Verbindung konfigurieren....133
Serielle RAC-Verbindung aktivieren....134

Grundlegenden seriellen IPMI-Verbindungs- und -Terminalmodus aktivieren... 134
Von der seriellen RAC-Verbindung auf die serielle Konsolenverbindung bei Verwendung eines DB9-Kabels umschalten... 136
Von der seriellen Konsole auf die serielle RAC-Verbindung umschalten... 136
Von der seriellen RAC-Verbindung auf die serielle Konsole umschalten... 136
Mit iDRAC über IPMI SOL kommunizieren... 137
BIOS für serielle Verbindung konfigurieren... 137
iDRAC für die Verwendung von SOL konfigurieren... 137
Unterstütztes Protokoll aktivieren... 138
Mit iDRAC über IPMI über LAN kommunizieren... 141
IPMI über LAN mithilfe der Web-Schnittstelle konfigurieren... 142
IPMI über LAN mithilfe des Dienstprogramms für die iDRAC-Einstellungen konfigurieren... 142
IPMI über LAN mithilfe von RACADM konfigurieren... 142
Remote-RACADM aktivieren oder deaktivieren... 143
Remote-RACADM über die Web-Schnittstelle aktivieren oder deaktivieren... 143
Remote-RACADM über RACADM aktivieren oder deaktivieren... 143
Lokalen RACADM deaktivieren... 143
IPMI auf Managed System aktivieren... 143
Linux während des Starts in RHEL 6 für die serielle Konsole konfigurieren... 143
Anmeldung an der virtuellen Konsole nach dem Start aktivieren... 144
Konfigurieren des seriellen Terminals in RHEL 7... 146
Steuern von GRUB von der seriellen Konsole... 146
Unterstützte SSH-Verschlüsselungssysteme... 147
Authentifizierung von öffentlichen Schlüsseln für SSH verwenden... 148

Kapitel 9: Benutzerkonten und Berechtigungen konfigurieren... 151
iDRAC-Benutzerrollen und -Berechtigungen... 151
Empfohlene Zeichen in Benutzernamen und Kennwörtern... 152
Lokale Benutzer konfigurieren... 153
Lokale Benutzer über die iDRAC-Webschnittstelle konfigurieren... 153
Lokale Benutzer über RACADM konfigurieren... 153
Konfigurieren von Active Directory-Nutzern... 155
Voraussetzungen für die Verwendung der Active Directory-Authentifizierung für iDRAC... 155
Unterstützte Active Directory-Authentifizierungsmechanismen... 157
Übersicht des Standardschema-Active Directory... 157
Active Directory-Standardschema konfigurieren... 158
Übersicht über Active Directory mit erweitertem Schema... 160
Active Directory mit erweitertem Schema konfigurieren... 162
Active Directory-Einstellungen testen... 170
Generische LDAP-Benutzer konfigurieren... 171
Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mit der iDRAC-Webschnittstelle... 171
Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mittels RACADM... 172
Einstellungen für LDAP-Verzeichnisdienst testen... 172

Kapitel 10: Systemkonfigurations-Sperrmodus... 173

Kapitel 11: iDRAC für die einfache Anmeldung oder Smart Card-Anmeldung konfigurieren... 175
Voraussetzungen für die einmalige Active Directory-Anmeldung oder die Smart Card-Anmeldung... 175
iDRAC im Domänennamensystem registrieren... 175

Active Directory-Objekte erstellen und Berechtigungen bereitstellen....176
iDRAC-SSO-Anmeldung für Active Directory-Benutzer konfigurieren....176
Erstellen eines Nutzers in Active Directory für SSO....176
Kerberos Keytab-Datei generieren....177
iDRAC-SSO-Anmeldung für Active Directory-Benutzer über die Webschnittstelle konfigurieren....177
iDRAC SSO-Anmeldung für Active Directory-Benutzer über RACADM konfigurieren....178
Management Station-Einstellungen....178
Smartcard-Anmeldung aktivieren oder deaktivieren....178
Smart Card-Anmeldung über die Web-Schnittstelle aktivieren oder deaktivieren....178
Smart Card-Anmeldung über RACADM aktivieren oder deaktivieren....179
Smart Card-Anmeldung über das Dienstprogramm für die iDRAC-Einstellungen aktivieren oder deaktivieren....179
Konfigurieren von Smart Card-Anmeldung....179
iDRAC-Smart-Card-Anmeldung für Active Directory-Benutzer konfigurieren....179
iDRAC-Smart Card-Anmeldung für lokale Benutzer konfigurieren....179
Anmelden mit Smart Card....181

Kapitel 12: iDRAC für das Versenden von Warnungen konfigurieren....182
Warnungen aktivieren und deaktivieren....182
Warnungen über die Web-Schnittstelle aktivieren oder deaktivieren....182
Warnungen über RACADM aktivieren oder deaktivieren....183
Warnungen über das Dienstprogramm für iDRAC-Einstellungen aktivieren oder deaktivieren....183
Warnungen filtern....183
Filtern von Warnungen über die iDRAC-Webschnittstelle....183
Warnungen über RACADM filtern....184
Ereigniswarnungen einrichten....184
Ereigniswarnungen über die Web-Schnittstelle einrichten....184
Ereigniswarnungen über RACADM einrichten....184
Alarmwiederholungsereignis einrichten....185
Alarmwiederholungsereignis über RACADM einrichten....185
Einrichten eines Alarmwiederholungsereignisses über die iDRAC-Webschnittstelle....185
Ereignismaßnahmen festlegen....185
Ereignismaßnahmen über die Web-Schnittstelle einrichten....185
Ereignismaßnahmen über RACADM einrichten....185
Einstellungen für E-Mail-Warnungs-SNMP-Trap oder IPMI-Trap konfigurieren....186
IP-basierte Warnziele konfigurieren....186
Konfigurieren von E-Mail-Benachrichtigungen....188
Konfigurieren von WS-Ereignisauslösung....190
Konfigurieren von Redfish-Ereignissen....190
Überwachung von Gehäuseereignissen....190
Überwachung von Gehäuseereignissen unter Verwendung der iDRAC-Webschnittstelle....191
Überwachung von Gehäuseereignissen unter Verwendung von RACADM....191
IDs für Warnungsmeldung....191

Kapitel 13: iDRAC 9 Group Manager....194
Group Manager....194
Ansicht „Zusammenfassung“....195
Konfigurationsanforderungen des Netzwerks....196
Anmeldungen verwalten....197
Einen neuen Benutzer hinzufügen....197

Benutzerkennwort ändern....198
Benutzer löschen....198
Warnungen konfigurieren....198
Exportieren....198
Ansicht „Discovered Servers“ (Ermittelte Server)....199
Ansicht „Jobs“ (Aufgaben)....200
Jobs-Export....201
Gruppeninformationsbedienfeld....201
Gruppeneinstellungen....201
Aktionen für einen ausgewählten Server....202
iDRAC-Gruppen-Firmwareupdates....202

Kapitel 14: Protokolle verwalten....204
Systemereignisprotokoll anzeigen....204
Systemereignisprotokoll über die Web-Schnittstelle anzeigen....204
Systemereignisprotokoll über RACADM anzeigen....204
Anzeigen des Systemereignisprotokolls unter Verwendung des Dienstprogramms für die iDRAC-Einstellungen....205
Lifecycle-Protokoll anzeigen....205
Lifecycle-Protokoll über die Web-Schnittstelle anzeigen....206
Lifecycle-Protokoll über RACADM anzeigen....206
Exportieren der Lifecycle Controller-Protokolle....206
Exportieren von Lifecycle Controller-Protokollen mithilfe der Webschnittstelle....206
Exportieren von Lifecycle Controller-Protokollen mit RACADM....207
Arbeitsanmerkungen hinzufügen....207
Remote-Systemprotokollierung konfigurieren....207
Remote-System-Protokollierung über die Web-Schnittstelle konfigurieren....207
Remote-Systemanmeldung über RACADM konfigurieren....207

Kapitel 15: Stromversorgung im iDRAC überwachen und verwalten....208
Stromversorgung überwachen....208
Überwachen des Leistungsindex von CPU, Speicher und E/A-Modulen über die Webschnittstelle....208
Überwachen des Leistungsindex für CPU-, Speicher- und E/A-Module über RACADM....209
Festlegen des Warnungsschwellenwerts für den Stromverbrauch....209
Einrichten der Warnschwelle für den Stromverbrauch über die Webschnittstelle....209
Stromsteuerungsvorgänge ausführen....210
Stromsteuerungsvorgänge über die Web-Schnittstelle ausführen....210
Stromsteuerungsvorgänge über RACADM ausführen....210
Strombegrenzung....210
Strombegrenzung bei Blade-Servern....210
Strombegrenzungsrichtlinie anzeigen und konfigurieren....211
Netzteiloptionen konfigurieren....212
Netzteiloptionen über die Web-Schnittstelle konfigurieren....212
Netzteiloptionen über RACADM konfigurieren....212
Netzteiloptionen über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren....212
Netzschalter aktivieren oder deaktivieren....213
Multi-Vektor-Kühlung....213

Kapitel 16: iDRAC Direct Updates....215

Kapitel 17: Durchführen einer Bestandsaufnahme, Überwachung und Konfiguration von Netzwerkgeräten....216
Bestandsaufnahme für Netzwerkgeräte erstellen und Netzwerkgeräte überwachen....216
Netzwerkgeräte über die Web-Schnittstelle überwachen....216
Netzwerkgeräte über RACADM überwachen....217
Verbindungsanzeige....217
Inventorying and monitoring FC HBA devices....219
FC-HBA-Geräte mit der Webschnittstelle überwachen....219
Überwachung von FC-HBA-Geräten unter Verwendung von RACADM....219
Inventorying and monitoring SFP Transceiver devices....219
Monitoring SFP Transceiver devices using web interface....220
Monitoring SFP Transceiver devices using RACADM....220
Telemetry Streaming....220
Serielle Datenerfassung....222
Dynamische Konfiguration von virtuellen Adressen, Initiator- und Speicherziel-Einstellungen....222
Unterstützte Karten für die E/A-Identitätsoptimierung....223
Unterstützte NIC-Firmware-Versionen für die E/A-Identitätsoptimierung....224
Virtuelle oder Remote-zugewiesene Adresse und Persistenzrichtlinien-Verhalten, wenn iDRAC auf Remote-zugewiesenen Address-Modus oder Konsolenmodus eingestellt ist....224
Systemverhalten für FlexAddress und E/A-Identität....226
Aktivieren oder Deaktivieren der E/A-Identitätsoptimierung....226
SSD-Verschleiß-Schwellenwerte....227
Konfigurieren der Einstellungen für die Beständigkeitsrichtlinie....228

Kapitel 18: Managing storage devices....231
Zum Verständnis von RAID-Konzepten....232
Was ist RAID?....233
Datenspeicher-Organisation zur erhöhten Verfügbarkeit und Leistung....234
Auswählen der RAID-Stufen....234
RAID-Level-Leistung vergleichen....240
Unterstützte Controller....241
Unterstützte Gehäuse....242
Übersicht über die unterstützten Funktionen für Speichergeräte....242
Bestandsaufnahme für Speichergeräte erstellen und Speichergeräte überwachen....248
Netzwerkgeräte über die Weboberfläche überwachen....249
Speichergerät über RACADM überwachen....249
Überwachen der Verwendung der Rückwandplatine über das Dienstprogramm für iDRAC-Einstellungen....249
Anzeigen der Speichergerätetopologie....250
Verwalten von physischen Festplatten....250
Zuweisen oder Aufheben der Zuweisung der physischen Festplatte als globales Hotspare....250
Konvertieren einer physischen Festplatte in den RAID- und Nicht-RAID-Modus....251
Löschen physischer Laufwerke....252
Löschen von SED/ISE-Gerätedaten....253
Physische Festplatte neu erstellen....254
Verwalten von virtuellen Festplatten....255
Erstellen von virtuellen Laufwerken....255
Bearbeiten von Cache-Richtlinien für virtuelle Laufwerke....257
Löschen von virtuellen Festplatten....258
Überprüfen der Übereinstimmung der virtuellen Festplatte....258

Initialisieren von virtuellen Festplatten....258
Verschlüsseln der virtuellen Laufwerke....259
Zuweisen oder Aufheben der Zuweisung von dezidierten Hotspares....259
Verwalten von virtuellen Festplatten über die Webschnittstelle....262
Verwalten von virtuellen Festplatten über RACADM....263
RAID-Konfigurationsfunktionen....263
Verwalten von Controllern....264
Konfigurieren der Controller-Eigenschaften....265
Importieren oder automatisches Importieren von Fremdkonfigurationen....268
Fremdkonfiguration löschen....269
Zurücksetzen der Controller-Konfiguration....270
Wechseln des Controller-Modus....270
12-GB/s-SAS-HBA-Adapter-Vorgänge....272
Überwachen der voraussagenden Fehleranalyse auf Festplatten....273
Controller-Vorgänge im Nicht-RAID-Modus oder HBA-Modus....273
Ausführen der RAID-Konfigurations-Jobs auf mehreren Speicher-Controllern....273
Manage Preserved Cache (Beibehaltenen Cache verwalten)....273
Managing PCIe SSDs....274
Erstellen einer Bestandsaufnahme für und Überwachen von PCIe-SSDs....274
Vorbereiten auf das Entfernen von PCIe-SSDs....275
Löschen von Daten auf PCIe-SSD-Geräten....276
Verwalten von Gehäusen oder Rückwandplatinen....278
Konfigurieren des Rückwandplatinen-Modus....278
Anzeigen von Universalsteckplätzen....281
Einrichten des SGPIO-Modus....281
Gehäusesystemkennnummer festlegen....282
Festlegen von Gehäusebestandsnamen....282
Auswählen des Betriebsmodus zum Anwenden von Einstellungen....282
Auswählen des Betriebsmodus über die Webschnittstelle....282
Auswählen des Betriebsmodus über RACADM....283
Anzeigen und Anwenden von ausstehenden Vorgängen....283
Anzeigen, Anwenden oder Löschen von ausstehenden Vorgängen über die Webschnittstelle....283
Anzeigen und Anwenden von ausstehenden Vorgänge über RACADM....284
Speicher-Geräte – Szenarien des Anwenden-Vorgangs....284
Blinken oder Beenden des Blinkens der Komponenten-LEDs....285
Blinken oder Beenden des Blinkens der Komponenten-LEDs über die Webschnittstelle....286
Aktivieren oder Deaktivieren der Komponenten-LEDs über RACADM....286
Softwareneustart....286

Kapitel 19: BIOS-Einstellungen....288
BIOS Live Scan....289
BIOS-Wiederherstellung und Hardware-RoT (Root of Trust)....290

Kapitel 20: Virtuelle Konsole konfigurieren und verwenden....291
Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen....292
Virtuelle Konsole konfigurieren....293
Virtuelle Konsole über die Weboberfläche konfigurieren....293
Virtuelle Konsole über RACADM konfigurieren....293
Vorschau der virtuellen Konsole....294

Virtuelle Konsole starten ... 294
Virtuelle Konsole über die Weboberfläche starten ... 294
Virtuelle Konsole über URL starten ... 295
Deaktivieren von Warnmeldungen beim Starten der Virtuellen Konsole oder Virtueller Datenträger mit dem Java- oder ActiveX-Plug-In ... 295
Viewer für virtuelle Konsole verwenden ... 295
eHTML5 based virtual console ... 296
HTML5 based virtual console ... 298
Mauszeiger synchronisieren ... 300
Weitergeben aller Tastenanschläge über die virtuelle Konsole für Java- oder ActiveX-Plugin ... 301

Kapitel 21: Verwenden des iDRAC Service Module ... 304
Installieren des iDRAC Service Module ... 304
Installieren des iDRAC-Servicemoduls in iDRAC Express und Basic ... 304
Installieren von iDRAC Service Module in iDRAC Enterprise ... 305
Unterstützte Betriebssysteme für das iDRAC Service Module ... 305
Überwachungsfunktionen des iDRAC-Servicemoduls ... 305
Verwendung des iDRAC Servicemoduls über die iDRAC-Weboberfläche ... 311
Verwenden des iDRAC Servicemodul von RACADM ... 312

Kapitel 22: Verwendung der USB-Schnittstelle für das Server-Management ... 313
Zugriff auf die iDRAC-Schnittstelle über eine direkte USB-Verbindung ... 313
Konfigurieren von iDRAC über das Server-Konfigurationsprofil auf dem USB-Gerät ... 314
Konfigurieren der USB-Verwaltungsschnittstelle ... 314
Importieren des Serverkonfigurationsprofils vom USB-Gerät ... 315

Kapitel 23: Verwenden von Quick Sync 2 ... 318
Konfigurieren von iDRAC Quick Sync 2 ... 318
Konfigurieren von iDRAC Quick Sync 2-Einstellungen unter Verwendung der Webschnittstelle ... 319
Konfigurieren von iDRAC Quick Sync 2-Einstellungen über RACADM ... 319
Konfigurieren von iDRAC Quick Sync 2-Einstellungen über das Dienstprogramm für iDRAC-Einstellungen ... 319
Verwenden vom Mobile-Gerät zum Anzeigen von iDRAC-Informationen ... 319

Kapitel 24: Virtuelle Datenträger verwalten ... 320
Unterstützte Laufwerke und Geräte ... 321
Virtuellen Datenträger konfigurieren ... 321
Konfigurieren von virtuellen Datenträgern über die iDRAC-Webschnittstelle ... 321
Virtuelle Datenträger über RACADM konfigurieren ... 321
Virtuelle Datenträger über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren ... 322
Status des verbundenen Datenträgers und Systemantwort ... 322
Auf virtuellen Datenträger zugreifen ... 322
Virtuellen Datenträger über die virtuelle Konsole starten ... 322
Virtuelle Datenträger ohne virtuelle Konsole starten ... 323
Images von virtuellen Datenträgern hinzufügen ... 323
Details zum virtuellen Gerät anzeigen ... 324
Zugriff auf Treiber ... 324
USB-Gerät zurücksetzen ... 324
Virtuelles Laufwerk zuordnen ... 325
Zuordnung für virtuelles Laufwerk aufheben ... 326

Startreihenfolge über das BIOS festlegen.... 326
Einmalstart für virtuelle Datenträger aktivieren....327

Kapitel 25: vFlash SD-Karte verwalten.... 328
Konfigurieren der vFlash-SD-Karte....328
Eigenschaften der vFlash-SD-Karte anzeigen....328
Aktivieren oder Deaktivieren der vFlash-Funktionalität....329
vFlash SD-Karte initialisieren....330
Aktuellen Status über RACADM abrufen.... 331
vFlash-Partitionen verwalten....331
Leere Partition erstellen.... 331
Partition unter Verwendung einer Imagedatei erstellen.... 332
Partition formatieren....333
Verfügbare Partitionen anzeigen....334
Partition modifizieren....334
Partitionen verbinden oder trennen....335
Vorhandene Partitionen löschen.... 336
Partitionsinhalte herunterladen....336
In eine Partition starten....337

Kapitel 26: SMCLP verwenden....338
System-Verwaltungsfunktionen über SMCLP.... 338
SMCLP-Befehle ausführen....338
iDRAC-SMCLP-Syntax....339
MAP-Adressbereich navigieren....342
Verb „show“ verwenden.... 342
Option -display verwenden.... 342
Option -level verwenden.... 342
Option -output verwenden....342
Anwendungsbeispiele....343
Server-Energieverwaltung.... 343
SEL-Verwaltung....343
MAP-Zielnavigation....344

Kapitel 27: Betriebssysteme bereitstellen....346
Betriebssystem über eine Remote-Dateifreigabe bereitstellen....346
Managing remote file shares....346
Remote-Dateifreigabe über die Web-Schnittstelle konfigurieren.... 347
Remote-Dateifreigabe über RACADM konfigurieren....348
Betriebssystem über virtuelle Datenträger bereitstellen....349
Betriebssystem über mehrere Festplatten bereitstellen.... 349
Integriertes Betriebssystem auf SD-Karte bereitstellen....349
SD-Modul und Redundanz im BIOS aktivieren....349

Kapitel 28: Fehler auf Managed System über iDRAC beheben.... 351
Diagnosekonsole verwenden.... 351
iDRAC zurücksetzen und iDRAC auf Standardeinstellungen zurücksetzen....351
Planen von Automatischer Remote-Diagnose....352
Planen von Automatischer Remote-Diagnose unter Verwendung von RACADM....353

POST-Codes anzeigen....353
Viewing boot and crash capture videos....353
Konfigurieren der Videoerfassungs-Einstellungen....354
Protokolle anzeigen....354
Bildschirm „Letzter Systemabsturz“ anzeigen....354
Anzeigen des Systemstatus....354
Status der LC-Anzeige auf der Frontblende des Systems anzeigen....355
Status der LE-Anzeige auf der Frontblende des Systems anzeigen....355
Anzeigen für Hardwareprobleme....355
Systemzustand anzeigen....356
Serverstatusbildschirm auf Fehlermeldungen überprüfen....356
iDRAC-Neustart....356
Auf Standardeinstellungen zurücksetzen (RTD)....356
Zurücksetzen des iDRAC über die iDRAC-Webschnittstelle....357
Zurücksetzen des iDRAC über RACADM....357
Löschen von System- und Nutzerdaten....357
Zurücksetzen des iDRAC auf die Standardeinstellungen....358
Zurücksetzen von iDRAC auf die Standardwerkseinstellungen unter Verwendung der iDRAC-Webschnittstelle....358
Zurücksetzen von iDRAC auf die Standardwerkseinstellungen unter Verwendung des Dienstprogramms für iDRAC-Einstellungen....358

Kapitel 29: Integration von SupportAssist im iDRAC....360
Registrierung von SupportAssist....360
Installieren des Servicemoduls....361
Server-BS-Proxy-Informationen....361
SupportAssist....361
Portal für Service-Anforderungen....361
Sammlung Melden....361
Generating SupportAssist Collection....362
Manuelles Generieren der SupportAssist-Erfassung unter Verwendung der iDRAC-Webschnittstelle....362
Einstellungen....363
Einstellungen für Datenerfassung....363
Kontaktinformationen....363

Kapitel 30: Häufig gestellte Fragen....364
System-Ereignisprotokoll....364
Benutzerdefinierte Absender-E-Mail-Konfiguration für iDRAC-Warnmeldungen....365
Netzwerksicherheit....365
Telemetrie-Streaming....366
Active Directory....366
Einmaliges Anmelden....367
Smart Card-Anmeldung....368
Virtuelle Konsole....369
Virtueller Datenträger....372
vFlash-SD-Karte....374
SNMP-Authentifizierung....374
Speichergeräte....374
GPU (Beschleuniger)....375
iDRAC-Service-Modul....375

RACADM..... 377
Standardkennwort dauerhaft auf „calvin“ setzen.....378
Verschiedenes.....378

Kapitel 31: Anwendungsszenarien..... 383
Fehler auf einem Managed System beheben, auf das nicht zugegriffen werden kann.....383
Systeminformationen abrufen und Systemzustand bewerten.....384
Einrichten von Warnungen und Konfigurieren von E-Mail-Warnungen.....384
Anzeigen und Exportieren des Systemereignisprotokoll und Lifecycle-Protokolls..... 384
Schnittstellen zum Aktualisieren der iDRAC-Firmware..... 384
Ordnungsgemäßes Herunterfahren durchführen.....385
Neues Administratorbenutzerkonto erstellen.....385
Starten einer Server-Remote-Konsole und Mounten eines USB-Laufwerks..... 385
Bare Metal-Betriebssystem über verbundenen virtuellen Datenträger und Remote-Dateifreigabe installieren...385
Rack-Dichte verwalten.....385
Neue elektronische Lizenz installieren.....386
Übernehmen der E/A-Identitätskonfigurationseinstellungen für mehrere Netzwerkkarten bei einem Einzel-Host-System-Neustart.....386

1

Übersicht über den iDRAC

Der Integrated Dell Remote Access Controller (iDRAC) wurde entwickelt, um Ihre Produktivität als Systemadministrator zu steigern und die Gesamtverfügbarkeit der Dell EMC Server zu verbessern. Der iDRAC warnt Sie bei Systemproblemen, hilft Ihnen bei der Remote-Verwaltung und reduziert die Notwendigkeit für physischen Zugriff auf das System.

Der iDRAC ist Teil einer größeren Lösung für Rechenzentren, die die Verfügbarkeit geschäftskritischer Anwendungen und Arbeitslasten erhöht. Diese Technologie ermöglicht die standortunabhängige Bereitstellung, Überwachung, Verwaltung, Konfiguration, Aktualisierung und Fehlerbehebung von Dell EMC Systemen ohne Verwendung von Agenten oder eines Betriebssystems.

Verschiedene Produkte arbeiten mit dem iDRAC zusammen, um IT-Vorgänge zu vereinfachen. Einige der Tools sind:

- OpenManage Enterprise
- OpenManage Power Center-Plug-in
- OpenManage Integration for VMware vCenter
- Dell Repository Manager

Der iDRAC wird in den folgenden Varianten angeboten:

- iDRAC Basic – standardmäßig für Server der Serien 100–500 verfügbar
- iDRAC Express – standardmäßig für Rack- oder Tower-Server der 600 Serie oder höher sowie für alle Blade-Server verfügbar
- iDRAC Enterprise – für alle Servermodelle verfügbar
- iDRAC Datacenter – für alle Servermodelle verfügbar

Themen:

- Vorteile der iDRAC-Verwendung
- Wichtige Funktionen
- Neue Funktionen hinzugefügt
- Verwendung dieses Benutzerhandbuchs
- Unterstützte Webbrowser
- iDRAC-Lizenzen
- Lizenzierte Funktionen in iDRAC9
- Schnittstellen und Protokoll für den Zugriff auf iDRAC
- iDRAC-Schnittstelleninformationen
- Weitere nützliche Dokumente
- Kontaktaufnahme mit Dell
- Zugriff auf Dokumente der Dell Support-Website
- Zugriff auf Redfish API-Handbuch

Vorteile der iDRAC-Verwendung

Sie können die folgenden Vorteile nutzen:

- Verbesserte Verfügbarkeit – Frühzeitige Benachrichtigungen zu potenziellen oder tatsächlichen Fehlern, die Sie dabei unterstützen, einen Server-Ausfall zu verhindern oder den zeitlichen Aufwand für die Wiederherstellung nach einem Ausfall zu reduzieren.
- Verbesserte Produktivität und geringere Gesamtbetriebskosten – Die Erweiterung des Server-Wartungsbereichs für Administratoren auf eine größere Anzahl an entfernt liegenden Servern kann Sie dabei unterstützen, die Produktivität der IT-Mitarbeiter zu erhöhen und gleichzeitig die Gesamtbetriebskosten, z. B. für Reisen, zu reduzieren.
- Sichere Umgebung – Durch die Bereitstellung eines sicheren Zugriffs auf Remote-Server können Administratoren kritische Verwaltungsaufgaben ausführen, ohne die Sicherheit von Servern und des Netzwerks zu beeinträchtigen.
- Verbessertes integriertes Management über Lifecycle Controller – Der Lifecycle Controller bietet Bereitstellungsfunktionen und vereinfacht Wartungsaufgaben durch die Lifecycle-Controller-Benutzeroberfläche für die lokale Bereitstellung und über Schnittstellen für Remote-Dienste (WSMan) für die Remote-Bereitstellung. Außerdem bietet Lifecycle-Controller eine Integration mit Dell OpenManage Essentials und Partner-Konsolen.

Weitere Informationen zum Lifecycle Controller GUI finden Sie unter *Benutzerhandbuch für den Lifecycle Controller* und Informationen zu Remote-Diensten finden Sie unter *Schnellstart-Benutzerhandbuch für Lifecycle Controller Remote Services*, verfügbar unter https://www.dell.com/idracmanuals.

Wichtige Funktionen

Zentrale Funktionen von iDRAC:

ANMERKUNG: Einige der Funktionen sind nur mit einer iDRAC Enterprise- oder Datacenter-Lizenz verfügbar. Informationen über die verfügbaren Funktionen der verschiedenen Lizenzen finden Sie unter iDRAC-Lizenzen auf Seite 20.

Bestandsaufnahme und Überwachung

- Telemetriedaten-Streaming
- Zustand verwalteter Server anzeigen
- Netzwerkadapter zur Bestandsaufnahme und Überwachung und Speichersubsysteme (PERC und direkt angehängter Speicher) ohne Betriebssystemagenten.
- Anzeigen und Exportieren der aktuellen Bestandsliste.
- Anzeigen der Sensorinformationen wie beispielsweise Temperatur, Spannung und Eingriff.
- Überwachen des CPU-Status, automatische Prozessordrosselung und vorhergesagte Fehler.
- Anzeigen der Speicherinformation.
- Stromverbrauch überwachen und steuern
- Support für SNMPv3-GETs und Warnungen.
- Für Blade-Server: Starten Sie die Weboberfläche des Managementmoduls, sehen Sie sich die Informationen von OpenManage Enterprise (OME) Modular und die WWN/MAC-Adressen an.

  ANMERKUNG: CMC ermöglicht den Zugriff auf iDRAC über das LCD-Bedienfeld des M1000E-Gehäuses und über lokale Konsolenverbindungen. Weitere Informationen finden Sie unter *Chassis Management Controller – Handbuch* verfügbar unter https://www.dell.com/cmcmanuals.
- Anzeigen von verfügbaren Netzwerk-Schnittstellen auf Host-Betriebssystemen.
- iDRAC9 bietet bessere Überwachungs- und -Managementfunktionen mit Quick Sync 2. Auf Ihrem Android- oder iOS-Mobilgerät muss die OpenManage Mobile-App konfiguriert sein.

Bereitstellung

- vFlash SD-Kartenpartitionen verwalten
- Anzeigeeinstellungen für das Bedienfeld auf der Vorderseite konfigurieren
- Verwalten von iDRAC-Netzwerkeinstellungen.
- Virtuelle Konsole und virtuelle Datenträger konfigurieren und verwenden
- Betriebssysteme mit Remote-Dateifreigabe und virtuellem Datenträger bereitstellen
- Aktivieren Sie die automatische Ermittlung.
- Die Serverkonfiguration unter Verwendung der Export- oder Import-XML-Profilfunktion durch RACADM, WSMan oder Redfish durchführen. Weitere Informationen finden Sie unter *Schnellstart-Benutzerhandbuch für Lifecycle Controller Remote Services* verfügbar unter https://www.dell.com/idracmanuals.
- Konfigurieren der Richtlinie für die Persistenz von virtuellen Adressen, Initiator und Speicherzielen.
- Remote-Konfiguration von Speichergeräten, die während der Laufzeit an das System angeschlossen sind.
- Führen Sie die folgenden Operationen für Speichergeräte aus:
  - Physische Laufwerke: Physische Laufwerke als globales Hot Spare zuweisen oder Zuweisung aufheben
  - Virtuelle Laufwerke:
    - Virtuelle Laufwerke erstellen
    - Cache-Richtlinien für virtuelle Laufwerke bearbeiten
    - Übereinstimmung der virtuellen Laufwerke überprüfen
    - Virtuelle Laufwerke initialisieren
    - Virtuelle Laufwerke verschlüsseln
    - Dediziertes Hot Spare zuweisen und Zuweisung aufheben
    - Virtuelle Laufwerke löschen
  - Controller:
    - Controller-Eigenschaften konfigurieren
    - Fremdkonfigurationen (automatisch) importieren
    - Fremdkonfiguration löschen
    - Controller-Konfiguration zurücksetzen

        - Sicherheitsschlüssel erstellen oder ändern
    - PCIe SSD-Geräte:
        - Bestandsaufnahme und die Remote-Überwachung des Status von PCIe SSD-Geräten im Server.
        - Entfernen der PCIe SSD vorbereiten
        - Daten sicher löschen
    - Festlegen des Rückwandplatine-Modus (Unified- oder Split-Betrieb).
    - Komponenten-LEDs blinken oder Blinken beenden
    - Wenden Sie die Geräteeinstellungen sofort, beim nächsten Neustart, zu einem festgelegten Zeitpunkt oder als eine ausstehende Operation an, um sie als Stapel als Teil des einzelnen Jobs anzuwenden.

Aktualisierung

- Verwalten von iDRAC-Lizenzen.
- BIOS und Gerätefirmware für Geräte aktualisieren, die durch Lifecycle Controller unterstützt werden
- Aktualisierung oder Rollback für iDRAC-Firmware und Lifecycle-Controller-Firmware mit einem einzigen Firmware-Image.
- Verwalten gestufter Aktualisierungen.
- Zugriff auf die iDRAC-Schnittstelle über direkte USB-Verbindung.
- iDRAC unter Verwendung des Server-Profiles auf dem USB-Gerät konfigurieren.

Wartung und Troubleshooting

- Stromversorgungsbezogene Vorgänge ausführen und Stromverbrauch überwachen
- Optimierte Systemleistung und Stromverbrauch durch Ändern der thermischen Einstellungen.
- Keine Abhängigkeit vom OpenManage Server Administrator für die Generierung von Warnmeldungen
- Ereignisdaten protokollieren: Lifecycle- und RAC-Protokolle.
- Festlegen von E-Mail-Warnungen, IPMI-Warnungen, Remote System-Protokollen, WS-Ereignisprotokollen, Redfish-Ereignissen und SNMP-Traps (v1 v2c und v3) für Ereignisse und verbesserte E-Mail-Warnungsbenachrichtigung.
- Image des letzten Systemabsturzes erfassen
- Videos zur Start- und Absturzerfassung anzeigen
- Bandexternes Performancemonitoring und Ausgabe von Warnmeldungen an den Leistungsindex von CPU, Speicher und E/A-Modulen.
- Konfigurieren des Warnungs-Schwellenwerts für die Temperatur und Energieverbrauch.
- Verwenden Sie das iDRAC-Service-Modul zum:
    - Anzeigen von Informationen zum Betriebssystem (BS).
    - Replizieren von Lifecycle Controller-Protokollen zu den Betriebssystemprotokollen
    - Optionen für die automatische Systemwiederherstellung.
    - Aktivieren oder Deaktivieren des Status eines vollständigen Ein- und Ausschaltvorgangs für alle Systemkomponenten mit Ausnahme des Netzteils.
    - Remote-Hardware-Zurücksetzung-iDRAC
    - Bandinterne iDRAC-SNMP-Warnungen aktivieren
    - Zugriff auf iDRAC unter Verwendung von Host-BS (experimentelle Funktion)
    - Bestücken der Windows Management Instrumentation (WMI)-Informationen
    - Integration mit SupportAssist-Sammlung. Dies gilt nur, wenn das iDRAC Service-Modul Version 2.0 oder höher installiert ist.
- Sie können die SupportAssist-Erfassung folgendermaßen generieren:
    - Automatisch – Verwendung des iDRAC Service Module, das das Betriebssystem-Collector-Tool automatisch aufruft.

Dell Best Practices für iDRAC

- Dell iDRACs sind für die Installation in einem separaten Verwaltungsnetzwerk vorgesehen. Sie sind nicht darauf ausgelegt oder dafür bestimmt, im Internet platziert oder direkt mit dem Internet verbunden zu werden. Dies könnte das verbundene System Sicherheitsrisiken und anderen Risiken aussetzen, für die Dell nicht verantwortlich ist.
- Dell EMC empfiehlt die Verwendung des dedizierten Gigabit-Ethernet-Ports, der bei Rack- und Tower-Servern verfügbar ist. Diese Schnittstelle wird nicht an das Hostbetriebssystem freigegeben und leitet den Managementverkehr auf ein separates physisches Netzwerk um, wodurch eine Trennung vom Anwendungsdatenverkehr erfolgt. Diese Option impliziert, dass die dedizierte iDRAC-Netzwerkschnittstelle den Datenverkehr getrennt von den LOM- oder NIC-Schnittstellen des Servers weiterleitet. Mit der Option „Dediziert“ kann dem iDRAC eine IP-Adresse aus demselben Subnetz oder einem anderen Subnetz zugewiesen werden, im Vergleich zu den IP-Adressen, die dem Host-LOM oder den NICs zugewiesen wurden.
- Abgesehen von der Platzierung der iDRACs auf einem separaten Verwaltungssubnetz, sollten Benutzer das Verwaltungssubnetz/vLAN mit einer geeigneten Technologie isolieren, wie z. B. Firewalls. Außerdem sollte der Zugriff auf das Subnetz/vLAN auf Serveradministratoren mit entsprechender Berechtigung begrenzt werden.

Konnektivität absichern

Die Sicherung des Zugriffs auf kritische Netzwerkressourcen hat Priorität. iDRAC implementiert eine Reihe von Sicherheitsfunktionen, darunter:

- Benutzerdefinierte Signaturzertifikate für Secure Socket Layer (SSL).
- Signierte Firmwareupdates
- Benutzerauthentifizierung durch Microsoft Active Directory, generischem Lightweight Directory Access Protocol (LDAP) Directory Service oder lokal verwalteten Nutzer-IDs und Kennwörtern.
- Zwei-Faktor-Authentifizierung über die Smartcard-Anmeldefunktion. Die Zwei-Faktor-Authentifizierung basiert auf der physischen Smartcard und der Smartcard-PIN.
- Authentifizierung über die einmalige Anmeldung und den öffentlichen Schlüssel
- Rollenbasierte Authentifizierung für die Konfiguration spezifischer Berechtigungen für jeden einzelnen Benutzer
- SNMPv3-Authentifizierung für Benutzerkonten, die lokal in iDRAC gespeichert sind. Es wird empfohlen, dies so zu benutzen, auch wenn die Option in den Standardeinstellungen deaktiviert ist.
- Nutzer-ID- und Kennwortkonfiguration
- Standardmäßige Anmeldekennwort-Modifikation.
- Einrichten von Kennwörtern und BIOS-Kennwörtern unter Verwendung des Einweg-Hash-Formats für verbesserte Sicherheit.
- FIPS 140-2 Ebene-1-Fähigkeit.
- Konfiguration der Sitzungs-Timeouts (in Sekunden)
- Konfigurierbare IP-Ports (für HTTP, HTTPS, SSH, virtuelle Konsole und virtuelle Datenträger).
- Secure Shell (SSH), die eine verschlüsselte Transportschicht für höhere Sicherheit verwendet.
- Beschränkung der Anmeldefehlschläge pro IP-Adresse, mit Anmeldeblockierung der IP-Adresse bei Überschreitung des Grenzwerts
- Beschränkter IP-Adressenbereich für Clients, die an den iDRAC angeschlossen werden
- Dedizierter Gigabit-Ethernet-Adapter auf Rack- und Tower-Servern verfügbar (ggf. zusätzliche Hardware erforderlich).

Neue Funktionen hinzugefügt

Dieser Abschnitt enthält eine Liste der neuen Funktionen, die in den folgenden Versionen hinzugefügt wurden:

Firmware version 5.00.00.00

This release includes all the features from the previous releases. Following are the new features that are added in this release:

NOTE: For information about supported systems, refer to the respective version of Release Notes available at https://www.dell.com/support/article/sln308699 .

In 5.00.00.00 release, following features are added in Storage page on iDRAC GUI:

General

- Support for PCIe VDM (Enabled by default)
- Option to clear the system critical status to healthy state when unconfigured internal drive is removed
- Support NVMe Boot over Fibre Channel (NVMeOF)
- Support firmware update of TPM 1.2 and 2.0 for 15G servers
- Rsyslog server and Redfish event listener supports streaming of all message IDs
- Support for DNS configuration using IPv6 Router Advertisement (RA) messages, per RFC 8106.

GUI Enhancement

- Prevent iDRAC user logging out during browser refresh
- Show PCIe slot inventory in a simplified view
- New filters in Storage page
- Show the last used domain name by default in the login page (AD users)

Redfish Updates— Added support for the following Redfish features:

- Redfish lifecycle eventing (RLCE) streams server lifecycle changes across all message IDs
- HTTP/2 network protocol
- Added support for following:
  - ComputerSystem.GraceFulRestart
  - OperationApplyTime option for updates operations including SimpleUpdate, TransferProtocaol and MultipartUpload
  - ConvergedInfra.1#AppRawData attribute
  - DelliDRACCardService.GetKVMSessionOEM action
  - ConvergedInfra.1#AppRawData attribute

Support/Diagnostics

- CPU & Memory Utilization logging in Support Assist Collection
- Add PCIe tree of the system in the Support Assist Collection
- SupportAssist Logs to include historical thermal inlet and outlet temperature

Reports

- All Metric Report Definitions (MRD) have three new properties ServiceTag, MetricReportDefinitionDigest, and iDRACFirmwareVersion. Digest property helps consumer identify out-of-band changes in Custom MRD outside the influence of the component that created it. It helps as a reference to customers to track any changes made to the MRDs

Verwendung dieses Benutzerhandbuchs

Der Inhalt dieses Benutzerhandbuchs ermöglicht es Ihnen, die Tasks auszuführen, indem Sie Folgendes verwenden:

- iDRAC Webschnittstelle – Hier sind nur die Task-bezogenen Informationen enthalten. Weitere Informationen über die Felder und Optionen finden Sie in der *iDRAC- Online-Hilfe*, die Sie über die Web-Schnittstelle aufrufen können.
- RACADM – Hier ist der RACADM-Befehl bzw. das zu verwendende Objekt enthalten. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.
- Das Dienstprogramm für die iDRAC-Einstellungen - Hier sind nur die Task-bezogenen Informationen enthalten. Informationen zu den Feldern und Optionen finden Sie in der *iDRAC Settings Utility Online Help* (Online-Hilfe zum Dienstprogramm für iDRAC-Einstellungen). Diese können Sie aufrufen, indem Sie in der GUI des Dienstprogramms auf **Hilfe** klicken (drücken Sie beim Starten die Taste <F2>, und klicken Sie dann auf der Seite **System-Setup – Hauptmenü** auf **iDRAC-Einstellungen**).
- Redfish – Hier sind nur die Task-bezogenen Informationen enthalten. Weitere Informationen über die Felder und Optionen finden Sie unter *iDRAC Redfish API-Handbuch* verfügbar unter www.api-marketplace.com.

Unterstützte Webbrowser

iDRAC wird auf folgenden Browsern unterstützt:

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

ANMERKUNG: Einige Funktionen der iDRAC-Benutzeroberfläche und Online-Hilfe sind möglicherweise nicht im Browser Internet Explorer verfügbar.

Eine Liste der unterstützten Versionen finden Sie unter *iDRAC-Versionshinweise* verfügbar unter https://www.dell.com/idracmanuals.

Unterstützte Betriebssysteme und Hypervisoren

iDRAC wird von folgenden Betriebssystemen, Hypervisoren unterstützt:

- Microsoft Windows Server und Windows PE
- VMware ESXI
- RedHat Enterprise Linux
- SuSe Linux Enterprise Server

ANMERKUNG: Eine Liste der unterstützten Versionen finden Sie unter *iDRAC-Versionshinweise* verfügbar unter https://www.dell.com/idracmanuals.

iDRAC-Lizenzen

iDRAC-Funktionen sind je nach Typ der Lizenz verfügbar. Abhängig vom Systemmodell wird die Lizenz iDRAC Basic oder iDRAC Express standardmäßig installiert. Die iDRAC Enterprise- iDRAC Datacenter- und iDRAC Secure Enterprise Key Manager (SEKM)-Lizenz sind als Upgrade erhältlich und können jederzeit erworben werden. In den Schnittstellen stehen nur lizenzierte Funktionen zur Verfügung, mit denen Sie iDRAC konfigurieren oder nutzen können. Weitere Informationen finden Sie unter Lizenzierte Funktionen in iDRAC9.

Types of licenses

iDRAC Basic or iDRAC Express are the standard licenses available by default on your system. iDRAC Enterprise and Datacenter licenses includes all the licensed features and can be purchased at any time. The types of upsell offered are:

- 30-day evaluation—Evaluation licenses are duration-based and the timer runs when power is applied to the system. This license cannot be extended.
- Perpetual—The license is bound to the Service Tag and is permanent.

Following table lists the default license available on the following systems:

iDRAC Basic License	iDRAC Express License	iDRAC Enterprise License	iDRAC Datacenter License
PowerEdge Rack/Tower severs series 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	All platforms, with upgrade option	All platforms, with upgrade option

Table 1. Default License

iDRAC Express License	iDRAC Enterprise License	iDRAC Datacenter License
• 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	All platforms, with upgrade option	All platforms, with upgrade option

NOTE: The default license available with PowerEdge C64XX and C65xx systems is BMC. The BMC license was custom made for C64XX systems.

NOTE: Express for Blades license is the default license for PowerEdge M6XX and MXXXX systems.

Methoden zum Erwerb von Lizenzen

Verwenden Sie zum Anfordern von Lizenzen eines der folgenden Verfahren:

- Dell Digital Locker – Mit dem Dell Digital Locker können Sie Ihre Produkte, Software und Lizenzinformationen an einem Ort anzeigen und verwalten. Ein Link zum Dell Digital Locker ist in der DRAC-Webschnittstelle verfügbar, gehen Sie zu **Konfiguration** > **Lizenzen**.

ANMERKUNG: Weitere Informationen über Dell Digital Locker finden Sie in den FAQs auf der Website.

- E-Mail – Die Lizenz ist an eine E-Mail angehängt, die nach der Anforderung der Lizenz durch das technische Support Center versendet wird.
- Point-of-sale – Die Lizenz wird im Rahmen der Systembestellung angefordert.

ANMERKUNG: Um Lizenzen zu verwalten oder neue Lizenzen zu erwerben, gehen Sie zum Dell digitalen Schließfach.

Erwerben von Lizenzschlüssel vom Dell digitalen Schließfach

Zum Abrufen der Lizenzschlüssel von Ihrem Konto müssen Sie zuerst Ihr Produkt unter Verwendung des Registrierungscodes registrieren, der Ihnen in der Bestätigungs-E-Mail gesendet wird. Dieser Code muss in der Registerkarte **Produktregistrierung** nach der Anmeldung beim Dell digitalen Schließfach eingegeben werden.

Klicken Sie im linken Fensterbereich auf die Registerkarte **Produkte** oder **Auftragsverlauf**, um die Liste Ihrer Produkte aufzurufen. Abonnement-basierte Produkte sind unter **Abrechnungskonten** aufgeführt.

So laden Sie den Lizenzschlüssel von Ihrem Dell digitalen Schließfachkonto herunter:

1. Melden Sie sich bei Ihrem Dell digitalen Schließfachkonto an.
2. Klicken Sie im linken Fensterbereich auf **Produkte**.
3. Klicken Sie auf das Produkt, das Sie anzeigen möchten.
4. Klicken Sie auf den Produktnamen.
5. Klicken Sie auf der Seite **Produktmanagement** auf **Schlüssel abrufen**.
6. Folgen Sie den Anweisungen auf dem Bildschirm, um den Lizenzschlüssel zu erhalten.

ANMERKUNG: Wenn Sie noch kein Dell digitales Schließfachkonto haben, erstellen Sie mit der E-Mail-Adresse ein Konto, mit der Sie den Einkauf abgeschlossen haben.

ANMERKUNG: Zum Erzeugen mehrerer Lizenzschlüsseln für neue Einkäufe befolgen Sie die Anweisungen unter **Tools** > **Lizenzaktivierung** > **Nicht aktivierte Lizenzen**

Lizenzvorgänge

Bevor Sie die Lizenzverwaltungsschritte ausführen, stellen Sie sicher, dass Sie die erforderlichen Lizenzen besitzen. Weitere Informationen finden Sie unter Methoden zum Erwerb von Lizenzen.

ANMERKUNG: Sollten Sie ein System erworben haben, auf dem sämtliche Lizenzen bereits vorinstalliert sind, ist eine Lizenzverwaltung nicht erforderlich.

Sie können die folgenden Lizenzvorgänge über iDRAC, RACADM, WSMan, Redfish und Lifecycle-Controller-Remote-Dienste für eine 1-zu-1-Lizenzverwaltung und Dell License Manager für eine 1-zu-n-Lizenzverwaltung ausführen:

- Ansicht – Zeigen Sie die aktuellen Lizenzinformationen an.
- Importieren – Nachdem Sie die Lizenz erhalten haben, speichern Sie die Lizenz in einem lokalen Speicher, und importieren Sie sie über eine unterstützte Schnittstelle nach iDRAC. Die Lizenz wird importiert, wenn Sie die Validierungsprüfungen bestanden hat.

  ANMERKUNG: Sie können die werkseitig installierte Lizenz zwar exportieren, aber nicht importieren. Um die Lizenz zu importieren, laden Sie die entsprechende Lizenz vom Digital Locker herunter, oder rufen Sie sie aus der E-Mail ab, die Sie beim Kauf der Lizenz erhalten haben.

  ANMERKUNG: Nach dem Importieren der Lizenz müssen Sie sich erneut bei iDRAC anmelden. Dies gilt nur für die iDRAC-Weboberfläche.
- Export – Exportiert die installierte Lizenz. Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.
- Löschen – Löscht die Lizenz. Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.
- Weitere Informationen – Hier finden Sie weitere Informationen zur installierten Lizenz oder zu den Lizenzen, die für eine auf dem Server installierte Komponente verfügbar sind.

  ANMERKUNG: Damit die Option "Weitere Informationen" die korrekte Seite anzeigt, stellen Sie sicher, dass ***.dell.com** der Liste der vertrauenswürdigen Sites in den Sicherheitseinstellungen hinzugefügt wurde. Weitere Informationen finden Sie in der Internet Explorer-Hilfe-Dokumentation.

Für die 1-zu-n-Lizenzbereitstellung können Sie Dell License Manager verwenden. Weitere Informationen finden Sie unter *Dell License Manager-Benutzerhandbuch* verfügbar unter https://www.dell.com/esmmanuals.

Im Folgenden sind die erforderlichen Nutzerberechtigungen für verschiedene Lizenzvorgänge aufgeführt:

- Ansicht und Exportieren einer Lizenz: Berechtigung zur Anmeldung
- Importieren und Löschen einer Lizenz: Berechtigung zur Anmeldung, iDRAC-Konfiguration und Serversteuerung

Lizenzen über die iDRAC-Webschnittstelle verwalten

Um Lizenzen über die iDRAC-Webschnittstelle zu verwalten, gehen Sie zu **Configuration (Konfiguration)** > **Licenses (Lizenzen)**.

Die Seite **Licensing** (Lizenzierung) zeigt die Lizenzen, die mit Geräten verknüpft sind, oder diejenigen Lizenzen an, die zwar installiert sind, das entsprechende Gerät im System jedoch nicht vorhanden ist. Weitere Informationen zum Importieren, Exportieren oder Löschen einer Lizenz finden Sie in der *iDRAC-Online-Hilfe*.

Lizenzen über RACADM verwalten

Um Lizenzen über RACADM zu verwalten, verwenden Sie den Unterbefehl **license**. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Lizenzierte Funktionen in iDRAC9

In der folgenden Tabelle werden die iDRAC9-Funktionen aufgeführt, die gemäß der erworbenen Lizenz aktiviert sind:

Tabelle 2. Lizenzierte Funktionen in iDRAC9

Funktion	iDRAC9 Basic	iDRAC9 Express	iDRAC9 Express für Blades	iDRAC9 Enterprise	iDRAC9-Datacenter
Schnittstellen/Standards					
iDRAC RESTful-API und Redfish	Ja	Ja	Ja	Ja	Ja
IPMI 2.0	Ja	Ja	Ja	Ja	Ja
DCMI 1.5	Ja	Ja	Ja	Ja	Ja
Webbasierte GUI	Ja	Ja	Ja	Ja	Ja
RACADM-Befehlszeile (lokal/Remote)	Ja	Ja	Ja	Ja	Ja
SSH	Ja	Ja	Ja	Ja	Ja
Serielle Umleitung	Ja	Ja	Ja	Ja	Ja
WSMan	Ja	Ja	Ja	Ja	Ja
Netzwerkzeitprotokoll	Nein	Ja	Ja	Ja	Ja
Konnektivität					
Gemeinsam genutzte NIC (LOM)	Ja	Ja	k. A.	Ja	Ja
Dedizierte NIC	Ja	Ja	Ja	Ja	Ja
VLAN-Tagging	Ja	Ja	Ja	Ja	Ja
IPv4	Ja	Ja	Ja	Ja	Ja
IPv6	Ja	Ja	Ja	Ja	Ja
DHCP	Ja	Ja	Ja	Ja	Ja
DHCP mit Zero-Touch	Nein	Nein	Nein	Ja	Ja
Dynamisches DNS	Ja	Ja	Ja	Ja	Ja
BS-Pass-Through	Ja	Ja	Ja	Ja	Ja
iDRAC Direct (USB-Frontblende)	Ja	Ja	Ja	Ja	Ja
Verbindungsanzeige	Ja	Ja	Nein	Ja	Ja

Tabelle 2. Lizenzierte Funktionen in iDRAC9 (fortgesetzt)

Funktion	iDRAC9 Basic	iDRAC9 Express	iDRAC9 Express für Blades	iDRAC9 Enterprise	iDRAC9-Datacenter
Sicherheit					
Rollenbasierte Autorität	Ja	Ja	Ja	Ja	Ja
Lokale Benutzer	Ja	Ja	Ja	Ja	Ja
SSL-Verschlüsselung	Ja	Ja	Ja	Ja	Ja
Secure-Enterprise-Schlüsselverwaltung	Nein	Nein	Nein	Ja (mit SEKM-Lizenz)	Ja (mit SEKM-Lizenz)
IP-Blockierung	Nein	Ja	Ja	Ja	Ja
Verzeichnisdienste (AD, LDAP)	Nein	Nein	Nein	Ja	Ja
Zwei-Faktor-Authentifizierung (Smartcard)	Nein	Nein	Nein	Ja	Ja
Einmaliges Anmelden	Nein	Nein	Nein	Ja	Ja
PK-Authentifizierung (für SSH)	Nein	Ja	Ja	Ja	Ja
OAuth-Integration in webbasierte Authentifizierungsservices	Nein	Nein	Nein	Nein	Ja
OpenID Connect für Dell EMC Konsolen	Nein	Nein	Nein	Nein	Ja
FIPS 140-2	Ja	Ja	Ja	Ja	Ja
Secure Boot (UEFI) – Zertifikatsverwaltung	Ja	Ja	Ja	Ja	Ja
Sperrmodus	Nein	Nein	Nein	Ja	Ja
Eindeutiges iDRAC-Standardkennwort	Ja	Ja	Ja	Ja	Ja
Benutzerdefinierte Banner für Sicherheitsrichtlinie – Anmeldeseite	Ja	Ja	Ja	Ja	Ja
Einfache Multifaktor-Authentifizierung	Nein	Nein	Nein	Nein	Ja
Automatische Zertifikatregistrierung (SSL-Zertifikate)	Nein	Nein	Nein	Nein	Ja
iDRAC Quick Sync 2 – optionale Authentifizierung für Lesevorgänge	Ja	Ja	Ja	Ja	Ja
iDRAC Quick Sync 2 – Nummer des Mobilgeräts zu LCL hinzufügen	Ja	Ja	Ja	Ja	Ja
System-Löschvorgang für interne Speichergeräte	Ja	Ja	Ja	Ja	Ja
Remote-Präsenz					
Betriebsschalter	Ja	Ja	Ja	Ja	Ja
Boot-Steuerung	Ja	Ja	Ja	Ja	Ja

Tabelle 2. Lizenzierte Funktionen in iDRAC9 (fortgesetzt)

Funktion	iDRAC9 Basic	iDRAC9 Express	iDRAC9 Express für Blades	iDRAC9 Enterprise	iDRAC9-Datacenter
Seriell-über-LAN	Ja	Ja	Ja	Ja	Ja
Virtueller Datenträger	Nein	Nein	Ja	Ja	Ja
Virtuelle Ordner	Nein	Nein	Nein	Ja	Ja
Remote-Dateifreigabe	Nein	Nein	Nein	Ja	Ja
HTML5-Zugriff auf die virtuelle Konsole	Nein	Nein	Ja	Ja	Ja
Virtuelle Konsole	Nein	Nein	Ja	Ja	Ja
VNC-Verbindung zum Betriebssystem	Nein	Nein	Nein	Ja	Ja
Qualität/Bandbreiten-Kontrolle	Nein	Nein	Nein	Ja	Ja
Virtuelle Konsolenzusammenarbeit (bis zu sechs Benutzer gleichzeitig)	Nein	Nein	Nein (Nur ein Benutzer)	Ja	Ja
Chat über virtuelle Konsole	Nein	Nein	Nein	Ja	Ja
Virtuelle Flash-Partitionen	Nein	Nein	Nein	Ja	Ja
ANMERKUNG: vFlash ist auf iDRAC9 für PowerEdge Rx5xx/Cx5xx nicht verfügbar.					
Group Manager	Nein	Nein	Nein	Ja	Ja
HTTP/HTTPS-Unterstützung mit NFS/CIFS	Ja	Ja	Ja	Ja	Ja
Strom und thermisch					
Echtzeit-Leistungsmesser	Ja	Ja	Ja	Ja	Ja
Stromschwellenwerte und Warnungen	Nein	Ja	Ja	Ja	Ja
Echtzeit-Stromdiagramme	Nein	Ja	Ja	Ja	Ja
Historische Stromzähler	Nein	Ja	Ja	Ja	Ja
Strombegrenzung	Nein	Nein	Nein	Ja	Ja
Power Center-Integration	Nein	Nein	Nein	Ja	Ja
Temperaturüberwachung	Ja	Ja	Ja	Ja	Ja
Temperatur-Diagramme	Nein	Ja	Ja	Ja	Ja
PCIe-Luftstrom-Anpassung (LFM)	Nein	Nein	Nein	Nein	Ja
Benutzerdefinierte Auslasssteuerung	Nein	Nein	Nein	Nein	Ja
Benutzerdefinierte Delta-T-Steuerung	Nein	Nein	Nein	Nein	Ja

Tabelle 2. Lizenzierte Funktionen in iDRAC9 (fortgesetzt)

Funktion	iDRAC9 Basic	iDRAC9 Express	iDRAC9 Express für Blades	iDRAC9 Enterprise	iDRAC9-Datacenter
System-Luftstromverbrauch	Nein	Nein	Nein	Nein	Ja
Benutzerdefinierte PCIe-Einlasstemperatur	Nein	Nein	Nein	Nein	Ja
Zustandsüberwachung					
Vollständig Agentenfreie Überwachung	Ja	Ja	Ja	Ja	Ja
Vorhergesagte Fehler-Überwachung	Ja	Ja	Ja	Ja	Ja
Unterstützung von SNMP v1, v2 und v3 (Traps und Gets)	Ja	Ja	Ja	Ja	Ja
E-Mail-Warnungen	Nein	Ja	Ja	Ja	Ja
Konfigurierbare Schwellenwerte	Ja	Ja	Ja	Ja	Ja
Überwachung des Lüfters	Ja	Ja	Ja	Ja	Ja
Überwachung der Stromversorgung	Ja	Ja	Ja	Ja	Ja
Speicherüberwachung	Ja	Ja	Ja	Ja	Ja
GPU	Nein	Nein	Nein	Ja	Ja
CPU-Überwachung	Ja	Ja	Ja	Ja	Ja
RAID-Überwachung	Ja	Ja	Ja	Ja	Ja
NIC-Überwachung	Ja	Ja	Ja	Ja	Ja
Optisches Inventar	Ja	Ja	Ja	Ja	Ja
Optische Statistiken	Nein	Nein	Nein	Nein	Ja
HD-Überwachung (Gehäuse)	Ja	Ja	Ja	Ja	Ja
Bandexternes Performancemonitoring	Nein	Nein	Nein	Ja	Ja
Warnungen für übermäßige SSD-Abnutzung	Ja	Ja	Ja	Ja	Ja
Benutzerdefinierte Einstellungen für die Eintrittstemperatur	Ja	Ja	Ja	Ja	Ja
Serielle Konsolenprotokolle	Nein	Nein	Nein	Nein	Ja
SMART-Protokolle für Speicherlaufwerke	Nein	Nein	Nein	Nein	Ja

Tabelle 2. Lizenzierte Funktionen in iDRAC9 (fortgesetzt)

Funktion	iDRAC9 Basic	iDRAC9 Express	iDRAC9 Express für Blades	iDRAC9 Enterprise	iDRAC9-Datacenter
Erkennung spannungsloser Server	Nein	Nein	Nein	Nein	Ja
Telemetrie-Streaming	Nein	Nein	Nein	Nein	Ja
ANMERKUNG: Die OpenManage Enterprise Advanced-Lizenz und das PowerManage-Plug-in unterstützen Telemetriedaten vom iDRAC.					
Aktualisierung					
Remote-Agentenfreie Aktualisierung	Ja	Ja	Ja	Ja	Ja
Integrierte Aktualisierung-Tools	Ja	Ja	Ja	Ja	Ja
Aktualisierung über Repository (Automatische Aktualisierung)	Nein	Nein	Nein	Ja	Ja
Aktualisierung über Repository planen	Nein	Nein	Nein	Ja	Ja
Verbesserte PSU-Firmwareupdates	Ja	Ja	Ja	Ja	Ja
Bereitstellung und Konfiguration					
Lokale Konfiguration über F10	Ja	Ja	Ja	Ja	Ja
Integrierte BS-Bereitstellungs-Tools	Ja	Ja	Ja	Ja	Ja
Integrierte Konfigurations-Tools	Ja	Ja	Ja	Ja	Ja
Automatische Ermittlung	Nein	Ja	Ja	Ja	Ja
Remote BS-Bereitstellung	Nein	Ja	Ja	Ja	Ja
Integriertes Treiberpaket	Ja	Ja	Ja	Ja	Ja
Vollständige Konfigurationsbestandsaufnahme	Ja	Ja	Ja	Ja	Ja
Inventar exportieren	Ja	Ja	Ja	Ja	Ja
Remote-Konfiguration	Ja	Ja	Ja	Ja	Ja
Berührungslose Konfiguration	Nein	Nein	Nein	Ja	Ja
System stillegen/ Neuzuweisung	Ja	Ja	Ja	Ja	Ja
Serverkonfigurationsprofil in der GUI	Ja	Ja	Ja	Ja	Ja

Tabelle 2. Lizenzierte Funktionen in iDRAC9 (fortgesetzt)

Funktion	iDRAC9 Basic	iDRAC9 Express	iDRAC9 Express für Blades	iDRAC9 Enterprise	iDRAC9-Datacenter
Hinzufügen der BIOS-Konfiguration zur iDRAC-GUI	Ja	Ja	Ja	Ja	Ja
GPU-Eigenschaften	Nein	Nein	Nein	Ja	Ja
Diagnose, Dienste und Protokolle					
Integrierte Diagnosetools	Ja	Ja	Ja	Ja	Ja
Teilersetzung	Nein	Ja	Ja	Ja	Ja
ANMERKUNG: Nach Austauschen von Komponenten der RAID-Hardware werden nach Abschluss des Austauschs von Firmware und der Konfiguration in den Lifecycle-Protokollen doppelte Einträge zum Austausch von Komponenten gemeldet, was das erwartete Verhalten darstellt.					
Einfache Wiederherstellung (Systemkonfiguration)	Ja	Ja	Ja	Ja	Ja
Automatisches Timeout für einfache Wiederherstellung	Ja	Ja	Ja	Ja	Ja
ANMERKUNG: Server-Backup- und -Wiederherstellungsfunktionen sind in iDRAC9 für PowerEdge Rx5xx/Cx5xx nicht verfügbar.					
LED-Anzeigen zum Funktionszustand	Ja	Ja	k. A.	Ja	Ja
LCD-Bildschirm (iDRAC9 optional erforderlich)	Ja	Ja	k. A.	Ja	Ja
iDRAC Quick Sync 2 (BLE/Wi-Fi-Hardware)	Ja	Ja	Ja	Ja	Ja
iDRAC Direkt (Vordere USB-Verwaltungsschnittstelle)	Ja	Ja	Ja	Ja	Ja
iDRAC-Servicemodul (iSM) integriert	Ja	Ja	Ja	Ja	Ja
iSM in bandinternen Warnungsweiterleitung auf Konsolen	Ja	Ja	Ja	Ja	Ja
SupportAssist-Sammlung(integriert)	Ja	Ja	Ja	Ja	Ja
Absturzbildschirm-Erfassung	Nein	Ja	Ja	Ja	Ja
Absturzvideo-Erfassung[1]	Nein	Nein	Nein	Ja	Ja
Agentenlose Absturzvideo-Erfassung (nur Windows)	Nein	Nein	Nein	Nein	Ja
Start-Erfassung	Nein	Nein	Nein	Ja	Ja
Manuelles Zurücksetzen für iDRAC (LCD-ID-Taste)	Ja	Ja	Ja	Ja	Ja

Tabelle 2. Lizenzierte Funktionen in iDRAC9 (fortgesetzt)

Funktion	iDRAC9 Basic	iDRAC9 Express	iDRAC9 Express für Blades	iDRAC9 Enterprise	iDRAC9-Datacenter
Remote-Zurücksetzung für iDRAC (erfordert iSM)	Ja	Ja	Ja	Ja	Ja
Virtuelles NMI	Ja	Ja	Ja	Ja	Ja
BS-Watchdog	Ja	Ja	Ja	Ja	Ja
System-Ereignisprotokoll	Ja	Ja	Ja	Ja	Ja
Lifecycle-Protokoll	Ja	Ja	Ja	Ja	Ja
Erweiterte Protokollierung im Lifecycle Controller-Protokoll	Ja	Ja	Ja	Ja	Ja
Arbeitsanmerkungen	Ja	Ja	Ja	Ja	Ja
Remote-Syslog	Nein	Nein	Nein	Ja	Ja
Lizenzverwaltung	Ja	Ja	Ja	Ja	Ja
Verbesserte Kundenerfahrung					
iDRAC – schnellerer Prozessor, mehr Arbeitsspeicher	k. A.	Ja	k. A.	Ja	Ja
GUI in HTML5 gerendert	k. A.	Ja	k. A.	Ja	Ja
Hinzufügen der BIOS-Konfiguration zur iDRAC-GUI	k. A.	Ja	k. A.	Ja	Ja

[1] Erfordert den iSM- oder OMSA-Agenten auf Zielserver.

Schnittstellen und Protokoll für den Zugriff auf iDRAC

In der folgenden Tabelle werden die Schnittstellen für den Zugriff auf iDRAC dargestellt.

ANMERKUNG: Die gleichzeitige Verwendung von mehr als einer Schnittstelle kann zu unerwarteten Ergebnissen führen.

Tabelle 3. Schnittstellen und Protokoll für den Zugriff auf iDRAC

Schnittstelle oder Protokoll	Beschreibung
Dienstprogramm für iDRAC-Einstellungen (F2)	Verwenden Sie das Dienstprogramm für die iDRAC-Einstellungen, um Pre-OS-Vorgänge durchzuführen. Dieses Dienstprogramm bietet einige Funktionen, die in der iDRAC-Weboberfläche verfügbar sind, sowie einige weitere Funktionen. Drücken Sie zum Zugreifen auf das Dienstprogramm für die iDRAC-Einstellungen während des Startvorgangs <F2> und klicken Sie dann auf **iDRAC-Einstellungen** auf der Seite **System-Setup-Hauptmenü**.
Lifecycle Controller (F10)	Verwenden Sie Lifecycle Controller, um iDRAC-Konfigurationen vorzunehmen. Um auf den Lifecycle Controller zuzugreifen, drücken Sie während des Starts die Taste <F10> und gehen Sie zu **System-Setup** > **Erweiterte Hardwarekonfiguration** > **iDRAC-Einstellungen**. Weitere Informationen finden Sie im *Benutzerhandbuch zum Lifecycle Controller* unter **dell.com/idracmanuals**.

Tabelle 3. Schnittstellen und Protokoll für den Zugriff auf iDRAC (fortgesetzt)

Schnittstelle oder Protokoll	Beschreibung
iDRAC-Weboberfläche	Über die iDRAC-Weboberfläche können Sie iDRAC verwalten und das verwaltete System überwachen. Der Browser stellt über den HTTPS-Port eine Verbindung zum Webserver her. Datenstreams werden für Datenschutz und Integrität mit der 128-Bit-SSL-Verschlüsselung verschlüsselt. Sämtliche Verbindungen zum HTTP-Port werden zu HTTPS umgeleitet. Administratoren können über einen SSL-CSR-Generierungsprozess eigene SSL-Zertifikate hochladen, um den Webserver zu sichern. Die standardmäßigen HTTP- und HTTPS-Ports können geändert werden. Der Benutzerzugriff basiert auf Benutzerberechtigungen.
Weboberfläche OpenManage Enterprise (OME) Modular	**ANMERKUNG:** Diese Schnittstelle ist nur für MX-Plattformen verfügbar. Neben der Überwachung und der Verwaltung des Gehäuses können Sie die OME-Modular-Weboberfläche für die folgenden Aktivitäten verwenden: ● Status eines Managed System anzeigen ● iDRAC-Firmware aktualisieren ● iDRAC-Netzwerkeinstellungen konfigurieren ● Bei der iDRAC-Weboberfläche anmelden ● Managed System starten, anhalten oder zurücksetzen ● BIOS, PERC und unterstützte Netzwerkadapter aktualisieren Weitere Informationen finden Sie im *OME - Modular für PowerEdge MX7000-Gehäuse – Benutzerhandbuch* verfügbar unter https://www.dell.com/openmanagemanuals.
CMC-Weboberfläche	**ANMERKUNG:** Diese Schnittstelle ist auf MX-Plattformen nicht verfügbar. Neben der Überwachung und der Verwaltung des Gehäuses können Sie die CMC-Weboberfläche für die folgenden Aktivitäten verwenden: ● Status eines Managed System anzeigen ● iDRAC-Firmware aktualisieren ● iDRAC-Netzwerkeinstellungen konfigurieren ● Bei der iDRAC-Weboberfläche anmelden ● Managed System starten, anhalten oder zurücksetzen ● BIOS, PERC und unterstützte Netzwerkadapter aktualisieren
Server-LCD-Bedienfeld/ Gehäuse-LCD-Bedienfeld	Verwenden Sie das LCD-Bedienfeld auf der Frontblende des Servers, um die folgenden Aktivitäten auszuführen: ● Warnungen, IP- oder MAC-Adresse für iDRAC oder benutzerprogrammierbare Zeichenfolgen anzeigen ● DHCP festlegen ● Statische IP-Einstellungen für iDRAC konfigurieren Bei Blade-Servern befindet sich das LCD-Bedienfeld auf der Frontblende des Gehäuses und wird von allen Blades gemeinsam verwendet. Um iDRAC ohne einen Neustart des Servers neu zu starten, halten Sie die Systemerkennungstaste 16 Sekunden lang gedrückt. **ANMERKUNG:** Das LCD-Bedienfeld ist nur bei Rack- oder Tower-Systemen verfügbar, die für die Frontverkleidung ausgelegt sind. Bei Blade-Servern befindet sich das LCD-Bedienfeld auf der Frontblende des Gehäuses und wird von allen Blades gemeinsam verwendet.
RACADM	Verwenden Sie das Befehlszeilendienstprogramm für iDRAC- und Serververwaltung. Sie können RACADM lokal und remote verwenden. ● Die lokale RACADM-Befehlszeilenschnittstelle wird auf verwalteten Systemen ausgeführt, auf dem Server Administrator installiert ist. Die lokale RACADM-Schnittstelle kommuniziert über die bandinterne IPMI-Hostschnittstelle mit iDRAC. Da es auf dem lokal verwalteten System installiert ist, müssen sich Benutzer zum Ausführen dieses Dienstprogramms beim Betriebssystem anmelden. Ein Benutzer muss über umfassende Administratorrechte verfügen oder ein Root-Benutzer sein, um dieses Dienstprogramm zu verwenden. ● Remote-RACADM ist ein Client-Dienstprogramm, das auf einer Management Station ausgeführt wird. Es verwendet die bandexterne Netzwerkschnittstelle, um die RACADM-Befehle auf dem Managed System

Tabelle 3. Schnittstellen und Protokoll für den Zugriff auf iDRAC (fortgesetzt)

Schnittstelle oder Protokoll	Beschreibung
	auszuführen, außerdem wird der HTTPs-Kanal verwendet. Die Option **–r** führt den RACADM-Befehl über ein Netzwerk aus. ● Sie können auf die Firmware-RACADM zugreifen, indem Sie sich über SSH bei iDRAC anmelden. Sie können die Firmware-RACADM-Befehle ohne Angabe der IP-Adresse, des Nutzernamens oder des Kennworts für iDRAC ausführen. ● Es ist nicht erforderlich, die IP-Adresse, den Nutzernamen oder das Kennwort für iDRAC anzugeben, um die Firmware-RACADM-Befehle auszuführen. Nach der Eingabe an der RACADM-Eingabeaufforderung können Sie die Befehle ohne das Präfix „racadm“ direkt ausführen.
iDRAC RESTful-API und Redfish	Der Redfish Scalable Platforms Management API-Standard wurde von der Distributed Management Task Force (DMTF) definiert. Redfish ist ein Verwaltungsschnittstellenstandard für Systeme der nächsten Generation, das eine skalierbare, sichere und offene Serververwaltung ermöglicht. Es ist eine neue Schnittstelle, die die RESTful-Schnittstellensemantik für den Zugriff auf die im Modellformat definierten Daten für die bandexterne Systemverwaltung verwendet. Sie ist für zahlreiche Server geeignet, von eigenständigen Servern bis hin zu Rack-Server- und Blade-Server-Umgebungen, sowie für große Cloud-Umgebungen. Redfish bietet die folgenden Vorteile gegenüber bestehenden Serververwaltungsmethoden: ● Einfachheit und Nutzbarkeit ● Hohe Datensicherheit ● Programmierbare Schnittstelle, für die problemlos Skripte erstellt werden können ● Entspricht weit verbreiteten Standards Das iDRAC Redfish API Benutzerhandbuch finden Sie unter www.api-marketplace.com
WSMan	Der LC-Remote Service basiert auf dem WSMan-Protokoll für One-to-many-Managementaufgaben. Sie müssen einen WSMan-Client verwenden, z. B. den WinRM-Client (Windows) oder den OpenWSMan-Client (Linux), um die LC-Remote Services-Funktion zu verwenden. Sie können außerdem Power Shell oder Python verwenden, um auf die WSMan-Schnittstelle zu schreiben. Web Services for Management (WSMan) ist ein SOAP-basiertes Protokoll (Simple Object Access Protocol), das für die Systemverwaltung verwendet wird. iDRAC verwendet WSMan zur Übertragung der DMTF-CIM-basierten Verwaltungsinformationen (Distributed Management Task Force Common Information Model). Die CIM-Informationen definieren die Semantik und Informationstypen, die in einem verwalteten System geändert werden können. Die durch WSMan zur Verfügung gestellten Daten werden durch die iDRAC-Instrumentierungsschnittstelle bereitgestellt, die den DMTF-Profilen und den Erweiterungsprofilen zugeordnet ist. Weitere Informationen stehen zur Verfügung unter: ● *Schnellstart-Benutzerhandbuch für Lifecycle Controller Remote Services* verfügbar unter https://www.dell.com/idracmanuals. ● MOFs und Profile – http://downloads.dell.com/wsman. ● DMTF-Website – dmtf.org/standards/profiles
SSH	Verwenden Sie SSH, um RACADM-Befehle auszuführen. Der SSH-Dienst ist standardmäßig für iDRAC aktiviert. Der SSH-Dienst kann in iDRAC deaktiviert werden. iDRAC unterstützt nur SSH Version 2 mit dem RSA-Hostschlüssel-Algorithmus. Ein eindeutiger 1024-Bit-RSA-Host-Schlüssel wird generiert, wenn iDRAC zum ersten Mal eingeschaltet wird.
IPMItool	Verwenden Sie IPMITool für den Zugriff auf Basismanagementfunktionen für das Remotesystem über iDRAC. Die Schnittstelle umfasst lokale IPMI, IPMI über LAN, IPMI über Seriell und Seriell über LAN. Weitere Informationen über IPMITool finden Sie im *Benutzerhandbuch für Dienstprogramme des Dell OpenManage Baseboard Management Controller* unter dell.com/idracmanuals. **ANMERKUNG:** IPMI Version 1.5 wird nicht unterstützt.
NTLM	iDRAC bietet für NTLM die Authentifizierung, Integrität und Vertraulichkeit für Benutzer. NT LAN Manager (**NTLM**) ist eine Suite von Microsoft-Sicherheitsprotokollen und funktioniert in einem Windows-Netzwerk.
SMB	iDRAC9 unterstützt das SMB-Protokoll (Server Message Block). Dies ist ein Protokoll für die Netzwerkfreigabe und die standardmäßig unterstützte Mindest-SMB-Version ist 2.0 SMBv1 wird nicht mehr unterstützt.

Tabelle 3. Schnittstellen und Protokoll für den Zugriff auf iDRAC (fortgesetzt)

Schnittstelle oder Protokoll	Beschreibung
NFS	iDRAC9 unterstützt **Network File System** (**NFS**). Dies ist ein verteiltes Dateisystemprotokoll, das es Benutzern ermöglicht, Remoteverzeichnisse auf den Servern **bereitzustellen**.

iDRAC-Schnittstelleninformationen

In der folgenden Tabelle sind die Ports aufgeführt, die für den Fernzugriff auf den iDRAC über die Firewall erforderlich sind. Dies sind die standardmäßigen Schnittstellen, auf die iDRAC für Verbindungen wartet. Optional können Sie die meisten Schnittstellen ändern. Informationen zum Ändern der Ports finden Sie unter Dienste konfigurieren auf Seite 101.

Tabelle 4. Schnittstellen, auf die iDRAC für Verbindungen wartet

Portnummer	Typ	Funktion	Konfigurierbare Schnittstelle	Maximale Verschlüsselungsstufe
22	TCP	SSH	Ja	256-Bit SSL
80	TCP	HTTP	Ja	Keine
161	UDP	SNMP-Agent	Ja	Keine
443	TCP	• Web-GUI-Zugriff mit HTTPS • Virtuelle Konsole und virtueller Datenträger mit eHTML5-Option • Virtuelle Konsole und virtueller Datenträger mit HTML5-Option, wenn die Webserver-Umleitung aktiviert ist	Ja	256-Bit SSL
623	UDP	RMCP/RMCP+	Nein	128 Bit SSL
5000	TCP	iDRAC zu iSM	Nein	256-Bit SSL
ANMERKUNG: Maximale Verschlüsselungsstufe ist 256-Bit-SSL, wenn sowohl iSM 3.4 oder höher und iDRAC-Firmware 3.30.30.30 oder höher installiert sind.				
5900	TCP	Virtuelle Konsole und virtueller Datenträger mit HTML5-, Java- und ActiveX-Option	Ja	128 Bit SSL
5901	TCP	VNC	Ja	128 Bit SSL
ANMERKUNG: Port 5901 wird geöffnet, wenn die VNC-Funktion aktiviert ist.				

Die folgende Tabelle listet die Schnittstellen auf, die iDRAC als Client verwendet:

Tabelle 5. Schnittstellen, die iDRAC als Client verwendet

Portnummer	Typ	Funktion	Konfigurierbare Schnittstelle	Maximale Verschlüsselungsstufe
25	TCP	SMTP	Ja	Keine
53	UDP	DNS	Nein	Keine
68	UDP	DHCP-zugewiesene IP-Adresse	Nein	Keine
69	TFTP	TFTP	Nein	Keine
123	UDP	Network Time Protocol (NTP)	Nein	Keine
162	UDP	SNMP-Trap	Ja	Keine
445	TCP	Common Internet File System (CIFS)	Nein	Keine

Tabelle 5. Schnittstellen, die iDRAC als Client verwendet (fortgesetzt)

Portnummer	Typ	Funktion	Konfigurierbare Schnittstelle	Maximale Verschlüsselungsstufe
636	TCP	LDAP über SSL (LDAPS)	Nein	256-Bit SSL
2049	TCP	Network File System (NFS)	Nein	Keine
3269	TCP	LDAPS für globalen Katalog (GC)	Nein	256-Bit SSL
5353	UDP	mDNS	Nein	Keine
ANMERKUNG: Wenn die vom Node initiierte Prüfung oder Group Manager aktiviert ist, verwendet der iDRAC mDNS für die Kommunikation über Port 5353. Wenn er jedoch beide Funktionen deaktiviert sind, wird Port 5353 durch die interne Firewall des iDRAC blockiert und erscheint als offener|gefilterter Port in den Port-Scans.				
514	UDP	Remote-Syslog	Ja	Keine

Weitere nützliche Dokumente

Einige der iDRAC-Schnittstellen haben das integrierte Dokument *Onlinehilfe*, auf das zugegriffen werden kann. Klicken Sie dazu auf das Hilfe-Symbol (?). Die *Onlinehilfe* enthält ausführliche Informationen zu den in der Webschnittstelle verfügbaren Feldern und den dazugehörigen Beschreibungen. Zusätzlich bieten die folgenden, auf der Dell Support-Website unter **dell.com/support/** verfügbaren Dokumente zusätzliche Informationen über das Setup und den Betrieb von iDRAC auf Ihrem System.

- Das iDRAC Redfish API-Handbuch, das unter https://developer.dell.com verfügbar ist, enthält Informationen über die Redfish API.
- Unter *iDRAC-RACADM-CLI-Handbuch* finden Sie Informationen zu den RACADM-Unterbefehlen, den unterstützten Schnittstellen und iDRAC-Eigenschaften-Datenbankgruppen und Objektdefinitionen.
- Unter *Systemverwaltungsübersicht-Handbuch* finden Sie zusammengefasste Informationen zu den verschiedenen Software-Produkten, die für Systemverwaltungsaufgaben verfügbar sind.
- Das *Benutzerhandbuch für das Dell Remote Access Configuration Tool* enthält Informationen zur Verwendung des Tools für die Ermittlung von iDRAC-IP-Adressen in Ihrem Netzwerk und zum Ausführen von 1-zu-n-Firmware-Aktualisierungen und Active Directory-Konfigurationen für die ermittelten IP-Adressen.
- Die *Dell Systems Software Support Matrix* bietet Informationen über die verschiedenen Dell-Systeme, über die von diesen Systemen unterstützten Betriebssysteme und über die Dell OpenManage-Komponenten, die auf diesen Systemen installiert werden können.
- Das *iDRAC-Servicemodul Benutzerhandbuch* enthält Informationen zum Installieren des iDRAC-Servicemoduls.
- Das *Dell OpenManage Server Administrator-Installationshandbuch* enthält Anleitungen zur Installation von Dell OpenManage Server Administrator.
- Das *Dell OpenManage Management Station Software-Installationshandbuch* enthält Anleitungen zur Installation der Dell OpenManage Management Station-Software, die das Baseboard Management-Dienstprogramm, DRAC Tools und Active Directory Snap-In enthält.
- Informationen zur IPMI-Schnittstelle finden Sie im *Benutzerhandbuch für Verwaltungsdienstprogramme des Dell OpenManage Baseboard-Verwaltungs-Controllers*.
- Die *Versionshinweise* geben den letzten Stand der Änderungen am System oder der Dokumentation wieder oder enthalten erweitertes technisches Referenzmaterial für erfahrene Benutzer oder Techniker.

Die folgenden Systemdokumente sind erhältlich, um weitere Informationen zur Verfügung zu stellen:

- In den mit dem System gelieferten Sicherheitshinweisen finden Sie wichtige Informationen zur Sicherheit und zu den Betriebsbestimmungen. Weitere Betriebsbestimmungen finden Sie auf der Website zur Einhaltung gesetzlicher Vorschriften unter **www.dell.com/regulatory_compliance**. Garantieinformationen können möglicherweise als separates Dokument beigelegt sein.
- In der zusammen mit der Rack-Lösung gelieferten *Anweisungen für die Rack-Montage* wird beschrieben, wie das System in einem Rack installiert wird.
- Unter *Handbuch zum Einstieg* finden Sie eine Übersicht über die Systemfunktionen, das Einrichten des Systems und die technischen Spezifikationen.
- Unter *Installations- und Service-Handbuch* finden Sie Informationen über Systemfunktionen, zur Fehlerbehebung am System und zur Installation oder zum Austausch von Systemkomponenten.

Kontaktaufnahme mit Dell

ANMERKUNG: Wenn Sie über keine aktive Internetverbindung verfügen, so finden Sie Kontaktinformationen auf der Eingangsrechnung, dem Lieferschein, der Rechnung oder im Dell Produktkatalog.

Dell bietet verschiedene Optionen für Online- und Telefonsupport an. Die Verfügbarkeit ist abhängig von Land und Produkt und einige Dienste sind in Ihrem Gebiet möglicherweise nicht verfügbar. Kontaktdaten zum Vertrieb, technischen Support und Kundendienst von Dell finden Sie unter https://www.dell.com/contactdell.

Zugriff auf Dokumente der Dell Support-Website

Sie können auf eine der folgenden Arten auf die folgenden Dokumente zugreifen:

- Verwendung der folgenden Links:
  - Für alle Dokumente zu Enterprise Systems Management und OpenManage Connections – https://www.dell.com/esmmanuals
  - Für Dokumente zu OpenManage – https://www.dell.com/openmanagemanuals
  - Für Dokumente zu iDRAC und Lifecycle Controller – https://www.dell.com/idracmanuals
  - Für Dokumente zu Serviceability Tools – https://www.dell.com/serviceabilitytools
  - Für Dokumente zu Client Command Suite Systems Management – https://www.dell.com/omconnectionsclient

Zugriff auf Dokumente über die Produktsuche

1. Gehen Sie zu https://www.dell.com/support.
2. Geben Sie im Suchfeld **Geben Sie eine Service-Tag -Seriennummer ein...** Den Produktnamen ein. Zum Beispiel **`PowerEdge`** oder **`iDRAC`**.

   Eine Liste passender Produkte wird angezeigt.
3. Wählen Sie Ihr Produkt aus und klicken Sie auf das Suchsymbol oder drücken Sie die Eingabetaste.
4. Klicken Sie auf **DOKUMENTATION**.
5. Klicken Sie auf **HANDBÜCHER UND DOKUMENTE**.

Zugriff auf Dokumente über die Produktauswahl

Sie können auch auf Dokumente zugreifen, indem Sie Ihr Produkt auswählen.

1. Gehen Sie zu https://www.dell.com/support.
2. Klicken Sie auf **Alle Produkte durchsuchen**.
3. Klicken Sie auf die gewünschte Produktkategorie, z. B. Server, Software, Speicher usw.
4. Klicken Sie auf das gewünschte Produkt und dann auf die gewünschte Version, falls zutreffend.

   ANMERKUNG: Für einige Produkte müssen Sie eventuell durch die Unterkategorien navigieren.
5. Klicken Sie auf **DOKUMENTATION**.
6. Klicken Sie auf **HANDBÜCHER UND DOKUMENTE**.

Zugriff auf Redfish API-Handbuch

Das Redfish API-Handbuch ist jetzt auf dem Dell API Marketplace verfügbar. So greifen Sie auf das Redfish API-Handbuch zu:

1. Besuchen Sie www.api-marketplace.com.
2. Klicken Sie auf **Explore API** und klicken Sie dann auf **APIs**.
3. Klicken Sie unter iDRAC9 Redfish API auf **Mehr anzeigen**.

2

Anmelden bei iDRAC

Sie können sich beim iDRAC als iDRAC-Benutzer, als Microsoft Active Directory-Benutzer oder als Lightweight Directory Access Protocol-Benutzer (LDAP-Benutzer) anmelden. Sie können sich auch mit OpenID Connect und Single Sign-On oder Smart Card anmelden.

Für höhere Sicherheit wird jedes System mit einem eindeutigen Kennwort für iDRAC ausgeliefert, das auf dem Tag mit Systemangaben verfügbar ist. Dieses eindeutige Kennwort sorgt für mehr Sicherheit für iDRAC und Ihren Server. Die Standardeinstellung für den Benutzernamen lautet *root*.

Bei der Bestellung des Systems können Sie das Legacy-Kennwort „calvin“ als Standardkennwort festlegen. Wenn Sie das Legacy-Kennwort gewählt haben, ist das Kennwort nicht auf dem Tag mit Systemangaben verfügbar.

In dieser Version ist DHCP standardmäßig aktiviert und die iDRAC-IP-Adresse wird dynamisch zugewiesen.

ANMERKUNG:

- Sie müssen über Berechtigungen zum Anmelden bei iDRAC verfügen, um sich bei iDRAC anzumelden.
- iDRAC-GUI unterstützt keine Browser Schaltflächen wie z. B. **Zurück**, **Vorwärts** oder **Aktualisieren**.

ANMERKUNG: Informationen zu empfohlenen Zeichen für Benutzernamen und Kennwörter finden Sie unter Empfohlene Zeichen in Benutzernamen und Kennwörtern auf Seite 152.

Informationen zum Ändern des Standardkennworts finden Sie unter Ändern des standardmäßigen Anmeldekennworts auf Seite 45.

Benutzerdefinierbare Sicherheitsbanner

Sie können den Sicherheitshinweis, der auf der Anmeldeseite angezeigt wird, anpassen. Sie können SSH, RACADM, Redfish oder WSMan zum Anpassen des Hinweises verwende. Je nach die Sprache kann der Hinweis entweder 1024 oder 512 UTF-8-Zeichen lang sein.

OpenID verbinden

ANMERKUNG: Diese Funktion ist nur auf MX-Plattformen verfügbar.

Sie können sich bei iDRAC mit Anmeldeinformationen anderer Webkonsolen wie Dell EMC OpenManage Enterprise (OME) – Modular anmelden. Wenn diese Funktion aktiviert ist, startet die Konsole die Verwaltung der Benutzerberechtigungen auf dem iDRAC. iDRAC stellt der Benutzersitzung alle Berechtigungen zur Verfügung, die von der Konsole festgelegt werden.

ANMERKUNG: Wenn der Sperrmodus aktiviert ist, werden OpenID Connect-Anmeldeoptionen nicht auf der iDRAC-Anmeldeseite angezeigt.

Sie können nun auf detaillierte Hilfe zugreifen, ohne sich bei iDRAC anzumelden. Verwenden Sie die Links auf der iDRAC-Anmeldungsseite, um Hilfe und Versionsinformationen, Treiber und Downloads, Handbücher und TechCenter aufzurufen.

Themen:

- Kennwortänderung erzwingen (FCP)
- Anmeldung bei iDRAC mit OpenID Connect
- Logging in to iDRAC as local user, Active Directory user, or LDAP user
- Bei iDRAC über eine Smartcard als lokaler Nutzer anmelden
- Bei iDRAC über die einmalige Anmeldung anmelden
- Über Remote-RACADM auf iDRAC zugreifen
- Über lokalen RACADM auf iDRAC zugreifen
- Über Firmware-RACADM auf iDRAC zugreifen
- Einfache Zwei-Faktor-Authentifizierung (einfache 2FA)
- RSA SecurID 2FA
- Systemzustand anzeigen

- Anmeldung beim iDRAC mit Authentifizierung mit öffentlichem Schlüssel
- Mehrere iDRAC-Sitzungen
- Standardkennwort sichern
- Ändern des standardmäßigen Anmeldekennworts
- Aktivieren oder Deaktivieren der standardmäßigen Kennwortwarnungsmeldung
- Richtlinie zur Kennwortsicherheit
- IP-Blockierung
- Aktivieren und Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung der Web-Schnittstelle
- Warnungen über RACADM aktivieren oder deaktivieren

Kennwortänderung erzwingen (FCP)

Die Funktion „Kennwortänderung erzwingen“ fordert Sie auf, das werkseitige Standardkennwort für das Gerät zu ändern. Die Funktion kann im Rahmen der werksseitigen Konfiguration aktiviert werden.

Der FCP-Bildschirm wird nach erfolgreicher Benutzerauthentifizierung angezeigt und kann nicht übersprungen werden. Erst nachdem der Benutzer ein Passwort eingegeben hat, ist der normale Zugriff und Betrieb zulässig. Der Status dieses Attributs wird durch den Vorgang „Konfiguration auf Standardeinstellungen zurücksetzen“ nicht beeinflusst.

ANMERKUNG: Um das FCP-Attribut einzustellen oder zurückzusetzen, müssen Sie über die Berechtigung zur Anmeldung und Benutzerkonfiguration verfügen.

ANMERKUNG: Wenn FCP aktiviert ist, wird die Einstellung für die standardmäßige Kennwortwarnung nach dem Ändern des Standard-Benutzerkennwortes deaktiviert.

ANMERKUNG: Wenn der Root-Benutzer sich über die Authentifizierung mit öffentlichem Schlüssel (PKA) anmeldet, wird FCP umgangen.

Wenn FCP aktiviert ist, werden folgende Aktionen nicht zugelassen:

- Melden Sie sich beim iDRAC über eine beliebige Benutzeroberfläche außer die IPMIpover-LAN-Schnittstelle an, die CLI mit Benutzeranmeldedaten verwendet.
- Anmelden bei iDRAC über die OMM-App über Quick Sync-2
- Hinzufügen eines Mitglieds-iDRAC in Group Manager.

Anmeldung bei iDRAC mit OpenID Connect

ANMERKUNG: Diese Funktion ist nur auf MX-Plattformen verfügbar.

So melden Sie sich mit OpenID Connect bei iDRAC an:

1. Geben Sie in einem unterstützten Webbrowser `https://[iDRAC-IP-address]` ein und drücken Sie die Eingabetaste.
   Die Seite für die Anmeldung wird angezeigt.
2. Wählen Sie im Menü **Anmelden mit: OME Modular** aus.
   Die Konsolen-Anmeldeseite wird angezeigt.
3. Geben Sie **Benutzernamen** und **Kennwort** für die Konsole ein.
4. Klicken Sie auf **Anmelden**.
   Sie werden mit den Konsolen-Benutzerberechtigungen am iDRAC angemeldet.
   ANMERKUNG: Wenn der Sperrmodus aktiviert ist, wird die OpenID Connect-Anmeldeoption nicht auf der iDRAC-Anmeldeseite angezeigt.

Logging in to iDRAC as local user, Active Directory user, or LDAP user

Before you log in to iDRAC using the web interface, ensure that you have configured a supported web browser and the user account is created with the required privileges.

NOTE: The user name is not case-sensitive for an Active Directory user. The password is case-sensitive for all users.

NOTE: In addition to Active Directory, openLDAP, openDS, Novell eDir, and Fedora-based directory services are supported.

NOTE: LDAP authentication with OpenDS is supported. The DH key must be larger than 768 bits.

NOTE: RSA feature can be configured and enabled for LDAP user, but the RSA does not support if the LDAP is configured on Microsoft active directory. Hence LDAP user login fails. RSA is supported only for OpenLDAP.

To log in to iDRAC as local user, Active Directory user, or LDAP user:

1. Open a supported web browser.
2. In the **Address** field, type `https://[iDRAC-IP-address]` and press Enter.

   NOTE: If the default HTTPS port number (port 443) changes, enter: `https://[iDRAC-IP-address]:[port-number]` where `[iDRAC-IP-address]` is the iDRAC IPv4 or IPv6 address and `[port-number]` is the HTTPS port number.

   The **Login** page is displayed.
3. For a local user:
   - In the **Username** and **Password** fields, enter your iDRAC user name and password.
   - From the **Domain** drop-down menu, select **This iDRAC**.
4. For an Active Directory user, in the **User name** and **Password** fields, enter the Active Directory user name and password. If you have specified the domain name as a part of the username, select **This iDRAC** from the drop-down menu. The format of the user name can be: <domain>\<username>, <domain>/<username>, or <user>@<domain>.

   For example, dell.com\john_doe, or JOHN_DOE@DELL.COM.

   Active Directory domain from the **Domain** drop-down menu displays the last used domain.
5. For an LDAP user, in the **Username** and **Password** fields, enter your LDAP user name and password. Domain name is not required for LDAP login. By default, **This iDRAC** is selected in the drop-down menu.
6. Click **Submit**. You are logged in to iDRAC with the required user privileges.

   If you log in with Configure Users privileges and the default account credentials, and if the default password warning feature is enabled, the **Default Password Warning** page is displayed allowing you to easily change the password.

Bei iDRAC über eine Smartcard als lokaler Nutzer anmelden

Bevor Sie sich als lokaler Benutzer unter Verwendung einer Smartcard anmelden können, müssen Sie die folgenden Schritte ausführen:

- Nutzer-Smartcard-Zertifikat und vertrauenswürdiges Zertifikat der Zertifizierungsstelle in iDRAC hochladen.
- Smartcard-Anmeldung aktivieren

Die iDRAC-Weboberfläche zeigt die Smartcard-Anmeldeseite für alle Benutzer an, die für die Verwendung der Smartcard konfiguriert wurden.

ANMERKUNG: Abhängig von den Browser-Einstellungen werden Sie aufgefordert, das Smartcardlesegerät-ActiveX-Plug-in herunterzuladen und zu installieren, wenn Sie diese Funktion zum ersten Mal anwenden.

So melden Sie sich bei iDRAC als lokaler Nutzer mit einer Smartcard an:

1. Rufen Sie die iDRAC-Weboberfläche über den Link `https://[IP address]` auf.

   Die **iDRAC-Anmeldeseite** wird eingeblendet und fordert Sie zum Einlegen der Smartcard auf.

   ANMERKUNG: Wenn die standardmäßige HTTPS-Portnummer (Port 443) geändert wird, geben Sie Folgendes ein: `https://[IP address]:[port number]` , wobei `[IP address]` die IP-Adresse für den iDRAC und `[port number]` die HTTPS-Portnummer ist.
2. Legen Sie die Smartcard in das Laufwerk ein und klicken Sie auf **Anmeldung**.
   Sie werden daraufhin aufgefordert, die PIN für die Smartcard einzugeben. Ein Kennwort ist nicht erforderlich.
3. Geben Sie die PIN der Smartcard für lokale Smartcard-Nutzer ein.

   Sie werden am iDRAC angemeldet.

ANMERKUNG: Wenn Sie ein lokaler Nutzer sind, für den **CRL-Prüfung für Smartcard-Anmeldung aktivieren** aktiviert ist, versucht iDRAC, die Zertifikatswiderrufsliste (CRL) herunterzuladen, und überprüft die CRL für das Nutzerzertifikat. Die Anmeldung schlägt fehl, wenn das Zertifikat in der CRL als widerrufen aufgeführt wird oder wenn die CRL aus irgendeinem Grund nicht heruntergeladen werden kann.

ANMERKUNG: Wenn Sie sich bei iDRAC mit Smartcard anmelden, während RSA aktiviert ist, wird das RSA-Token umgangen und Sie können sich direkt anmelden.

Bei iDRAC über eine Smart Card als Active Directory-Benutzer anmelden

Bevor Sie sich über eine Smart Card als Active Directory-Benutzer anmelden, müssen Sie die folgenden Schritte ausführen:

- Laden Sie ein vertrauenswürdiges Zertifikat einer Zertifizierungsstelle (ein von einer Zertifizierungsstelle signiertes Active Directory-Zertifikat) nach iDRAC hoch.
- Konfigurieren Sie den DNS-Server.
- Aktivieren Sie die Active Directory-Anmeldung.
- Smart Card-Anmeldung aktivieren

So melden Sie sich über eine Smart Card als Active Directory-Benutzer bei iDRAC an:

1. Melden Sie sich über den Link `https://[IP address]` bei iDRAC an.

   Die **iDRAC-Anmeldeseite** wird eingeblendet und fordert Sie zum Einlegen der Smart Card auf.

   ANMERKUNG: Wenn die standardmäßige HTTPS-Portnummer (Port 443) geändert wurde, geben Sie Folgendes ein: `https://[IP address]:[port number]`, wobei `[IP address]` für die IP-Adresse des iDRAC und `[port number]` für die HTTPS-Portnummer steht.

2. Legen Sie die Smart Card ein und klicken Sie auf **Anmeldung**.
   Es wird eine Eingabeaufforderung zur Eingabe der Smart Card-**PIN** angezeigt.
3. Geben Sie die PIN ein und klicken Sie auf **Senden**.

   Sie sind über Ihre Active Directory-Anmeldedaten bei iDRAC angemeldet.

   ANMERKUNG:

   Wenn der Smart Card-Benutzer in Active Directory vorhanden ist, wird kein Active Directory-Kennwort benötigt.

Bei iDRAC über die einmalige Anmeldung anmelden

Wenn die einmalige Anmeldung (SSO) aktiviert ist, können Sie sich ohne die Eingabe Ihrer Anmeldeinformationen für die Domänen-Benutzerauthentifizierung (also Nutzername und Kennwort) bei iDRAC anmelden.

ANMERKUNG: Wenn ein AD-Nutzer SSO konfiguriert, während RSA aktiviert ist, wird das RSA-Token umgangen und der Nutzer wird direkt angemeldet.

Bei iDRAC SSO über die iDRAC-Webschnittstelle anmelden

Bevor Sie sich über das Verfahren für die einmalige Anmeldung bei iDRAC anmelden, müssen Sie Folgendes sicherstellen:

- Sie haben sich über ein gültiges Active Directory-Benutzerkonto bei Ihrem System angemeldet.
- Die Option für die einmalige Anmeldung ist während der Active Directory-Konfiguration aktiviert.

So melden Sie sich über die Webschnittstelle bei iDRAC an:

1. Melden Sie sich unter Verwendung eines gültigen Active Directory-Kontos an der Verwaltungsstation an.
2. Geben Sie in einem Webbrowser `https://[FQDN address]` ein.

   ANMERKUNG: Wenn die Standard-HTTPS-Portnummer (Port 443) geändert wurde, geben Sie Folgendes ein: `https://[FQDN address]:[port number]`, wobei `[FQDN address]` für den iDRAC-FQDN (idracdnsname.domain. Name) und `[port number]` für die HTTPS-Schnittstellennummer steht.

ANMERKUNG: Wenn Sie die IP-Adresse statt des FQDN verwenden, schlägt die SSO fehl.

iDRAC meldet Sie mit den entsprechenden Microsoft Active Directory-Berechtigungen an und verwendet dabei die Anmeldeinformationen, die durch das Betriebssystem erfasst wurden, während Sie sich über ein gültiges Active Directory-Konto angemeldet haben.

Bei iDRAC SSO über die CMC-Webschnittstelle anmelden

ANMERKUNG: Diese Funktion ist auf MX-Plattformen nicht verfügbar.

Mithilfe der SSO-Funktion können Sie die iDRAC-Webschnittstelle über die CMC-Webschnittstelle starten. Ein CMC-Benutzer besitzt die CMC-Benutzerberechtigungen, wenn er iDRAC über CMC startet. Wenn das Benutzerkonto in CMC vorhanden ist, jedoch nicht in iDRAC, kann der Benutzer iDRAC dennoch über CMC starten.

Wenn iDRAC-Netzwerk-LAN deaktiviert ist (LAN aktiviert = Nein), ist die SSO (Einzelanmeldung) nicht verfügbar.

Wenn der Server aus dem Gehäuse entfernt oder die iDRAC-IP-Adresse geändert wird, oder wenn ein Problem bei der iDRAC-Netzwerkverbindung vorliegt, wird die Option zum Starten von iDRAC in der CMC-Web-Schnittstelle ausgegraut dargestellt.

Weitere Informationen finden Sie im *Chassis Management Controller – Handbuch* verfügbar unter https://www.dell.com/cmcmanuals.

Über Remote-RACADM auf iDRAC zugreifen

Sie können Remote-RACADM für den Zugriff auf iDRAC über das RACADM-Dienstprogramm verwenden.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Wenn die Management Station das iDRAC-SSL-Zertifikat nicht in ihrem Standard-Zertifikatspeicher gespeichert hat, wird eine Warnmeldung angezeigt, wenn Sie den RACADM-Befehl ausführen. Der Befehl wird jedoch erfolgreich ausgeführt.

ANMERKUNG: Bei dem iDRAC-Zertifikat handelt es sich um das Zertifikat, das iDRAC an den RACADM-Client sendet, um die sichere Sitzung aufzubauen. Dieses Zertifikat wird entweder von einer Zertifikatzertifizierungsstelle oder selbst signiert ausgegeben. Wenn die Management Station die Zertifikatzertifizierungsstelle oder die signierende Stelle nicht erkennt, wird in beiden Fällen eine Warnung angezeigt.

Zertifizierungsstellenzertifikat für die Verwendung von Remote-RACADM auf Linux validieren

Bevor Sie Remote-RACADM-Befehle ausführen, validieren Sie zunächst das Zertifizierungsstellenzertifikat, das für die sichere Kommunikation verwendet wird.

So validieren Sie das Zertifikat für die Verwendung von Remote-RACADM:

1. Konvertieren Sie das Zertifikat vom DER-Format in das PEM-Format (verwenden Sie dazu das Befehlszeilen-Tool „openssl“):

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

2. Suchen Sie den Speicherort des standardmäßigen CA-Zertifikatpakets auf der Managementstation. Für RHEL5 64-Bit ist dies z. B. **/etc/pki/tls/cert.pem**.
3. Hängen Sie das PEM-formatierte CA-Zertifikat an das CA-Zertifikat der Management Station an.

   Verwenden Sie beispielsweise `cat command: cat testcacert.pem >> cert.pem`
4. Generieren Sie das Server-Zertifikat, und laden Sie es auf iDRAC hoch.

Über lokalen RACADM auf iDRAC zugreifen

Weitere Informationen zum Zugriff auf iDRAC unter Verwendung des lokalen RACADM finden Sie unter *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Über Firmware-RACADM auf iDRAC zugreifen

Sie können die SSH-Schnittstelle für den Zugriff auf iDRAC und zum Ausführen der Firmware-RACADM-Befehle verwenden. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Einfache Zwei-Faktor-Authentifizierung (einfache 2FA)

Der iDRAC bietet eine einfache Zwei-Faktor-Authentifizierungsoption zur Verbesserung der Sicherheit für lokale Nutzer bei der Anmeldung. Wenn Sie sich über eine Quell-IP-Adresse anmelden, die sich von der letzten Anmeldung unterscheidet, werden Sie aufgefordert, die Authentifizierungsdetails für den zweiten Faktor einzugeben.

Die einfache Zwei-Faktor-Authentifizierung umfasst zwei Authentifizierungsschritte:

- iDRAC-Nutzername und -Kennwort
- Ein einfacher sechsstelliger Code, der per E-Mail an den Nutzer gesendet wird. Der Nutzer muss diesen sechsstelligen Code eingeben, wenn er auf bei der Anmeldung dazu aufgefordert wird.

ANMERKUNG:

- Um den sechsstelligen Code zu erhalten, ist es zwingend erforderlich, die Option „Nutzerdefinierte Absenderadresse“ zu konfigurieren und eine gültige SMTP-Konfiguration zu haben.
- Der 2FA-Code läuft nach zehn Minuten ab oder wird ungültig, wenn er bereits vor Ablauf verwendet wurde.
- Wenn ein Nutzer versucht, sich von einem anderen Speicherort mit einer anderen IP-Adresse anzumelden, während eine ausstehende 2FA-Aufforderung für die ursprüngliche IP-Adresse noch ausstehend ist, wird derselbe Token für den Anmeldeversuch von der neuen IP-Adresse gesendet.
- Für diese Funktion ist eine iDRAC Enterprise oder Datacenter Lizenz erforderlich.

Wenn 2FA aktiviert ist, werden folgende Aktionen nicht zugelassen:

- Anmelden beim iDRAC über eine beliebige Nutzeroberfläche an, die CLI mit Nutzerzugangsdaten verwendet.
- Anmelden bei iDRAC über die OMM-App über Quick Sync-2
- Hinzufügen eines Mitglieds-iDRAC in Group Manager.

ANMERKUNG: RACADM, Redfish, WSMAN, IPMI-LAN, seriell und CLI von einer Quell-IP-Adresse funktionieren nur nach erfolgreicher Anmeldung von unterstützten Schnittstellen wie der iDRAC-GUI und SSH.

RSA SecurID 2FA

iDRAC can be configured to authenticate with a single RSA AM server at a time. The global settings on RSA AM server apply to all iDRAC local users, AD, and LDAP users.

NOTE: RSA SecurID 2FA feature is available only on Datacenter license.

Following are the pre-requisites before you configure iDRAC to enable RSA SecurID:

- Configure Microsoft Active Directory server.
- If you try to enable RSA SecurID on all AD users, add the AD server to the RSA AM server as an Identity Source.
- Ensure you have a generic LDAP server.
- For all LDAP users, the Identity Source to the LDAP server must be added in RSA AM server.

To enable RSA SecurID on iDRAC, the following attributes from the RSA AM server are required:

1. **RSA Authentication API URL** — The URL syntax is: `https://<rsa-am-server-hostname>:<port>/mfa/v1_1`, and by default the port is 5555.
2. **RSA Client-ID** — By default, the RSA client ID is the same as the RSA AM server hostname. Find the RSA client ID at RSA AM server's authentication agent configuration page.
3. **RSA Access Key** — The Access Key can be retreived on RSA AM by navigating to **Setup** > **System Settings** > **RSA SecurID** > **Authentication API**section, which is usually displayed as `198cv5x195fdi86u43jw0q069byt0x37umlfwxc2gnp4s0xk11ve2lffum4s8302`. To configure the settings through iDRAC GUI:
   - Go to **iDRAC Settings** > **Users**.
   - From **Local Users** section, select an existing local user and click **Edit**.

- Scroll down to the bottom of the Configuration page.
- In **RSA SecurID** section, Click the link **RSA SecurID Configuration** to view or edit these settings.

You can also configure the settings as follows:

- Go to **iDRAC Settings** > **Users**.
- From **Directory Services** section, select **Microsoft Active Service** or **Generic LDAP Directory Service**, and click **Edit**.
- In **RSA SecurID** section, Click the link **RSA SecurID Configuration** to view or edit these settings.

4. **RSA AM server certificate (chain)**

You can login to iDRAC using RSA SecurID token via iDRAC GUI and SSH.

RSA SecurID Token App

You need to install RSA SecurID Token app on you system or on smart phone. When you try to log in to iDRAC, you are asked to input the passcode shown in the app.

If a wrong passcode is entered, the RSA AM server challenges the user to provide the "Next Token." This may happen even though the user may have entered the correct passcode. This entry proves that the user owns the right Token that generates the right passcode.

You get the **Next Token** from RSA SecurID Token app by clicking on **Options**. Check **Next Token**, and the next passcode is available. Time is critical in this step. Otherwise, iDRAC may fail the verification of the next token. If the iDRAC user login session times out, it requires another attempt to log in

If a wrong passcode is entered, the RSA AM server will challenge the user to provide the "Next Token." This challenge happens even though the user may have later entered the correct passcode. This entry proves that the user owns the right Token that generates the right passcodes.

To get the next token from RSA SecurID Token app, click on **Options** and check **Next Token**. A new token is generated. Time is critical in this step. Otherwise, iDRAC may fail the verification of the next token. If the iDRAC user login session times out, it requires another attempt to log in.

Systemzustand anzeigen

Bevor Sie eine Aufgabe ausführen oder ein Ereignis auslösen, können Sie RACADM verwenden, um zu überprüfen, ob das System sich in einem passenden Zustand befindet. Zum Anzeigen des Remotedienst-Status über RACADM verwenden Sie den Befehl `getremoteservicesstatus`.

Tabelle 6. Mögliche Werte für den Systemstatus

Hostsystem	Lifecycle-Controller (LC)	Echtzeit-Status	Allgemeiner Status
• Ausgeschaltet • In POST • POST abgeschlossen • Erfassen der Systembestandaufnahme • Automatisierte Aufgabenausführung • Lifecycle Controller Unified Server Configurator • Der Server wurde bei der F1/F2-Fehlereingabeaufforderung aufgrund eines POST-Fehlers angehalten • Der Server wurde bei der F1/F2-Fehlereingabeaufforderung angehalten, weil keine startfähigen Geräte verfügbar sind	• Bereit • Nicht initialisiert • Daten werden erneut geladen • Deaktiviert • Im Wiederherstellungsmodus • In Verwendung	• Bereit • Nicht Bereit	• Bereit • Nicht Bereit

Tabelle 6. Mögliche Werte für den Systemstatus (fortgesetzt)

Hostsystem	Lifecycle-Controller (LC)	Echtzeit-Status	Allgemeiner Status
• Server ist in das F2-Setup-Menü gewechselt • Server ist in das F11-Boot-Manager-Menü gewechselt			

1. Lesen/Schreiben: Schreibgeschützt
2. Benutzerberechtigung: Benutzeranmeldung
3. Erforderliche Lizenz: iDRAC Express oder iDRAC Enterprise
4. Abhängigkeit: Keine

Anmeldung beim iDRAC mit Authentifizierung mit öffentlichem Schlüssel

Sie können sich beim iDRAC über SSH ohne Kennwort anmelden. Sie können auch einen einzelnen RACADM-Befehl als Befehlszeilenargument an die SSH-Anwendung senden. Die Befehlszeilenoptionen verhalten sich wie Remote-RACADM, da die Sitzung endet, wenn der Befehl abgeschlossen ist.

Zum Beispiel:

Anmeldung:

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

oder

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

wobei `IP_address` die IP-Adresse des iDRAC ist.

Senden von RACADM-Befehlen:

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

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

Mehrere iDRAC-Sitzungen

Aus der folgenden Tabelle können Sie die Anzahl der iDRAC-Sitzungen entnehmen, die durch die Verwendung der diversen Schnittstellen möglich sind.

Tabelle 7. Mehrere iDRAC-Sitzungen

Schnittstelle	Anzahl der Sitzungen
iDRAC-Weboberfläche	8
Remote-RACADM	4
Firmware RACADM	SSH – 4 Seriell – 1

iDRAC erlaubt mehrere Sitzungen für denselben Nutzer. Nachdem ein Nutzer die maximale Anzahl zulässiger Sitzungen erstellt hat, können sich andere Nutzer nicht bei iDRAC anmelden. Dies kann einen *Denial-of-Service* für einen legitimen Administratornutzer zur Folge haben.

Im Falle, dass alle Sitzungen aufgebraucht sind, führen Sie die folgenden Maßnahmen durch:

- Wenn Webserver-basierte Sitzungen aufgebraucht sind, können Sie sich weiterhin über SSH oder lokales RACADM anmelden.
- Ein Administrator kann dann vorhandene Sitzungen mithilfe von RACADM-Befehlen (`racadm getssninfo`; `racadm closessn -i <index>`) beenden.

Standardkennwort sichern

Alle unterstützten Systeme werden mit einem eindeutigen Standardkennwort für iDRAC ausgeliefert, es sei denn, Sie möchten *calvin* bei der Bestellung des Systems als Kennwort festlegen. Das eindeutige Kennwort sorgt für mehr Sicherheit für iDRAC und Ihren Server. Um die Sicherheit weiter zu verbessern, wird empfohlen, das Standardkennwort zu ändern.

Das eindeutige Kennwort für Ihr System ist auf dem Systeminformations-Tag verfügbar. Die Position des Tag finden Sie in der Dokumentation zum Server unter https://www.dell.com/support.

ANMERKUNG: Für PowerEdge C6420, M640 und FC640 lautet das Standardkennwort *calvin*.

ANMERKUNG: Durch das Zurücksetzen des iDRAC auf die werkseitigen Standardeinstellungen wird das Standardkennwort auf das Kennwort zurückgesetzt, mit dem der Server ausgeliefert wurde.

Wenn Sie das Kennwort vergessen haben und keinen Zugriff auf das Systeminformations-Tag haben, gibt es einige Methoden, um das Kennwort lokal oder remote zurückzusetzen.

Lokales Zurücksetzen des standardmäßigen iDRAC-Kennworts

Wenn Sie über direkten Zugriff auf das System verfügen, können Sie das Kennwort mithilfe der folgenden Methoden zurücksetzen:

- Dienstprogramm für die iDRAC-Einstellungen (System-Setup)
- Lokaler RACADM
- OpenManage Mobile
- USB-Serververwaltungsschnittstelle
- USB-NIC

Zurücksetzen des Standardkennworts mithilfe des Dienstprogramms für die iDRAC-Einstellungen

Sie können auf das iDRAC-Einstellungsdienstprogramm über das System-Setup Ihres Servers zugreifen. Mit dem iDRAC-Reset können Sie alle iDRAC-Anmeldedaten auf die Standardwerte zurücksetzen.

WARNUNG: Wenn Sie den iDRAC auf den Standardwert all zurücksetzen, wird der iDRAC auf die Werkseinstellungen zurückgesetzt.

So setzen Sie iDRAC über das Dienstprogramm für die iDRAC-Einstellungen zurück:

1. Starten Sie den Server neu und drücken Sie <F2>.
2. Klicken Sie auf der Seite **System-Setup** auf **iDRAC-Einstellungen**.
3. Klicken Sie auf **iDRAC-Konfigurationen auf Standardeinstellungen zurücksetzen**.
4. Klicken Sie auf **Ja**, um zu bestätigen, und klicken Sie dann auf **Zurück**.
5. Klicken Sie auf **Fertigstellen**.

Der Server wird neu gestartet, sobald alle iDRAC-Einstellungen auf die Standardeinstellungen zurückgesetzt wurden.

Zurücksetzen des Standardkennwort mittels lokalem RACADM

1. Melden Sie sich bei der Host-BS an, das auf dem System installiert ist.
2. Rufen Sie die lokale RACADM-Schnittstelle auf.
3. Folgen Sie den Anweisungen unter Ändern des in den Standardeinstellungen festgelegten Anmeldungskennworts unter Verwendung von RACADM auf Seite 45.

Standardmäßiges Kennwort unter Verwendung von OpenManage Mobile wiederherstellen

Sie können sich mit OpenManage Mobile (OMM) anmelden und das Standardkennwort ändern. Um sich mit OMM bei iDRAC anzumelden, scannen Sie den QR-Code auf dem Systeminformations-Tag. Weitere Informationen zur Verwendung von OMM finden Sie in der OMM-Dokumentation unter *OME - Modular für PowerEdge MX7000-Gehäuse – Benutzerhandbuch* verfügbar unter https://www.dell.com/openmanagemanuals.

ANMERKUNG: Beim Scannen des QR-Codes werden Sie nur bei iDRAC angemeldet, wenn die Standardanmeldedaten Standardwerte sind. Wenn Sie die Anmeldedaten von den Standardwerten abweichend geändert haben, geben Sie die aktualisierten Daten ein.

Zurücksetzen des Standardkennworts mithilfe der USB-Serververwaltungsschnittstelle

ANMERKUNG: Für diese Schritte muss die USB-Verwaltungsschnittstelle aktiviert und konfiguriert sein.

Verwenden der SCP-Datei

Erstellen Sie eine SCP-Datei (Server Configuration Profile) mit einem neuen Kennwort für das Standardkonto, speichern Sie sie auf einem Speicherstick und verwenden Sie die USB-Serververwaltungsschnittstelle auf dem Server, um die SCP-Datei hochzuladen. Weitere Informationen zum Erstellen der Datei finden Sie unter Verwendung der USB-Schnittstelle für das Server-Management auf Seite 313.

Zugreifen auf iDRAC auf einem Notebook

Verbinden Sie das Notebook mit der UBS-Serververwaltungsschnittstelle und greifen Sie auf iDRAC zu, um das Kennwort zu ändern. Weitere Informationen finden Sie unter Zugriff auf die iDRAC-Schnittstelle über eine direkte USB-Verbindung auf Seite 313.

Ändern des Standardkennworts unter Verwendung von USB-NIC

Wenn Sie Zugang zu einer Tastatur, Maus und einem Anzeigegerät haben, stellen Sie eine Verbindung zum Server unter der Verwendung von USB-NIC her, um auf die iDRAC-Schnittstelle zuzugreifen und das Standardkennwort zu ändern.

1. Verbinden Sie die Geräte mit dem System.
2. Verwenden Sie einen unterstützten Browser, um auf die iDRAC-Schnittstelle über die iDRAC-IP-Adresse zuzugreifen.
3. Folgen Sie den Anweisungen unter Ändern des standardmäßigen Anmeldekennworts unter Verwendung der Webschnittstelle auf Seite 45.

Wiederherstellen des iDRAC-Standardkennworts im Remote-Zugriff

Wenn Sie keinen direkten Zugang zum System haben, können Sie das Standardkennwort remote zurücksetzen.

Remote – bereitgestelltes System

Wenn auf dem System ein Betriebssystem installiert ist, verwenden Sie einen Remote-Desktop-Client für die Anmeldung am Server. Verwenden Sie nach der Anmeldung am Server eine beliebige lokale Schnittstelle wie RACADM oder eine Webschnittstelle, um das Kennwort zu ändern.

Remote – Nicht bereitgestelltes System

Wenn kein Betriebssystem auf dem Server installiert ist und wenn Sie über ein PXE-Setup verfügen, verwenden Sie PXE und dann RACADM zum Zurücksetzen des Kennworts.

Ändern des standardmäßigen Anmeldekennworts

Die Warnmeldung, mithilfe der Sie das standardmäßige Anmeldungskennwort ändern können, wird angezeigt, wenn:

- Melden Sie sich bei iDRAC mit der Berechtigung „Benutzer konfigurieren“ an.
- Die Warnungsfunktion des standardmäßigen Kennworts ist aktiviert.
- Der standardmäßige iDRAC-Nutzername und das Standard-iDRAC-Kennwort werden auf der Systemkennzeichnung bereitgestellt.

Es wird auch eine Warnmeldung angezeigt, wenn Sie sich über SSH, Remote-RACADM oder die Weboberfläche bei iDRAC anmelden. Für die Weboberfläche und SSH wird für jede Sitzung eine einzige Warnmeldung angezeigt. Für Remote-RACADM wird die Warnmeldung für jeden Befehl angezeigt.

ANMERKUNG: Informationen zu empfohlenen Zeichen für Nutzernamen und Kennwörter finden Sie unter Empfohlene Zeichen in Benutzernamen und Kennwörtern auf Seite 152.

Ändern des standardmäßigen Anmeldekennworts unter Verwendung der Webschnittstelle

Wenn Sie sich bei der iDRAC-Webschnittstelle anmelden und die Seite **Default Password Warning (Standardmäßige Kennwortwarnung)** angezeigt wird, können Sie das Kennwort ändern. Führen Sie dazu folgende Schritte durch:

1. Wählen Sie die Option **Standardmäßiges Kennwort ändern**.
2. Geben Sie im Feld **Neues Kennwort** das neue Kennwort ein.

   ANMERKUNG: Informationen zu empfohlenen Zeichen für Benutzernamen und Kennwörter finden Sie unter Empfohlene Zeichen in Benutzernamen und Kennwörtern auf Seite 152.

3. Geben Sie in dem Feld **Kennwort bestätigen** das Kennwort erneut ein.
4. Klicken Sie auf **Continue** (Weiter).

   Das neue Kennwort wird konfiguriert und Sie werden bei DRAC angemeldet.

   ANMERKUNG: Das Feld **Fortfahren** ist nur aktiviert, wenn die Felder **Neues Kennwort** und **Kennwort bestätigen** übereinstimmen.

   Weitere Informationen zu den anderen Feldern finden Sie in der *iDRAC-Online-Hilfe*.

Ändern des in den Standardeinstellungen festgelegten Anmeldungskennworts unter Verwendung von RACADM

So ändern Sie ein Kennwort mithilfe der Ausführung des folgenden RACADM-Befehls:

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

wobei `<index>` ein Wert zwischen 1 und 16 ist (und für das Benutzerkonto steht) und `<password>` das neue benutzerdefinierte Kennwort ist.

ANMERKUNG: Der Index für das Standardkonto ist 2.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

ANMERKUNG: Informationen zu empfohlenen Zeichen für Benutzernamen und Kennwörter finden Sie unter Empfohlene Zeichen in Benutzernamen und Kennwörtern auf Seite 152.

Ändern des standardmäßigen Anmeldekennworts unter Verwendung des Dienstprogramms für iDRAC-Einstellungen

So ändern Sie das standardmäßige Anmeldekennwort unter Verwendung des Dienstprogramms für iDRAC-Einstellungen:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Benutzerkonfiguration**.
   Daraufhin wird die Seite **iDRAC-Einstellungen – Benutzerkonfiguration** angezeigt.

2. Geben Sie im Feld **Kennwort ändern** das neue Kennwort ein.

   ANMERKUNG: Informationen zu empfohlenen Zeichen für Benutzernamen und Kennwörter finden Sie unter Empfohlene Zeichen in Benutzernamen und Kennwörtern auf Seite 152.

3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
   Die Details werden gespeichert.

Aktivieren oder Deaktivieren der standardmäßigen Kennwortwarnungsmeldung

Sie können die Anzeige der standardmäßigen Kennwortwarnmeldung aktivieren oder deaktivieren. Dazu müssen Sie über die Berechtigung „Configure Users“ (Benutzer konfigurieren) verfügen.

Richtlinie zur Kennwortsicherheit

Über die iDRAC-Schnittstelle können Sie die Richtlinie zur Kennwortsicherheit überprüfen und Fehler überprüfen, wenn die Richtlinie nicht erfüllt ist. Die Kennwortrichtlinie kann nicht auf zuvor gespeicherte Kennwörter, Serverkonfigurationsprofile (SCP), die von anderen Servern kopiert wurden, und eingebettete Kennwörter im Profil angewendet werden.

Um auf die Kennworteinstellungen zuzugreifen, gehen Sie zu **iDRAC-Einstellungen** > **Benutzer** > **Kennworteinstellungen**.

Die folgenden Felder sind in diesem Abschnitt verfügbar:

- **Mindestwert** – Gibt den Richtlinien-Mindestwert für die Kennwortstärke an. Werte für dieses Feld sind:
  - 0 – kein Schutz
  - 1 – schwacher Schutz
  - 2 – mittlerer Schutz
  - 3 – starker Schutz
- **Einfache Richtlinie** – Gibt die erforderlichen Zeichen für ein sicheres Kennwort an. Die folgenden Optionen stehen zur Verfügung:
  - Großbuchstaben
  - Zahlen
  - Symbole
  - Mindestlänge
- **Regulärer Ausdruck** – Der reguläre Ausdruck wird zusammen mit dem Mindestwert für die Kennworteinhaltung verwendet. Die Werte sind 1-4.

IP-Blockierung

Mit der IP-Blockierung können Sie dynamisch feststellen, wenn von einer IP-Adresse aus übermäßige Anmeldefehlversuche auftreten und die Adresse eine bestimmte Zeit lang blockieren bzw. daran hindern, eine Anmeldung am iDRAC9 durchzuführen. Die IP-Blockierung umfasst:

- Die Anzahl von zulässigen Anmeldungsfehlern.
- Der Zeitrahmen in Sekunden, zu dem diese Fehler auftreten müssen.
- Der Zeitraum in Sekunden, in dem die IP-Adresse daran gehindert wird, eine Sitzung zu erstellen, nachdem die insgesamt zulässige Anzahl von Fehlern überschritten wurde.

Wenn sich aufeinanderfolgende Anmeldefehler von einer spezifischen IP-Adresse aus ansammeln, werden sie durch einen internen Zähler erfasst. Wenn sich der Benutzer erfolgreich anmeldet, wird die Aufzeichnung der Fehlversuche gelöscht und der interne Zähler zurückgesetzt.

ANMERKUNG: Wenn Anmeldeversuche von der Client-IP-Adresse abgelehnt werden, können einige SSH-Clients die Meldung anzeigen:

```
ssh exchange identification: Connection closed by remote host
```

.

ANMERKUNG: Die IP-Blockierungsfunktion unterstützt bis zu 5 IP-Bereiche. Sie können diese nur über RACADM sehen/einstellen.

Tabelle 8. Einschränkungseigenschaften für erneute Anmeldeversuche

Eigenschaft	Definition

`iDRAC.IPBlocking.BlockEnable`	Aktiviert die IP-Sperrfunktion. Bei aufeinanderfolgenden Fehlern
	`iDRAC.IPBlocking.FailCount`
	von einer einzigen IP-Adresse innerhalb eines bestimmten Zeitraums
	`iDRAC.IPBlocking.FailWindow`
	Werden alle weiteren Versuche, eine Sitzung von dieser Adresse herzustellen, für eine bestimmte Zeitspanne abgelehnt.
	`iDRAC.IPBlocking.PenaltyTime`

`iDRAC.IPBlocking.FailCount`	Legt die Anzahl der fehlgeschlagenen Anmeldeversuche fest, die von einer IP-Adresse möglich sind, bevor die Anmeldeversuche von dieser Adresse abgelehnt werden.
`iDRAC.IPBlocking.FailWindow`	Der Zeitraum in Sekunden, in dem die fehlgeschlagenen Versuche gezählt werden. Wenn die Fehler über diesen Zeitraum hinaus auftreten, wird der Zähler zurückgesetzt.
`iDRAC.IPBlocking.PenaltyTime`	Definiert den Zeitraum (in Sekunden), innerhalb dessen alle Anmeldeversuche von einer IP-Adresse mit exzessiven Fehlern abgelehnt werden.

Aktivieren und Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung der Web-Schnittstelle

So aktivieren Sie das Betriebssystem zum iDRAC-Passthrough mithilfe der Web-Schnittstelle:

1. Navigieren Sie zu **iDRAC-Einstellungen** > **Verbindungen** > **Netzwerk** > **Betriebssystem zu iDRAC-Passthrough**.
   Die Seite **Betriebssystem zu iDRAC-Passthrough** wird angezeigt.
2. Ändern Sie den Status auf **Aktiviert**.
3. Wählen Sie eine der folgenden Optionen für den Pass-Through-Modus aus:
   - **LOM** – Der BS zu iDRAC PassThrough-Link zwischen dem iDRAC und dem Host-Betriebssystem wird über das LOM oder die NDC hergestellt.
   - **USB-NIC** – Der BS zu iDRAC PassThrough-Link zwischen dem iDRAC und dem Host-Betriebssystem wird über den internen USB hergestellt.

   ANMERKUNG: Wenn Sie den Pass-Through-Modus auf LOM einstellen, stellen Sie Folgendes sicher:
   - OS und iDRAC befinden sich im gleichen Subnetz
   - Die NIC-Auswahl in den Netzwerkeinstellungen ist auf ein LOM eingestellt.
4. Wenn der Server im freigegebenen LOM-Modus verbunden ist, ist das Feld **Betriebssystem-IP-Adresse** deaktiviert.

   ANMERKUNG: Wenn VLAN auf dem iDRAC aktiviert ist, funktioniert der LOM-Passthrough nur im freigegebenen LOM-Modus und wenn VLAN-Tagging auf dem Host konfiguriert ist.

   ANMERKUNG:
   - Wenn der Pass-Through-Modus auf LOM eingestellt ist, ist es nicht möglich, den iDRAC vom Host-BS nach dem Kaltstart zu starten.
   - Wir haben die LOM-Pass-Through-Funktion mithilfe des dedizierten Modus absichtlich entfernt.

5. Wenn Sie **USB-NIC** als PassThrough-Konfiguration auswählen, geben Sie die IP-Adresse der USB-NIC ein.

   Der Standardwert ist 169.254.1.1. Es wird empfohlen, die Standard-IP-Adresse zu verwenden. Wenn jedoch ein Konflikt dieser IP-Adresse mit anderen Schnittstellen des Host-Systems oder des lokalen Netzwerks vorliegt, müssen Sie sie ändern.

   Geben Sie nicht die IP-Adressen 169.254.0.3 und 169.254.0.4 ein. Diese IP-Adressen sind für den USB-NIC-Anschluss an der Vorderseite, wenn ein A/A-Kabel verwendet wird, reserviert.

   ANMERKUNG: Wenn IPv6 bevorzugt wird, ist die Standardadresse fde1:53ba:e9a0:de11::1. Falls erforderlich, kann diese Adresse in der Einstellung idrac.OS-BMC.UsbNicULA geändert werden. Wenn IPv6 auf dem USB-NIC nicht erwünscht ist, kann es deaktiviert werden, indem die Adresse in "::" geändert wird.

6. Klicken Sie auf **Anwenden**.
7. Klicken Sie auf **Netzwerkkonfiguration testen**, um zu überprüfen ob die IP zugreifbar ist und die Verbindung zwischen dem iDRAC und dem Host-Betriebssystem hergestellt ist.

Warnungen über RACADM aktivieren oder deaktivieren

Geben Sie folgenden Befehl ein:

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

n=0 – Deaktiviert

n=1 – Aktiviert

3

Managed System einrichten

Wenn Sie das lokale RACADM ausführen oder die Erfassung von „Bildschirm Letzter Absturz“ aktivieren möchten, installieren Sie die folgenden Komponenten von der *Dell Systems Management Tools and Documentation*-DVD:

- Lokaler RACADM
- Server Administrator

Weitere Informationen zu Server Administrator finden Sie unter *OpenManage Server Administrator – Benutzerhandbuch* verfügbar unter https://www.dell.com/openmanagemanuals.

Themen:

- iDRAC-IP-Adresse einrichten
- Einstellungen für lokales Administratorkonto ändern
- Standort für das Managed System einrichten
- Systemleistung und Stromverbrauch optimieren
- Management Station einrichten
- Konfigurieren von unterstützten Webbrowsern
- Updating device firmware
- Anzeigen und Verwalten von gestuften Aktualisierungen
- Rollback der Geräte-Firmware durchführen
- Easy Restore (Einfache Wiederherstellung)
- iDRAC über andere Systemverwaltungs-Tools überwachen
- Unterstützung des Serverkonfigurationsprofils – Import und Export
- Sichere Startfunktion-Konfiguration über BIOS-Einstellungen oder F2
- BIOS recovery

iDRAC-IP-Adresse einrichten

Sie müssen die anfänglichen Netzwerkeinstellungen auf der Basis Ihrer Netzwerkinfrastruktur konfigurieren, um die bilaterale Kommunikation mit iDRAC zu aktivieren. Sie können die iDRAC-IP-Adresse über eine der folgenden Schnittstellen einrichten:

- Dienstprogramm für die iDRAC-Einstellungen
- Lifecycle Controller (Siehe *Benutzerhandbuch für den Lifecycle Controller*)
- LCD-Bedienfeld auf der Gehäuse- oder Server-Frontblende (siehe *Installations- und Service-Handbuch* für das System)

  ANMERKUNG: Auf Blade-Servern können Sie die Netzwerkeinstellungen über das Gehäuse-LCD-Bedienfeld nur bei der Erstkonfiguration von CMC konfigurieren. Sie können keine Neukonfiguration von iDRAC über das Gehäuse-LCD-Bedienfeld durchführen, nachdem das Gehäuse bereitgestellt wurde.
- CMC-Weboberfläche (gilt nicht für MX-Plattformen) (siehe *Chassis Management Controller – Handbuch*)

Bei Rack- und Tower-Servern können Sie die IP-Adresse einrichten oder die iDRAC-Standard-IP-Adresse 192.168.0.120 für die Erstkonfiguration der Netzwerkeinstellungen verwenden. Im Rahmen dieser Konfiguration können Sie auch DHCP oder die statische IP-Adresse für iDRAC einrichten.

Bei Blade-Servern wird standardmäßig die iDRAC-Netzwerkschnittstelle angezeigt.

Nach der Konfiguration der iDRAC-IP-Adresse:

- Stellen Sie sicher, dass Sie Standard-Nutzername und -Kennwort ändern.
- Greifen Sie über die folgenden Schnittstellen auf iDRAC zu:
  - iDRAC Weboberfläche unter Verwendung eines unterstützten Browsers (Internet Explorer, Firefox, Chrome oder Safari)
  - Secure Shell (SSH) – Erfordert einen Client, wie z. B. PuTTY unter Windows. SSH ist standardmäßig auf den meisten Linux-Systemen verfügbar, sodass kein Client benötigt wird.
  - IPMITool (verwendet den IPMI-Befehl) oder Shell-Befehlseingabe (erfordert ein von Dell angepasstes Installationsprogramm unter Windows oder Linux, das von der *Systems Management Documentation and Tools*-DVD oder unter https://www.dell.com/support abgerufen werden kann)

iDRAC-IP-Adresse über das Dienstprogramm für die iDRAC-Einstellungen einrichten

So richten Sie die iDRAC-IP-Adresse ein:

1. Schalten Sie das verwaltete System ein.
2. Drücken Sie während des Einschaltselbsttests (POST) die Taste <F2>.
3. Klicken Sie auf der Seite **System-Setup-Hauptmenü** auf **iDRAC-Einstellungen**.
   Die Seite **iDRAC-Einstellungen** wird angezeigt.
4. Klicken Sie auf **Netzwerk**.
   Die Seite **Netzwerk** wird angezeigt.
5. Legen Sie die folgenden Einstellungen fest:
   - Network Settings (Netzwerkeinstellungen)
   - Allgemeine Einstellungen
   - IPv4-Einstellungen
   - IPv6-Einstellungen
   - IPMI-Einstellungen
   - VLAN-Einstellungen
6. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
   Die Netzwerkinformationen werden gespeichert, und das System wird neu gestartet.

Konfigurieren der Netzwerkeinstellungen

So konfigurieren Sie die Netzwerkeinstellungen:

ANMERKUNG: Weitere Informationen zu den Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

1. Wählen Sie unter **NIC aktivieren** die Option **Aktiviert** aus.
2. Wählen Sie aus dem Drop-Down-Menü **NIC-Auswahl** auf der Basis der Netzwerkanforderung eine der folgenden Schnittstellen aus:

   ANMERKUNG: Diese Option ist auf MX-Plattformen nicht verfügbar.

   - **Dediziert** – Aktiviert das Remote-Zugriffsgerät, um die auf dem Remote-Access-Controller (RAC) verfügbare dedizierte Netzwerkschnittstelle zu verwenden. Diese Schnittstelle wird nicht an das Host-Betriebssystem freigegeben und leitet den Managementverkehr auf ein separates physisches Netzwerk um, wodurch eine Trennung vom Anwendungsdatenverkehr erfolgt.

     Diese Option impliziert, dass die dedizierte iDRAC-Netzwerkschnittstelle den Datenverkehr getrennt von den LOM- oder NIC-Schnittstellen des Servers weiterleitet. Mit der Dedicated-Option kann iDRAC eine IP-Adresse aus demselben Subnetz oder einem anderen Subnetz zugewiesen werden, im Vergleich zu den IP-Adressen, die dem Host-LOM oder den NICs zur Verwaltung des Netzwerkverkehrs zugewiesen wurden.

     ANMERKUNG: Bei Blade-Servern wird die Option "Dediziert" als **Gehäuse (Dediziert)** angezeigt.
   - **LOM1**
   - **LOM2**
   - **LOM3**
   - **LOM4**

   ANMERKUNG: Bei Rack- und Tower-Servern sind zwei LOM-Optionen (LOM1 und LOM2) oder alle vier LOM-Optionen verfügbar. Maßgeblich dafür ist das jeweilige Server-Modell. Bei Blade-Servern mit zwei NDC-Ports sind zwei LOM-Optionen (LOM1 und LOM2) verfügbar und auf Servern mit vier NDC-Ports stehen alle vier LOM-Optionen zur Verfügung.

   ANMERKUNG: Shared LOM wird jedoch auf *Intel 2P X520–k bNDC 10 G* nicht unterstützt, wenn sie in einem Server mit voller Höhe und zwei NDCs verwendet werden, weil sie keine Hardware-Arbitrierung unterstützen.

3. Wählen Sie im Dropdown-Menü **NIC-Auswahl** den Port aus, von dem aus Sie auf das System zugreifen möchten. Folgende Optionen sind verfügbar:

   ANMERKUNG: Diese Funktion ist auf MX-Plattformen nicht verfügbar.

ANMERKUNG: Sie können entweder die dedizierte Netzwerkschnittstellenkarte oder aus einer Liste von LOMs auswählen, die im Quad-Port oder Dual-Port Mezzanine-Karten verfügbar sind.

- **Gehäuse (dezidiert)**: Aktiviert das Remote-Zugriffsgerät, um die auf dem Remote-Access-Controller (RAC) verfügbare dedizierte Netzwerkschnittstelle zu verwenden. Diese Schnittstelle wird nicht an das Host-Betriebssystem freigegeben und leitet den Managementverkehr auf ein separates physisches Netzwerk um, wodurch eine Trennung vom Anwendungsdatenverkehr erfolgt.

  Diese Option impliziert, dass die dedizierte iDRAC-Netzwerkschnittstelle den Datenverkehr getrennt von den LOM- oder NIC-Schnittstellen des Servers weiterleitet. Mit der Dedicated-Option kann iDRAC eine IP-Adresse aus demselben Subnetz oder einem anderen Subnetz zugewiesen werden, im Vergleich zu den IP-Adressen, die dem Host-LOM oder den NICs zur Verwaltung des Netzwerkverkehrs zugewiesen wurden.

- **Für Quad-Core-Karten – LOM1-LOM16**
- **Für Dual-Port-Karten – LOM1, LOM2, LOM5, LOM6, LOM9, LOM10, LOM13, LOM14**

4. Wählen Sie im Drop-Down-Menü **Failover-Netzwerk** einen der verbleibenden LOMs aus: Wenn ein Netzwerk ausfällt, wird der Datenverkehr über das Failover-Netzwerk umgeleitet.

   Wenn beispielsweise der iDRAC-Netzwerkverkehr über LOM2 umgeleitet werden soll, wenn LOM1 ausgefallen ist, wählen Sie **LOM1** unter **NIC-Auswahl** und **LOM2** unter **Failover-Netzwerk** aus.

   ANMERKUNG: Diese Option wird deaktiviert, wenn die **NIC-Auswahl** auf **Dediziert** festgelegt ist.

   ANMERKUNG: Bei Verwendung der Failover-Netzwerkeinstellungen wird empfohlen, dass alle LOM-Ports an dasselbe Netzwerk angeschlossen werden.

   Weitere Informationen finden Sie im Abschnitt Netzwerkeinstellungen über die Weboberfläche ändern auf Seite 96

5. Wählen Sie unter **Automatische Verhandlung** die Option **Ein**, wenn iDRAC den Duplexmodus und die Netzwerkgeschwindigkeit automatisch festlegen muss.

   Diese Option steht nur im dedizierten Modus zur Verfügung. Wenn sie aktiviert ist, legt iDRAC die Netzwerkgeschwindigkeit auf der Basis der Netzwerkgeschwindigkeit auf 10, 100 oder 1.000 MB/s fest.

6. Wählen Sie unter **Netzwerkgeschwindigkeit** entweder 10 oder 100 MB/s aus.

   ANMERKUNG: Sie können die Netzwerkgeschwindigkeit nicht manuell auf 1000 MB/s setzen. Diese Option ist nur dann verfügbar, wenn **Automatische Verhandlung** aktiviert ist.

7. Wählen Sie unter **Duplexmodus** die Option **Halbduplex** oder **Vollduplex** aus.

   ANMERKUNG: Diese Option ist nicht verfügbar, wenn die **Auto-Verhandlung aktiviert** ist.

   ANMERKUNG: Wenn Netzwerk-Teaming für das Host-Betriebssystem mit demselben Netzwerkadapter wie NIC Selection konfiguriert ist, sollte auch das Failover-Netzwerk konfiguriert werden. NIC-Auswahl und Failover-Netzwerk sollten die Ports verwenden, die als Teil des Netzwerkteams konfiguriert sind. Wenn mehr als zwei Ports als Teil des Netzwerkteams verwendet werden, sollte die Failover-Netzwerkauswahl "Alle" sein.

8. Geben Sie unter **NIC MTU** die Größe für die Maximum Transmission Unit (MTU) auf dem NIC ein.

   ANMERKUNG: Die Standard- und Höchstgrenze für MTU auf NIC beträgt 1.500, der Mindestwert 576. Ein MTU Wert von 1280 oder höher ist erforderlich, wenn IPv6 aktiviert ist.

Allgemeine Einstellungen

Wenn die Netzwerkinfrastruktur über einen DNS-Server verfügt, registrieren Sie iDRAC auf dem DNS. Hierbei handelt es sich um die erforderlichen Anfangseinstellungen für erweiterte Funktionen wie z. B. Verzeichnisdienste – Active Directory oder LDAP, Single Sign-On und Smartcard.

So registrieren Sie iDRAC:

1. **DRAC auf DNS registrieren** aktivieren.
2. Geben Sie den **DNS-DRAC-Namen** ein.
3. Wählen Sie **Domänennamen automatisch konfigurieren**, um den Domänennamen automatisch von DHCP abzurufen. Geben Sie andernfalls den **DNS-Domänennamen** an.

Im Feld **DNS-iDRAC-Name** ist das Standardnamensformat *idrac-Service_Tag*, wobei Service_Tag die Service-Tag-Nummer des Servers ist. Die maximale Länge beträgt 63 Zeichen und die folgenden Zeichen werden unterstützt:

- A-Z
- a-z
- 0-9
- Bindestrich (-)

Konfigurieren der IPv4-Einstellungen

So konfigurieren Sie die IPv4-Einstellungen:

1. Wählen Sie die Option **Enabled (Aktiviert)** unter **Enable IPv4 (IPv4 aktivieren)** aus.

   ANMERKUNG: Auf den Power Edge-Servern der 14. Generation ist DHCP standardmäßig aktiviert.

2. Wählen Sie die Option **Enabled (Aktiviert)** unter **Enable DHCP (DHCP aktivieren)** aus, sodass DHCP die IP-Adresse, das Gateway und die Subnetzmaske automatisch zu iDRAC zuweisen kann. Wählen Sie andernfalls die Option **Disabled (Deaktiviert)** aus, und geben Sie die Werte für die folgenden Elemente ein:
   - Statische IP-Adresse
   - Statisches Gateway
   - Statische Subnetzmaske
3. Aktivieren Sie optional die Option **Use DHCP to obtain DNS server address** (DHCP zum Abrufen der DNS-Serveradresse verwenden), damit der DHCP-Server den **bevorzugten statischen DNS-Server** und den **alternativen statischen DNS-Server** zuweisen kann. Geben Sie andernfalls die IP-Adressen für **Static Preferred DNS Server** (Bevorzugter statischer DNS-Server) und **Static Alternate DNS Server** (Alternativer statischer DNS-Server) ein.

Configuring the IPv6 settings

Based on the infrastructure setup, you can use IPv6 address protocol.

To configure the IPv6 settings:

NOTE: If IPv6 is set to static, ensure that you configure the IPv6 gateway manually, which is not needed in case of dynamic IPV6. Failing to configure manually in case of static IPv6 results in loss of communication.

1. Select **Enabled** option under **Enable IPv6**.
2. For the DHCPv6 server to automatically assign the IP address and prefix length to iDRAC, select the **Enabled** option under **Enable Auto-configuration**.

   NOTE: You can configure both static IP and DHCP IP at the same time.

3. In the **Static IP Address 1** box, enter the static IPv6 address.
4. In the **Static Prefix Length** box, enter a value between 1 and 128.
5. In the **Static Gateway** box, enter the gateway address.

   NOTE: If you configure static IP, the current IP address 1 displays static IP and the IP address 2 displays dynamic IP. If you clear the static IP settings, the current IP address 1 displays dynamic IP.

6. If you are using DHCP, enable **DHCPv6 to obtain DNS Server addresses** to obtain Primary and Secondary DNS server addresses from DHCPv6 server. You can configure the following if required:
   - In the **Static Preferred DNS Server** box, enter the static DNS server IPv6 address.
   - In the **Static Alternate DNS Server** box, enter the static alternate DNS server.
7. When DNS information is not obtainable by either DHCPv6 or static configuration, you can use RFC 8106 "IPv6 Router Advertisement Options for DNS Configuration. It is identified by IPv6 Router. Using RA DNS configuration does not impact existing DNS configurations (either DHCPv6 or static).
   - The iDRAC can obtain DNS name server and DNS search domain information from IPv6 Router Advertisement messages. Please refer to RFC 8106 and your IPv6 router's user guide for details on how to configure the router to advertise this information.
   - If DNS information is available from both the DHCPv6 server and the IPv6 Router Advertisement, the iDRAC uses both. In case of conflict, the DHCPv6 server's DNS information takes precedence in the iDRAC's /etc/resolv.conf settings.

NOTE: For iDRAC to use RA DNS information, IPv6.Enable and IPv6.Autoconfig must be enabled. If Auto-configuration is disabled, the iDRAC does not process IPv6 RA messages, and uses only static DNS settings as configured.

Konfigurieren der IPMI-Einstellungen

So aktivieren Sie die IPMI-Einstellungen:

1. Wählen Sie unter **IPMI-über-LAN aktivieren Aktiviert** aus.
2. Wählen Sie unter **Berechtigungsbeschränkung des Kanals Administrator**, **Operator** oder **Benutzer** aus.
3. Geben Sie in das Feld **Verschlüsselungsschlüssel** den Verschlüsselungsschlüssel mit hexadezimalen Zeichen von 0 bis 40 ohne Leerzeichen ein. Der Standardwert sind Nullen.

VLAN-Einstellungen

Sie können den iDRAC für die VLAN-Infrastruktur konfigurieren. Führen Sie zum Konfigurieren der VLAN-Einstellungen die folgenden Schritte aus:

ANMERKUNG: Auf Blade-Servern, für die **Gehäuse (dezidiert)** eingestellt ist, sind die VLAN-Einstellungen schreibgeschützt und können nur über den CMC geändert werden. Wenn der Server im gemeinsamen Modus eingerichtet ist, können Sie im iDRAC die VLAN-Einstellungen im gemeinsamen Modus konfigurieren.

1. Wählen Sie unter **VLAN-ID aktivieren** die Option **Aktiviert** aus.
2. Geben Sie im Feld **VLAN-ID** eine gültige Zahl zwischen 1 und 4.094 ein.
3. Geben Sie in das Feld **Priorität** eine Zahl zwischen 0 und 7 ein, um die Priorität der VLAN-ID zu definieren.

   ANMERKUNG: Nach der Aktivierung von VLAN ist die iDRAC-IP-Adresse eine Zeit lang nicht zugänglich.

iDRAC-IP-Adresse über die CMC-Webschnittstelle einrichten

So richten Sie die iDRAC-IP-Adresse über die Chassis Management Controller-(CMC-)Webschnittstelle ein:

ANMERKUNG: Sie müssen Administratorberechtigungen für die Gehäusekonfiguration (Chassis Configuration Administrator) besitzen, um iDRAC-Netzwerkeinstellungen über den CMC vornehmen zu können. Die CMC-Option ist nur für Blade-Server anwendbar.

1. Melden Sie sich bei der CMC-Web-Schnittstelle an.
2. Navigieren Sie zu **iDRAC-Einstellungen Einstellungen CMC**.
   Die Seite **iDRAC** bereitstellen wird angezeigt.
3. Wählen Sie unter **iDRAC-Netzwerkeinstellungen** die Option **LAN aktivieren** und ggf. weitere Netzwerkparameter aus. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.
4. Für Informationen zu Blade-Server-spezifischen Netzwerkeinstellungen gehen Sie zu **Server-Übersicht<Server-Name>**.
   Die Seite **Serverstatus** wird angezeigt.
5. Klicken Sie auf **iDRAC starten**, und gehen Sie zu**iDRAC-EinstellungenKonnektivität** > **Netzwerk**.
6. Machen Sie auf der Seite **Netzwerk** Angaben zu den folgenden Aspekten:
   - Netzwerkeinstellungen
   - Allgemeine Einstellungen
   - IPv4-Einstellungen
   - IPv6-Einstellungen
   - IPMI-Einstellungen
   - VLAN-Einstellungen
   - Erweiterte Netzwerkeinstellungen

   ANMERKUNG: Weitere Informationen finden Sie in der *iDRAC Online-Hilfe*.

7. Klicken Sie zum Speichern der Netzwerkinformationen auf **Anwenden**.
   Weitere Informationen finden Sie im *Chassis Management Controller – Handbuch* verfügbar unter https://www.dell.com/cmcmanuals.

Auto-discovery

The Auto-discovery feature allows newly installed servers to automatically discover the remote management console that hosts the provisioning server. The provisioning server provides custom administrative user credentials to iDRAC so that the unprovisioned server can be discovered and managed from the management console. For more information about provisioning server, see the *Schnellstart-Benutzerhandbuch für Lifecycle Controller Remote Services* verfügbar unter https://www.dell.com/idracmanuals.

Provisioning server works with a static IP address. Auto-discovery feature on the iDRAC is used to find the provisioning server using DHCP/Unicast DNS/mDNS.

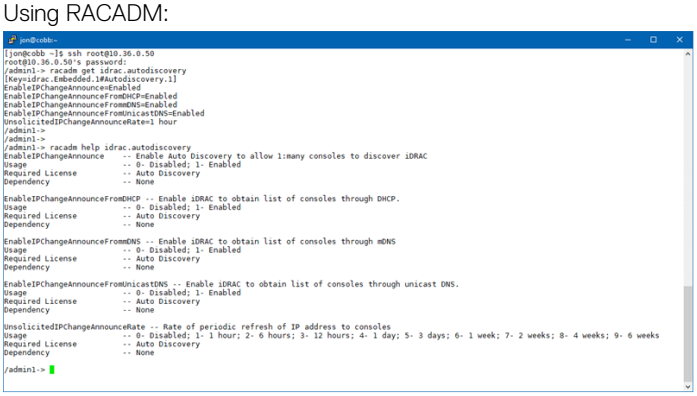
- When iDRAC has the console address, it sends its own service tag, IP address, Redfish port number, Web certificate etc.
- This information is periodically published to consoles.

DHCP, DNS server, or the default DNS host name discovers the provisioning server. If DNS is specified, the provisioning server IP is retrieved from DNS and the DHCP settings are not required. If the provisioning server is specified, discovery is skipped so neither DHCP nor DNS is required.

Auto-discovery can be enabled using the following ways:

1. Using iDRAC GUI: **iDRAC Settings** > **Connectivity** > **iDRAC Auto Discover**

2. Using RACADM:



To enable provisioning server using iDRAC Settings utility:

1. Turn on the managed system.
2. During POST, press F2, and go to **iDRAC Settings** > **Remote Enablement**.
   The **iDRAC Settings Remote Enablement** page is displayed.
3. Enable auto-discovery, enter the provisioning server IP address, and click **Back**.

   NOTE: Specifying the provisioning server IP is optional. If it is not set, it is discovered using DHCP or DNS settings (step 7).

4. Click **Network**.
   The **iDRAC Settings Network** page is displayed.
5. Enable NIC.
6. Enable IPv4.

   NOTE: IPv6 is not supported for auto-discovery.

7. Enable DHCP and get the domain name, DNS server address, and DNS domain name from DHCP.

   NOTE: Step 7 is optional if the provisioning server IP address (step 3) is provided.

Konfigurieren von Servern und Serverkomponenten mithilfe der automatischen Konfiguration

Die Funktion Auto Config (automatische Konfiguration) ermöglicht Ihnen die Konfiguration und Bereitstellung aller Komponenten in einem Server in einem einzigen Arbeitsgang. Diese Komponenten umfassen BIOS, iDRAC und PERC. Dies erfolgt durch automatisches Importieren einer XML- oder JSON-Datei eines Server-Konfigurationsprofils (SCP), die alle konfigurierbaren Parameter enthält. Der DHCP-Server, der die IP-Adresse zuweist, stellt gleichfalls die Details für den Zugriff auf die SCP Datei bereit.

SCP-Dateien werden durch das Konfigurieren eines „Goldkonfigurations"-Servers erstellt. Diese Konfiguration wird dann in einen freigegebenen Speicherort (NFS, CIFS, HTTP oder HTTPS) exportiert, auf den über den DHCP-Server und den iDRAC des Servers, der konfiguriert wird, zugegriffen werden kann. Der SCP-Dateiname kann auf der Service-Tag- oder auf der Modellnummer des Zielservers basieren oder einen allgemeinen Namen erhalten. Der DHCP-Server verwendet eine DHCP-Serveroption, um den SCP-Dateinamen (optional), den SCP-Dateistandort und die Benutzeranmeldeinformationen zum Zugriff auf das Dateiverzeichnis zu spezifizieren.

Wenn der iDRAC eine IP-Adresse vom DHCP-Server erhält, der für Auto Config konfiguriert wird, verwendet iDRAC das SCP, um die Geräte des Servers zu konfigurieren. Auto Config wird erst dann aufgerufen, wenn iDRAC seine IP-Adresse vom DHCP-Server erhält. Falls keine Antwort bzw. keine IP-Adresse vom DHCP-Server eingeht, wird Auto Config nicht aufgerufen.

HTTP- und HTTPS-Dateifreigabeoptionen werden ab iDRAC-Firmware 3.00.00.00 unterstützt. Es müssen Details der HTTP- oder HTTPS-Adresse angegeben werden. Wenn der Proxy auf dem Server aktiviert ist, muss der Benutzer weitere Proxy-Einstellungen vornehmen, damit Daten über HTTP oder HTTPS übertragen werden können. Die Optionskennzeichnung `-s` wird wie folgt aktualisiert:

Tabelle 9. Verschiedene Freigabetypen und Übergabewerte

-s (Freigabetyp)	Pass-in
NFS	`0` oder `nfs`
CIFS	`2` oder `cifs`
HTTP	`5` oder `http`
HTTPS	`6` oder `https`

ANMERKUNG: HTTPS-Zertifikate werden nicht mit automatischer Konfiguration unterstützt. Die automatische Konfiguration ignoriert Zertifikatswarnungen.

In der folgenden Liste sind die erforderlichen und optionalen Parameter zur Übergabe des Zeichenkettenwertes aufgeführt:

`-f (Filename)`: Name der exportierten Server-Profil Datei. Dies ist für iDRAC Firmware-Versionen vor 2.20.20.20 erforderlich.

`-n (Sharename)`: Name der Netzwerkfreigabe. Dies ist für NFS oder CIFS erforderlich.

`-s (ShareType)`: 0 für NFS, 2 für CIFS, 5 für HTTP oder 6 für HTTPS eingeben. Dies ist ein Pflichtfeld für die iDRAC-Firmware-Version 3.00.00.00.

`-i (IPAddress)`: IP-Adresse der Netzwerkfreigabe. Dies ist ein Pflichtfeld.

`-u (Username)`: Benutzername, der Zugriff auf die Netzwerkfreigabe hat. Dies ist ein Pflichtfeld für CIFS.

`-p (Password)`: Benutzerkennwort für den Zugriff auf die Netzwerkfreigabe. Dies ist ein Pflichtfeld für CIFS.

`-d (ShutdownType)`: Entweder 0 für ordentliches oder 1 für erzwungenes Herunterfahren (Standardeinstellung: 0). Dieses Feld ist optional.

`-t (Timetowait)`: Wartezeitdauer auf das Herunterfahren des Hosts (Standardeinstellung: 300). Dieses Feld ist optional.

`-e (EndHostPowerState)`: Entweder 0 für AUS oder 1 für EIN (Standardeinstellung 1). Dieses Feld ist optional.

Die zusätzlichen Options-Kennzeichnungen werden in der iDRAC-Firmware 3.00.00.00 oder höher unterstützt, um die Konfiguration der HTTP-Proxy-Parameter zu ermöglichen und die Wiederholungs-Zeitüberschreitung für den Zugriff auf die Profildatei festzulegen:

`–pd (ProxyDefault)`: Standard-Proxy -Einstellung verwenden. Dieses Feld ist optional.

`–pt (ProxyType)`: Der Benutzer kann `http` oder `socks` eingeben (Standardeinstellung http). Dieses Feld ist optional.

`–ph (ProxyHost)`: IP-Adresse des Proxy-Hosts. Dieses Feld ist optional.

`–pu (ProxyUserName)`: Benutzername, der Zugriff auf den Proxyserver hat. Dies ist für Proxy-Unterstützung erforderlich.

`–pp (ProxyPassword)`: Benutzerkennwort für den Zugriff auf den Proxyserver. Dies ist für Proxy-Unterstützung erforderlich.

`–po (ProxyPort)`: Port für den Proxyserver (Standardeinstellung ist 80). Dieses Feld ist optional.

`–to (Timeout)`: gibt die Wiederholungs-Zeitüberschreitung in Minuten für das Beziehen der Konfigurationsdatei an (Standard ist 60 Minuten).

Für iDRAC-Firmware-Version 3.00.00.00 oder höher werden Profildateien im JSON-Format unterstützt. Die folgenden Dateinamen werden verwendet, wenn der Dateiname-Parameter nicht vorhanden ist:

- <Service-Tag-Nummer>-config.xml, z. B.: CDVH7R1-config.xml
- <Modellnummer>-config.xml, z. B.: R640-config.xml
- config.xml
- <Service-Tag-Nummer>-config.json, z. B.: CDVH7R1-config.json
- <Modellnummer>-config.json, z. B.: R630-config.json
- config.json

ANMERKUNG: Weitere Informationen zu HTTP finden Sie im Whitepaper *14G Support for HTTP and HTTPS across IDRAC9 with Lifecycle Controller Interfaces* (14G-Unterstützung für HTTP und HTTPS bei IDRAC9 mit Lifecycle Controller-Schnittstellen) unter https://www.dell.com/support.

ANMERKUNG:

- Die automatische Konfiguration kann nur aktiviert werden, wenn die Optionen **DHCPv4** und **IPV4 aktivieren** aktiviert sind.
- Auto Config und die automatische Erkennung schließen sich gegenseitig aus. Sie müssen die automatische Erkennung deaktivieren, damit Auto Config ordnungsgemäß funktioniert.
- Die Funktion Auto Config wird deaktiviert, nachdem ein Server einen Autokonfigurationsvorgang durchgeführt hat.

Wenn alle Dell PowerEdge-Server im DHCP-Serverpool den gleichen Modelltyp und die gleiche Nummer aufweisen, ist eine einzige SCP-Datei (`config.xml`) erforderlich. Der Dateiname `config.xml` wird als Standard-SCP-Dateiname verwendet. Neben der `.xml`-Datei können auch `.json`-Dateien mit 14G-Systemen verwendet werden. Der Dateiname kann `config.json` lauten.

Benutzer können einzelne Server konfigurieren. Hierfür benötigen sie unterschiedliche Konfigurationsdateien, die über einzelne Service-Tag-Nummern der Server oder Servermodelle zugeordnet werden. In einer Umgebung mit verschiedenen Servern mit spezifischen Anforderungen können verschiedene SCP-Dateinamen für die Unterscheidung der einzelnen Server oder Servertypen verwendet werden. Wenn beispielsweise zwei Servermodelle konfiguriert werden sollen – ein PowerEdge R540 und ein PowerEdge R540, verwenden Sie zwei SCP-Dateien, `R740-config.xml` und `R540-config.xml`.

ANMERKUNG: Der iDRAC-Serverkonfigurations-Agent generiert den Konfigurationsdateinamen automatisch unter Verwendung der Server-Service-Tag-Nummer, der Modellnummer oder des Standarddateinamens – `config.xml`.

ANMERKUNG: Wenn sich keine dieser Dateien auf der Netzwerkfreigabe befindet, ist der Importauftrag des Serverkonfigurationsprofils als fehlgeschlagen gekennzeichnet und die Datei kann nicht gefunden werden.

Automatische Konfigurationssequenz

1. Erstellen oder ändern Sie die SCP-Datei, mit der die Attribute von Dell-Servern konfiguriert werden.

2. Speichern Sie die SCP-Datei an einem freigegebenen Speicherort, der für DHCP-Server und alle Dell-Server, denen IP-Adressen vom DHCP-Server zugewiesen werden, verfügbar ist.
3. Geben Sie die SCP-Datei im Feld „vendor-option 43“ des DHCP-Servers an.
4. iDRAC teilt während des Abrufs der IP-Adresse die Anbieterklassenkennung mit. (Option 60)
5. Der DHCP-Server vergleicht die Anbieterklasse mit der Anbieteroption in der Datei `dhcpd.conf` und sendet, falls angegeben, den Speicherort und Namen der SCP-Datei an iDRAC.
6. iDRAC verarbeitet die SCP-Datei und konfiguriert alle in der Datei aufgeführten Attribute.

DHCP-Optionen

DHCPv4 ermöglicht das Übergeben vieler global definierter Parameter an DHCP-Clients. Die einzelnen Parameter werden als DHCP-Optionen bezeichnet. Jede Option wird mit einem Options-Tag gekennzeichnet, bei dem es sich um einen 1-Byte-Wert handelt. Die Options-Tags 0 und 255 sind jeweils zum Auffüllen und Abschließen von Optionen reserviert. Alle anderen Werte stehen für die Definition von Optionen zur Verfügung.

Die DHCP-Option 43 wird zum Senden von Informationen vom DHCP-Server an den DHCP-Client verwendet. Diese Option ist als Textzeichenfolge definiert. Diese Textzeichenfolge enthält die Werte des SCP-Dateinamens, des freigegebenen Speicherorts und die Anmeldedaten für den Zugriff auf den Speicherort. Beispiel:

```
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";
```

wobei -i der Speicherort der Remote-Dateifreigabe und -f zusammen mit den Anmeldeinformationen der Dateiname in der Zeichenkette für die Remote-Dateifreigabe ist.

Die DHCP-Option 60 dient der Identifizierung und Zuordnung eines DHCP-Clients zu einem bestimmten Anbieter. Für alle DHCP-Server, die für das Ergreifen entsprechender Maßnahmen auf Grundlage einer Client-Anbieter-ID konfiguriert sind, müssen die Optionen 60 und 43 konfiguriert sein. Bei Dell Power Edge-Servern wird iDRAC mit der folgenden Anbieter-ID identifiziert: *iDRAC*. Aus diesem Grund müssen Sie eine neue Anbieterklasse (Vendor Class) hinzufügen und für diese eine Bereichsoption (Scope Option) für „Code 60“ erstellen und diese Bereichsoption anschließend für den DHCP-Server aktivieren.

Konfigurieren der Option 43 unter Windows

So konfigurieren Sie die Option 43 unter Windows:

1. Gehen Sie auf dem DHCP-Server zu **Start** > **Administration Tools (Administrationstools)** > **DHCP**, um das DHCP-Serveradministrationstool zu öffnen.
2. Gehen Sie auf den Server, und erweitern Sie alle Servereinträge.
3. Klicken Sie mit der rechten Maustaste auf **Bereichsoptionen** und wählen Sie **Optionen konfigurieren** aus.
   Daraufhin wird das Dialogfeld **Bereichsoptionen** angezeigt.
4. Führen Sie einen Bildlauf nach unten durch, und wählen Sie **043 Anbieterspezifische Informationen** aus.
5. Klicken Sie im Feld **Data Entry (Dateneintrag)** auf eine beliebige Stelle im Bereich **ASCII** , und geben Sie die IP-Adresse des Servers mit dem freigegebenen Speicherort an, an dem sich die SCP-Datei befindet.
   Der Wert wird während der Eingabe sowohl unter **ASCII** angezeigt, als auch im Binärcode auf der linken Seite.
6. Klicken Sie auf **OK**, um die Konfiguration zu speichern.

Konfigurieren der Option 60 unter Windows

So konfigurieren Sie die Option 60 unter Windows:

1. Gehen Sie auf dem DHCP-Server auf **Start** > **Administrationstools** > **DHCP**, um die DHCP-Serveradministrationstools zu öffnen.
2. Gehen Sie auf den Server, und erweitern Sie die Servereinträge.

3. Klicken Sie mit der rechten Maustaste auf **IPv4**, und wählen Sie **Anbieter-Klassen definieren** aus.
4. Klicken Sie auf **Hinzufügen**.
   Es wird ein Dialogfeld mit den folgenden Feldern angezeigt:
   - **Anzeigename:**
   - **Beschreibung:**
   - **ID: Binär: ASCII:**
5. Geben Sie im Feld **Anzeigename:** `iDRAC` ein.
6. Geben Sie im Feld **Beschreibung:** `Anbieterklasse` ein.
7. Klicken Sie in den Abschnitt **ASCII:**, und geben Sie `iDRAC` ein.
8. Klicken Sie auf **OK** und anschließend auf **Schließen**.
9. Klicken Sie im DHCP-Fenster mit der rechten Maustaste auf **IPv4**, und wählen Sie **Vordefinierte Optionen festlegen** aus.
10. Wählen Sie aus dem Dropdown-Menü **Optionsklasse** die (in Schritt 4 erstellte) Option **iDRAC** aus, und klicken Sie auf **Hinzufügen**.
11. Geben Sie im Dialogfeld **Optionstyp** die folgenden Informationen ein:
    - **Name** – `iDRAC`
    - **Datentyp** – Zeichenfolge
    - **Code** – 060
    - **Beschreibung** – Dell Anbieterklassen-Kennung
12. Klicken Sie auf **OK**, um zum Fenster **DHCP** zurückzukehren.
13. Erweitern Sie alle Einträge unter dem Servernamen, klicken Sie mit der rechten Maustaste auf **Bereichsoptionen**, und wählen Sie **Optionen konfigurieren** aus.
14. Klicken Sie auf die Registerkarte **Erweitert**.
15. Wählen Sie im Drop-Down-Menü **Vendor class** (Anbieterklasse) **iDRAC** aus. `060 iDRAC` wird in der Spalte **Available Options** (verfügbare Optionen) angezeigt.
16. Wählen Sie die Option **060 iDRAC** aus.
17. Geben Sie die Zeichenfolge ein, die (mit einer über DHCP bereitgestellten Standard-IP-Adresse) an iDRAC gesendet werden muss. Die Zeichenfolge ermöglicht den Import der richtigen SCP-Datei.

    Verwenden Sie für die Option **DATEN-Eintrag, Zeichenfolge-Wert** einen Text-Parameter mit den folgenden Buchstaben-Optionen und Werten:
    - `Filename (-f)` - Zeigt den Namen der exportierten Serverkonfigurationsprofildatei (SCP-Datei) an.
    - `Sharename (-n)` – Gibt den Namen der Netzwerkfreigabe an.
    - `ShareType (-s)` –

      Neben der Unterstützung für NFS- und CIFS-basierte Dateifreigaben bietet iDRAC-Firmware 3.00.00.00 oder höher Unterstützung für den Zugriff auf Profildateien über HTTP und HTTPS. Das `Optionsflag -s` wird folgendermaßen aktualisiert:

      `-s (ShareType)`: Geben Sie nfs oder 0 für NFS, cifs oder 2 für CIFS; http oder 5 für HTTP; oder https oder 6 für HTTPS (erforderlich) ein.

    - `IPAddress (-i)` – Gibt die IP-Adresse der Dateifreigabe an.

      ANMERKUNG: `IPAddress (-i)`, `Sharename (-n)` und `ShareType (-s)` sind erforderlichen Attribute, die übergeben werden müssen. -n ist für HTTP oder HTTPS nicht erforderlich.
    - `Username (-u)` – Gibt den für den Zugriff auf die Netzwerkfreigabe benötigten Benutzernamen an. Diese Informationen sind nur für CIFS erforderlich.
    - `Password (-p)` – Gibt das für den Zugriff auf die Netzwerkfreigabe benötigte Kennwort an. Diese Informationen sind nur für CIFS erforderlich.
    - `ShutdownType (-d)` – Gibt den Modus für das Herunterfahren an. 0 bedeutet „Ordentliches Herunterfahren“ und 1 bedeutet „Erzwungenes Herunterfahren“.

      ANMERKUNG: Die Standardeinstellung ist 0.
    - `Timetowait (-t)` – Gibt die Zeitspanne an, die das Host-System vor dem Herunterfahren wartet. Die Standardeinstellung ist 300.
    - `EndHostPowerState (-e)` – Zeigt den Betriebszustand des Hosts an. 0 bedeutet AUS und 1 bedeutet EIN. Die Standardeinstellung lautet 1.

      ANMERKUNG: `ShutdownType (-d)`, `Timetowait (-t)` und `EndHostPowerState (-e)` sind optionale Attribute.

    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 <*BENUTZERNAME*> -p <*KENNWORT*> -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

Konfigurieren der Optionen 43 und 60 auf Linux

Aktualisieren Sie die Datei `/etc/dhcpd.conf`. Die Schritte zur Konfiguration der Optionen ähneln den Schritten bei Windows:

1. Reservieren Sie einen Block oder Pool von Adressen, die von diesem DHCP-Server zugewiesen werden können.
2. Stellen Sie die Option 43 ein und verwenden Sie die Anbieterklassenkennung für Option 60.

```
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;
        }
}
```

Im Folgenden sind die erforderlichen und optionalen Parameter angegeben, die in der Zeichenkette der Anbieterklassenkennung weitergereicht werden müssen:

- Dateiname (-f) – Zeigt den Namen der exportierten Serverprofildatei an.
  ANMERKUNG: Weitere Informationen zu Regeln für die Dateibenennung finden Sie unter Konfigurieren von Servern und Serverkomponenten mithilfe der automatischen Konfiguration auf Seite 56.
- Freigabename (-n) – Gibt den Namen der Netzwerkfreigabe an.
- ShareType (Freigabetyp) (-s) – Gibt den Freigabetyp an. 0 steht für NFS, 2, CIFS, 5 steht für HTTP und 6 steht für HTTPS.
  ANMERKUNG: Beispiel für die Linux NFS-, CIFS-, HTTP-, HTTPS-Freigabe:
  - **NFS**: `-f system_config.xml -i 192.168.0.130 -n /nfs -s 0 -d 0 -t 500`

    Stellen Sie sicher, dass Sie NFS2 oder NFS3 für die NFS-Netzwerkfreigabe verwenden.
  - **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`
- IPAdresse (-i) – Gibt die IP-Adresse der Dateifreigabe an.
  ANMERKUNG: Freigabename (-n), FreigabeTyp (-s) und IPAdresse (-i) sind erforderliche Attribute, die weitergereicht werden müssen. -n ist für HTTP oder HTTPS nicht erforderlich.
- Username (Benutzername) (-u) – Gibt den für den Zugriff auf die Netzwerkfreigabe benötigten Benutzernamen an. Diese Informationen sind nur für CIFS erforderlich.
- Password (Kennwort) (-p) – Gibt das für den Zugriff auf die Netzwerkfreigabe benötigte Kennwort an. Diese Informationen sind nur für CIFS erforderlich.
- ShutdownType (Typ für das Herunterfahren) (-d) – Gibt den Modus für das Herunterfahren an. 0 bedeutet „Ordentliches Herunterfahren“ und 1 bedeutet „Erzwungenes Herunterfahren“.
  ANMERKUNG: Die Standardeinstellung ist 0.
- Timetowait (Wartezeit) (-t) – Gibt die Zeitspanne an, die das Host-System vor dem Herunterfahren wartet. Die Standardeinstellung ist 300.
- EndHostPowerState (Betriebszustand) (-e) – Zeigt den Betriebszustand des Hosts an. 0 bedeutet AUS und 1 bedeutet EIN. Die Standardeinstellung lautet 1.
  ANMERKUNG: Der Typ für das Herunterfahren (-d), die Wartezeit (-t) und der Energiezustand des End-Hosts (-e) sind optionale Attribute.

Es folgt ein Beispiel für eine statische DHCP-Reservierung von einer dhcpd.conf-Datei:

```
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";
}
```

ANMERKUNG: Stellen Sie nach dem Bearbeiten der `dhcpd.conf`-Datei sicher, dass Sie den dhcpd-Service neu starten, um die Änderungen zu übernehmen.

Voraussetzungen vor dem Aktivieren von Auto Config

Stellen Sie vor der Aktivierung der Funktion Auto Config sicher, dass folgende Voraussetzungen bereits gegeben sind:

- Unterstützte Netzwerkfreigabe (NFS, CIFS, HTTP und HTTPS) steht auf dem gleichen Subnetz wie die iDRAC- und DHCP-Server zur Verfügung. Testen Sie die Netzwerkfreigabe, um sicherzustellen, dass darauf zugegriffen werden kann und dass die Firewall und die Benutzerberechtigungen korrekt eingerichtet wurden.
- Das Serverkonfigurationsprofil wird an die Netzwerkfreigabe exportiert. Stellen Sie außerdem sicher, dass die notwendigen Änderungen in der SCP-Datei abgeschlossen sind, sodass die ordnungsgemäßen Einstellungen zur Anwendung kommen können, sobald der Autokonfigurationsvorgang initiiert wird.
- Der DHCP-Server ist eingerichtet und die DHCP-Konfiguration wird nach Bedarf für iDRAC aktualisiert, um den Server aufzurufen und die Funktion Auto Config zu initiieren.

Aktivieren der Automatischen Konfiguration mithilfe der iDRAC-Webschnittstelle

Stellen Sie sicher, dass DHCPv4 und die IPv4-Aktivierungsoptionen aktiviert und die automatische Erkennung deaktiviert ist.

So aktivieren Sie Auto Config:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC-Einstellungen** > > **Netzwerk Konnektivität** > **Auto Config**.
   Die Seite **Netzwerk** wird angezeigt.
2. Wählen Sie im Abschnitt **Auto Config** eine der folgenden Optionen aus dem Drop-Down-Menü **DHCP-Bereitstellung aktivieren** aus:
   - **Einmal aktivieren** – Konfiguriert die Komponente nur einmal mit der SCP-Datei, auf die der DHCP-Server verweist. Danach wird die Funktion „Auto Config“ deaktiviert.
   - **Einmal nach Reset aktivieren** – Konfiguriert nach dem iDRAC-Reset die Komponente nur einmal mit der SCP-Datei, auf die der DHCP-Server verweist. Danach wird die Funktion „Auto Config“ deaktiviert.
   - **Deaktivieren** – Deaktiviert die Funktion „Auto Config“.
3. Klicken Sie auf **Anwenden,** um die Einstellung zu übernehmen.
   Die Seite „Netzwerk“ wird automatisch aktualisiert.

Aktivieren der Automatischen Konfiguration mithilfe von RACADM

Verwenden Sie das Objekt `iDRAC.NIC.AutoConfig`, um die Funktion des automatischen Konfigurierens unter Verwendung von RACADM zu aktivieren.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Weitere Informationen über die automatische Konfigurationsfunktion finden Sie im Whitepaper *Zero-Touch für die Bereitstellung des Bare Metal-Servers unter Verwendung von Dell iDRAC mit Lifecycle Controller Auto Config* unter https://www.dell.com/support.

Verwenden von Hash-Kennwörtern für mehr Sicherheit

Auf Power Edge-Servern mit iDRAC-Version 3.00.00.00 können Sie Benutzerkennwörter und BIOS-Kennwörter unter Verwendung des Einweg-Hash-Formats einrichten. Der Benutzerauthentifizierungsmechanismus ist nicht betroffen (mit Ausnahme von SNMPv3 und IPMI) und Sie können das Kennwort im Klartextformat angeben.

Mit der neuen Kennwort-Hash-Funktion:

- Können Sie Ihre eigenen SHA256-Hashes erstellen, um iDRAC-Benutzerkennwörter und BIOS-Kennwörter zu generieren. Damit können Sie die SHA256-Werte im Server-Konfigurationsprofil, in RACADM und WSMan hinterlegen. Wenn Sie die Kennwortwerte für SHA256 bereitstellen, ist eine Authentifizierung über SNMPv3 und IPMI nicht möglich.

  ANMERKUNG: Remote RACADM oder WSMan oder Redfish können nicht für die Konfiguration/den Ersatz von Hash-Kennwörtern für iDRAC verwendet werden. Für die Konfiguration/den Ersatz von Hash-Kennwörtern auf Remote RACADM, WS-Man oder Redfish können Sie SCP verwenden.
- Können Sie einen Vorlagenserver einschließlich aller iDRAC-Benutzerkonten und BIOS-Kennwörter über den aktuellen Nur-Text-Mechanismus einrichten. Nachdem der Server eingerichtet ist, können Sie das Server-Konfigurationsprofil mit den Kennwort-Hash-Werten exportieren. Der Export enthält die für die SNMPv3- und IPMI-Authentifizierung erforderlichen Hash-Werte. Nach dem Import dieses Profils müssen Sie das neueste Dell IPMI-Tool verwenden. Wenn Sie ein älteres Tool verwenden, schlägt die IPMI-Authentifizierung für die Benutzer fehl, die die Hash-Passwortwerte festgelegt haben.
- Die anderen Schnittstellen, z. B. die IDRAC-GUI, zeigen die Benutzerkonten als aktiviert an.

Können Sie das Hash-Kennwort mit und ohne Salt über SHA256 generieren.

Sie müssen über eine Berechtigung zur Serversteuerung verfügen, um Hash-Kennwörter einschließen und exportieren zu können.

Wenn der Zugriff auf alle Konten verloren gegangen ist, verwenden Sie das Dienstprogramm für die iDRAC-Einstellungen oder den lokalen RACADM, und setzen Sie iDRAC auf den Standard-Task zurück.

Wenn das Kennwort für das iDRAC-Benutzerkonto nur mit dem SHA256-Kennwort-Hash und keinen anderen Hashes (SHA1v3Key, MD5v3Key oder IPMIKey) festgelegt wurde, ist die Authentifizierung über SNMP v3 nicht verfügbar.

Hash-Kennwort unter Verwendung von RACADM

Um Hash-Kennwörter einzurichten, verwenden Sie die folgenden Objekte mit dem Befehl `set`:

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

ANMERKUNG: Die Felder `SHA256Password` und `SHA256PasswordSalt` sind für den XML-Import reserviert und werden nicht mithilfe von Befehlszeilentools eingerichtet. Wenn Sie eines der Felder festlegen, kann der aktuelle Benutzer potenziell für die Anmeldung beim iDRAC gesperrt sein. Wenn ein Kennwort mithilfe von `SHA256Password` importiert wird, wird die Überprüfung der Kennwortlänge durch den iDRAC nicht erzwungen.

Verwenden Sie den folgenden Befehl, um das Hash-Kennwort im exportierten Server-Profil einzuschließen:

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

Sie müssen das Salt-Attribut festlegen, wenn der zugeordnete Hash eingestellt wird.

ANMERKUNG: Die Attribute sind nicht für die INI-Konfigurationsdatei anwendbar.

Hash-Kennwort in Server-Konfigurationsprofil

Die neuen Hash-Kennwörter können optional in das Server-Konfigurationsprofil exportiert werden.

Beim Importieren von Serverkonfigurationsprofilen können Sie die Kommentierung des vorhandenen Kennwort-Attributs oder des/der neuen Kennwort-Hash-Attributs/Attribute aufheben. Wenn beide Kommentierungen aufgehoben sind, wird ein Fehler generiert und das Kennwort wird nicht eingestellt. Eine kommentiertes Attribut wird während eines Imports nicht angewendet.

Hash-Kennwort ohne SNMPv3- und IPMI-Authentifizierung erstellen

Ein Hash-Kennwort kann ohne SNMPv3- und IPMI-Authentifizierung mit oder ohne Salt erzeugt werden. Beide Möglichkeiten erfordern SHA256.

So generieren Sie ein Hash-Kennwort mit Salt:

1. Bei iDRAC-Benutzerkonten müssen Sie das Kennwort mithilfe von Salt über SHA256 generieren.

   Wenn Sie das Kennwort mithilfe von Salt generieren, wird eine binären 16-Byte-Zeichenkette angehängt wird. Salt muss 16 Byte lang sein, falls bereitgestellt. Sobald sie angehängt ist, wird sie zu einer 32-Byte-Zeichenkette. Das Format lautet "password" + "salt", zum Beispiel:

   Password = SOMEPASSWORD

   Salt = ALITTLEBITOFSALT – 16 Zeichen werden angehängt

2. Öffnen Sie eine Linux-Eingabeaufforderung und führen Sie den folgenden Befehl aus:

   ```
   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. Stellen Sie den Hash-Wert und Salt im importierten Serverkonfigurationsprofil, in den RACADM-Befehlen, in Redfish oder in WS-MAN bereit.

   ANMERKUNG: Wenn Sie ein zuvor mit Salt erzeugtes Kennwort löschen möchten, dann stellen Sie sicher, dass der Kennwort-Salt explizit auf eine leere Zeichenkette festgelegt ist.

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

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

4. Nach dem Festlegen des Kennworts funktioniert die normale Nur-Text-Kennwortauthentifizierung mit der Ausnahme, dass die Authentifizierung von SNMP v3 und IPMI für die iDRAC-Benutzerkonten fehlschlägt, bei denen die Kennwörter mit Hash aktualisiert wurden.

Einstellungen für lokales Administratorkonto ändern

Nachdem Sie die iDRAC-IP-Adresse festgelegt haben, können Sie die Einstellungen für das lokale Administratorkonto (hier Benutzer 2) über das Dienstprogramm für die iDRAC-Einstellungen ändern. Führen Sie dazu folgende Schritte durch:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Benutzerkonfiguration**.
   Daraufhin wird die Seite **iDRAC-Einstellungen – Benutzerkonfiguration** angezeigt.
2. Geben Sie die Details für den **Benutzernamen**, die **LAN-Benutzerberechtigungen**, die **Benutzerberechtigungen für die seriellen Schnittstellen** und das **Kennwort** an.

   Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
   Mit diesem Schritt sind die Einstellungen für das lokale Administratorkonto konfiguriert.

Standort für das Managed System einrichten

Sie können die Standortdetails des Managed System im Rechenzentrum über die iDRAC-Webschnittstelle oder das Dienstprogramm für die iDRAC-Einstellungen festlegen.

Standort des Managed System über die Web-Schnittstelle einrichten

So legen Sie die Details für den Systemstandort fest:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **System** > **Details** > **System Details (Systemdetails)**.
   Die Seite **Systemdetails** wird angezeigt.
2. Geben Sie unter **Systemstandort** die Standortdetails für das Managed System im Rechenzentrum ein.
   Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.
3. Klicken Sie auf **Anwenden**. Daraufhin werden die Details zum Systemstandort in iDRAC gespeichert.

Standort für Managed System über RACADM einrichten

Um die Details für den Systemstandort anzugeben, verwenden Sie die Gruppenobjekte `System.Location`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Standort für Managed System über das Dienstprogramm für die iDRAC-Einstellungen einrichten

So legen Sie die Details für den Systemstandort fest:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Systemstandort**.
   Daraufhin wird die Seite **iDRAC-Einstellungen – Systemstandort** angezeigt.
2. Geben Sie die Standortdetails für das Managed System im Rechenzentrum ein. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
   Die Details werden gespeichert.

Systemleistung und Stromverbrauch optimieren

Der Strom, der zur Kühlung eines Servers erforderlich ist, kann einen Großteil des Gesamtstrombedarfs eines Systems ausmachen. Die thermische Überwachung dient zur aktiven Verwaltung der Systemkühlung durch Anpassung der Lüftergeschwindigkeit und Verwaltung des Systemstromverbrauchs, um sicherzustellen, dass das System zuverlässig funktioniert, und gleichzeitig den Stromverbrauch, die Luftzirkulation und die akustische Leistung des Systems auf ein Minimum zu reduzieren. Sie können die Einstellungen für die thermische Steuerung anpassen und in Bezug auf die Systemleistung und die Leistung pro Watt optimieren.

Unter Verwendung der iDRAC-Web-Schnittstelle, über RACADM oder über das Dienstprogramm für die iDRAC-Einstellungen können Sie die folgenden Einstellungen für die Kühlung ändern:

- Optimierung für bessere Leistung
- Optimierung für minimalen Stromverbrauch
- Einstellen der maximalen Luftauslasstemperatur
- Erhöhen des Luftstroms durch Lüfter-Offset, falls erforderlich
- Erhöhen des Luftstroms durch die minimale Lüftergeschwindigkeit

Nachfolgend finden Sie eine Liste der Funktionen in der Thermoverwaltung:

- **Luftstrom-Verbrauch des Systems**: zeigt den Echtzeit-Luftstromverbrauch des Systems (in CFM) an, um einen Ausgleich des Luftstroms auf Rack-und Rechenzentrumsebene zu ermöglichen.
- **Benutzerdefinierte Delta-T-Steuerung**: Begrenzung des Temperaturanstiegs von der Einlassluft zum Auslass, zur richtigen Dimensionierung Ihrer Kühlung auf Infrastrukturebene.
- **Auslasstemperatur-Steuerung**: Angabe des Temperaturgrenzwertes der Luft aus dem Server, um den Anforderungen Ihres Datacenters zu entsprechen.
- **Benutzerdefinierte PCIe-Einlasstemperatur**: Auswahl der richtigen Eingangs-Einlasstemperatur, um die Anforderungen von Drittanbietergeräten zu erfüllen.
- **PCIe-Luftstrom-Einstellungen**: bietet eine umfassende PCIe-Gerätekühlungsansicht des Servers und ermöglicht eine benutzerdefinierte Kühlung der Karten von Drittanbietern.

Thermische Einstellungen über die iDRAC-Webschnittstelle ändern

So ändern Sie die Standardeinstellungen:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Systemeinstellungen** > **Hardwareeinstellungen** > **Kühlungskonfiguration**.
2. Geben Sie folgendes an:
   - **Optimierung von thermischem Profil** – Wählen Sie das thermische Profil aus:
     - **Standard-Temperatur-Profil-Einstellungen (Minimalstrom)** – Bedeutet, dass der Temperaturalgorithmus dieselben Systemprofileinstellungen verwendet, die unter der Seite **System-BIOS** > **System-BIOS-Einstellungen** > **Systemprofileinstellungen** definiert sind.

     Standardmäßig ist diese Option auf **Standard-Temperatur-Profil-Einstellungen** eingestellt. Sie können auch einen benutzerdefinierten Algorithmus auswählen, der unabhängig vom BIOS-Profil ist. Die folgenden Optionen sind verfügbar:
     - **Maximale Leistung (Leistung wird optimiert)** :
       - Geringere Wahrscheinlichkeit von Speicher- oder CPU-Drosselung.
       - Höhere Wahrscheinlichkeit der Turbo-Modus-Aktivierung.
       - Im Allgemeinen höhere Lüftergeschwindigkeiten im Leerlauf und bei Spannungsladungen.
     - **Minimalstrom (optimierte Leistung pro Watt)**:
       - Optimiert für geringsten Energieverbrauch des Systems basierend auf optimalem Status des Lüfters
       - Im Allgemeinen niedrigere Lüftergeschwindigkeiten im Leerlauf und bei Spannungsladungen.
     - **Sound-Obergrenze** – Die Sound-Obergrenze liefert eine reduzierte akustische Ausgabe von einem Server auf Kosten der Leistung. Das Aktivieren der Sound-Obergrenze enthält möglicherweise die temporäre Bereitstellung oder Evaluation eines Servers in einem belegten Speicherplatz, aber es sollte nicht während Benchmarking oder leistungsempfindlichen Anwendungen verwendet werden.

     ANMERKUNG: Die Auswahl von **Maximale Leistung** oder **Minimalstrom** setzt die thermischen Einstellungen im Zusammenhang mit der Systemprofileinstellung auf der Seite **System-BIOS** > **System-BIOS-Einstellungenen.Systemprofileinstellungen** außer Kraft.
   - **Maximaler Ablufttemperatur-Grenzwert** – Wählen Sie im Dropdownmenü die maximale Ablufttemperatur aus. Die Werte werden basierend auf dem System angezeigt.

     Der Standardwert ist **Standard, 70 °C (158 °F)**.

     Mit dieser Option können sich die Lüftergeschwindigkeiten des Systems so ändern, dass die Ablufttemperatur den ausgewählten Ablufttemperaturgrenzwert nicht überschreitet. Dies kann nicht immer unter allen Systembetriebsbedingungen garantiert werden, und zwar wegen der Abhängigkeit von der Systemlast und der Systemkühlungskapazität.
   - **Lüftergeschwindigkeits-Offset** – Die Auswahl dieser Option ermöglicht eine zusätzliche Kühlung des Servers. Wenn Hardware hinzugefügt wird (z. B. neue PCIe-Karten), wird evtl. zusätzliche Kühlung benötigt. Durch Festlegung eines Lüfterdrehzahl-Offsets steigt die Lüfterdrehzahl (um den %-Wert des Offsets) über die Drehzahl der Baseline an, die mithilfe des Algorithmus für die thermische Steuerung berechnet wurde. Zu den möglichen Werten gehören:
     - **Niedrige Lüftergeschwindigkeit** – Bewirkt eine moderate Lüftergeschwindigkeit.
     - **Mittlere Lüftergeschwindigkeit** – Bewirkt eine mittelschnelle Lüftergeschwindigkeit.
     - **Hohe Lüftergeschwindigkeit** – Bewirkt eine nahezu maximale Lüfterdrehzahl.
     - **Maximale Lüftergeschwindigkeit** – Bewirkt volle Lüftergeschwindigkeit.
     - **Aus** – Der Offset für die Lüftergeschwindigkeit ist auf „Aus“ gesetzt. Dies ist der Standardwert. Wenn die Option auf "Aus" gesetzt ist, wird der Prozentsatz nicht angezeigt. Die Standard-Lüftergeschwindigkeit wird ohne Offset angewendet. Im Gegensatz dazu führt die maximale Einstellung dazu, dass alle Lüfter mit maximaler Geschwindigkeit laufen.

     Der Lüftergeschwindigkeits-Offset ist dynamisch und basiert auf dem System. Die Lüftergeschwindigkeit wird für jeden Offset neben jeder Option angezeigt.

     Der Lüftergeschwindigkeits-Offset erhöht alle Lüftergeschwindigkeiten um denselben Prozentsatz. Die Lüftergeschwindigkeiten können sich über die Offset-Geschwindigkeiten hinaus erhöhen, je nach dem Kühlungsbedarf der einzelnen Komponenten. Es ist davon auszugehen, dass sich der Gesamtenergieverbrauch des Systems erhöht.

     Der Lüftergeschwindigkeits-Offset ermöglicht es Ihnen, die Lüftergeschwindigkeit des Systems mit vier Schritten zu erhöhen. Diese Schritte sind gleichmäßig zwischen der Standard-Baseline-Geschwindigkeit und der maximalen Geschwindigkeit des Serversystemlüfters verteilt. Einige Hardwarekonfigurationen führen zu höheren Baseline-Lüftergeschwindigkeiten, was in einem anderen Offset als dem maximalen Offset resultiert, um die Maximalgeschwindigkeit zu erreichen.

     Das häufigste Verwendungsszenario ist eine nicht standardmäßige PCIe-Adapterkühlung. Die Funktion kann jedoch dazu verwendet werden, die Systemkühlung für andere Zwecke zu erhöhen.

ANMERKUNG: Die Einstellung der Lüfter-Konfiguration ist in iDRAC verfügbar, selbst wenn das System nicht über Lüfter verfügt. Der Grund dafür ist, dass iDRAC die angegebene Konfiguration an den Gehäuse-Manager sendet, der die Daten von iDRAC verarbeitet und die Kühlungsanforderungen gemäß Konfiguration an das System sendet.

- **Grenzwerte**
  - **Maximale PCIe-Einlasstemperaturgrenze** – Der Standardwert ist 55 °C. Wählen Sie die untere Temperatur von 45 °C für PCIe-Karten von Drittanbietern aus, die eine geringere Eingangstemperatur erfordern.
  - **Ablufttemperatur-Grenzwerte** – Durch das Ändern der Werte für die folgenden Optionen können Sie die Ablufttemperatur-Grenzwerte einstellen:
    - **Maximalen Ablufttemperatur-Grenzwert festlegen**
    - **Lufttemperaturanstieg-Grenzwert festlegen**
  - **Mindestlüftergeschwindigkeit in PWM (% vom Höchstwert)** – Wählen Sie diese Option zur Feineinstellung der Lüftergeschwindigkeit aus: Mit dieser Option können Sie eine höhere Basissystemlüftergeschwindigkeit festlegen oder die Geschwindigkeit des Systemlüfters erhöhen, wenn andere benutzerdefinierte Lüftergeschwindigkeitsoptionen nicht zu den erforderlichen höheren Lüftergeschwindigkeiten führen.
    - **Standardeinstellung** – Legt die Mindestlüftergeschwindigkeit auf den Standardwert fest, der durch den Systemkühlungsalgorithmus bestimmt wird.
    - **Benutzerdefiniert** – Geben Sie den Prozentsatz ein, um den Sie die Lüftergeschwindigkeit ändern möchten. Der Bereich liegt zwischen 9 und 100.

    Der zulässige Bereich für den Mindestlüftergeschwindigkeits-PWM ist dynamisch und basiert auf der Systemkonfiguration. Der erste Wert ist die Leerlaufgeschwindigkeit und der zweite Wert ist die Maximalkonfiguration (je nach Systemkonfiguration kann die maximale Geschwindigkeit bis zu 100 % betragen).

    Systemlüfter können mit einer höheren Geschwindigkeit als dieser laufen, je nach Temperaturanforderungen des Systems. Sie können jedoch nicht die festgelegte Mindestgeschwindigkeit unterschreiten. Zum Beispiel wird bei einer minimalen Lüftergeschwindigkeit von 35 % festgelegt, dass die Lüftergeschwindigkeit niemals 35 % PMW unterschreitet.

    ANMERKUNG: 0 % PWM bedeutet nicht, dass der Lüfter ausgeschaltet ist. Dies ist die niedrigste Geschwindigkeit, mit der der Lüfter betrieben werden kann.

Die Einstellungen sind dauerhaft, d. h., sobald diese festgelegt und angewendet wurden, werden sie während eines Systemneustarts, beim Aus- und Einschalten oder bei iDRAC- oder BIOS-Aktualisierungen nicht automatisch in die Standardeinstellung geändert. Die benutzerdefinierten Kühlungsoptionen werden möglicherweise nicht auf allen Servern unterstützt. Wenn die Optionen nicht unterstützt werden, werden sie nicht angezeigt, oder Sie können keinen benutzerdefinierten Wert festlegen.

3. Klicken Sie auf **Anwenden**, um die Einstellungen zu übernehmen.

   Die folgende Meldung wird angezeigt:

   ```
   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. Klicken Sie auf **Jetzt neu starten** oder **Später neu starten**.

ANMERKUNG: Führen Sie einen Neustart des Systems durch, damit die Aktualisierung wirksam wird.

Thermische Einstellungen unter Verwendung von RACADM ändern

Verwenden Sie zum Ändern der thermischen Einstellungen die Objekte in der Gruppe **system.thermalsettings** mit dem untergeordneten Befehl **set**, wie in der folgenden Tabelle aufgeführt.

Tabelle 10. Temperatureinstellungen

Objekt	Beschreibung	Verwendung	Beispiel

`AirExhaustTemp`	Ermöglicht das Festlegen der maximalen Luftauslasstemperaturgrenze.	Legen Sie die Eigenschaft auf einen der folgenden Werte fest (basierend auf dem System):
		• 0 – Zeigt 40 °C an
		• 1 – Zeigt 45 °C an
		• 2 – Zeigt 50 °C an
		• 3 – Zeigt 55 °C an
		• 4 – Zeigt 60 °C an
			So prüfen Sie die vorhandenen Einstellungen auf dem System:
			`racadm get system.thermalsettings.AirExhaustTemp`
			Das Ergebnis ist Folgendes:
			`AirExhaustTemp=70`

Tabelle 10. Temperatureinstellungen (fortgesetzt)

Objekt	Beschreibung	Verwendung	Beispiel

		• 255 – Zeigt 70 °C an (Standard)	Diese Ausgabe zeigt an, dass das System auf die Luftauslasstemperatur vion 70°C eingestellt ist.
			So stellen Sie den Auslasstemperatur-Grenzwert auf 60 °C ein:
			`racadm set system.thermalsettings.AirExhaustTemp 4`
			Das Ergebnis ist Folgendes:
			`Object value modified successfully.`
			Wenn ein System einen bestimmten Luftauslasstemperatur-Grenzwert nicht unterstützt, führen Sie den folgenden Befehl aus:
			`racadm set system.thermalsettings.AirExhaustTemp 0`
			Die folgende Fehlermeldung wird angezeigt:
			`ERROR: RAC947: Invalid object value specified.`
			Stellen Sie sicher, dass Sie den Wert je nach den Objekttyp angeben.
			Lesen Sie für weitere Informationen die RACADM-Hilfe.
			So legen Sie die Grenze auf den Standardwert zurück:
			`racadm set system.thermalsettings.AirExhaustTemp 255`

`FanSpeedHighOffsetVal`	• Diese Variable liest den Lüftergeschwindigkeit-Offset-Wert in %PWM für die Einstellung „Offset für hohe Lüftergeschwindigkeit“. • Dieser Wert richtet sich nach dem System. • Verwenden Sie das `FanSpeedOffset`-Objekt,	Werte zwischen 0 und 100	`racadm get system.thermalsettings FanSpeedHighOffsetVal` Ein numerischer Wert, zum Beispiel 66, wird zurückgegeben. Dieser Wert

Tabelle 10. Temperatureinstellungen (fortgesetzt)

Objekt	Beschreibung	Verwendung	Beispiel
	um diesen Wert unter Verwendung von Index-Wert 1 festzulegen.		bedeutet, dass, wenn Sie den folgenden Befehl verwenden, ein Offset für Lüftergeschwindigkeit von „Hoch“ (66 % PWM) über die Drehzahl der Basislinie angewendet wird. `racadm set system.thermalsettings FanSpeedOffset 1`

`FanSpeedLowOffsetVal`	• Diese Variable liest den Lüftergeschwindigkeit-Offset-Wert in %PWM für die Einstellung „Offset für niedrige Lüftergeschwindigkeit“.
	• Dieser Wert richtet sich nach dem System.
	• Verwenden Sie das `FanSpeedOffset`-Objekt, um diesen Wert unter Verwendung von Index-Wert 0 festzulegen.
		Werte zwischen 0 und 100	`racadm get system.thermalsettings FanSpeedLowOffsetVal`
			Dies gibt einen Wert wie „23“ zurück. Das bedeutet, dass, wenn Sie den folgenden Befehl verwenden, ein Offset für Lüftergeschwindigkeit von „Niedrig“ (23 % PWM) über die Drehzahl der Basislinie angewendet wird.
			`racadm set system.thermalsettings FanSpeedOffset 0`

`FanSpeedMaxOffsetVal`	• Diese Variable liest den Lüftergeschwindigkeit-Offset-Wert in %PWM für die Einstellung „Offset für maximale Lüftergeschwindigkeit“.
	• Dieser Wert richtet sich nach dem System.
	• Verwenden Sie das `FanSpeedOffset`-Objekt, um diesen Wert unter Verwendung von Index-Wert 3 festzulegen.
		Werte zwischen 0 und 100	`racadm get system.thermalsettings FanSpeedMaxOffsetVal`
			Dies gibt einen Wert wie „100“ zurück. Das bedeutet, dass, wenn Sie den folgenden Befehl verwenden, ein Offset für Lüftergeschwindigkeit von „Hoch“ (100 % PWM) angewendet wird. Normalerweise bewirkt dieses Offset eine maximale Lüftergeschwindigkeit.
			`racadm set system.thermalsettings FanSpeedOffset 3`

`FanSpeedMediumOffsetVal`	• Diese Variable liest den Lüftergeschwindigkeit-Offset-Wert in %PWM für die Einstellung „Offset für mittlere Lüftergeschwindigkeit“. • Dieser Wert richtet sich nach dem System.	Werte zwischen 0 und 100	`racadm get system.thermalsettings FanSpeedMediumOffsetVal` Dies gibt einen Wert wie „47“ zurück. Das bedeutet, dass, wenn Sie den folgenden

Tabelle 10. Temperatureinstellungen (fortgesetzt)

Objekt	Beschreibung	Verwendung	Beispiel
	• Verwenden Sie das `FanSpeedOffset`-Objekt, um diesen Wert unter Verwendung von Index-Wert 2 festzulegen.		Befehl verwenden, ein Offset für Lüftergeschwindigkeit von „Mittel“ (47 % PWM) über die Drehzahl der Basislinie angewendet wird. `racadm set system.thermalsettings FanSpeedOffset 2`

`FanSpeedOffset`	• Das Verwenden dieses Objekts mit dem Get-Befehl zeigt den vorhandenen Lüfterdrehzahl-Offset-Wert an.
	• Das Verwenden dieses Objekts mit dem Get-Befehl ermöglicht die Einstellung des erforderlichen Lüfterdrehzahl-Offset-Werts.
	• Der Indexwert entscheidet über den Offset, der angewendet wird, und die Objekte `FanSpeedLowOffsetVal`, `FanSpeedMaxOffsetVal`, `FanSpeedHighOffsetVal` und `FanSpeedMediumOffsetVal` (zuvor definiert) sind die Werte, bei denen der Offset angewendet wird.
		Mögliche Werte sind:
		• 0 – für niedrige Lüfterdrehzahl
		• 1 – für hohe Lüfterdrehzahl
		• 2 – für mittlere Lüfterdrehzahl
		• 3 – für maximale Lüfterdrehzahl
		• 255 – Keine
			So zeigen Sie die vorhandene Einstellung an:
			`racadm get system.thermalsettings.FanSpeedOffset`
			So legen Sie den Lüfterdrehzahl-Offset-Wert (wie in `FanSpeedHighOffsetVal` definiert) auf „Hoch“ fest
			`racadm set system.thermalsettings.FanSpeedOffset 1`

`MFSMaximumLimit`	Maximalwerte für MFS lesen	Werte von 1 – 100	So zeigen Sie den höchsten Wert an, der mithilfe der `MinimumFanSpeed`-Option eingestellt werden kann: `racadm get system.thermalsettings.MFSMaximumLimit`
`MFSMinimumLimit`	Minimalwerte für MFS lesen	Werte von 0 bis `MFSMaximumLimit` Der Standardwert ist 255 (das bedeutet Keine)	So zeigen Sie den niedrigsten Wert an, der mithilfe der `MinimumFanSpeed`-Option eingestellt werden kann: `racadm get system.thermalsettings.MFSMinimumLimit`
`MinimumFanSpeed`	• Ermöglicht die Konfiguration der Mindest-Lüftergeschwindigkeit, die erforderlich ist, damit das System betrieben werden kann.	Werte von `MFSMinimumLimit` bis `MFSMaximumLimit` Wenn der Befehl 255 meldet, bedeutet dies, dass der	Gehen Sie wie folgt vor, um sicherzustellen, dass die Systemmindestgeschwindigkeit nicht unter 45 % des PWM fällt (45 muss ein Wert

Tabelle 10. Temperatureinstellungen (fortgesetzt)

Objekt	Beschreibung	Verwendung	Beispiel
	• Sie definiert den Basiswert für die Lüftergeschwindigkeit und versetzt Lüfter in die Lage, diesen Wert für die Lüftergeschwindigkeit zu unterschreiten. • Dieser Wert ist der PWM-Wert für die Lüftergeschwindigkeit, angegeben in Prozent.	benutzerdefinierte Versatz nicht angewendet wurde.	zwischen `MFSMinimumLimit` und `MFSMaximumLimit` sein): `racadm set system.thermalsettings.MinimumFanSpeed 45`

`ThermalProfile`	• Ermöglicht die Angabe des thermischen Base-Algorithmus.
	• Ermöglicht das Festlegen des Systemprofils für thermisches Verhalten, das dem Profil zugeordnet ist.
		Werte:
		• 0 – Auto
		• 1 – Maximale Leistung
		• 2: Minimale Stromversorgung
			So zeigen Sie die vorhandene thermische Profileinstellung an:
			`racadm get system.thermalsettings.ThermalProfile`
			So legen Sie das thermische Profil auf maximale Leistung fest:
			`racadm set system.thermalsettings.ThermalProfile 1`

`ThirdPartyPCIFanResponse`	• Thermische Überschreibungen für PCI-Karten von Drittanbietern. • Ermöglicht das Deaktivieren oder Aktivieren der Lüfterreaktion des Standardsystems für erkannte PCI-Karten von Drittanbietern. • Sie können die Existenz der PCI-Karte von Drittanbietern durch das Anzeigen der Meldungs-ID PCI3018 im Lifecycle Controller-Protokoll bestätigen.	Werte: • 1 – Aktiviert • 0 – Deaktiviert **ANMERKUNG:** Der Standardwert ist 1.	So deaktivieren Sie jegliche eingestellte Standard-Lüftergeschwindigkeitsreaktion für eine erkannte PCI-Karte von Drittanbietern: `racadm set system.thermalsettings.ThirdPartyPCIFanResponse 0`

Thermische Einstellungen unter Verwendung vom Dienstprogramm für die iDRAC-Einstellungen ändern

So ändern Sie die Standardeinstellungen:

1. Gehen Sie im Dienstprogramm für die iDRAC -Einstellungen zu **Thermisch**.
   Die Seite **iDRAC-Einstellungen Thermisch** wird angezeigt.
2. Geben Sie folgendes an:
   - Thermisches Profil
   - Maximaler Ablufttemperatur-Grenzwert
   - Offset für Lüftergeschwindigkeit
   - Minimale Lüftergeschwindigkeit

   Die Einstellungen sind dauerhaft: Sobald sie festgelegt und angewendet wurden, werden sie während eines Systemneustarts, beim Aus- und Einschalten oder bei iDRAC- oder BIOS-Aktualisierungen nicht mehr automatisch in die Standardeinstellung geändert. Einige

Dell Server unterstützen möglicherweise keine oder nicht alle dieser benutzerdefinierten Kühlungsoptionen. Wenn die Optionen nicht unterstützt werden, werden sie nicht angezeigt, oder Sie können keinen benutzerdefinierten Wert festlegen.

3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
   Die Konfiguration der Temperatureinstellungen ist damit abgeschlossen.

Ändern von PCIe Airflow-Einstellungen über die iDRAC-Webschnittstelle

Verwenden Sie die PCIe Airflow-Einstellungen, wenn ein höherer Temperaturspielraum für benutzerdefinierte Hochleistungs-PCIe-Karten gewünscht ist.

ANMERKUNG: PCIe Airflow-Einstellungen sind auf MX-Plattformen nicht verfügbar.

So ändern Sie die PCIe Airflow-Einstellungen:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Systemeinstellungen** > **Hardwareeinstellungen** > **Kühlungskonfiguration**.
   Die Seite **PCIe Airflow-Einstellungen** wird unter dem Abschnitt „Lüftereinstellungen“ angezeigt.
2. Geben Sie folgendes an:
   - **LFM-Modus** – Wählen Sie den Modus **Benutzerdefiniert** aus, um die benutzerdefinierte LFM-Option zu aktivieren.
   - **Benutzerdefinierte LFM** – Geben Sie den LFM-Wert ein.
3. Klicken Sie auf **Anwenden**, um die Einstellungen zu übernehmen.

   Die folgende Meldung wird angezeigt:

   ```
   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.
   ```

   Klicken Sie auf **Jetzt neu starten** oder **Später neu starten**.

   ANMERKUNG: Führen Sie einen Neustart des Systems durch, damit die Aktualisierung wirksam wird.

Management Station einrichten

Eine Management Station ist ein Computer, der für den Zugriff auf iDRAC-Schnittstellen zur Remote-Überwachung und -Verwaltung von PowerEdge-Servern verwendet wird.

So richten Sie die Management Station ein.

1. Installieren Sie ein unterstütztes Betriebssystem. Weitere Informationen finden Sie in den Versionshinweisen.
2. Installieren und konfigurieren Sie einen unterstützten Webbrowser. Weitere Informationen finden Sie in den Versionshinweisen.
3. Installieren Sie die aktuelle Java Runtime Environment (JRE) (erforderlich, wenn der Java-Plug-in-Typ für den Zugriff auf iDRAC über einen Webbrowser verwendet wird).

   ANMERKUNG: Zur Nutzung dieser Funktion und zum Starten der virtuellen iDRAC-Konsole über ein IPv6-Netzwerk ist Java 8 oder höher erforderlich.

4. Installieren Sie Remote-RACADM-VMCLI aus dem Ordner SYSMGMT der *Dell Systems Management Tools and Documentation*-DVD. Andernfalls führen Sie auf der DVD **Setup** aus, um Remote RACADM standardmäßig sowie weitere OpenManage-Software zu installieren. Weitere Informationen zu RACADM finden Sie unter *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.
5. Installieren Sie nach Bedarf auch die folgenden Komponenten:
   - SSH-Client
   - TFTP
   - Dell OpenManage Essentials

Per Remote auf iDRAC zugreifen

Für den Remote-Zugriff auf die iDRAC-Webschnittstelle über eine Management Station müssen Sie sicherstellen, dass sich die Management Station im selben Netzwerk wie iDRAC befindet. Beispiel:

- Blade-Server – Die Management Station muss sich im selben Netzwerk wie CMC und OME – Modular befinden. Weitere Informationen zum Isolieren des CMC-Netzwerks vom Netzwerk des verwalteten Systems finden Sie unter *Chassis Management Controller – Handbuch* verfügbar unter https://www.dell.com/cmcmanuals.
- Rack- und Tower-Server – Definieren Sie iDRAC NIC-Schnittstelle auf „Dediziert“ oder LOM1, und stellen Sie sicher, dass sich die Management Station auf dem gleichen Netzwerk wie iDRAC befindet.

Verwenden Sie für den Zugriff auf die Managed System-Konsole über eine Management Station die virtuelle Konsole über die iDRAC-Webschnittstelle.

Konfigurieren von unterstützten Webbrowsern

ANMERKUNG: Informationen zu den unterstützten Browsern und deren Versionen finden Sie in *Versionshinweisen* unter https://www.dell.com/idracmanuals.

Auf die meisten Funktionen der iDRAC-Webschnittstelle kann mit diesen Browsern mit Standardeinstellungen zugegriffen werden. Damit bestimmte Funktionen funktionieren, müssen Sie einige Einstellungen ändern. Diese Einstellungen umfassen das Deaktivieren von Popup-Blockern, das Aktivieren von Java-, ActiveX- oder HTML5-Plug-Ins usw.

Wenn Sie von einer Management Station aus, die über einen Proxyserver mit dem Internet verbunden ist, eine Verbindung zur iDRAC-Webschnittstelle herstellen, konfigurieren Sie den Webbrowser so, dass er über diesen Server auf das Internet zugreifen kann.

ANMERKUNG: Wenn Sie den Internet Explorer oder Firefox zum Zugriff auf die iDRAC-Webschnittstelle verwenden, müssen Sie möglicherweise bestimmte Einstellungen, wie in diesem Abschnitt beschrieben, konfigurieren. Sie können andere unterstützte Browser mit ihren Standardeinstellungen verwenden.

ANMERKUNG: Leere Proxy-Einstellungen werden wie die Einstellung „Kein Proxy“ behandelt.

Internet Explorer konfigurieren

Dieser Abschnitt enthält Details zur Konfiguration von Internet Explorer (IE), um sicherzustellen, dass Sie Zugriff auf alle Funktionen der iDRAC-Webschnittstelle haben und diese verwenden können. Diese Einstellungen umfassen:

- Zurücksetzen der Sicherheitseinstellungen
- Hinzufügen von iDRAC-IP zu vertrauenswürdigen Sites
- IE für die Aktivierung von Active Directory SSO konfigurieren
- Deaktivieren der verstärkten Sicherheitskonfiguration für IE

Internet Explorer-Sicherheitseinstellungen zurücksetzen

Stellen Sie sicher, dass Internet Explorer- (IE) Einstellungen auf die von Microsoft empfohlenen Standardeinstellungen eingestellt sind und passen Sie die Einstellungen, wie in diesem Abschnitt beschrieben, an.

1. Öffnen Sie IE als Administrator oder unter Verwendung eines Administratorkontos.
2. Klicken Sie auf **Extras Internetoptionen Sicherheit Lokales Netzwerk** oder **Lokales Intranet**.
3. Klicken Sie auf **Stufe anpassen**, wählen Sie **Mittelniedrig** und klicken Sie auf **Zurücksetzen**. Klicken Sie zum Bestätigen auf **OK**.

Hinzufügen von iDRAC-IP zur Liste vertrauenswürdiger Webseiten

Wenn Sie auf die iDRAC-Webschnittstelle zugreifen, werden Sie dazu aufgefordert, eine iDRAC-IP-Adresse zur Liste vertrauenswürdiger Domänen hinzuzufügen, wenn sich die IP-Adresse nicht in der Liste befindet. Klicken Sie anschließend auf **Update** (Aktualisieren) oder starten Sie den Webbrowser neu, um eine Verbindung zur iDRAC-Webschnittstelle herzustellen. Wenn Sie nicht aufgefordert werden, die IP-Adresse hinzuzufügen, wird empfohlen, die IP-Adresse manuell zur Liste vertrauenswürdiger Sites hinzuzufügen.

ANMERKUNG: Wenn Sie sich an der iDRAC-Webschnittstelle mit einem Zertifikat anmelden wollen, dem der Browser nicht vertraut, wird die Zertifikatfehlerwarnung des Browsers nach dem Bestätigen der ersten Meldung möglicherweise ein zweites Mal angezeigt.

So fügen Sie iDRAC-IP-Adresse der Liste vertrauenswürdiger Websites hinzu:

1. Klicken Sie auf **Extras** > **Internetoptionen** > **Sicherheit** > **Vertrauenswürdige Sites** > **Sites**.
2. Geben Sie die IP-Adresse des iDRAC in das Feld **Diese Website zur Zone hinzufügen** ein.
3. Klicken Sie auf **Hinzufügen**, dann auf **OK** und schließlich auf **Schließen**.

4. Klicken Sie auf **OK** und aktualisieren Sie dann den Browser.

Internet Explorer für die Aktivierung von Active Directory SSO konfigurieren

So konfigurieren Sie die Browser-Einstellungen für Internet Explorer:

1. Navigieren Sie im Internet Explorer zu **Lokales Intranet**, und klicken Sie dann auf **Sites**.
2. Wählen Sie nur die folgenden Optionen aus:
   - Schließen Sie alle lokalen (Intranet-) Sites ein, die nicht auf anderen Zonen aufgeführt sind.
   - Schließen Sie alle Sites ein, die den Proxy-Server umgehen.
3. Klicken Sie auf **Advanced** (Erweitert).
4. Fügen Sie alle betreffenden Domänennamen ein, die für iDRAC-Instanzen, die Teil der SSO-Konfiguration sind, verwendet werden (z. B. **myhost.example.com**.)
5. Klicken Sie auf **Schließen** und anschließend auf **OK** zweimal.

Deaktivieren der verstärkten Sicherheitskonfiguration für Internet Explorer

Um sicherzustellen, dass Sie Protokolldateien und andere lokale Elemente über die Webschnittstelle herunterladen können, wird empfohlen, die verstärkte Sicherheitskonfiguration für Internet Explorer in den Windows-Funktionen zu deaktivieren. Weitere Informationen zum Deaktivieren dieser Funktion unter Ihrer Windows-Version finden Sie in der Microsoft-Dokumentation.

Konfiguration von Mozilla Firefox

Dieser Abschnitt enthält Details zur Konfiguration von Firefox, um sicherzustellen, dass Sie Zugriff auf alle Funktionen der iDRAC-Webschnittstelle haben und diese verwenden können. Diese Einstellungen umfassen:

- Weiße Liste-Funktion deaktivieren
- Firefox für die Aktivierung von Active Directory SSO konfigurieren

ANMERKUNG: Der Mozilla Firefox-Browser hat möglicherweise keine Bildlaufleiste für die iDRAC-Online-Hilfeseite.

Weiße Liste-Funktion in Firefox deaktivieren

Firefox verfügt über eine Whitelist-Sicherheitsfunktion, für die Benutzerberechtigungen zum Installieren von Plug-Ins für jede Site erforderlich sind, die ein Plug-In hostet. Wenn diese Funktion aktiviert ist, müssen Sie für die Whitelist-Funktion einen Viewer für die virtuelle Konsole für jeden iDRAC installieren, selbst wenn die Viewer-Versionen identisch sind.

Führen Sie folgende Schritte aus, um die Funktion „Weiße Liste“ zu deaktivieren und unnötige Plug-in-Installationen zu vermeiden:

1. Öffnen Sie ein Internet-Browser-Fenster in Firefox.
2. Geben Sie in das Adressfeld `about:config` ein und drücken Sie <Eingabe>.
3. Machen Sie in der Spalte **Einstellungsname** den Eintrag **xpinstall.whitelist.required** ausfindig und doppelklicken Sie darauf.

   Die Werte für **Preference Name** (Einstellungsname), **Status**, **Type** (Typ), und **Value** (Value) werden fett formatiert. Der Wert für **Status** ändert sich zum festgelegten Benutzer und der Wert für **Value** (Wert) ändert sich zu „false“.
4. Machen Sie in der Spalte **Einstellungs**name den Eintrag xpinstall.enabled ausfindig.
   Stellen Sie sicher, dass **Value** (Value) auf **true** festgelegt ist. Ist dies nicht der Fall, doppelklicken Sie auf **xpinstall.enabled**, um **Value** (Wert) auf **true** festzulegen.

Firefox für die Aktivierung von Active Directory SSO konfigurieren

So konfigurieren Sie die Browser-Einstellungen für Firefox:

1. Geben Sie `about:config` in die Firefox-Adresszeile ein.
2. Geben Sie unter **Filter** `network.negotiate` ein.
3. Fügen Sie den Domänen-Namen zu network.negotiate-auth.trusted-uris (kommaseparierte Liste verwenden) hinzu.
4. Fügen Sie den Domänen-Namen zu network.negotiate-auth.delegation-uris (kommaseparierte Liste verwenden) hinzu.

Web-Browser für die Verwendung der virtuellen Konsole konfigurieren

So verwenden Sie die virtuelle Konsole auf Ihrer Management Station:

1. Stellen Sie sicher, dass eine unterstützte Browserversion installiert ist (Internet Explorer (Windows) oder Mozilla Firefox (Windows oder Linux), Google Chrome, Safari).

   Weitere Informationen zu den unterstützten Browserversionen finden Sie in den *Versionshinweisen* unter https://www.dell.com/idracmanuals.

2. Wenn Sie Internet Explorer verwenden, setzen Sie IE auf **Als Administrator ausführen**.
3. Konfigurieren Sie den Web-Browser für die Verwendung des ActiveX-, Java- oder HTML5-Plugin.

   Der ActiveX Viewer funktioniert nur mit dem Internet Explorer. HTML5 oder ein Java-Viewer werden auf jedem Browser unterstützt.

   ANMERKUNG: Zur Nutzung dieser Funktion und zum Starten der virtuellen iDRAC-Konsole über ein IPv6-Netzwerk ist Java 8 oder höher erforderlich.

4. Importieren Sie die Stammzertifikate auf das Managed System, um Popup-Fenster zu unterbinden, die Sie zur Überprüfung der Zertifikate auffordern.
5. Installieren Sie das verknüpfte Paket **compat-libstdc++-33-3.2.3-61**.

   ANMERKUNG: Unter Windows ist das verknüpfte Paket `compat-libstdc++-33-3.2.3-61` möglicherweise im .NET Framework-Paket oder im Betriebssystempaket enthalten.

6. Wenn Sie ein MAC-Betriebssystem nutzen, wählen Sie die Option **Zugriff für Hilfsgeräte aktivieren** im Fenster **Universeller Zugriff**.

   Weitere Informationen finden Sie in der Dokumentation des MAC-Betriebssystems.

Internet Explorer zur Verwendung des HTML-5-basierten Plug-In konfigurieren

Für die Erstellung der virtuellen HTML5-Konsole und virtuellen Datenträger-APIs wurde HTML5 verwendet. Im Folgenden werden die Vorteile bei der Verwendung von HTML5 aufgeführt:

- Auf der Client Workstation ist keine Installation erforderlich.
- Die Kompatibilität basiert auf dem Browser und nicht auf dem Betriebssystem oder den installierten Komponenten.
- Kompatibel mit den meisten des Desktops und mobilen Plattformen.
- Schnelle Bereitstellung und Herunterladen des Clients als Teil einer Webseite.

Sie müssen Einstellungen des Internet Explorer (IE) konfigurieren, bevor Sie HTML5-basierte Anwendungen der virtuellen Konsole und des virtuellen Datenträgers starten und ausführen. So konfigurieren Sie die Browser-Einstellungen:

1. Deaktivieren Sie den Popupblocker. Klicken Sie dazu auf **Tools (Extras)** > **Internet Options (Internetoptionen)** > **Privacy (Datenschutz**, und deaktivieren Sie das Kontrollkästchen **Turn on Pop-up Blocker** (Popupblocker einschalten).
2. Starten Sie die virtuelle HTML5-Konsole unter Verwendung von einer der folgenden Methoden:
   - Klicken Sie in IE auf **Tools (Extras)** > **Compatibility View Settings (Einstellungen der Kompatibilitätsansicht)**, und entfernen Sie die Markierung bei **Display intranet sites in Compatibility View** (Intranetsites in Kompatibilitätsansicht anzeigen).
   - Modifizieren Sie bei Verwendung einer IPv6-Adresse diese Adresse in IE wie folgt:

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

   - Direkte virtuelle HTML5-Konsole. Modifizieren Sie bei Verwendung einer IPv6-Adresse diese Adresse in IE wie folgt:

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

3. Wechseln Sie zum Anzeigen der Titelleisteninformationen in IE zu **Control Panel (Systemsteuerung)** > **Appearance and Personalization (Darstellung und Anpassung)** > **Personalization (Anpassung)** > **Window Classic (Windows – klassisch)**.

Konfigurieren von Internet Explorer für Verwendung des HTML5-basierten Plug-ins

Sie müssen die Edge-Einstellungen konfigurieren, bevor Sie die virtuelle HTML5-basierte Konsole und virtuelle Datenträgeranwendungen starten und ausführen. So konfigurieren Sie die Browser-Einstellungen:

1. Klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen anzeigen** und deaktivieren Sie die Option **Pop-ups blockieren**.
2. Ändern Sie die IPv6-Adresse wie folgt:

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

Web-Browser für die Verwendung des Java-Plugin konfigurieren

Installieren Sie eine Java Runtime Environment (JRE), wenn Sie Firefox oder IE verwenden und den Java Viewer verwenden möchten.

ANMERKUNG: Installieren Sie eine 32-Bit- oder 64-Bit-JRE-Version auf einem 64-Bit-Betriebssystem oder eine 32-Bit-JRE-Version auf einem 32-Bit-Betriebssystem.

So konfigurieren Sie IE für die Verwendung des Java-Plugin:

- Deaktivieren Sie die automatische Anforderung von Datei-Downloads im Internet Explorer.
- Deaktivieren Sie die Option *Verstärkter Sicherheitsmodus* im Internet Explorer.

IE für die Verwendung des ActiveX-Plugin konfigurieren

Sie müssen die IE-Browser-Einstellungen konfigurieren, bevor Sie die virtuelle ActiveX-basierte Konsole starten und Anwendungen der virtuellen Datenträger ausführen. Die ActiveX-Anwendungen werden als signierte CAB-Dateien vom iDRAC-Server bereitgestellt. Wenn der Plug-In-Typ in der virtuellen Konsole auf den Native-ActiveX-Typ festgelegt ist, werden beim Starten der virtuellen Konsole die CAB-Datei auf dem Clientsystem heruntergeladen und die virtuelle ActiveX-basierte Konsole gestartet. Für Internet Explorer sind einige Konfigurationen für das Herunterladen, Installieren und Ausführen von ActiveX-basierten Anwendungen erforderlich.

Auf 64-Bit-Betriebssystemen können Sie sowohl 32-Bit- als auch 64-Bit-Versionen von Internet Explorer installieren. Sie können die 32-Bit- oder 64-Bit-Version verwenden, müssen jedoch das entsprechende Plug-in installieren. Wenn Sie zum Beispiel das Plug-in im 64-Bit-Browser installieren und dann das Anzeigeprogramm in einem 32-Bit-Browser öffnen, müssen Sie das Plug-in erneut installieren.

ANMERKUNG: Sie können das ActiveX-Plugin nur mit Internet Explorer verwenden.

ANMERKUNG: Um das ActiveX-Plugin auf Systemen mit Internet Explorer 9 zu verwenden, stellen Sie vor dem Konfigurieren von Internet Explorer sicher, dass Sie den erweiterten Sicherheitsmodus in Internet Explorer oder im Server-Manager in den Betriebssystemen von Windows Server deaktivieren.

Bei ActiveX-Anwendungen in Windows 7, Windows 2008 und Windows 10 müssen Sie die folgenden Internet Explorer-Einstellungen konfigurieren, um das ActiveX-Plug-in verwenden zu können:

1. Leeren Sie den Browser-Cache.
2. Fügen Sie die iDRAC-IP-Adresse oder den Host-Namen zur Liste **Local Internet site** (Lokale Internetsite) hinzu.
3. Setzen Sie die benutzerdefinierten Einstellungen auf **Mittelhoch (Standard)** zurück, oder ändern Sie die Einstellungen, um die Installation von signierten ActiveX-Plugins zu ermöglichen.
4. Aktivieren Sie den Browser für das Herunterladen von verschlüsselten Inhalten und das Aktivieren von Drittanbieter-Browsererweiterungen. Wechseln Sie dazu zu **Tools (Extras)** > **Internet Options (Internetoptionen)** > **Advanced (Erweitert)**, deaktivieren Sie die Option **Do not save encrypted pages to disk (Verschlüsselte Seiten nicht auf der Festplatte speichern)** und wählen Sie die Option **Enable third-party browser extensions (Browsererweiterungen von Drittanbietern aktivieren)**.

   ANMERKUNG: Starten Sie Internet Explorer neu, damit die Einstellung „Browsererweiterungen von Drittanbietern aktivieren“ aktiviert wird.

5. Gehen Sie zu **Extras** > **Internetoptionen** > **Sicherheit** und wählen Sie die Zone aus, in der Sie die Anwendung ausführen möchten.
6. Klicken Sie auf **Custom level** (Stufe anpassen). Nehmen Sie im Fenster **Security Settings** (Sicherheitseinstellungen) die folgenden Einstellungen vor:
   - Wählen Sie die Option **Aktivieren** für **Automatische Eingabeaufforderung für ActiveX-Steuerelemente** aus.
   - Wählen Sie die Option **Auffordern** für **Signierte ActiveX-Steuerelemente herunterladen** aus.

- Wählen Sie die Option **Aktivieren** oder **Auffordern** für **ActiveX-Steuerelemente und -Plugins ausführen** aus.
- Wählen Sie die Option **Aktivieren** oder **Auffordern** für **Script-ActiveX-Steuerelemente, die für das Scripting als sicher gekennzeichnet wurden** aus.

7. Klicken Sie auf **OK**, um das Fenster **Sicherheitseinstellungen** zu schließen.
8. Klicken Sie auf **OK**, um das Fenster **Internetoptionen** zu schließen.

ANMERKUNG: Stellen Sie auf Systemen mit Internet Explorer 11 sicher, dass Sie die iDRAC-IP-Adresse hinzufügen, indem Sie auf **Tools (Extras)** > **Compatibility View settings (Einstellungen der Kompatibilitätsansicht)** klicken.

ANMERKUNG:

- Die unterschiedlichen Versionen von Internet Explorer verwenden **Internet Options (Internetoptionen)** gemeinsam. Nachdem Sie also den Server zur Liste der *vertrauenswürdigen Websites* für einen Browser hinzugefügt haben, verwendet der andere Browser die gleiche Einstellung.
- Vor der Installation des ActiveX-Steuerelements kann Internet Explorer eventuell eine Sicherheitswarnung anzeigen. Akzeptieren Sie die ActiveX-Steuerung, um das Installationsverfahren abzuschließen, wenn der Internet Explorer Sie mit einer Sicherheitswarnung dazu auffordert.
- Wenn die Fehlermeldung **Unknown Publisher** (Unbekannter Herausgeber) beim Starten der virtuellen Konsole angezeigt wird, wurde möglicherweise der Pfad des Codesignaturzertifikats geändert. Um diesen Fehler zu beheben, müssen Sie einen zusätzlichen Schlüssel herunterladen. Verwenden Sie eine Suchmaschine für die Suche nach **Symantec SO16958** und folgenden Sie in den Suchergebnissen den Anweisungen auf der Symantec-Website.

Zusätzliche Einstellungen für Windows Vista oder neuere Microsoft-Betriebssysteme

Die Internet Explorer-Browser in Windows Vista oder neueren Betriebssystemen weisen eine zusätzliche Sicherheitsfunktion mit der Bezeichnung *Schutzmodus* auf.

Um ActiveX-Anwendungen in Internet Explorer-Browsern mit dem *Schutzmodus* zu starten und auszuführen:

1. Führen Sie IE als Administrator aus.
2. Gehen Sie zu **Extras** > **Internetoptionen** > **Sicherheit** > **Vertrauenswürdige Sites**.
3. Stellen Sie sicher, dass die Option **Schutzmodus aktivieren** nicht als Zone für vertrauenswürdige Sites ausgewählt ist. Alternativ dazu können Sie die iDRAC-Adresse den Sites in der Intranetzone hinzufügen. Standardmäßig ist der Schutzmodus für Sites in der Intranetzone und in der Zone vertrauenswürdiger Sites ausgeschaltet.
4. Klicken Sie auf **Sites**.
5. Geben Sie in das Feld **Diese Website zur Zone hinzufügen** die Adresse des iDRAC ein, und klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **Schließen** und dann auf **OK**.
7. Schließen Sie den Browser und starten Sie ihn neu, damit die Einstellungen wirksam werden.

Browser-Cache leeren

Wenn beim Betrieb der virtuellen Konsole Probleme auftreten (Fehler des Typs Außerhalb des Bereichs, Synchronisierungsprobleme usw.) löschen Sie den Browser-Cache, um alte Viewer-Versionen zu entfernen oder zu löschen, die auf dem System gespeichert sein könnten, und wiederholen Sie den Vorgang.

ANMERKUNG: Um den Browser-Cache löschen zu können, müssen Sie über Administratorrechte verfügen.

Frühere Java-Versionen löschen

So löschen Sie ältere Versionen von Java-Viewer in Windows oder Linux:

1. Führen Sie bei der Eingabeaufforderung `javaws-viewer` oder `javaws-uninstall` aus.
   Der **Java Cache-Viewer** wird angezeigt.
2. Löschen Sie die Elemente mit der Bezeichnung *Client der virtuellen iDRAC-Konsole*.

Zertifizierungsstellenzertifikate auf die Management Station importieren

Beim Starten der virtuellen Konsole oder virtueller Datenträger werden Eingabeaufforderungen zur Überprüfung der Zertifikate angezeigt. Wenn Sie über benutzerdefinierte Webserverzertifikate verfügen, können Sie diese Aufforderungen vermeiden, indem Sie die CA-Zertifikate in den vertrauenswürdigen Java- oder ActiveX-Zertifikatspeicher importieren.

Weitere Informationen über die automatische Zertifikatregistrierung (ACE) finden Sie im Abschnitt Automatische Zertifikatregistrierung auf Seite 114

Zertifizierungsstellenzertifikat in den Speicher für vertrauenswürdige Java-Zertifikate importieren

So importieren Sie das Zertifizierungsstellenzertifikat in den vertrauenswürdigen Java-Speicher:

1. Starten Sie das **Java-Systemsteuerung**.
2. Klicken Sie auf die Registerkarte **Sicherheit** und dann auf **Zertifikate**.
   Das Dialogfeld **Zertifikate** wird angezeigt.
3. Wählen Sie aus dem Drop-Down-Menü „Zertifikattyp“ die Option **Vertrauenswürdige Zertifikate** aus.
4. Klicken Sie auf **Importieren**, browsen Sie zum gewünschten Zertifizierungsstellenzertifikat (im in Base64-verschlüsselten Format), wählen Sie es aus, und klicken Sie dann auf **Öffnen**.
   Das ausgewählte Zertifikat wird in den vertrauenswürdigen, web-basierten Zertifikatspeicher importiert.
5. Klicken Sie auf **Schließen** und dann auf **OK**. Das Fenster **Java Control Panel** (Java-Systemsteuerung) wird geschlossen.

Zertifizierungsstellenzertifikat in den Speicher für vertrauenswürdige ActiveX-Zertifikate importieren

Sie müssen das OpenSSL-Befehlszeilentool verwenden, um den Zertifikat-Hash mit SHA (Secure Hash Algorithm) zu erstellen. Es wird empfohlen, das OpenSSL-Tool Version 1.0.x und höher zu verwenden, da es SHA standardmäßig verwendet. Das Zertifizierungsstellenzertifikat muss im Base64-verschlüsselten PEM-Format vorliegen. Dies ist ein einmaliger Vorgang für den Import jedes einzelnen Zertifizierungsstellenzertifikats.

So importieren Sie das Zertifizierungsstellenzertifikat in den vertrauenswürdigen ActiveX-Speicher:

1. Öffnen Sie die OpenSSL-Befehlseingabe.
2. Führen Sie einen 8-Byte-Hash auf dem Zertifizierungsstellenzertifikat aus, das derzeit auf der Management Station verwendet wird. Verwenden Sie dazu den folgenden Befehl: `openssl x509 -in (name of CA cert) -noout -hash`.

   Es wird eine Ausgabedatei generiert. Wenn der Dateiname des Zertifizierungsstellenzertifikats beispielsweise **cacert.pem** lautet, lautet der Befehl wie folgt:

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

   Es wird eine Ausgabedatei generiert, die dem folgenden Beispiel ähnelt: „431db322“.
3. Nennen Sie die Datei für das Zertifizierungsstellenzertifikat in den Namen der Ausgabedatei um, und fügen Sie die Erweiterung „.0“ hinzu. z.B. 431db322.0.
4. Kopieren Sie das umbenannte Zertifizierungsstellenzertifikat in das Stammverzeichnis. Zum Beispiel **C:\Documents and Settings\<Benutzer>-Verzeichnis**.

Lokalisierte Versionen der Webschnittstelle anzeigen

Die iDRAC-Webschnittstelle wird in den folgenden Sprachen unterstützt:

- Englisch (en-us)
- Französisch (fr)
- Deutsch (de)
- Spanisch (es)
- Japanisch (ja)
- Vereinfachtes Chinesisch (zh-cn)

Die ISO-Sprachcodes in Klammern geben die unterstützten Sprachvarianten an. Bei einigen unterstützten Sprachen ist es erforderlich, das Browserfenster auf eine Breite von 1024 Pixel einzustellen, um alle Funktionen anzuzeigen.

Die iDRAC-Webschnittstelle wurde für den Einsatz mit den entsprechenden Tastaturen für die unterstützten Sprachvarianten entwickelt. Einige Funktionen der iDRAC-Webschnittstelle, wie z. B. virtuelle Konsole können zusätzliche Schritte für den Zugriff auf bestimmte Funktionen/Buchstaben erfordern. Andere Tastaturen werden nicht unterstützt und können ggf. unerwartete Probleme verursachen.

ANMERKUNG: Lesen Sie in der Dokumentation zum Browser nach, wie verschiedene Sprachen konfiguriert und eingerichtet werden, und lassen Sie sich lokalisierte Versionen der iDRAC-Webschnittstelle anzeigen.

Updating device firmware

Using iDRAC, you can update the iDRAC, BIOS, and all device firmware that is supported by using Lifecycle Controller update such as:

- Fibre Channel (FC) cards
- Diagnostics
- Operating System Driver Pack
- Network Interface Card (NIC)
- RAID Controller
- Power Supply Unit (PSU)
- NVMe PCIe devices
- SAS/SATA hard drives
- Backplane update for internal and external enclosures
- OS Collector

CAUTION: The PSU firmware update may take several minutes depending on the system configuration and PSU model. To avoid damaging the PSU, do not interrupt the update process or power on the system during PSU firmware update.

NOTE:

- While performing a PSU firmware update through the host OS in the 15th Generation PowerEdge servers, ensure that you perform a cold reboot to apply the update.

When updating the PSU firmware for PowerEdge C series servers, ensure that all servers in the same chassis are powered OFF first. If any of the other servers in the chassis are powered ON, the update process fails.

Upload the required firmware to iDRAC. After the upload is complete, the current version of the firmware that is installed on the device and the version being applied is displayed. If the firmware being uploaded is not valid, an error message is displayed. Updates that do not require a reboot are applied immediately. Updates that require a system reboot are staged and committed to run on the next system reboot. Only one system reboot is required to perform all updates.

NOTE:

- When SEKM mode is enabled on a controller, iDRAC Firmware downgrade/upgrade shall fail when tried from a SEKM to a non-SEKM iDRAC version. iDRAC Firmware upgrade/downgrade shall pass when done within the SEKM versions.
- PERC firmware downgrade shall fail when SEKM is enabled.

After the firmware is updated, the **System Inventory** page displays the updated firmware version and logs are recorded.

The supported firmware image file types are:

- `.exe` — Windows-based Dell Update Package (DUP). You must have Control and Configure Privilege to use this image file type.
- `.d9` — Contains both iDRAC and Lifecycle Controller firmware

For files with `.exe` extension, you must have the System Control privilege. The Remote Firmware Update (licensed feature) and Lifecycle Controller must be enabled.

For files with `.d9` extension, you must have the Configure privilege.

NOTE: Ensure that all nodes in the system are powered off before updating the PSU firmware.

NOTE: After upgrading the iDRAC firmware, you may notice a difference in the timestamp displayed in the Lifecycle Controller log. Time that is displayed in LC Log is different from NTP/Bios-Time for few logs during idrac reset.

You can perform firmware updates by using the following methods:

- Uploading a supported image type, one at a time, from a local system or network share.
- Connecting to an FTP, TFTP, HTTP or HTTPS site or a network repository that contains Windows DUPs and a corresponding catalog file.

You can create custom repositories by using the Dell Repository Manager. For more information, see *Dell Repository Manager Data Center User's Guide*. iDRAC can provide a difference report between the BIOS and firmware that is installed on the system and the updates available in the repository. All applicable updates that are contained in the repository are applied to the system. This feature is available with iDRAC Enterprise or Datacenter license.

NOTE: HTTP/HTTPS only supports with either digest authentication or no authentication.

- Scheduling recurring automated firmware updates by using the catalog file and custom repository.

There are multiple tools and interfaces that can be used to update the iDRAC firmware. The following table is applicable only to iDRAC firmware. The table lists the supported interfaces, image-file types, and whether Lifecycle Controller must be in enabled state for the firmware to be updated.

Table 11. Image file types and dependencies

	.D9 Image		iDRAC DUP	
Interface	**Supported**	**Requires LC enabled**	**Supported**	**Requires LC enabled**
BMCFW64.exe utility	Yes	No	No	N/A
Racadm FWUpdate (old)	Yes	No	No	N/A
Racadm Update (new)	Yes	Yes	Yes	Yes
iDRAC UI	Yes	Yes	Yes	Yes
WSMan	Yes	Yes	Yes	Yes
In-band OS DUP	No	N/A	Yes	No
Redfish	Yes	N/A	Yes	N/A

The following table provides information about whether a system restart is required when firmware is updated for a particular component:

NOTE: When multiple firmware updates are applied through out-of-band methods, the updates are ordered in the most efficient possible manner to reduce unnecessary system restart.

Table 12. Firmware update—supported components

Component Name	Firmware Rollback Supported? (Yes or No)	Out-of-band—System Restart Required?	In-band — System Restart Required?	Lifecycle Controller GUI—Restart Required?
Diagnostics	No	No	No	No
OS Driver Pack	No	No	No	No
iDRAC	Yes	No	No*	Yes
BIOS	Yes	Yes	Yes	Yes
RAID Controller	Yes	Yes	Yes	Yes
BOSS	Yes	Yes	Yes	Yes
NVDIMM	No	Yes	Yes	Yes
Backplanes	Yes	Yes	Yes	Yes
NOTE: • For Expander (Active) backplanes, system restart is required. • For SEP (Passive) backplanes, rebootless update is supported only from 4.00.00.00 release onwards.				
Enclosures	Yes	Yes	No	Yes
NIC	Yes	Yes	Yes	Yes
Power Supply Unit	Yes	Yes	Yes	Yes
CPLD	No	Yes	Yes	Yes

Table 12. Firmware update—supported components (continued)

Component Name	Firmware Rollback Supported? (Yes or No)	Out-of-band—System Restart Required?	In-band — System Restart Required?	Lifecycle Controller GUI—Restart Required?
NOTE: After CPLD firmware upgrade is complete, iDRAC restarts automatically.				
FC Cards	Yes	Yes	Yes	Yes
NVMe PCIe SSD drives	Yes	Yes	Yes	Yes
SAS/SATA hard drives	No	Yes	Yes	No
OS Collector	No	No	No	No
CMC (on PowerEdge FX2 servers)	No	Yes	Yes	Yes
TPM	No	Yes	Yes	Yes
Non-SDL Software and Peripherals Application	No	No	No	No

NOTE:

- TPM firmware update is supported from 5.00.00.00 release onwards and this action is staged. Downgrading (rollback) or reinstalling the same firmware version is not supported.
- TPM does not support rollback.
- When stacking TPM firmware update with BIOS update (unsupported TPM version), TPM update fails.
- Once iDRAC is flashed or TPM is inserted, first-time host reboot with POST completion is required to fetch the TPM details from BIOS and detect TPM in software inventory.
- Latest BIOS version is needed for TPM firmware updates to be supported using iDRAC interfaces. Recommended to update BIOS first before updating iDRAC.
- TPM must be enabled in BIOS first before you can perform firmware update using iDRAC interfaces.

NOTE: For details of supported components for MX platform, see Table 13.

Table 13. Firmware update—supported components for MX platforms

Component Name	Firmware Rollback Supported? (Yes or No)	Out-of-band—System Restart Required?	In-band—System Restart Required?	Lifecycle Controller GUI—Restart Required?
Diagnostics	No	No	No	No
OS Driver Pack	No	No	No	No
iDRAC	Yes	No	No*	Yes
BIOS	Yes	Yes	Yes	Yes
RAID Controller	Yes	Yes	Yes	Yes
BOSS	Yes	Yes	Yes	Yes
NVDIMM	No	Yes	Yes	Yes
Backplanes	Yes	Yes	Yes	Yes
Enclosures	Yes	Yes	No	Yes
NIC	Yes	Yes	Yes	Yes
Power Supply Unit	No	No	No	No
CPLD	No	Yes	Yes	Yes
FC Cards	Yes	Yes	Yes	Yes

Table 13. Firmware update—supported components for MX platforms (continued)

Component Name	Firmware Rollback Supported? (Yes or No)	Out-of-band—System Restart Required?	In-band—System Restart Required?	Lifecycle Controller GUI—Restart Required?
NVMe PCIe SSD drives	Yes	Yes	No	No
SAS/SATA hard drives	No	Yes	Yes	No
OS Collector	No	No	No	No

* Indicates that though a system restart is not required, iDRAC must be restarted to apply the updates. iDRAC communication and monitoring may temporarily be interrupted.

When you check for updates, the version marked as **Available** does not always indicate that it is the latest version available. Before you install the update, ensure that the version you choose to install is newer than the version currently installed. If you want to control the version that iDRAC detects, create a custom repository using Dell Repository Manager (DRM) and configure iDRAC to use that repository to check for updates.

Firmware über die iDRAC-Webschnittstelle aktualisieren

Sie können zur Aktualisierung der Geräte-Firmware Firmware-Images vom lokalen System, von einem Repository auf einer Netzwerkfreigabe (CIFS, NFS, HTTP oder HTTPS) oder von FTP verwenden.

Einzelgeräte-Firmware aktualisieren

Vor der Aktualisierung der Firmware mithilfe der Einzelgeräte-Aktualisierung stellen Sie sicher, dass das Firmware-Abbild an einen Speicherort auf dem lokalen System heruntergeladen ist.

ANMERKUNG: Stellen Sie sicher, dass der Dateiname der Einzelkomponenten-DUPs keine Leerzeichen enthält.

So aktualisieren Sie die Gerätefirmware eines einzelnen Gerätes mithilfe der iDRAC-Webschnittstelle:

1. Gehen Sie zu **Wartung** > **Systemaktualisierung**.

   Die Seite **Firmware-Aktualisierung** wird angezeigt.

2. Wählen Sie auf der Registerkarte **Aktualisieren** die Option **Lokal** als **Speicherorttyp** aus.

   ANMERKUNG: Wenn Sie „Lokal“ auswählen, vergewissern Sie sich, dass Sie das Firmware-Image in einen Speicherort auf dem lokalen System herunterladen. Wählen Sie eine Datei aus, die iDRAC zur Aktualisierung bereitgestellt werden soll. Sie können weitere Dateien (einzeln) für das Hochladen auf den iDRAC auswählen. Die Dateien werden in einen temporären Speicherplatz auf dem iDRAC hochgeladen. Die maximale Kapazität des Speicherplatzes beträgt ca. 300 MB.

3. Klicken Sie auf **Durchsuchen**, wählen Sie die Firmware-Image-Datei für die gewünschte Komponente aus und klicken Sie dann auf **Hochladen**.
4. Nachdem der Hochladevorgang abgeschlossen ist, wird im Abschnitt **Aktualisierungsdetails** jede auf iDRAC hochgeladene Firmware-Datei mit ihrem Status angezeigt.

   Wenn die Firmware-Imagedatei gültig ist und erfolgreich hochgeladen wurde, zeigt die **Inhaltsspalte** ein Pluszeichen (+) neben dem Dateinamen des Firmware-Image an. Erweitern Sie den Namen, um Informationen zu **Gerätenamen**, **Aktuellen** und **Verfügbaren Firmware-Versionen** anzuzeigen.

5. Wählen Sie die erforderliche Firmware-Datei aus und führen Sie einen der folgenden Schritte aus:
   - Für Firmware-Images, bei denen kein Neustart des Hostsystems erforderlich ist, klicken Sie auf **Installieren** (einzige verfügbare Option). Zum Beispiel: iDRAC-Firmwaredatei.
   - Für Firmwareimages, bei denen ein Neustart des Hostsystems erforderlich ist, klicken Sie auf **Installieren und Neustart** oder **Beim nächsten Systemstart installieren**.
   - Um die Aktualisierung der Firmware abzubrechen, klicken Sie auf **Abbrechen**.

   Wenn Sie auf **Installieren**, **Installieren und Neustart** oder **Beim nächsten Neustart installieren** klicken, wird die Meldung `Updating Job Queue` angezeigt.

6. Um die Seite **Job-Warteschlange** anzuzeigen, klicken Sie auf **Job-Warteschlange**. Verwenden Sie diese Seite, um die bereitgestellten Firmware-Aktualisierungen anzuzeigen und zu verwalten, oder klicken Sie auf **OK**, um die aktuelle Seite zu aktualisieren und den Status der Firmware-Aktualisierung anzuzeigen.

ANMERKUNG: Wenn Sie die Seite verlassen, ohne die Aktualisierungen zu speichern, wird eine Fehlermeldung angezeigt und der gesamte hochgeladene Inhalt geht verloren.

ANMERKUNG: Wenn die Sitzung nach dem Hochladen der Firmware-Datei abgelaufen ist, können Sie nicht fortfahren. Dieses Problem kann nur durch RACADM `reset` behoben werden.

ANMERKUNG: Nachdem das Firmwareupdate abgeschlossen wurde, wird eine Fehlermeldung angezeigt: `RAC0508: An unexpected error occurred. Wait for few minutes and retry the operation. If the problem persists, contact service provider.` Dies ist zu erwarten. Sie können ein wenig warten und den Browser aktualisieren. Anschließend werden Sie zur Anmeldeseite weitergeleitet.

Planung automatischer Firmware-Aktualisierungen

Sie können einen wiederkehrenden Zeitplan für iDRAC angeben, um nach Firmware-Aktualisierungen zu suchen. Zum geplanten Zeitpunkt verbindet sich der iDRAC mit dem angegebenen Ziel, sucht nach neuen Updates und wendet alle anwendbaren Updates an oder stellt sie bereit. Auf dem Remote-Server wird eine Protokolldatei erstellt, die Informationen über den Serverzugriff und bereitgestellte Firmware-Updates enthält.

Es wird empfohlen, ein Repository mit Dell Repository Manager (DRM) zu erstellen und den iDRAC so zu konfigurieren, dass er dieses Repository verwendet, um nach Firmware-Updates zu suchen und diese durchzuführen. Die Verwendung eines internen Repositorys ermöglicht Ihnen, die für den iDRAC verfügbare Firmware und Versionen zu steuern und unbeabsichtigte Firmwareänderungen zu vermeiden.

ANMERKUNG: Weitere Informationen zu DRM finden Sie unter www.dell.com/openmanagemanuals > Repository Manager..

Eine iDRAC Enterprise oder Datacenter Lizenz ist erforderlich, um automatische Updates zu planen.

Sie können automatische Firmware-Aktualisierungen mithilfe der iDRAC-Webschnittstelle oder mit RACADM planen.

ANMERKUNG: Die IPv6-Adresse wird bei der Planung automatischer Firmware-Aktualisierungen nicht unterstützt.

Planen der automatischen Firmware-Aktualisierung mithilfe der Webschnittstelle

So erstellen Sie einen Zeitplan für die automatische Aktualisierung der Firmware mithilfe der Webschnittstelle:

ANMERKUNG: Erstellen Sie nicht die nächste geplante Ausführung eines automatischen Aktualisierungsjobs, wenn bereits ein Job geplant ist. Dabei wird der aktuell geplante Job außer Kraft gesetzt.

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Maintenance (Wartung)** > **System Update (Systemaktualisierung)** > **Automatic Update (Automatische Aktualisierung)**.
   Die Seite **Firmware-Aktualisierung** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Automatische Aktualisierung**.
3. Wählen Sie die Option **Automatische Aktualisierung aktivieren** aus.
4. Wählen Sie eine der folgenden Optionen aus, um anzugeben, ob ein Systemneustart erforderlich ist, nachdem die Aktualisierungen bereitgestellt wurden:
   - **Aktualisierungen planen** – Stellt die Firmware-Aktualisierungen bereit, führt aber keinen Serverneustart aus.
   - **Aktualisierungen planen und Server neu starten** – Initiiert einen Server-Neustart, nachdem die Firmware-Aktualisierungen bereitgestellt wurden.
5. Wählen Sie eine der folgenden Optionen, um den Speicherort der Firmware-Abbilder anzugeben:
   - **Network** (Netzwerk) – Verwenden Sie die Katalogdatei einer Netzwerkfreigabe (CIFS, NFS, HTTP oder HTTPS, TFTP). Geben Sie die Details zur Netzwerkfreigabe ein.
     ANMERKUNG: Beim Angeben der Netzwerkfreigabe wird empfohlen, für Benutzername und Kennwort Sonderzeichen zu vermeiden oder Prozent kodieren Sie diese Sonderzeichen.
   - **FTP** – Verwenden Sie die Katalogdatei der FTP-Site. Geben Sie die Details zur FTP-Site ein.
   - **HTTP** oder **HTTPS** – Ermöglicht Streaming der Katalogdatei und HTTP- oder HTTPS-Dateiübertragung.
6. Geben Sie anhand der Auswahl in Schritt 5 die Netzwerkeinstellungen oder die FTP-Einstellungen ein.
   Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

7. Geben Sie im Abschnitt **Aktualisierungszeitplan** die Startzeit für die Firmware-Aktualisierung und die Häufigkeit der Aktualisierung (täglich, wöchentlich oder monatlich) ein.

   Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

8. Klicken Sie auf **Aktualisierung planen**.

   Der nächste geplante Job wird in der Job-Warteschlange erstellt. Fünf Minuten, nachdem die erste Instanz des wiederkehrenden Jobs begonnen hat, wird der Job für den nächsten Zeitraum erstellt.

Planen des automatischen Firmwareupdates mithilfe von RACADM

Verwenden Sie zum Erstellen von Zeitplänen für das automatische Firmwareupdate die folgenden Befehle:

- Für die Aktivierung des automatischen Firmwareupdates:

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

- Zum Anzeigen des Status des automatischen Firmwareupdates:

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

- Zum Planen der Startzeit und Häufigkeit des Firmwareupdates:

```
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)>
```

  Beispiel:

  - Für die automatische Aktualisierung der Firmware mithilfe einer CIFS-Freigabe:

```
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
```

  - Für die automatische Aktualisierung der Firmware mithilfe von FTP:

```
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
```

- Zum Anzeigen des aktuellen Zeitplans des Firmwareupdates:

```
racadm AutoUpdateScheduler view
```

- Zum Deaktivieren des automatischen Firmwareupdates:

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

- Zum Löschen der Einzelheiten der Zeitpläne:

```
racadm AutoUpdateScheduler clear
```

Aktualisieren der Gerätefirmware über RACADM

Verwenden Sie zum Update der Gerätefirmware mit RACADM den Unterbefehl `update`. Weitere Informationen dazu finden Sie unter *iDRAC-RACADM-CLI-Handbuch*, verfügbar unter https://www.dell.com/idracmanuals.

Beispiele:

- Laden Sie die Update-Datei von einer Remote-HTTP-Freigabe hoch:

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

- Laden Sie die Update-Datei von einer Remote-HTTPS-Freigabe hoch:

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

- So erstellen Sie einen Vergleichsreport mit einem Update-Repository:

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

- So führen Sie alle verfügbaren Updates aus dem Update-Repository mit `myfile.xml` als Katalogdatei sowie einen ordentlichen Neustart durch:

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

- So führen Sie alle verfügbaren Updates von einem FTP-Update-Repository mit `Catalog.xml` als Katalogdatei durch:

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

Firmware über die CMC-Web-Schnittstelle aktualisieren

Sie können die iDRAC-Firmware für Blade-Server über die CMC-Webschnittstelle aktualisieren.

So aktualisieren Sie die iDRAC-Firmware über die CMC-Webschnittstelle:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Gehen Sie zu **iDRAC Settings (iDRAC-Einstellungen)** > **Settings (Einstellungen)** > **CMC**.
   Die Seite **iDRAC** bereitstellen wird angezeigt.
3. Klicken Sie auf **iDRAC-Web-Schnittstelle starten**, und führen Sie dann die **iDRAC-Firmware-Aktualisierung** aus.

Firmware über DUP aktualisieren

Bevor Sie die Firmware über das Dell Update Package (DUP) aktualisieren, müssen Sie Folgendes sicherstellen:

- Installieren und aktivieren Sie die IPMI und die Treiber des verwalteten Systems.
- Aktivieren und starten Sie den Windows-Verwaltungsinstrumentationsdienst (WMI), wenn Ihr System auf einem Windows-Betriebssystem läuft.

  ANMERKUNG: Während Sie die iDRAC-Firmware über das DUP-Dienstprogramm für Linux aktualisieren und Fehlermeldungen wie `usb 5-2: device descriptor read/64, error -71` auf der Konsole angezeigt werden, können Sie diese Fehlermeldungen ignorieren.
- Wenn auf dem System der ESX-Hypervisor installiert ist, müssen Sie für das Ausführen der DUP-Datei sicherstellen, dass der Dienst „usbarbitrator“ über den folgenden Befehl angehalten wird: `service usbarbitrator stop`

Einige Versionen von DUPs sind so konstruiert, dass sie miteinander in Konflikt stehen. Dies geschieht im Laufe der Zeit, wenn neue Versionen der Software erstellt werden. Bei einer neueren Software-Version kann die Unterstützung für ältere Geräte entfallen. Unterstützung für neue Geräte kann hinzugefügt werden. Betrachten Sie zum Beispiel die beiden DUPs Network_Firmware_NDT09_WN64_21.60.5.EXE und Network_Firmware_8J1P7_WN64_21.60.27.50.EXE. Die von diesen DUPs unterstützten Geräte lassen sich in drei Gruppen einteilen.

- Gruppe A sind Altgeräte, die nur vom NDT09 unterstützt werden.
- Gruppe B sind Geräte, die sowohl von NDT09 als auch von 8J1P7 unterstützt werden.
- Gruppe C sind neue Geräte, die nur von 8J1P7 unterstützt werden.

Betrachten Sie einen Server, der über ein oder mehrere Geräte aus jeder der Gruppen A, B und C verfügt. Wenn die DUPs einzeln eingesetzt werden, sollten sie erfolgreich sein. Die Verwendung von NDT09 allein aktualisiert die Geräte in Gruppe A und Gruppe B. Die Verwendung von 8J1P7 allein aktualisiert Geräte in Gruppe B und Gruppe C. Wenn Sie jedoch versuchen, beide DUPs gleichzeitig zu verwenden, kann dies dazu führen, dass Sie versuchen, zwei Aktualisierungen für die Geräte der Gruppe B gleichzeitig zu erstellen. Das kann mit einem gültigen Fehler fehlschlagen: „Auftrag für dieses Gerät ist bereits vorhanden“. Die Aktualisierungssoftware ist nicht in der Lage, den Konflikt zweier gültiger DUPs zu lösen, die gleichzeitig zwei gültige Aktualisierungen auf denselben Geräten versuchen. Gleichzeitig sind beide DUPs verpflichtet, Geräte der Gruppe A und der Gruppe C zu unterstützen. Der Konflikt erstreckt sich auch auf die Durchführung von Rollbacks auf den Geräten. Als bewährte Vorgehensweise wird vorgeschlagen, jede DUP einzeln zu verwenden.

So aktualisieren Sie iDRAC über DUP:

1. Laden Sie das DUP-Dienstprogramm auf der Basis des installierten Betriebssystems herunter, und führen Sie es auf dem Managed System aus.
2. Führen Sie DUP aus.
   Die Firmware wurde aktualisiert. Ein Systemneustart ist nicht erforderlich, nachdem die Firmware-Aktualisierung abgeschlossen ist.

Firmware über Remote-RACADM aktualisieren

1. Laden Sie das Firmware-Image auf den FTP- oder TFTP-Server herunter. Beispiel: `C:\downloads\firmimg.d9`
2. Führen Sie den folgenden RACADM-Befehl aus:

   TFTP-Server:

   - Unter Verwendung des Befehls `fwupdate`:

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

     path

     der Speicherort auf dem TFTP-Server, auf dem `firmimg.d9` gespeichert ist.

   - Unter Verwendung des Befehls `update`:

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

   FTP-Server

   - Unter Verwendung des Befehls `fwupdate`:

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

     path

     der Speicherort auf dem FTP-Server, auf dem `firmimg.d9` gespeichert ist.

   - Unter Verwendung des Befehls `update`:

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

   Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Firmware über die Lifecycle-Controller-Remote-Dienste aktualisieren

Weitere Informationen zum Aktualisieren der Firmware über die Lifecycle-Controller-Remote-Dienste finden Sie unter *Schnellstart-Benutzerhandbuch für Lifecycle Controller Remote Services* verfügbar unter https://www.dell.com/idracmanuals.

Aktualisieren der CMC-Firmware über iDRAC

Bei PowerEdge FX2-/FX2s-Gehäusen können Sie die Firmware für den Chassis Management Controller und alle Komponenten aktualisieren, die von CMC aktualisiert und über die Server von iDRAC aus freigegeben werden können.

Bevor Sie die Aktualisierung anwenden, stellen Sie Folgendes sicher:

- Server dürfen nicht durch CMC eingeschaltet werden.
- Gehäuse mit LCD müssen die folgende Meldung anzeigen: „Die Aktualisierung von <Name der Komponente> läuft“.
- Gehäuse ohne LCD müssen den Aktualisierungsvorgang durch Blinken eines LED-Musters anzeigen.
- Während der Aktualisierung sind die Gehäuse-Aktionsstrombefehle deaktiviert.

Die Aktualisierungen für Komponenten wie Programmable System-on-Chip (PSoC) von EAM, die erfordern, dass alle Server im Ruhezustand sind, werden beim nächsten Aus- und Einschaltvorgang des Gehäuses angewandt.

CMC-Einstellungen zur Aktualisierung der iDRAC-Firmware über iDRAC

Führen Sie bei PowerEdge FX2-/FX2s-Gehäusen vor der Firmware-Aktualisierung über iDRAC für CMC und dessen freigegebenen Komponenten die folgenden Schritte aus:

1. Starten der CMC-Webschnittstelle
2. Gehen Sie zu **iDRAC Settings (iDRAC-Einstellungen)** > **Settings (Einstellungen)** > **CMC**.
   Die Seite **iDRAC** bereitstellen wird angezeigt.
3. Wählen Sie aus **Chassis Management at Server Mode** (Chassis Management in Servermodus) den Eintrag **Manage and Monitor** (Verwalten und überwachen) aus und klicken Sie auf **Apply** (Anwenden).

iDRAC-Einstellungen zur Aktualisierung der CMC-Firmware

Nehmen Sie bei FX2-/FX2s-Gehäusen vor der Aktualisierung der Firmware für CMS und dessen freigegebener Komponenten über iDRAC die folgenden Einstellungen in iDRAC vor:

1. Gehen Sie zu **iDRAC Settings (iDRAC-Einstellungen)** > **Settings (Einstellungen)** > **CMC**.
2. Klicken Sie auf **Chassis Management Controller Firmware Update** (Firmware-Aktualisierung für Chassis Management Controller). Daraufhin wird die Seite **Firmware-Aktualisierungseinstellungen für den Chassis Management Controller** angezeigt.
3. Wählen Sie für **CMC-Aktualisierungen über das BS und Lifecycle Controller zulassen**, und wählen Sie **Aktiviert** aus, um die CMC-Firmware-Aktualisierung über iDRAC zu aktivieren.
4. Stellen Sie unter **Current CMC Setting** (Aktuelle CMC-Einstellung) sicher, dass die Option **Chassis Management at Server Mode** (Gehäuseverwaltung im Servermodus) **Manage and Monitor** (Verwalten und überwachen) anzeigt wird. Sie können dies im CMC ändern.

Anzeigen und Verwalten von gestuften Aktualisierungen

Sie können die geplanten Jobs anzeigen und löschen, einschließlich Aufgaben zum Konfigurieren und Aktualisieren. Hierbei handelt es sich um eine lizenzierte Funktion. Alle Jobs, die während des nächsten Neustarts ausgeführt werden sollen, können gelöscht werden.

Anzeigen und Verwalten gestufter Aktualisierungen unter Verwendung der iDRAC Webschnittstelle

Gehen Sie zum Anzeigen der geplanten Jobs unter Verwendung der iDRAC-Webschnittstelle zu **Maintenance (Wartung)** > **Job Queue (Job-Warteschlange)**. Auf der Seite **Job Queue** (Job-Warteschlange) wird der Status der Jobs in der Job-Warteschlange des Lifecycle Controllers angezeigt. Weitere Informationen zu den verschiedenen Feldern finden Sie in der *iDRAC-Online-Hilfe*.

Markieren Sie die zu löschen Jobs und klicken Sie auf **Delete** (Löschen). Die Seite wird aktualisiert, und der ausgewählte Job wird aus der Jobwarteschlange des Lifecycle Controller entfernt. Sie können alle Jobs aus der Warteschlange, die während des nächsten Neustarts ausgeführt werden sollen. Sie können keine aktiven Jobs löschen, das heißt Jobs mit dem Status *Running* (Wird ausgeführt) oder *Downloading* (Wird heruntergeladen).

Sie brauchen Berechtigungen zur Serversteuerung, um Jobs zu löschen.

Anzeigen und Verwalten gestufter Aktualisierungen unter Verwendung von RACADM

Zur Anzeige der gestuften Aktualisierungen unter Verwendung von RACADM verwenden Sie den Unterbefehl `jobqueue`. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Rollback der Geräte-Firmware durchführen

Sie können die Firmware für den iDRAC oder jedes Gerät, das vom Lifecycle Controller unterstützt wird, zurücksetzen, auch wenn das Upgrade zuvor über eine andere Schnittstelle durchgeführt wurde. Beispiel: Wenn das Upgrade über die GUI von Lifecycle Controller durchgeführt wurde, können Sie die Firmware über die iDRAC-Webschnittstelle zurücksetzen. Sie können die Firmware für mehrere Geräte gleichzeitig im Rahmen eines einzigen Systemneustarts zurücksetzen.

Bei PowerEdge-Servern der 14. Generation, die über einen einzelnen iDRAC und Lifecycle Controller-Firmware verfügen, setzt das Zurücksetzen der iDRAC-Firmware gleichzeitig auch die Lifecycle-Controller-Firmware zurück.

Es wird empfohlen, die Firmware zu aktualisieren, um sicherzustellen, dass Sie über die neuesten Funktionen und Sicherheitsupdates verfügen. Möglicherweise müssen Sie eine Aktualisierung zurücksetzen oder eine frühere Version installieren, wenn nach einer Aktualisierung Probleme auftreten. Verwenden Sie für die Installation einer früheren Version den Lifecycle Controller, um nach Updates zu suchen und die Version auszuwählen, die Sie installieren möchten.

Informationen zu den unterstützten und nicht unterstützten Komponenten für ein Firmware-Rollback finden Sie in der Tabelle Firmware update—supported components auf Seite 79

Sie können die Firmware der folgenden Komponenten zurücksetzen:

- iDRAC mit Lifecycle Controller

- BIOS
- Netzwerkschnittstellenkarte (NIC)
- Netzteileinheit (PSU)
- RAID-Controller
- Rückwandplatine

ANMERKUNG: Für das Diagnoseprogramm, Treiberpakete und CPLD kann die Firmware nicht zurückgesetzt werden.

Stellen Sie vor dem Zurücksetzen der Firmware Folgendes sicher:

- Sie verfügen über Konfigurationsberechtigungen zum Zurücksetzen der iDRAC-Firmware.
- Sie verfügen über Serversteuerungsberechtigungen und haben Lifecycle Controller für das Zurücksetzen der Firmware für andere Geräte als den iDRAC aktiviert.
- Ändern Sie den NIC-Modus auf **Dediziert**, wenn der Modus als **Gemeinsam genutztes LOM** eingestellt wurde.

Sie können ein Rollback der Firmware auf die zuvor installierte Version über eines der folgenden Verfahren ausführen:

- iDRAC-Weboberfläche
- CMC-Webschnittstelle (nicht unterstützt auf MX-Plattformen)
- OME-modulare Webschnittstelle (Unterstützt auf MX-Plattformen)
- CMC RACADM CLI (nicht unterstützt auf MX-Plattformen)
- iDRAC RACADM CLI
- Lifecycle-Controller-GUI
- Lifecycle Controller-Remote-Dienste

Rollback für die Firmware über die iDRAC-Webschnittstelle durchführen

So führen Sie einen Rollback der Geräte-Firmware aus:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Maintenance (Wartung)** > **System Update (Systemaktualisierung)** > **Rollback**.
   Die Seite **Rollback** zeigt die Geräte an, deren Firmware zurückgesetzt werden kann. Sie können den Gerätenamen, die zugehörigen Geräte, die derzeit installierte Firmware-Version und die verfügbare Firmware-Version, auf die zurückgesetzt werden soll, anzeigen.
2. Wählen Sie eines oder mehrere Geräte aus, für die Sie einen Firmware-Rollback ausführen möchten.
3. Klicken Sie je nach ausgewählten Geräten auf **Install and Reboot (Installieren und neu starten)** oder **Install Next Reboot** (Beim nächsten Neustart installieren). Wenn nur iDRAC ausgewählt ist, klicken Sie dann auf **Install** (Installieren).
   Wenn Sie auf **Installieren und neu starten** oder **Nächsten Neustart installieren** klicken, wird die Meldung „Job-Warteschlange wird aktualisiert“ angezeigt.
4. Klicken Sie auf **Job-Warteschlange**.
   Die Seite **Job-Warteschlange** wird angezeigt, auf der Sie die bereitgestellten Firmwareaktualisierungen anzeigen und verwalten können.

   ANMERKUNG:
   - Wenn Sie sich im Rollback-Modus befinden, wird der Rollback-Vorgang auch dann im Hintergrund fortgesetzt, wenn Sie zu einer anderen Seite wechseln.

   In folgenden Fällen wird eine Fehlermeldung angezeigt:
   - Sie verfügen nicht über die erforderliche Serversteuerungsberechtigung zum Zurücksetzen der Firmware für andere Geräte als den iDRAC, oder Sie verfügen nicht über die erforderliche Konfigurationsberechtigung zum Zurücksetzen der iDRAC-Firmware.
   - Die Firmware wird bereits in einer anderen Sitzung zurückgesetzt.
   - Es wurden Aktualisierungen zur Ausführung bereitgestellt oder sie werden bereits ausgeführt.

   Wenn Lifecycle Controller deaktiviert ist oder sich im Wiederherstellungszustand befindet und Sie versuchen, die Firmware für ein anderes Gerät als iDRAC zurückzusetzen, wird eine Warnmeldung mit Hinweisen zum Aktivieren von Lifecycle-Controller angezeigt.

Rollback der Firmware über die CMC-Web-Schnittstelle durchführen

So führen Sie ein Rollback über die CMC-Web-Schnittstelle durch:

1. Melden Sie sich bei der CMC-Webschnittstelle an.

2. Gehen Sie zu **iDRAC Settings (iDRAC-Einstellungen)** > **Settings (Einstellungen)** > **CMC**.
   Die Seite **iDRAC** bereitstellen wird angezeigt.
3. Klicken Sie auf **Launch iDRAC** (iDRAC starten) und führen Sie gemäß Abschnitt Rollback für die Firmware über die iDRAC-Webschnittstelle durchführen auf Seite 87 den Rollback der Geräte-Firmware durch.

Rollback der Firmware über RACADM durchführen

1. Überprüfen Sie den Status von Rollback-Vorgang und FQDD mit dem Befehl `swinventory`:

   ```
   racadm swinventory
   ```

   Für das Gerät, für das Sie den Firmware-Rollback ausführen möchten, muss die `Rollback Version` als `Available` angezeigt werden. Notieren Sie außerdem die FQDD.

2. Führen Sie den Rollback der Geräte-Firmware mithilfe des folgenden Befehls aus:

   ```
   racadm rollback <FQDD>
   ```

   Weitere Informationen finden Sie unter *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Rollback der Firmware über Lifecycle-Controller durchführen

Informationen hierzu finden Sie unter *Benutzerhandbuch für den Lifecycle Controller* verfügbar unter https://www.dell.com/idracmanuals.

Rollback der Firmware über die Remote-Dienste für den Lifecycle Controller durchführen

Informationen hierzu finden Sie unter *Schnellstart-Benutzerhandbuch für Lifecycle Controller Remote Services* verfügbar unter https://www.dell.com/idracmanuals.

iDRAC wiederherstellen

iDRAC unterstützt zwei Betriebssystem-Images, um ein startfähiges iDRAC sicherzustellen. Gehen Sie bei einem nicht vorhersehbaren Fehler mit schwerwiegenden Folgen und dem Verlust der beiden Startpfade wie folgt vor:

- Der iDRAC-Bootloader erkennt, dass kein startfähiges Image vorhanden ist.
- Die LED für „System Health“ (Systemzustand) und „Identify“ (Identifizieren) blinkt etwa alle 0,5 Sekunden. (Die LED befindet sich auf der Rückseite von Rack- und Tower-Systemen sowie auf der Vorderseite von Blade-Servern.)
- Der Bootloader fragt den SD-Kartensteckplatz ab.
- Formatieren Sie eine SD-Karte mit FAT über ein Windows-Betriebssystem oder EXT3 über ein Linux-Betriebssystem.
- Kopieren Sie das Image **firmimg.d9** auf die SD-Karte.
- Legen Sie die SD-Karte in den Server ein.
- Bootloader erkennt die SD-Karte, schaltet die blinkende LED auf eine dauerhaft gelbe Anzeige, liest das Image „firmimg.d9“, programmiert iDRAC um und startet iDRAC neu.

Easy Restore (Einfache Wiederherstellung)

Easy Restore verwendet den Easy Restore-Flash-Speicher, um die Daten zu sichern. Wenn Sie die Hauptplatine ersetzen und das System einschalten, fragt das BIOS den iDRAC ab und fordert Sie auf, die gesicherten Daten wiederherzustellen. Der erste BIOS-Bildschirm fordert Sie auf, die Service-Tag-Nummer, Lizenzen und UEFI-Diagnoseanwendung wiederherzustellen. Der zweite BIOS-Bildschirm fordert Sie auf, die Systemkonfiguration wiederherzustellen. Wenn Sie die Daten auf dem ersten BIOS-Bildschirm nicht wiederherstellen und wenn Sie die Service-Tag-Nummer nicht mit einer anderen Methode festlegen, wird der erste BIOS-Bildschirm wieder angezeigt. Der zweite BIOS-Bildschirm wird nur einmal angezeigt.

ANMERKUNG:

- Die Einstellungen der Systemkonfigurationen werden nur gesichert, wenn CSIOR (Collect System Inventory On Reboot) aktiviert ist. Stellen Sie sicher, dass der Lifecycle Controller und CSIOR aktiviert sind.
- System Erase (System löschen) löscht keine Daten aus dem Easy Restore-Flash-Speicher.
- Easy Restore (Einfache Wiederherstellung) sichert keine anderen Daten (z.B. Firmware-Images, vFlash-Daten oder Erweiterungskarten-Daten).

Nach dem Austausch der Hauptplatine auf Ihrem Server können Sie mithilfe von Easy Restore die folgenden Daten automatisch wiederherstellen:

- System Service Tag (Service-Tag-Nummer des Systems)
- Bestands-Tag
- Daten zu Lizenzen
- UEFI-Diagnoseanwendung
- Systemkonfigurationseinstellungen - BIOS, iDRAC und NIC

ANMERKUNG: Bei Servern mit iDRAC-Version 3.00.00.00 und höher wird Easy Restore automatisch nach 5 Minuten fortgesetzt, wenn keine Benutzerinteraktion erfolgt.

Nachfolgend sind die Details zur Dauer einiger Wiederherstellungsaktionen aufgeführt:

- Das Wiederherstellen von Systeminhalten wie Diagnose, Systemereignisprotokoll (SEL) und OEM ID-Modul dauert in der Regel weniger als eine Minute.
- Die Wiederherstellung der Systemkonfigurationsdaten (iDRAC, BIOS, NIC) kann mehrere Minuten in Anspruch nehmen, in einigen Fällen ca. 10 Minuten.

ANMERKUNG: Während dieser Zeit gibt es keine Anzeige oder Fortschrittsleiste und der Server kann mehrmals neu gestartet werden, um die Wiederherstellung der Konfiguration abzuschließen.

iDRAC über andere Systemverwaltungs-Tools überwachen

Sie können iDRAC über Dell Management Console und Dell OpenManage Essentials ermitteln und überwachen. Sie können außerdem DRACT (Dell Remote Access Configuration Tool) verwenden, um iDRACs zu ermitteln, die Firmware zu aktualisieren und Active Directory einzurichten. Weitere Informationen finden Sie in den jeweiligen Benutzerhandbüchern.

Unterstützung des Serverkonfigurationsprofils – Import und Export

Das Serverkonfigurationsprofil (SCP) ermöglicht den Import und Export von Serverkonfigurationsdateien.

ANMERKUNG: Sie benötigen Administratorrechte, um die SCP-Aufgabe Export und Import auszuführen.

Sie können Importe und Exporte über eine lokale Management Station oder eine lokale Netzwerkfreigabe über CIFS, NFS, HTTP oder HTTPS durchführen. Mithilfe von Serverkonfigurationsprofilen können Sie ausgewählte Konfigurationen für BIOS, NIC und RAID auf Komponentenebene importieren oder exportieren. Sie können SCP auf die lokale Management Station importieren und exportieren oder in eine CIFS-, NFS-, HTTP- oder HTTPS-Netzwerkfreigabe. Sie können entweder einzelne Profile von iDRAC, BIOS, NIC und RAID importieren und exportieren oder alle zusammen als eine einzige Datei.

Sie können eine Vorschau der importierten oder exportierten Serverkonfigurationsprofile anzeigen. Dabei wird die Aufgabe ausgeführt und das Konfigurationsergebnis generiert, es wird jedoch keine Konfiguration angewendet.

Eine Aufgabe wird erstellt, sobald der Export oder Import über die GUI initiiert wurde. Der Aufgabenstatus kann auf der Seite „Job Queue“ (Job-Warteschlange) angezeigt werden.

ANMERKUNG:

- Es sind nur der Hostname oder die IP-Adresse als Zieladresse zulässig.
- Sie können zum Importieren der Serverkonfigurationsdateien zu einem bestimmten Speicherort navigieren. Sie müssen die Serverkonfigurationsdatei auswählen, die Sie importieren möchten. Zum Beispiel import.xml.
- Je nach Format der exportierten (zuvor ausgewählten) wird die Erweiterung automatisch hinzugefügt. Zum Beispiel `export_system_config.xml`.

- Beim Export kann sich der SCP-Dateiname ändern. Zum Beispiel kann con.xml zu _con.xml werden.
- SCP wendet die komplette Konfiguration in einem einzigen Job mit minimaler Anzahl von Neustarts an. In einigen wenigen Systemkonfigurationen ändern jedoch einige Attribute die Betriebsart eines Gerätes oder können Untergeräte mit neuen Attributen anlegen. In diesem Fall kann SCP möglicherweise nicht alle Einstellungen während eines einzelnen Auftrags übernehmen. Überprüfen Sie die ConfigResult-Einträge für den Job, um alle anstehenden Konfigurationseinstellungen aufzulösen.

SCP ermöglicht Ihnen die Durchführung der BS-Bereitstellung (OSD) mit einer einzigen XML/JSON-Datei über mehrere Systeme hinweg. Außerdem können Sie vorhandene Vorgänge wie Konfigurationen und Repository-Aktualisierungen auf einmal durchführen.

SCP ermöglicht außerdem den Export und Import von öffentlichen SSH-Schlüsseln für alle iDRAC-Nutzer. Es gibt 4 öffentliche SSH-Schlüssel für alle Nutzer.

Im Folgenden finden Sie die Schritte für die BS-Bereitstellung mit SCP:

1. Exportieren der SCP-Datei
2. Die SCP-Datei enthält alle unterdrückten Attribute, die für die BS-Bereitstellung erforderlich sind.
3. Bearbeiten/aktualisieren Sie die OSD-Attribute und führen Sie dann den Importvorgang durch.
4. Diese OSD-Attribute werden dann vom SCP-Orchestrator validiert.
5. Der SCP-Orchestrator führt die in der SCP-Datei angegebenen Konfigurations- und Repository-Aktualisierungen aus.
6. Nachdem die Konfiguration und die Aktualisierungen abgeschlossen sind, wird das Host-Betriebssystem heruntergefahren.

   ANMERKUNG: Nur CIFS- und NFS-Freigaben werden für das Hosten von BS-Medien unterstützt.
7. Der SCP-Orchestrator initiiert das OSD durch Anhängen der Treiber für das ausgewählte Betriebssystem und initiiert dann einen Neustart des BS-Datenträgers, der in NFS/Share vorhanden ist.
8. LCL zeigt den Fortschritt des Jobs an.
9. Nach dem Starten des BIOS auf dem Betriebssystemmedium wird der SCP-Job als abgeschlossen angezeigt.
10. Der angeschlossene Datenträger und der Betriebssystemdatenträger werden nach 65535 Sekunden oder nach der durch das Attribut `OSD.1#ExposeDuration` angegebenen Dauer automatisch getrennt.

Importieren des Server-Konfigurationsprofils mithilfe der iDRAC-Webschnittstelle

So importieren Sie das Server-Konfigurationsprofil:

1. Navigieren Sie zu **Konfiguration** > **Server-Konfigurationsprofil**.
   Die Seite **Server-Konfigurationsprofil** wird angezeigt.
2. Wählen Sie eine der folgenden Optionen, um den Speicherorttyp anzugeben:
   - **Lokal** zum Importieren der Konfigurationsdatei, die in einem lokalen Laufwerk gespeichert ist.
   - **Netzwerkfreigabe** zum Importieren der Konfigurationsdatei von einer CIFS- oder NFS-Freigabe.
   - **HTTP oder HTTPS** zum Importieren der Konfigurationsdatei aus einer lokalen Datei mittels HTTP/HTTPS-Dateiübertragung.

   ANMERKUNG: Je nach Speicherorttyp müssen Sie die Netzwerkeinstellungen oder HTTP/HTTPS-Einstellungen eingeben. Wenn Proxy für HTTP/HTTPS konfiguriert ist, sind auch die Proxy-Einstellungen erforderlich.
3. Wählen Sie die in der Option **Komponenten importieren** aufgeführten Komponenten aus.
4. Wählen Sie den Typ für **Herunterfahren** aus.
5. Wählen Sie die **Maximale Wartezeit** aus, um die Wartezeit bis zum Herunterfahren des Systems nach Abschluss des Imports festzulegen.
6. Klicken Sie auf **Importieren**.

Exportieren des Server-Konfigurationsprofils mithilfe der iDRAC-Webschnittstelle

So exportieren Sie das Server-Konfigurationsprofil:

1. Navigieren Sie zu **Konfiguration** > **Server-Konfigurationsprofil**.
   Die Seite **Server-Konfigurationsprofil** wird angezeigt.
2. Klicken Sie auf **Exportieren**.
3. Wählen Sie eine der folgenden Optionen, um den Speicherorttyp anzugeben:

- **Lokal** zum Speichern der Konfigurationsdatei auf einem lokalen Laufwerk.
- **Netzwerkfreigabe** zum Speichern der Konfigurationsdatei auf einer CIFS- oder NFS-Freigabe.
- **HTTP oder HTTPS** zum Speichern der Konfigurationsdatei in einer lokalen Datei mittels HTTP/HTTPS-Dateiübertragung.

ANMERKUNG: Je nach Speicherorttyp müssen Sie die Netzwerkeinstellungen oder HTTP/HTTPS-Einstellungen eingeben. Wenn Proxy für HTTP/HTTPS konfiguriert ist, sind auch die Proxy-Einstellungen erforderlich.

4. Wählen Sie die Komponenten aus, die Sie zum Sichern der Konfiguration benötigen für.
5. Wählen Sie den **Exporttypen** aus. Die folgenden Optionen sind verfügbar:
   - **Einfach**
   - **Ersatzexport**
   - **Klonexport**
6. Wählen Sie ein **Export-Dateiformat** aus.
7. Wählen Sie **Zusätzliche Exportelemente** aus.
8. Klicken Sie auf **Exportieren**.

Sichere Startfunktion-Konfiguration über BIOS-Einstellungen oder F2

UEFI Secure Boot ist eine Technologie, die eine große Sicherheitslücke beseitigt, die bei einer Übergabe zwischen der UEFI-Firmware und dem UEFI-Betriebssystem (OS) auftreten kann. Beim sicheren UEFI-Start wird jede Komponente in der Kette validiert und anhand eines bestimmten Zertifikats autorisiert, bevor sie geladen oder ausgeführt werden darf. Secure Boot eliminiert die Bedrohung und bietet eine Software-Identitätsprüfung für jeden Schritt des Startvorgangs – Plattform-Firmware, Erweiterungskarten und OS-Boot-Loader.

Das Unified Extensible Firmware Interface Forum (UEFI) – ein Branchenverband, der Standards für vor dem Start ausgeführte Software entwickelt – definiert Secure Boot in der UEFI-Spezifikation. Anbieter von Computersystemen, Erweiterungskarten und Betriebssystemen arbeiten an dieser Spezifikation zusammen, um die Interoperabilität zu fördern. Als Teil der UEFI-Spezifikation stellt Secure Boot einen branchenweiten Standard für die Sicherheit in der Pre-Boot-Umgebung dar.

Im aktivierten Zustand verhindert UEFI Secure Boot das Laden der unsignierten UEFI-Gerätetreiber, zeigt eine Fehlermeldung an und hindert das Gerät am Arbeiten. Sie müssen Secure Boot deaktivieren, um die nicht signierten Gerätetreiber zu laden.

Ab der 14. Generation von Dell PowerEdge-Servern können Sie die Secure Boot-Funktion über verschiedene Schnittstellen (RACADM, WSMAN, REDFISH und LC-UI) aktivieren oder deaktivieren.

Zulässige Dateiformate

Die Secure Boot-Richtlinie enthält nur einen Schlüssel im PK, es können sich jedoch mehrere Schlüssel im KEK befinden. Im Idealfall verwaltet entweder der Hersteller oder Besitzer der Plattform den passenden privaten Schlüssel zum PK. Die zu den öffentlichen Schlüsseln im KEK passenden privaten Schlüssel werden von Dritten (z. B. Betriebssystem- und Geräteanbietern) aufbewahrt. Auf diese Weise können Plattformbesitzer oder Dritte Einträge in der db oder dbx eines bestimmten Systems hinzufügen oder entfernen.

Die Secure Boot-Richtlinie verwendet db und dbx, um die Ausführung von Abbilddateien vor dem Start zu autorisieren. Damit eine Abbilddatei ausgeführt wird, muss sie einem Schlüssel oder Hash-Wert in der db zugeordnet werden und nicht einem Schlüssel oder Hash-Wert in der dbx. Jeder Versuch, den Inhalt der db oder dbx zu aktualisieren, muss von einem privaten PK oder KEK signiert werden. Jeder Versuch, den Inhalt des PK oder KEK zu aktualisieren, muss von einem privaten PK signiert werden.

Tabelle 14. Zulässige Dateiformate

Richtlinienkomponente	Zulässige Dateiformate	Zulässige Dateierweiterungen	Max. erlaubte Datensätze
PK	X.509-Zertifikat (nur binäres DER-Format)	1. `.cer` 2. `.der` 3. .crt	Eins
KEK	X.509-Zertifikat (nur binäres DER-Format) Öffentlicher Schlüsselspeicher	1. `.cer` 2. `.der`	Mehr als einer

Tabelle 14. Zulässige Dateiformate (fortgesetzt)

Richtlinienkomponente	Zulässige Dateiformate	Zulässige Dateierweiterungen	Max. erlaubte Datensätze
		3. .crt 4. .pbk	
DB und DBX	X.509-Zertifikat (nur binäres DER-Format) EFI-Image (System-BIOS berechnet und importiert das Image-Digest)	1. .cer 2. .der 3. .crt 4. .efi	Mehr als einer

Die Einstellungen für Secure Boot können in den System-BIOS-Einstellungen durch Klicken auf „Systemsicherheit“ aufgerufen werden. Um zu den System-BIOS-Einstellungen zu gelangen, drücken Sie F2, wenn das Firmenlogo während des POST angezeigt wird.

- Standardmäßig ist Secure Boot deaktiviert und die Secure Boot-Richtlinie auf Standard eingestellt. Um die Secure Boot-Richtlinie zu konfigurieren, müssen Sie Secure Boot aktivieren.
- Wenn der Secure Boot-Modus auf Standard eingestellt ist, zeigt dies an, dass das System über Standard-Zertifikate und Image-Digests verfügt oder werkseitig ein Hash-Wert geladen wurde. Damit wird die Sicherheit von Standard-Firmware, Treibern, Options-ROMs und Boot Loadern gewährleistet.
- Zur Unterstützung neuer Treiber oder Firmware auf einem Server muss das entsprechende Zertifikat in die Datenbank des Secure Boot-Zertifikatsspeichers eingetragen werden. Daher muss die Secure Boot-Richtlinie auf Benutzerdefiniert eingestellt werden.

Ist die Secure Boot-Richtlinie auf Benutzerdefiniert eingestellt, erbt sie die standardmäßig im System geladenen Standardzertifikate und Image-Digests, die Sie ändern können. Mit einer als Benutzerdefiniert konfigurierten Secure Boot-Richtlinie können Sie Aktionen wie Anzeigen, Exportieren, Importieren, Löschen, Alles löschen, Zurücksetzen und Alles zurücksetzen ausführen. Mit diesen Operationen können Sie die Secure Boot-Richtlinien konfigurieren.

Durch die Konfiguration der Secure Boot-Richtlinie als Benutzerdefiniert können die Optionen zur Verwaltung des Zertifikatsspeichers mit verschiedenen Aktionen wie Exportieren, Importieren, Löschen, Alle löschen, Zurücksetzen und Alles zurücksetzen für PK, KEK, DB und DBX verwendet werden. Durch Klicken auf den entsprechenden Link können Sie die Richtlinie auswählen (PK/KEK/DB/DBX), an der Sie die Änderung vornehmen möchten und die entsprechende Aktionen durchführen. Jeder Abschnitt verfügt über Links, um die Operationen Import, Export, Löschen und Zurücksetzen auszuführen. Links sind je nach zutreffender Anwendung aktiv, was von der jeweils aktuellen Konfiguration abhängt. Die Operationen Alle löschen und Alle zurücksetzen wirken sich auf alle Richtlinien aus. Alle löschen löscht alle Zertifikate und Image-Digests in der benutzerdefinierten Richtlinie und Alle zurücksetzen stellt alle Zertifikate und Image-Digests aus dem Standard-Zertifikatsspeicher wieder her.

BIOS recovery

Mit der BIOS-Wiederherstellungsfunktion können Sie das BIOS von einem gespeicherten Image aus manuell wiederherstellen. Das BIOS wird geprüft, wenn das System eingeschaltet ist. Wenn ein beschädigtes oder gefährdetes BIOS gefunden wird, wird eine Fehlermeldung angezeigt. Sie können dann den BIOS-Wiederherstellungsprozess mit RACADM einleiten. Informationen zum Durchführen einer manuellen BIOS-Wiederherstellung finden Sie im Referenzhandbuch für die iDRAC RACADM-Befehlszeilenschnittstelle unter https://www.dell.com/idracmanuals.

4

Plugin Management

A plugin is individually packaged in a DUP. Plugins do not get removed on iDRAC reboot, reset, or AC cycles, they can only be removed by iDRAC sanitize operation or LC wipe operation. You can enable or disable the plugins. When enabled, plugins are only installed but not started.

To manage plugins from iDRAC GUI, go to **iDARC Settings** > **Settings** > **Plugins**.

NOTE: You must have Login privilege and Control and Configure Privilege to install, update, and remove the plugins. You can only view the installed plugins with Login privilege.

Following are the information available in Plugin inventory:

- Name — Name of the plugin. Maximum number of characters-512
- Version — Version of Installed plugin
- State — Enabled / Disabled
- Status — Starting, Not Started, Running, Stopping, Updating, Stopped: Disabled, Stopped: Installed— No Hardware, Stopped: Installed— Version Dependency, Stopped: Plugin Failure, Stopped: Internal Error — Unknown Error, Stopped: Plugin Conflict.
- Manufacture — Name of the company, maximum 512characters
- ReleaseDate — Date of creation of DUP
- SoftwareId — Component ID

Installing/Upgrading plugin

1. Download Plugin from Dell.com
2. Go to iDRAC Update page
3. Select Plugin DUP file
4. Install Plugin

   NOTE: If a plugin is valid, a success message is shown after the plugin installed. If the hardware is not present, then an LC message is logged indicating that Plugin is not started. If the plugin is invalid, an error message is displayed.

Remove Plugin

1. Go to Plugins page - **iDARC Settings** > **Settings** > **Plugins**
2. Select Uninstall/Remove
3. Plugin is then stopped and removed from iDRAC.

When a non-SDL (Non Supported Device List) card is installed, iDRAC cannot detect a SDK plugin. You need to manually find and install the SDK plugin. iDRAC firmware downgrade can result in plugins being disabled or limited functionality.

NOTE: Installing, updating, or removing a plugin takes less than 5 minutes.

5

iDRAC konfigurieren

Mit iDRAC können Sie iDRAC-Eigenschaften konfigurieren, Benutzer einrichten und Warnungen für die Ausführung von Remote-Managementaufgaben einrichten.

Stellen Sie vor der Konfiguration von iDRAC sicher, dass die iDRAC-Netzwerkeinstellungen und ein unterstützter Browser konfiguriert und die erforderlichen Lizenzen aktualisiert sind. Weitere Informationen zur lizenzierbaren Funktion im iDRAC finden Sie unter iDRAC-Lizenzen auf Seite 20.

Sie können iDRAC über die folgenden Komponenten konfigurieren:

- iDRAC-Weboberfläche
- RACADM
- Remote-Dienste (siehe *Dell Lifecycle Controller Remote Services-Benutzerhandbuch*)
- IPMITool (siehe *Benutzerhandbuch zu den Dienstprogrammen des Dell OpenManage Baseboard Management Controller*)

So konfigurieren Sie iDRAC:

1. Melden Sie sich bei iDRAC an.
2. Ändern der Netzwerkeinstellungen falls erforderlich.

   ANMERKUNG: Wenn Sie die iDRAC-Netzwerkeinstellungen während der Einrichtung der iDRAC-IP-Adresse über das Dienstprogramm für die iDRAC-Einstellungen konfiguriert haben, können Sie diesen Schritt übergehen.

3. Konfigurieren Sie Schnittstellen für den Zugriff auf iDRAC.
4. Konfigurieren Sie die Anzeige auf der Frontblende.
5. Konfigurieren Sie ggf. den Systemstandort.
6. Konfigurieren Sie ggf. Zeitzone und Network Time Protocol (NTP).
7. Bauen Sie eine der folgenden alternativen Verfahren für die Kommunikation mit iDRAC auf:
   - Serielle IPMI- oder RAC-Verbindung
   - Serielle IPMI-Verbindung über LAN
   - IPMI über LAN
   - SSH
8. Erforderliche Zertifikate abrufen.
9. Hinzufügen und Konfiguration von iDRAC-Benutzern mit Berechtigungen.
10. Konfigurieren und aktivieren Sie E-Mail-Warnungen, SNMP-Traps oder IPMI-Warnungen.
11. Einrichten der Strombegrenzungsrichtlinie falls erforderlich.
12. Bildschirm des letzten Systemabsturzes anzeigen
13. Konfigurieren Sie ggf. die virtuelle Konsole und die virtuellen Datenträger.
14. Konfigurieren Sie ggf. die vFlash SD-Karte.
15. Richten Sie ggf. das erste Startlaufwerk ein.
16. Stellen Sie das Betriebssystem ggf. auf iDRAC-Passthrough.

Themen:

- iDRAC-Informationen anzeigen
- Netzwerkeinstellungen ändern
- Chiffresammlungs-Auswahl
- Modus FIPS (Konfiguration)
- Dienste konfigurieren
- Using VNC client to manage remote server
- Anzeige auf der Frontblende konfigurieren
- Das Konfigurieren von Zeitzone und NTP
- Erstes Startlaufwerk einstellen
- Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough

- Zertifikate abrufen
- Mehrere iDRACs über RACADM konfigurieren
- Zugriff zum Ändern der iDRAC-Konfigurationseinstellungen auf einem Host-System deaktivieren

iDRAC-Informationen anzeigen

Sie können die iDRAC-Basiseigenschaften anzeigen.

iDRAC-Informationen über die Webschnittstelle anzeigen

Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Overview (Übersicht)**, um die folgenden Informationen zu iDRAC anzuzeigen. Informationen zu den Eigenschaften finden Sie in der *iDRAC Online-Hilfe*.

iDRAC-Informationen

- Gerätetyp
- Hardwareversion
- Firmware-Version
- Firmware-Aktualisierung
- RAC-Uhrzeit
- IPMI-Version
- Anzahl von möglichen Sitzungen
- Anzahl von aktuellen Sitzungen
- IPMI-Version

iDRAC-Service-Modul

- Status

Verbindungsanzeige

- Status
- Switch-Verbindungs-ID
- Switch-Portverbindung-ID

Aktuelle Netzwerkeinstellungen

- iDRAC MAC-Adresse
- Aktive NIC-Schnittstelle
- DNS-Domänenname

Aktuelle IPv4-Einstellung

- IPv4 aktiviert
- DHCP
- Aktuelle IP-Adresse
- Aktuelle Subnetzmaske
- Aktuelles Gateway
- DHCP zum Abrufen der DNS-Serveradresse verwenden
- Gegenwärtig bevorzugter DNS-Server
- Gegenwärtiger alternativer DNS-Server

Gegenwärtige IPv6-Einstellungen

- IPv6 aktivieren
- Autokonfiguration
- Aktuelle IP-Adresse
- Aktuelles IP-Gateway
- Link-Local-Adresse
- Verwenden von DHCPv6 zum Abrufen der DNS
- Gegenwärtig bevorzugter DNS-Server
- Gegenwärtiger alternativer DNS-Server

iDRAC-Informationen über RACADM anzeigen

Informationen zum Anzeigen von iDRAC-Informationen mithilfe von RACADM finden Sie unter den Unterbefehlen `getsysinfo` oder `get` unter *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Netzwerkeinstellungen ändern

Nach der Konfiguration der iDRAC Netzwerkeinstellungen unter Verwendung des Dienstprogramms „iDRAC Settings“ können Sie die Einstellungen auch über die iDRAC-Webschnittstelle, RACADM, Lifecycle Controller und Server Administrator (nach dem Start des Betriebssystems) ändern. Weitere Informationen zu den Tools und Berechtigungseinstellungen finden Sie in den jeweiligen Benutzerhandbüchern.

Zum Ändern der Netzwerkeinstellungen über die iDRAC-Web-Schnittstelle oder RACADM müssen Sie über Berechtigungen zum **Konfigurieren** verfügen.

ANMERKUNG: Durch das Ändern der Netzwerkeinstellungen werden möglicherweise die aktuellen Netzwerkverbindungen mit iDRAC beendet.

Netzwerkeinstellungen über die Weboberfläche ändern

So ändern Sie die iDRAC-Netzwerkeinstellungen:

1. Navigieren Sie in der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Konnektivität** > **Netzwerk** > **Netzwerkeinstellungen**. Die Seite **Netzwerk** wird angezeigt.
2. Geben Sie Netzwerkeinstellungen, allgemeine Einstellungen, IPv4, IPv6, IPMI und/oder VLAN-Einstellungen je nach Bedarf an und klicken Sie auf **Anwenden**.

   Wenn Sie unter **Netzwerkeinstellungen** die Option **Autom. dedizierter NIC** auswählen, wenn der iDRAC seine NIC-Auswahl als freigegebenes LOM (1, 2, 3 oder 4) hat und eine Verbindung auf der iDRAC-dedizierten NIC erkannt wird, ändert der iDRAC seine NIC-Auswahl, um die dedizierte NIC zu verwenden. Wird kein Link auf der dedizierten NIC erkannt, verwendet iDRAC das freigegebene LOM. Der Wechsel von freigegebenem zu dediziertem Timeout dauert fünf Sekunden und von dediziertem zu freigegebenem 30 Sekunden. Sie können diesen Timeout-Wert mithilfe von RACADM oder WSMan konfigurieren.

   Weitere Informationen zu den verschiedenen Feldern finden Sie in der *iDRAC-Online-Hilfe*.

   ANMERKUNG: Wenn iDRAC DHCP verwendet und über ein Leasing seiner IP-Adresse verfügt, wird diese für den DHCP-Server-Adressenpool freigegeben, wenn NIC, Ipv4 oder DHCP deaktiviert ist.

Netzwerkeinstellungen über einen lokalen RACADM ändern

Um eine Liste verfügbarer Netzwerkeigenschaften zu erstellen, verwenden Sie den Befehl

```
racadm get iDRAC.Nic
```

Wenn DHCP zur Ermittlung einer IP-Adresse verwendet werden soll, kann der folgende Befehl zum Schreiben des Objekts `DHCPEnable` und zum Aktivieren dieser Funktion verwendet werden.

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

Das folgende Beispiel zeigt, wie der Befehl zur Konfiguration benötigter LAN-Netzwerkeigenschaften verwendet werden kann:

```
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
```

ANMERKUNG: Wenn `iDRAC.Nic.Enable` auf **0** gesetzt ist, wird das iDRAC-LAN selbst dann deaktiviert, wenn DHCP aktiviert ist.

IP-Filterung konfigurieren

Verwenden Sie neben der Benutzerauthentifizierung die folgenden Optionen für zusätzliche Sicherheit, während Sie auf iDRAC zugreifen:

- IP-Filterung beschränkt den IP-Adressbereich der Clients, die auf iDRAC zugreifen. Dabei wird die IP-Adresse einer eingehenden Anmeldung mit dem angegebenen Bereich verglichen, und der Zugang zu iDRAC wird nur über eine Management Station genehmigt, deren IP-Adresse sich innerhalb dieses Bereichs befindet. Alle anderen Anmeldeaufforderungen werden abgewiesen.
- Wenn fehlgeschlagene Anmeldeversuche von einer bestimmten IP-Adresse wiederholt auftreten, wird die Adresse für eine vorgewählte Zeitspanne daran gehindert, sich bei iDRAC anzumelden. Nach zwei erfolglosen Anmeldeversuchen können Sie sich erst nach 30 Sekunden erneut anmelden. Nach mehr als zwei erfolglosen Anmeldeversuchen können Sie sich erst nach 60 Sekunden erneut anmelden.

ANMERKUNG: Diese Funktion unterstützt bis zu 5 IP-Bereiche. Sie können diese Funktion mithilfe von RACADM und Redfish anzeigen/einstellen.

Wenn sich Anmeldefehler von einer spezifischen IP-Adresse aus ansammeln, werden sie durch einen internen Zähler registriert. Wenn sich der Benutzer erfolgreich anmeldet, wird die Aufzeichnung der Fehlversuche gelöscht und der interne Zähler zurückgesetzt.

ANMERKUNG: Wenn Anmeldeversuche von der Client-IP-Adresse abgelehnt werden, können einige SSH-Clients die Meldung anzeigen: `ssh exchange identification: Connection closed by remote host.`

IP-Filterung über die iDRAC-Webschnittstelle konfigurieren

Sie müssen über Berechtigungen zum Konfigurieren verfügen, um diese Schritte auszuführen.

So konfigurieren Sie die IP-Filterung:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **iDRAC-EinstellungenKonnektivitätNetzwerkNetzwerkeinstellungenErweiterte Netzwerkeinstellungen**.
   Die Seite **Netzwerk** wird angezeigt.
2. Klicken Sie auf **Advanced Network Settings** (Erweiterte Netzwerkeinstellungen).
   Die Seite **Netzwerksicherheit** wird angezeigt.
3. Legen Sie die IP-Filterungseinstellungen mithilfe von **IP Range Address** (IP-Adressbereich) und **IP Range Subnet Mask** (Subnetzmaske für IP-Bereich) fest.
   Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.
4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.
   Federal Information Processing Standards – FIPS sind von Regierungseinrichtungen in den USA und ihren Vertragslieferanten verwendete Standards. FIPS-Modus dient dazu, die Anforderungen von FIPS 140-2 Ebene 1 zu erfüllen. Weitere Informationen über FIPS finden Sie im Benutzerhandbuch zu FIPS für iDRAC und CMC für Nicht-MX-Plattformen.
   ANMERKUNG: Beim Aktivieren des **FIPS Mode** (FIPS-Modus) werden die Standardeinstellungen von iDRAC wiederhergestellt.

#IP-Filterung über RACADM konfigurieren

Sie müssen über Berechtigungen zum Konfigurieren verfügen, um diese Schritte auszuführen.

Verwenden Sie zum Konfigurieren der IP-Filterung die folgenden RACADM-Objekte in der Gruppe `iDRAC.IPBlocking`:

- RangeEnable
- RangeAddr
- RangeMask

Die Eigenschaft `RangeMask` wird sowohl auf die eingehende IP-Adresse als auch auf die Eigenschaft `RangeAddr` angewendet. Sind die Ergebnisse identisch, wird für die eingehende Anmeldeaufforderung der Zugriff auf den iDRAC zugelassen. Die Anmeldung von IP-Adressen außerhalb dieses Bereichs führt zu einer Fehlermeldung.

ANMERKUNG: Das Konfigurieren der IP-Filterung unterstützt bis zu 5 IP-Bereiche.

Die Anmeldung wird fortgeführt, wenn der folgende Ausdruck Null entspricht:

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

&

Bitweise UND der Mengen

^

Bitweise ausschließliche ODER

Beispiele für die IP-Filterung

Die folgenden RACADM-Befehle blockieren alle IP-Adressen außer 192.168.0.57:

```
racadm set iDRAC.IPBlocking.RangeEnable 1
racadm set iDRAC.IPBlocking.RangeAddr 192.168.0.57
racadm set iDRAC.IPBlocking.RangeMask 255.255.255.255
```

Zur Beschränkung von Anmeldungen auf einen Satz von vier angrenzenden IP-Adressen (z. B. 192.168.0.212 bis 192.168.0.215) wählen Sie alle außer den niederwertigsten zwei Bits in der Maske aus:

```
racadm set iDRAC.IPBlocking.RangeEnable 1
racadm set iDRAC.IPBlocking.RangeAddr 192.168.0.212
racadm set iDRAC.IPBlocking.RangeMask 255.255.255.252
```

Das letzte Byte der Bereichsmaske ist auf 252 eingestellt, das Dezimaläquivalent von 11111100b.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Chiffresammlungs-Auswahl

Chiffresammlungs-Auswahl kann verwendet werden, um die Verschlüsselung in der iDRAC- oder Client-Kommunikation einzuschränken und zu bestimmen, wie sicher die Verbindung sein wird. Sie bietet eine weitere Stufe der Filterung der effektiven TLS-Chiffresammlung. Diese Einstellungen können über die iDRAC-Webschnittstelle, RACADM und WSMAN-Befehlszeilenschnittstellen konfiguriert werden.

Chiffresammlungs-Auswahl über die iDRAC-Webschnittstelle konfigurieren

VORSICHT: Die Verwendung des OpenSSL-Chiffrierbefehls zum Parsen von Zeichenfolgen mit ungültiger Syntax kann zu unerwarteten Fehlern führen.

ANMERKUNG: Hierbei handelt es sich um eine erweiterte Sicherheitsoption. Bevor Sie diese Option konfigurieren, vergewissern Sie sich, dass Sie die folgenden Punkte genau kennen:

- Die OpenSSL-Chiffriersyntax und ihre Verwendung.
- Tools und Vorgehensweisen zur Validierung der resultierenden Chiffresammlungs-Konfiguration, um sicherzustellen, dass die Ergebnisse mit den Erwartungen und Anforderungen übereinstimmen.

ANMERKUNG: Bevor Sie die erweiterten Einstellungen für TLS-Chiffresammlungen konfigurieren, stellen Sie sicher, dass Sie einen unterstützten Webbrowser verwenden.

So fügen Sie benutzerdefinierte Verschlüsselungszeichenfolgen (Cipher Strings) hinzu:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC-Einstellungen** > **Dienste** > **Webserver**.
2. Klicken Sie auf **Verschlüsselungszeichenfolge festlegen** unter der Option **Benutzerdefinierte Verschlüsselungszeichenfolge**. Die Seite **Benutzerdefinierte Verschlüsselungszeichenfolge festlegen** wird angezeigt.
3. Geben Sie im Feld **Benutzerdefinierte Verschlüsselungszeichenfolge** eine gültige Zeichenfolge ein und klicken Sie auf **Verschlüsselungszeichenfolge festlegen**.

ANMERKUNG: Weitere Informationen zu Verschlüsselungszeichenfolgen (Cipher Strings) finden Sie unter www.openssl.org/docs/man1.0.2/man1/ciphers.html.

4. Klicken Sie auf **Anwenden**.
   Durch Einstellen der benutzerdefinierten Verschlüsselungszeichenfolge wird die aktuelle iDRAC-Sitzung beendet. Warten Sie ein paar Minuten, bevor Sie eine neue iDRAC-Sitzung öffnen.

Die von iDRAC auf Port 5000 unterstützten Chiffren sind:

ssl-enum-ciphers:

TSLv1.1-Chiffren:
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_RC4_128_SHA (secp256r1)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_RC4_128_MD5 (rsa 2048)
- TLS_RSA_WITH_RC4_128_SHA (rsa 2048)
- TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048)

TLSv1.2-Chiffren:
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)
- TLS_ECDHE_RSA_WITH_RC4_128_SHA (secp256r1)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_RC4_128_MD5 (rsa 2048)
- TLS_RSA_WITH_RC4_128_SHA (rsa 2048)
- TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048)

Chiffresammlungs-Auswahl mithilfe von RACADM konfigurieren

Zum Konfigurieren der Chiffresammlungs-Auswahl mithilfe von RACADM verwenden Sie einen der folgenden Befehle:
- `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`

Weitere Informationen zu diesen Objekten finden Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter dell.com/idracmanuals.

Modus FIPS (Konfiguration)

FIPS ist ein Computer-Sicherheitsstandard, den US-Regierungsbehörden und Vertragspartner verwenden müssen. Ab iDRAC-Version 2.40.40.40 unterstützt iDRAC das Aktivieren des FIPS-Modus.

iDRAC wird offiziell zertifiziert zur Unterstützung des FIPS-Modus in der Zukunft.

Unterschied zwischen FIPS-Modus-unterstützt und FIPS-validiert

Software, die durch das Durchführen des „Cryptographic Module Validation Program“ (Validierungsprogramm für das Kryptografiemodul) validiert wurde, wird als FIPS-validiert bezeichnet. Aufgrund der Zeitspanne, die für eine vollständige FIPS-Validierung benötigt wird, sind nicht alle Versionen von iDRAC validiert. Weitere Informationen zum aktuellen Status der FIPS-Validierung für iDRAC finden Sie auf der Seite Cryptographic Module Validation Program (Validierungsprogramm für das Kryptografiemodul) auf der NIST-Website.

FIPS-Modus aktivieren

VORSICHT: Durch das Aktivieren des FIPS-Modus wird iDRAC auf die standardmäßigen Werkseinstellungen zurückgesetzt. Wenn Sie die Einstellungen wiederherstellen möchten, sichern Sie das Server-Konfigurationsprofil (SCP) vor dem Aktivieren des FIPS-Modus, und stellen Sie das SCP nach dem Neustart von iDRAC wieder her.

ANMERKUNG: Wenn Sie Sie iDRAC-Firmware erneut installieren oder aktualisieren, wird der FIPS-Modus deaktiviert.

Aktivieren des FIPS-Modus unter Verwendung des Internets

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Connectivity (Konnektivität)** > **Network (Netzwerk)** > **Network Settings (Netzwerkeinstellungen)** > **Advanced Network Settings (Erweiterte Netzwerkeinstellungen)**.
2. Unter **FIPS-Modus** wählen Sie **Aktiviert** und klicken auf **Anwenden**.

   ANMERKUNG: Beim Aktivieren des FIPS-Modus wird iDRAC auf die Standardeinstellungen zurückgesetzt.

3. Es wird eine Meldung angezeigt, in der Sie aufgefordert werden, die Änderung zu bestätigen. Klicken Sie auf **OK**. iDRAC wird im FIPS-Modus neu gestartet. Warten Sie mindestens 60 Sekunden, bevor Sie erneut eine Verbindung zu iDRAC herstellen.
4. Installieren Sie ein vertrauenswürdiges Zertifikat für iDRAC.

   ANMERKUNG: Das Standard-SSL-Zertifikat ist nicht zulässig im FIPS-Modus.

ANMERKUNG: Einige iDRAC-Schnittstellen, wie z. B. die standardmäßig konformen Implementierungen von IPMI und SNMP unterstützen keine FIPS-Übereinstimmung.

FIPS-Modus über RACADM aktivieren

Verwenden Sie RACADM-CLI, um den folgenden Befehl auszuführen:

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

Deaktivieren des FIPS-Modus

Zum Deaktivieren des FIPS-Modus müssen Sie einen Reset von iDRAC auf die werksseitigen Voreinstellungen durchführen.

Dienste konfigurieren

Sie können die folgenden Dienste auf iDRAC konfigurieren und aktivieren:

Lokale Konfiguration	Deaktivieren Sie den Zugriff auf die iDRAC-Konfiguration (vom Host-System) über den lokalen RACADM und das Dienstprogramm für iDRAC-Einstellungen.
Webserver	Aktivieren Sie den Zugriff auf die iDRAC-Weboberfläche. Wenn Sie die Weboberfläche deaktivieren, wird auch der Remote-RACADM deaktiviert. Verwenden Sie den lokalen RACADM, um den Webserver und den Remote-RACADM erneut zu aktivieren.
SEKM-Konfiguration	Aktiviert die sichere Enterprise-Schlüssel-Verwaltungsfunktion auf dem iDRAC mithilfe einer Client-Server-Architektur.
SSH	Greifen Sie über die Firmware-RACADM auf iDRAC zu.
Remote-RACADM	Greifen Sie remote auf iDRAC zu.
SNMP-Agent	Aktiviert Unterstützung für SNMP-Anfragen (GET-, GETNEXT- und GETBULK-Vorgänge) in iDRAC.
Automatisierter System-Wiederherstellungsagent	Aktivieren Sie den Bildschirm „Letzter Systemabsturz“.
Redfish	Aktiviert Unterstützung für Redfish RESTful-API.
VNC-Server	Aktivieren Sie VNC-Server mit oder ohne SSL-Verschlüsselung.

Services unter Verwendung der Weboberfläche konfigurieren

Dienste über die iDRAC-Weboberfläche konfigurieren:

1. Gehen Sie in der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Dienste**.
   Die Seite **Dienste** wird angezeigt.
2. Geben Sie die erforderlichen Informationen ein und klicken Sie auf **Anwenden**.
   Weitere Informationen zu den verschiedenen Einstellungen finden Sie in der *iDRAC-Online-Hilfe*.

   ANMERKUNG: Aktivieren Sie nicht das Kontrollkästchen **Verhindern, dass diese Seite zusätzliche Dialoge erstellt**. Durch Auswahl dieser Option wird verhindert, dass Sie Dienste konfigurieren.

   Sie können **SEKM** auch auf der Seite der iDRAC-Einstellungen konfigurieren. Klicken Sie auf **iDRAC-Einstellungen** > **Dienste** > **SEKM-Konfiguration**.

   ANMERKUNG: Detaillierte Schritt-für-Schritt-Verfahren zum Konfigurieren von SEKM finden Sie in der *iDRAC Online-Hilfe*.

   ANMERKUNG: Wenn der Modus **Sicherheit (Verschlüsselung)** von **Keine** zu **SEKM** geändert wird, steht der Echtzeitberichterstellungsjob nicht zur Verfügung. Er wird jedoch der Liste der bereitgestellten Jobs hinzugefügt. Der Echtzeit-Job ist jedoch erfolgreich, wenn der Modus von **SEKM** auf **Keine** geändert wird.

   Beim Ändern des Werts im Feld **Nutzername** im Clientzertifikat-Abschnitt auf dem KeySecure-Server (z. B.: Änderung des Werts von **Allgemeiner Name** zu **Nutzer-ID**) muss Folgendes sichergestellt werden:

   a. Bei Verwendung eines bestehenden Kontos:
      - Überprüfen Sie im iDRAC SSL-Zertifikat, dass anstelle des Felds **Allgemeiner Name** das Feld **Nutzername** nun dem auf dem KMS vorhandenen Nutzernamen entspricht. Wenn dies nicht der Fall ist, müssen Sie das Nutzername-Feld einrichten und das SSL-Zertifikat erneut generieren, um es auf dem KMS anzumelden und auf dem iDRAC erneut zu laden.

   b. Bei Verwendung eines neues Nutzerkontos:
      - Stellen Sie sicher, dass die Zeichenkette **Nutzername** dem Nutzername-Feld im iDRAC-SSL-Zertifikat entspricht.
      - Wenn sie nicht übereinstimmen, müssen Sie den Nutzernamen und das Kennwort der iDRAC KMS-Attribute erneut konfigurieren.
      - Nachdem überprüft wurde, ob das Zertifikat einen Nutzernamen enthält, muss nur noch der Schlüsselbesitz vom alten Benutzer auf den neuen Besitzer geändert werden, damit der neu erstellte KMS-Nutzername übereinstimmt.

   Wenn Sie Vormetric Data Security Manager als KMS verwenden, vergewissern Sie sich, dass das Feld „Common Name“ (CN) im iDRAC SSL-Zertifikat mit dem Hostnamen übereinstimmt, der zu Vormetric Data Security Manager hinzugefügt wurde. Andernfalls wird das Zertifikat möglicherweise nicht erfolgreich importiert.

ANMERKUNG:

- Die Option **Neueingabe** wird deaktiviert, wenn `racadm sekm getstatus`-Berichte als **Fehlgeschlagen** angezeigt werden.
- SEKM unterstützt nur **Allgemeiner Name**, **Nutzer-ID** oder **Organisationseinheit** im Feld **Nutzername** des Client-Zertifikats.
- Wenn Sie ein Drittanbieter-CA zur Anmeldung des iDRAC-CSR verwenden, müssen Sie sicherstellen, dass dies den Wert **UID** für das Feld **Nutzername** im Client-Zertifikat unterstützt. Wird dies nicht unterstützt, verwenden Sie **Allgemeiner Name** als Wert für das Feld **Nutzername**.
- Wenn Sie die Felder „Nutzername“ und „Kennwort“ verwenden, stellen Sie sicher, dass der KMS-Server diese Attribute unterstützt.

ANMERKUNG: Bei KeySecure-Schlüsselverwaltungsservern

- müssen Sie bei der Erstellung einer SSL-Zertifikatanfrage die IP-Adresse des Schlüsselverwaltungsservers in das Feld **Alternativer Servername** eingeben.
- Die IP-Adresse muss das folgende Format aufweisen: IP:xxx.xxx.xxx.xxx.

Dienste über RACADM konfigurieren

Um Dienste über RACADM zu aktivieren und konfigurieren, verwenden Sie den Befehl `set` mit den Objekten in den folgenden Objektgruppen:

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

Weitere Informationen zu diesen Objekten finden Sie unter *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

SEKM-Funktionen

Im folgenden sind die SEKM-Funktionen aufgelistet, die in iDRAC verfügbar sind:

1. **SEKM-Richtlinie zum Löschen von Schlüsseln** – iDRAC enthält eine Richtlinieneinstellung, mit der Sie iDRAC so konfigurieren können, dass alte ungenutzte Schlüssel auf dem Schlüsselverwaltungsserver (KMS) gelöscht werden, wenn der Vorgang zur Schlüsselneuerstellung ausgeführt wird. Sie können für iDRAC das Lese-Schreib-Attribut von KMSKeyPurgePolicy auf einen der folgenden Werte einstellen:
   - Alle Schlüssel behalten: Dies ist die Standardeinstellung, bei der iDRAC alle Schlüssel auf der KMS während der Durchführung der Schlüsselneuerstellung unangetastet lässt.
   - N- und N-1-Schlüssel aufbewahren: iDRAC löscht alle Schlüssel auf dem KMS außer dem aktuellen (N) und dem vorherigen Schlüssel (N-1) während der Durchführung der Schlüsselneuerstellung.
2. **Schlüssellöschung für KMS auf SEKM deaktivieren**: Im Rahmen der SEKM-Lösung (Secure Enterprise Key Manager) ermöglicht iDRAC es, das SEKM auf dem iDRAC zu deaktivieren. Nach der Deaktivierung von SEKM werden die von iDRAC auf dem KMS generierten Schlüssel nicht verwendet und bleiben im KMS. Diese Funktion ermöglicht es iDRAC, diese Schlüssel zu löschen, wenn SEKM deaktiviert ist. iDRAC bietet eine neue Option „-purgeKMSKeys“ zum vorhandenen Legacy-Befehl „racadm sekm disable“, mit dem Sie Schlüssel auf dem KMS löschen können, wenn SEKM auf iDRAC deaktiviert ist.

   ANMERKUNG: Wenn SEKM bereits deaktiviert ist und Sie alte Schlüssel löschen möchten, müssen Sie SEKM erneut aktivieren und dann unter Verwendung der Option „-purgeKMSKeys“ deaktivieren.
3. **Schlüsselerstellungsrichtlinie**: Als Teil dieser Version wurde iDRAC mit einer Schlüsselerstellungsrichtlinie vorkonfiguriert. Das Attribut KeyCreationPolicy ist schreibgeschützt und wird auf den Wert „Key per iDRAC“ festgelegt.
   - Das schreibgeschützte iDRAC-Attribut iDRAC.SEKM.KeyIdentifierN meldet die Schlüsselkennung, die vom KMS erstellt wurde.

```
racadm get iDRAC.SEKM.KeyIdentifierN
```

- Das schreibgeschützte iDRAC-Attribut iDRAC.SEKM.KeyIdentifierNMinusOne meldet die vorherige Schlüsselkennung nach Durchführung einer Schlüsselneuerstellung.

  ```
  racadm get iDRAC.SEKM.KeyIdentifierNMinusOne
  ```

4. **SEKM-Schlüsselneuerstellung**: iDRAC bietet zwei Optionen zur Schlüsselneuerstellung für Ihre SEKM-Lösung, entweder Schlüsselneuerstellung über iDRAC oder PERC. Es wird empfohlen, iDRAC zur Schlüsselneuerstellung zu verwenden, da dadurch alle SEKM-Secure-fähigen/-aktivierten Geräte neue Schlüssel erhalten.
   - *SEKM iDRAC Schlüsselneuerstellung [Schlüsselneuerstellung auf iDRAC.Embedded.1 FQDD]*: Bei der Durchführung von `racadm sekm rekey iDRAC.Embedded.1` werden alle SEKM-Secure-fähigen/-aktivierten Geräte mit einem neuen Schlüssel von KMS verschlüsselt. Dies ist ein allgemeiner Schlüssel für alle SEKM-aktivierten Geräte. Die iDRAC-Schlüsselneuerstellung kann auch über die iDRAC-GUI erfolgen: **iDRAC Einstellungen** > **Services** > **SEKM-Konfiguration** > **Schlüsselneuerstellung**. Nach der Ausführung dieses Vorgangs kann die Änderung des Schlüssels durch Lesen der Attribute KeyIdentifierN und KeyIdentifierNMinusOne validiert werden.
   - *SEKM PERC Schlüsselneuerstellung (Schlüsselneuerstellung auf Controller [Beispiel RAID.Slot.1-1] FQDD)*: Wenn der Vorgang `racadm sekm rekey <controller FQDD>` durchgeführt wird, wird für den entsprechenden SEKM-fähigen Controller mit dem derzeit aktiven, vom KMS erstellten allgemeinen iDRAC-Schlüssel ein neuer Schlüssel erstellt. Die Schlüsselneuerstellung für den Speicher-Controller kann auch über die iDRAC-GUI erfolgen: **Speicher** > **Controller** > **<Controller FQDD>** > **Aktionen** > **Bearbeiten** > **Sicherheit** > **Sicherheit (Verschlüsselung)** > **Schlüsselneuerstellung**.

Aktivieren oder Deaktivieren der HTTPS-Umleitung

Wenn Sie aufgrund des Zertifikatwarnungs-Problems beim Standard iDRAC-Zertifikat oder zur vorübergehenden Einstellung für den Debug-Modus nicht möchten, dass die automatische HTTP-zu-HTTPS-Umleitung erfolgt, können Sie iDRAC so konfigurieren, dass die Umleitung vom http-Port (Standardeinstellung 80) zum https-Port (Standardeinstellung 443) deaktiviert ist. Standardmäßig ist dieser aktiviert. Sie müssen sich von iDRAC ab- und wieder anmelden, damit diese Einstellung wirksam wird. Wenn Sie diese Funktion deaktivieren, wird eine Warnmeldung angezeigt.

Sie müssen über die Berechtigung zum Konfigurieren von iDRAC verfügen, damit Sie die HTTPS-Umleitung aktivieren oder deaktivieren können.

Beim Aktivieren oder Deaktivieren dieser Funktion wird ein Ereignis in der Lifecycle Controller-Protokolldatei aufgezeichnet.

So deaktivieren Sie die HTTP-zu-HTTPS-Umleitung:

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

So aktivieren Sie die HTTP-zu-HTTPS-Umleitung:

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

So zeigen Sie den Status der HTTP-zu-HTTPS-Umleitung an:

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

Using VNC client to manage remote server

You can use a standard open VNC client to manage the remote server using both desktop and mobile devices such as Dell Wyse PocketCloud. When servers in data centers stop functioning, the iDRAC or the operating system sends an alert to the console on the management station. The console sends an email or SMS to a mobile device with required information and launches VNC viewer application on the management station. This VNC viewer can connect to OS/Hypervisor on the server and provide access to keyboard, video, and mouse of the host server to perform the necessary remediation. Before launching the VNC client, you must enable the VNC server and configure the VNC server settings in iDRAC such as password, VNC port number, SSL encryption, and the time-out value. You can configure these settings using iDRAC Web interface or RACADM.

NOTE: VNC feature is licensed and is available in the iDRAC Enterprise or Datacenter license.

NOTE: You may see VNC login error if you are using Chrome browser.

You can choose from many VNC applications or Desktop clients such as the ones from RealVNC or Dell Wyse PocketCloud.

Two VNC client sessions can be activated simultaneously. Second session is in Read-Only mode.

If a VNC session is active, you can only launch the Virtual Media using Launch Virtual Console and not the Virtual Console Viewer.

If video encryption is disabled, the VNC client starts RFB handshake directly, and an SSL handshake is not required. During VNC client handshake (RFB or SSL), if another VNC session is active or if a Virtual Console session is open, the new VNC client session is rejected. After completion of the initial handshake, VNC server disables Virtual Console and allows only Virtual Media. After termination of the VNC session, VNC server restores the original state of Virtual Console (enabled or disabled).

NOTE:

- While launching a VNC session, if you get an RFB protocol error, change the VNC client settings to High quality and then relaunch the session.
- When iDRAC NIC is in shared mode and the host system is power cycled, the network connection is lost for a few seconds. During this time, if you perform any action in the active VNC client, the VNC session may close. You must wait for timeout (value configured for the VNC Server settings in the **Services** page in iDRAC Web interface) and then re-establish the VNC connection.
- If the VNC client window is minimized for more than 60 seconds, the client window closes. You must open a new VNC session. If you maximize the VNC client window within 60 seconds, you can continue to use it.

Konfigurieren von VNC-Server unter Verwendung der iDRAC-Webschnittstelle

So konfigurieren Sie die VNC-Servereinstellungen:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Configuration (Konfiguration)** > **Virtual Console (Virtuelle Konsole)**. Daraufhin wird die Seite **Virtuelle Konsole** angezeigt.
2. Aktivieren Sie im Abschnitt **VNC-Server** den VNC-Server, geben Sie das Kennwort und die Portnummer ein, und aktivieren oder deaktivieren Sie die SSL-Verschlüsselung.

   Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.
3. Klicken Sie auf **Anwenden**.
   Der VNC-Server ist konfiguriert.

VNC-Server unter Verwendung von RACADM konfigurieren

Verwenden Sie zum Konfigurieren des VNC-Servers den Befehl `set` mit den Objekten in `VNCserver`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Einrichten von VNC Viewer mit SSL-Verschlüsselung

Während der Konfiguration der VNC-Server-Einstellungen in iDRAC muss die SSL-Tunnelanwendung zusammen mit dem VNC-Viewer verwendet werden, um die verschlüsselte SSL-Verbindung mit dem iDRAC-VNC-Server herzustellen, falls die Option **SSL-Verschlüsselung** aktiviert ist.

ANMERKUNG: Die meisten VNC-Clients haben keinen integrierten SSL-Verschlüsselungs-Support.

So konfigurieren Sie die SSL-Tunnel-Anwendung:

1. Konfigurieren Sie den SSL-Tunnel, um eine Verbindung mit `<localhost>:<localport number>` zu akzeptieren. Beispielsweise 127.0.0.1:5930.
2. Konfigurieren Sie den SSL-Tunnel, um eine Verbindung mit `<iDRAC IP address>:<VNC server port Number>` herzustellen. Beispielsweise 192.168.0.120:5901.
3. Starten Sie die Tunnelanwendung.

   Um eine Verbindung zum iDRAC-VNC-Server über den verschlüsselten SSL-Kanal herzustellen, verbinden Sie den VNC-Viewer mit dem localhost (Link-Local-IP-Adresse) und der lokalen Schnittstellennummer (127.0.0.1: <lokale Schnittstellennummer>).

Einrichten von VNC Viewer ohne SSL-Verschlüsselung

Im Allgemeinen müssen alle mit Remote-Frame Buffer (RFB) kompatiblen VNC Viewer über die für den VNC-Server konfigurierte iDRAC-IP-Adresse und -Schnittstellennummer eine Verbindung mit dem VNC-Server herstellen. Wenn bei der Konfiguration der VNC-

Servereinstellungen in iDRAC die Option für die SSL-Verschlüsselung deaktiviert ist, gehen Sie folgendermaßen vor, um eine Verbindung mit dem VNC Viewer herzustellen:

Geben Sie im Dialogfeld **VNC Viewer** die iDRAC-IP-Adresse und die VNC-Schnittstellennummer in das Feld **VNC-Server** ein.

Sie sollte folgendes Format aufweisen: `<iDRAC IP address:VNC port number>`.

Beispiel: Wenn die iDRAC-IP-Adresse 192.168.0.120 und die VNC-Schnittstellennummer 5901 ist, dann geben Sie `192.168.0.120:5901` ein.

Anzeige auf der Frontblende konfigurieren

Sie können die Anzeige der LC- und LE-Anzeigen auf der Frontblende des Managed System konfigurieren.

Bei Rack- und Tower-Servern sind zwei Frontblendentypen verfügbar:

- LC-Anzeige auf der Frontblende und System-ID-LED
- LE-Anzeige auf der Frontblende und System-ID-LED

Bei Blade-Servern ist nur die System-ID-LED auf der Frontblende des Servers verfügbar, da das Blade-Gehäuse mit einer LC-Anzeige ausgerüstet ist.

LCD-Einstellung konfigurieren

Sie können eine Standardzeichenkette, wie z. B. den iDRAC-Namen, die IP-Adresse, usw. oder eine benutzerdefinierte Zeichenkette auf der LC-Anzeige auf der Frontblende des Managed System definieren und anzeigen.

Einstellungen für die LC-Anzeige über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die LC-Anzeige auf der Frontblende eines Servers:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Configurations (Konfigurationen)** > **System Settings (Systemeinstellungen)** > **Hardware Settings (Hardwareeinstellungen)** > **Front Panel configuration (Frontblendenkonfiguration)**.
2. Wählen Sie im Abschnitt **Einstellungen für LC-Anzeige** über das Drop-Down-Menü **Nachricht auf der Startseite einrichten** einen der folgenden Aspekte aus:
   - Service-Tag-Nummer (Standardeinstellung)
   - Systemkennnummer
   - DRAC-MAC-Adresse
   - DRAC-IPv4-Adresse
   - DRAC-IPv6-Adresse
   - Systemstrom
   - Umgebungstemperatur
   - Systemmodell
   - Host Name (Hostname)
   - Benutzerdefiniert
   - Keine

     Wenn Sie **Benutzerdefiniert** auswählen, geben Sie die erforderliche Nachricht in das Textfeld ein.

     Wenn Sie **Keine** auswählen, wird die Nachricht auf der Startseite nicht auf der LC-Anzeige auf der Frontblende angezeigt.
3. Aktivieren Sie die Anzeige der virtuellen Konsole (optional). Wenn sie aktiviert ist, zeigen der Abschnitt „Live-Status“ an der Frontblende und das LCD-Display am Server die Meldung `Virtual console session active` an, wenn es eine aktive Sitzung der virtuellen Konsole gibt.
4. Klicken Sie auf **Anwenden**.
   Die LC-Anzeige auf der Frontblende des Servers zeigt die konfigurierte Nachricht für die Startseite an.

LCD-Einstellungen über RACADM konfigurieren

Um die Server-LCD-Frontblendenanzeige zu konfigurieren, verwenden Sie die Objekte in der Gruppe `System.LCD`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

LCD-Einstellungen über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren

So konfigurieren Sie die LC-Anzeige auf der Frontblende eines Servers:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Frontblendensicherheit**.
   Die Seite **iDRAC-Einstellungen.Frontblendensicherheit** wird angezeigt.
2. Aktivieren oder deaktivieren Sie den Netzschalter.
3. Geben Sie folgendes an:
   - Zugang zur Frontblende
   - LCD-Meldungszeichenkette
   - Systemstromeinheiten, Umgebungstemperatureinheiten und Fehleranzeige
4. Aktivieren oder deaktivieren Sie die Anzeige der virtuellen Konsole.
   Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.
5. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

LED-Einstellung für die System-ID konfigurieren

Aktivieren oder deaktivieren Sie für die Identifizierung eines Servers das Blinken der System-ID-LED auf dem Managed System.

LED-Einstellung für die System-ID über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die LE-Anzeige für die System-ID:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Hardware Settings (Hardwareeinstellungen)** > **Front Panel configuration (Frontblendenkonfiguration)**. Es wird die Seite **System ID LED Settings** (LED-Einstellungen für die System-ID) angezeigt.
2. Wählen Sie im Abschnitt **LED-Einstellungen für die System-ID** beliebige der folgenden Optionen aus, um das Blinken der LED zu aktivieren oder zu deaktivieren:
   - Blinken ausgeschaltet
   - Blinken eingeschaltet
   - Blinken einschalten bei Zeitüberschreitung von einem Tag
   - Blinken einschalten bei Zeitüberschreitung von einer Woche
   - Blinken einschalten bei Zeitüberschreitung von einem Monat
3. Klicken Sie auf **Anwenden**.
   Das Blinken der LED auf der Frontblende ist konfiguriert.

LED-Einstellung der System-ID über RACADM konfigurieren

Um die System-ID-LED zu konfigurieren, verwenden Sie den Befehl `setled`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Das Konfigurieren von Zeitzone und NTP

Sie können die Zeitzone in iDRAC konfigurieren und die iDRAC-Zeit synchronisieren, indem Sie das Network Time Protocol (NTP) anstelle von BIOS oder Host-Systemzeiten verwenden.

Sie müssen über die Berechtigung zur Konfiguration verfügen, um die Zeitzone oder NTP-Einstellungen zu konfigurieren.

Konfigurieren von Zeitzone und NTP unter Verwendung der iDRAC-Web-Schnittstelle

So konfigurieren Sie Zeitzone und NTP mithilfe der iDRAC-Web-Schnittstelle:

1. Navigieren Sie zu **iDRAC Settings (iDRAC-Einstellungen)** > **Settings (Einstellungen)** > **Time zone and NTP Settings (Zeitzonen- und NTP-Einstellungen)**.
   Die Seite **Zeitzone und NTP** wird angezeigt.
2. Um die Zeitzone zu konfigurieren, wählen Sie im Drop-Down-Menü **Zeitzone** die gewünschte Zeitzone aus und klicken dann auf **Anwenden**.
3. Um NTP zu konfiguriere, aktivieren Sie NTP, geben Sie die NTP-Serveradressen ein und klicken Sie dann auf **Anwenden**.
   Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

Konfigurieren von Zeitzone und NTP unter Verwendung von RACADM

Verwenden Sie zum Konfigurieren von Zeitzone und NTP den Befehl `set` mit den Objekten in den Gruppen `iDRAC.Time` und `iDRAC.NTPConfigGroup`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

ANMERKUNG: iDRAC synchronisiert die Zeit mit dem Host (Ortszeit). Es wird daher empfohlen, iDRAC und den Host mit derselben Zeitzone zu konfigurieren, damit die Zeitsynchronisierung korrekt ist. Wenn Sie eine Zeitzone ändern möchten, müssen Sie sie auf dem Host und iDRAC ändern und der Host muss neu gestartet werden.

Erstes Startlaufwerk einstellen

Sie können das erste Startgerät nur für den nächsten Startvorgang oder für alle nachfolgenden Neustarts festlegen. Wenn Sie festlegen, dass das Gerät für alle nachfolgenden Startvorgänge verwendet werden soll, verbleibt es als das erste Startgerät in der BIOS-Startreihenfolge, bis eine erneute Änderung entweder über die iDRAC-Webschnittstelle oder von der BIOS-Startreihenfolge aus erfolgt.

Sie können das erste Startgerät auf einen der folgenden Punkte einstellen:

- Normaler Start
- PXE
- BIOS-Setup
- Lokale Floppy/Primäre Wechselmedien
- Lokale CD/DVD
- Festplattenlaufwerk
- Virtuelle Diskette
- Virtuelle CD/DVD/ISO
- Lokale SD-Karte
- Lifecycle-Controller
- BIOS Boot Manager
- UEFI-Gerätepfad
- UEFI HTTP

ANMERKUNG:

- BIOS-Setup (F2), Lifecycle Controller (F10) und BIOS Boot Manager (F11) können nicht als permanentes Startgerät eingestellt werden.
- Die Einstellungen für das erste Startgerät in der iDRAC-Webschnittstelle überschreiben die Starteinstellungen im System-BIOS.

Erstes Startgerät über die Web-Schnittstelle einrichten

So richten Sie das erste Startgerät über die iDRAC-Webschnittstelle ein:

1. Wechseln Sie zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Hardware Settings (Hardwareeinstellungen)** > **First Boot Device (Erstes Startgerät)**.
   Der Bildschirm **Erstes Startgerät** wird angezeigt.
2. Wählen Sie das gewünschte erste Startgerät aus der Drop-Down-Liste aus, und klicken Sie dann auf **Anwenden**.
   Das System startet bei den nachfolgenden Neustarts vom ausgewählten Gerät.
3. Um vom ausgewählten Gerät beim nächsten Starten nur einmal zu starten, wählen Sie **Boot Once** (Einmalstart). Das System startet nun vom ersten Startgerät aus gemäß der BIOS-Startreihenfolge.

Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

Erstes Startgerät über RACADM festlegen

- Um das erste Startlaufwerk festzulegen, verwenden Sie das Objekt `iDRAC.ServerBoot.FirstBootDevice`.
- Um den einmaligen Start für ein Gerät zu aktivieren, verwenden Sie das Objekt `iDRAC.ServerBoot.BootOnce`.

Weitere Informationen zu diesen Objekten finden Sie unter *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Einstellen des ersten Startgeräts unter Verwendung der virtuellen Konsole

Sie können das Gerät auswählen, von dem der Start ausgeführt werden soll, wenn der Server in der Anzeige der virtuellen Konsole angezeigt wird, bevor der Server die Startsequenz befolgt. Der einmalige Start wird von allen in Erstes Startlaufwerk einstellen auf Seite 107 aufgeführten Geräten unterstützt.

So stellen Sie das erste Startgerät mithilfe der virtuellen Konsole ein:

1. Starten Sie die virtuelle Konsole.
2. Stellen Sie im Viewer der virtuellen Konsole im Menü **Nächster Start** das gewünschte Gerät als erstes Startgerät ein.

Bildschirm „Letzter Absturz“ aktivieren

Um den Grund für den Absturz unter einem Managed System zu beheben, können Sie das Image des Systemabsturzes über iDRAC erfassen.

ANMERKUNG: Informationen über Server Administrator finden Sie unter *OpenManage – Installationshandbuch* verfügbar unter https://www.dell.com/openmanagemanuals.

Das Host-System sollte über ein Windows Betriebssystem verfügen, um diese Funktion verwenden zu können.

ANMERKUNG:

- Diese Funktion gilt nicht auf Linux-Systemen.
- Diese Funktion ist unabhängig von Agents oder Attributen.

Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough

Bei Servern, die Network-Daughter-Card (NDC)- oder integrierte LAN-On-Motherboard (LOM)-Geräte enthalten, können Sie die Funktion „Betriebssystem-zu-iDRAC-Passthrough“ aktivieren. Diese Funktion stellt eine bidirektionale bandinterne Hochgeschwindigkeitskommunikation zwischen iDRAC und dem Host-Betriebssystem mittels eines freigegebenen LOM, einer dedizierten NIC oder der USB-NIC bereit. Diese Funktion ist mit einer iDRAC Enterprise- oder Datacenter-Lizenz verfügbar.

ANMERKUNG: iDRAC-Service-Modul (iSM) enthält weitere Funktionen zum Verwalten von iDRAC über das Betriebssystem. Weitere Informationen finden Sie im Benutzerhandbuch zu iDRAC-Servicemodul unter www.dell.com/idracservicemodule.

Wenn der Browser durch eine dedizierte NIC aktiviert wurde, kann dieser im Host-Betriebssystem gestartet werden und dann auf die iDRAC-Webschnittstelle zugreifen. Die dedizierte NIC für die Blade-Server befindet sich im Chassis Management Controller.

Das Wechseln zwischen dedizierter NIC und freigegebenem LOM erfordert keinen Neustart oder Reset des Host-Betriebssystems oder des iDRAC.

Der Kanal kann folgendermaßen aktiviert werden:

- iDRAC-Weboberfläche
- RACADM oder WSMan (Nachbetriebssystemumgebung)
- Dienstprogramm für iDRAC-Einstellungen (Vorbetriebssystemumgebung)

Wenn die Netzwerkkonfiguration durch die iDRAC-Web-Schnittstelle geändert wird, müssen Sie mindestens 10 Sekunden warten, bevor das Betriebssystem zu iDRAC-Passthrough aktiviert wird.

Wenn Sie den Server mit einem Serverkonfigurationsprofil über RACADM, WSMan oder Redfish konfigurieren und die Netzwerkeinstellungen in dieser Datei geändert werden, müssen Sie 15 Sekunden warten, um entweder die Funktion „Betriebssystem zu iDRAC-Passthrough“ zu aktivieren oder die IP-Adresse des Host-Betriebssystems einzustellen.

Vor Aktivierung des Betriebssystems zum iDRAC-Passthrough stellen Sie Folgendes sicher:

- iDRAC wurde zur Verwendung von dedizierten NIC oder dem gemeinsamen Modus konfiguriert (das heißt, die NIC-Auswahl wird einer der LOMs zugewiesen).
- Host-Betriebssystem und iDRAC befinden sich auf dem gleichen Subnetz und auf dem gleichen VLAN.
- Die IP-Adresse des Host-Betriebssystems ist konfiguriert.
- Eine Karte ist installiert, die Betriebssystem-zu-iDRAC-Passthrough-Funktion unterstützt.
- Sie verfügen über die Berechtigung zum Konfigurieren.

Wenn Sie diese Funktion aktivieren:

- Im freigegebenen Modus wird die IP-Adresse des Host-Betriebssystems verwendet.
- Im dedizierten Modus müssen Sie eine gültige IP-Adresse des Host-Betriebssystems angeben. Wenn mehr als ein LOM aktiv ist, geben Sie die IP-Adresse des ersten LOM ein.

Falls die Funktion „Betriebssystem-zu-iDRAC-Passthrough“ nach der Aktivierung nicht funktioniert, überprüfen Sie Folgendes:

- Das für iDRAC dedizierte NIC-Kabel ist richtig angeschlossen.
- Es ist mindestens ein LOM aktiv.

ANMERKUNG: Verwenden Sie die Standard-IP-Adresse. Stellen Sie sicher, dass die IP-Adresse der USB-NIC-Schnittstelle sich nicht in demselben Netzwerk-Subnetz wie die iDRAC- oder Host-BS-IP-Adressen befindet. Wenn jedoch ein Konflikt dieser IP-Adresse mit anderen Schnittstellen des Host-Systems oder des lokalen Netzwerks vorliegt, müssen Sie sie ändern.

ANMERKUNG: Wenn Sie das iDRAC-Servicemodul starten, während sich USB-NIC im deaktivierten Zustand befindet, ändert das iDRAC-Servicemodul die USB-NIC-IP-Adresse zu 169.254.0.1.

ANMERKUNG: Verwenden Sie nicht die IP-Adressen 169.254.0.3 und 169.254.0.4. Diese IP-Adressen sind für die USB-NIC-Schnittstelle an der Vorderseite reserviert, wenn ein A/A-Kabel verwendet wird.

ANMERKUNG: iDRAC ist möglicherweise nicht vom Host-Server aus über LOM-Pass-Through zugänglich, wenn NIC-Teaming aktiviert ist. Dann kann auf den iDRAC vom Host-Server-Betriebssystem über die iDRAC-USB-Netzwerkkarte oder über das externe Netzwerk über die iDRAC-eigene Netzwerkkarte zugegriffen werden.

Unterstützte Karten für Betriebssystem-zu-iDRAC-Passthrough

Die folgende Tabelle zeigt eine Liste der Karten, die die Funktion von Betriebssystem-zu-iDRAC-Passthrough mithilfe von LOM unterstützen.

Tabelle 15. Betriebssystem-zu-iDRAC-Passthrough mithilfe von LOM – Unterstützte Karten

Kategorie	Hersteller	Typ
NDC	Broadcom	• 5720 QP rNDC 1G BASE-T
	Intel	• x520/i350 QP rNDC 1G BASE-T

Integrierte LOM-Karten unterstützen ebenfalls die Betriebssystem-zu-iDRAC-Passthrough-Funktion.

Unterstützte Betriebssysteme für USB-NIC

Die unterstützten Betriebssysteme für USB-NIC sind:

- 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 (Basis und R2 mit 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

Für Linux-Betriebssysteme müssen Sie vor dem Aktivieren der USB-NIC die USB-NIC als DHCP auf dem Host-Betriebssystem konfigurieren.

Für vSphere müssen Sie vor dem Aktivieren von USB-NIC die VIB-Datei installieren.

ANMERKUNG: Informationen zur Konfiguration der USB-Netzwerkkarte als DHCP im Linux-Betriebssystem oder XenServer finden Sie in der Dokumentation des Betriebssystems oder des Hypervisors.

Installieren der VIB-Datei

Für vSphere-Betriebssystemen muss vor der Aktivierung des USB-NIC die VIB-Datei installiert werden.

So installieren Sie die VIB-Datei:

1. Kopieren Sie mit Win SCP die VIB-Datei in den Ordner `/tmp/` des ESX-i-Host-Betriebssystems.
2. Wechseln Sie zur ESXi-Eingabeaufforderung, und führen Sie den folgenden Befehl aus:

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

   Das Ergebnis ist Folgendes:

   ```
   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. Starten Sie den Server neu.
4. Führen Sie an der ESXi-Eingabeaufforderung den folgenden Befehl aus: `esxcfg-vmknic -l`.
   Die Ausgabe zeigt den usb0-Eintrag.

Aktivieren und Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung der Web-Schnittstelle

So aktivieren Sie das Betriebssystem zum iDRAC-Passthrough mithilfe der Web-Schnittstelle:

1. Navigieren Sie zu **iDRAC-Einstellungen** > **Verbindungen** > **Netzwerk** > **Betriebssystem zu iDRAC-Passthrough**.
   Die Seite **Betriebssystem zu iDRAC-Passthrough** wird angezeigt.
2. Ändern Sie den Status auf **Aktiviert**.
3. Wählen Sie eine der folgenden Optionen für den Pass-Through-Modus aus:
   - **LOM** – Der BS zu iDRAC PassThrough-Link zwischen dem iDRAC und dem Host-Betriebssystem wird über das LOM oder die NDC hergestellt.
   - **USB-NIC** – Der BS zu iDRAC PassThrough-Link zwischen dem iDRAC und dem Host-Betriebssystem wird über den internen USB hergestellt.

   ANMERKUNG: Wenn Sie den Pass-Through-Modus auf LOM einstellen, stellen Sie Folgendes sicher:
   - OS und iDRAC befinden sich im gleichen Subnetz
   - Die NIC-Auswahl in den Netzwerkeinstellungen ist auf ein LOM eingestellt.
4. Wenn der Server im freigegebenen LOM-Modus verbunden ist, ist das Feld **Betriebssystem-IP-Adresse** deaktiviert.

   ANMERKUNG: Wenn VLAN auf dem iDRAC aktiviert ist, funktioniert der LOM-Passthrough nur im freigegebenen LOM-Modus und wenn VLAN-Tagging auf dem Host konfiguriert ist.

ANMERKUNG:

- Wenn der Pass-Through-Modus auf LOM eingestellt ist, ist es nicht möglich, den iDRAC vom Host-BS nach dem Kaltstart zu starten.
- Wir haben die LOM-Pass-Through-Funktion mithilfe des dedizierten Modus absichtlich entfernt.

5. Wenn Sie **USB-NIC** als PassThrough-Konfiguration auswählen, geben Sie die IP-Adresse der USB-NIC ein.

   Der Standardwert ist 169.254.1.1. Es wird empfohlen, die Standard-IP-Adresse zu verwenden. Wenn jedoch ein Konflikt dieser IP-Adresse mit anderen Schnittstellen des Host-Systems oder des lokalen Netzwerks vorliegt, müssen Sie sie ändern.

   Geben Sie nicht die IP-Adressen 169.254.0.3 und 169.254.0.4 ein. Diese IP-Adressen sind für den USB-NIC-Anschluss an der Vorderseite, wenn ein A/A-Kabel verwendet wird, reserviert.

   ANMERKUNG: Wenn IPv6 bevorzugt wird, ist die Standardadresse fde1:53ba:e9a0:de11::1. Falls erforderlich, kann diese Adresse in der Einstellung idrac.OS-BMC.UsbNicULA geändert werden. Wenn IPv6 auf dem USB-NIC nicht erwünscht ist, kann es deaktiviert werden, indem die Adresse in "::" geändert wird.

6. Klicken Sie auf **Anwenden**.
7. Klicken Sie auf **Netzwerkkonfiguration testen**, um zu überprüfen ob die IP zugreifbar ist und die Verbindung zwischen dem iDRAC und dem Host-Betriebssystem hergestellt ist.

Aktivieren und Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung von RACADM

Um das Betriebssystem zum iDRAC-Passthrough unter Verwendung von RACADM zu aktivieren oder deaktivieren, verwenden Sie die Objekte in der Gruppe `iDRAC.OS-BMC`.

Weitere Informationen finden Sie unter*iDRAC-Attributregistrierung* verfügbar unter https://www.dell.com/idracmanuals.

Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung des Dienstprogramms für iDRAC-Einstellungen

So aktivieren oder deaktivieren Sie das Betriebssystem zum iDRAC-Passthrough mithilfe des Dienstprogramms für iDRAC-Einstellungen:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Kommunikationsberechtigungen**.
   Die Seite **iDRAC-Einstellungen.Kommunikationsberechtigungen** wird angezeigt.
2. Wählen Sie eine der folgenden Optionen, um Betriebssystem-zu-iDRAC-Passthrough zu aktivieren:
   - **LOM** – Der BS zu iDRAC PassThrough-Link zwischen dem iDRAC und dem Host-Betriebssystem wird über das LOM oder die NDC hergestellt.
   - **USB-NIC** – Der BS zu iDRAC PassThrough-Link zwischen dem iDRAC und dem Host-Betriebssystem wird über den internen USB hergestellt.

   ANMERKUNG: Wenn Sie den Pass-Through-Modus auf LOM einstellen, stellen Sie Folgendes sicher:

   - OS und iDRAC befinden sich im gleichen Subnetz
   - Die NIC-Auswahl in den Netzwerkeinstellungen ist auf ein LOM eingestellt.

   Zum Deaktivieren der Funktion klicken Sie auf **Deaktiviert**.

   ANMERKUNG: Die LOM-Option kann nur ausgewählt werden, wenn eine der installierten Karten das Durchreichen vom Betriebssystem zum iDRAC unterstützt. Andernfalls ist die Option ausgegraut.

3. Wenn Sie **LOM** als PassThrough-Konfiguration auswählen und wenn der Server über den dedizierten Modus verbunden ist, geben Sie die IPv4-Adresse des Betriebssystems ein.

   ANMERKUNG: Wenn der Server im freigegebenen LOM-Modus verbunden ist, ist das Feld **Betriebssystem-IP-Adresse** deaktiviert.

4. Wenn Sie **USB-NIC** als PassThrough-Konfiguration auswählen, geben Sie die IP-Adresse der USB-NIC ein.

Der Standardwert ist 169.254.1.1. Wenn jedoch ein Konflikt dieser IP-Adresse mit anderen Schnittstellen des Host-Systems oder des lokalen Netzwerks vorliegt, müssen Sie sie ändern. Geben Sie nicht die IP-Adressen 169.254.0.3 und 169.254.0.4 ein. Diese IP-Adressen sind für den USB-NIC-Anschluss an der Vorderseite, wenn ein A/A-Kabel verwendet wird, reserviert.

ANMERKUNG: Wenn IPv6 bevorzugt wird, ist die Standardadresse fde1:53ba:e9a0:de11::1. Falls erforderlich, kann diese Adresse in der Einstellung idrac.OS-BMC.UsbNicULA geändert werden. Wenn IPv6 auf dem USB-NIC nicht erwünscht ist, kann es deaktiviert werden, indem die Adresse in "::" geändert wird.

5. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
Die Details werden gespeichert.

Zertifikate abrufen

In der folgenden Tabelle werden die Zertifikattypen auf der Basis des Anmeldetyps aufgelistet.

Tabelle 16. Zertifikattypen auf der Basis des Anmeldetyps

Anmeldetyp	Zertifikattyp	Abrufmöglichkeit
Einmalige Anmeldung über Active Directory	Vertrauenswürdiges Zertifizierungsstellenzertifikat	Zertifikatsignierungsanforderung (CSR) generieren und diese von einer Zertifizierungsstelle signieren lassen SHA-2-Zertifikate werden ebenfalls unterstützt.
Smart Card-Anmeldung als lokaler oder Active Directory-Benutzer	• Benutzerzertifikat • Vertrauenswürdiges Zertifizierungsstellenzertifikat	• Benutzerzertifikat – Smart Card-Benutzerzertifikat als Base64-kodierte Datei unter Verwendung der Kartenverwaltungssoftware exportieren, die durch den Smart Card-Anbieter bereitgestellt wird. • Vertrauenswürdiges Zertifizierungsstellenzertifikat – Dieses Zertifikat wird von einer Zertifizierungsstelle ausgegeben. SHA-2-Zertifikate werden ebenfalls unterstützt.
Active Directory-Benutzeranmeldung	Vertrauenswürdiges Zertifizierungsstellenzertifikat	Dieses Zertifikat wird durch eine Zertifizierungsstelle ausgegeben. SHA-2-Zertifikate werden ebenfalls unterstützt.
Lokale Benutzeranmeldung	SSL-Zertifikat	Zertifikatsignierungsanforderung (CSR) generieren und diese von einer vertrauenswürdigen Zertifizierungsstelle signieren lassen **ANMERKUNG:** iDRAC wird mit einem standardmäßigen selbstsignierten SSL-Serverzertifikat ausgeliefert. Dieses Zertifikat wird vom iDRAC-Webserver, von virtuellen Datenträgern und der virtuellen Konsole verwendet. SHA-2-Zertifikate werden ebenfalls unterstützt.

SSL-Serverzertifikate

iDRAC umfasst einen Webserver, der für das zum Branchenstandard gehörende SSL-Sicherheitsprotokoll konfiguriert ist, um über das Netzwerk verschlüsselte Daten zu übermitteln. Eine SSL-Verschlüsselungsoption dient zum Deaktivieren von schwachen Chiffrierschlüsseln. Auf der Basis einer asymmetrischen Verschlüsselungstechnologie wird SSL als eine allgemein akzeptierte Methode für die Bereitstellung einer authentifizierten und verschlüsselten Kommunikation zwischen Clients und Servern betrachtet, um unbefugtes Abhören in einem Netzwerk zu vermeiden.

Ein SSL-aktiviertes System kann die folgenden Aufgaben ausführen:

- Sich an einem SSL-aktivierten Client authentifizieren
- Beiden Systemen gestatten, eine verschlüsselte Verbindung herzustellen

ANMERKUNG: Wenn die SSL-Verschlüsselung auf 256 Bit oder höher und 168 Bit oder höher festgelegt ist, erfordern die Kryptografie-Einstellungen für die Umgebung Ihrer virtuellen Maschine (JVM, IcedTea) möglicherweise eine Installation der Unlimited Strength Java Cryptography Extension Richtliniendateien, um die Verwendung von iDRAC-Plugins wie der vConsole mit dieser Verschlüsselungsebene zuzulassen. Weitere Informationen über das Installieren der Richtliniendateien finden Sie in der Dokumentation zu Java.

iDRAC Webserver verfügt standardmäßig über ein von Dell selbst signiertes, eindeutiges digitales SSL-Zertifikat. Sie können das standardmäßige SSL-Zertifikat durch ein von einer bekannten Zertifizierungsstelle signiertes Zertifikat ersetzen. Eine Zertifizierungsstelle ist ein Unternehmen, das in der IT-Industrie dafür anerkannt ist, hohe Ansprüche bezüglich des zuverlässigen Screenings, der Identifizierung und anderen wichtigen Sicherheitskriterien zu erfüllen. Beispiele für Zertifizierungsstellen sind Thawte und VeriSign. Um den Prozess des Abrufens signierter Zertifikate zu initiieren, verwenden Sie entweder die iDRAC-Web-Schnittstelle oder die RACADM-Schnittstelle. Über diese Schnittstellen können Sie eine Zertifikatsignierungsanforderung (CSR) mit den Daten für Ihr Unternehmen generieren. Übermitteln Sie anschließend die generierte Zertifikatsignierungsanforderung (CSR) an eine Zertifizierungsstelle wie VeriSign oder Thawte. Bei der Zertifizierungsstelle kann es sich um eine Stammzertifizierungsstelle oder um eine Zwischenzertifizierungsstelle handeln. Nachdem Sie das von der Zertifizierungsstelle signierte SSL-Zertifikat erhalten haben, laden Sie es in iDRAC hoch.

Für jeden iDRAC, dem die Management Station vertrauen soll, muss das jeweilige iDRAC-SSL-Zertifikat im Zertifikatspeicher der Management Station platziert werden. Wenn das SSL-Zertifikat auf den Management Stations installiert ist, können unterstützte Browser auf iDRAC ohne Zertifikatswarnungen zugreifen.

Sie können zur Signierung des SSL-Zertifikats auch ein benutzerdefiniertes Signaturzertifikat hochladen, anstatt des Standardsignaturzertifikats für diese Funktion. Durch den Import eines benutzerdefinierten Signaturzertifikats in alle Management Stations werden alle iDRACs als vertrauenswürdig gekennzeichnet, die dieses benutzerdefinierte Signaturzertifikat verwenden. Falls ein benutzerdefiniertes Signaturzertifikat hochgeladen wird, wenn ein anderes benutzerdefiniertes SSL-Zertifikat bereits verwendet wird, wird das benutzerdefinierte SSL-Zertifikat deaktiviert und ein einmaliges, automatisch generiertes SSL-Zertifikat verwendet, das mit dem benutzerdefinierten Signaturzertifikat signiert ist. Sie können das benutzerdefinierte Signaturzertifikat (ohne den privaten Schlüssel) herunterladen. Sie können auch das vorhandenen Signaturzertifikat löschen. Nach Löschen des benutzerdefinierten Signaturzertifikats setzt iDRAC dieses zurück und generiert automatisch ein neues, selbst signiertes SSL-Zertifikat. Wenn ein selbst signiertes Zertifikat erneut generiert wird, muss die Vertrauensstellung zwischen iDRAC und der Management Workstation erneut konfiguriert werden. Automatisch generierte SSL-Zertifikate sind selbst signiert und haben ein Ablaufdatum von sieben Jahren und einem Tag; das Startdatum liegt einen Tag zurück (wegen verschiedener Zeitzoneneinstellungen für die Management Stations und iDRAC).

Das SSL-Zertifikat für iDRAC-Webserver unterstützt Sternchen (*) als Teil der am weitesten links stehenden Komponente des allgemeinen Namens im Rahmen der Generierung einer Zertifikatsignierungsanforderung (CSR). Beispiel: *.qa.com oder *.company.qa.com. Dies wird als Platzhalterzertifikat bezeichnet. Wenn eine Zertifikatsignierungsanforderung mit Platzhaltern außerhalb von iDRAC generiert wird, können Sie ein einzelnes signiertes SSL-Platzhalterzertifikat für mehrere iDRACs hochladen. Alle iDRACs gelten für unterstützte Browser als vertrauenswürdig. Beim Herstellen einer Verbindung zur iDRAC Webschnittstelle unter Verwendung eines unterstützten Browsers, das ein Platzhalterzertifikat unterstützt, gilt iDRAC für den Browser als vertrauenswürdig. Beim Starten der Ansichten gelten die iDRACs für die Anzeigeclients als vertrauenswürdig.

Neue Zertifikatsignierungsanforderung erstellen

Eine CSR ist eine digitale Anforderung eines sicheren SSL-Serverzertifikats an die Zertifizierungsstelle. SSL-Serverzertifikate ermöglichen Clients des Servers, die Identität des Servers als vertrauenswürdig einzustufen und eine verschlüsselte Sitzung mit dem Server auszuhandeln.

Nachdem die Zertifizierungsstelle eine Zertifikatssignierungsanforderung erhalten hat, verifiziert und bestätigt sie die darin enthaltenen Informationen. Wenn der Anmeldende die Sicherheitsstandards der Zertifikatzertifizierungsstelle erfüllt, gibt die Zertifikatzertifizierungsstelle ein digital signiertes SSL-Serverzertifikat aus, das den Server des Anmeldenden beim Aufbau von SSL-Verbindungen über Browser, die auf Management Stations ausgeführt werden, eindeutig identifiziert.

Nach der Genehmigung der Zertifikatsignierungsanforderung (CSR) und der Ausgabe des SSL-Serverzertifikats durch die Zertifizierungsstelle kann die CSR in iDRAC hochgeladen werden. Die Informationen, die zum Generieren der CSR verwendet und auf

der iDRAC-Firmware gespeichert werden, müssen mit den Informationen auf dem SSL-Serverzertifikat übereinstimmen, dies bedeutet, dass das Zertifikat mithilfe der durch iDRAC erstellten CSR generiert worden sein muss.

CSR unter Verwendung der Webschnittstelle erstellen

Um neue CSR zu erstellen:

ANMERKUNG: Jede neue CSR überschreibt alle zuvor auf der Firmware gespeicherten CSR-Daten. Die Informationen in der CSR müssen mit den Informationen im SSL-Serverzertifikat übereinstimmen. Andernfalls akzeptiert iDRAC das Zertifikat nicht.

1. Gehen Sie in der iDRAC-Web-Schnittstelle zu **iDRAC-Einstellungen** > **Services** > **Web Server** > **SSL-Zertifikat**, wählen Sie **Eine neue Zertifikatsignierungsanforderung erstellen (CSR)** aus, und klicken Sie auf **Weiter**.
   Daraufhin wird die Seite **Ein neues Zertifikat erstellen** angezeigt.
2. Geben Sie einen Wert für jedes CSR-Attribut ein.
   Weitere Informationen finden Sie in de *iDRAC Onlinehilfe*.
3. Klicken Sie auf **Erstellen**.
   Daraufhin wird eine neue CSR generiert. Speichern Sie sie auf der Management Station.

CSR über RACADM generieren

Um eine CSR unter Verwendung von RACADM zu erzeugen, verwenden Sie den Befehl `set` mit den Objekten in der Gruppe `iDRAC.Security` und verwenden dann den Befehl `sslcsrgen`, um die CSR zu generieren

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Automatische Zertifikatregistrierung

Im iDRAC ermöglicht die Funktion zur automatischen Zertifikatregistrierung die automatische Installation und Erneuerung von Zertifikaten, die vom Webserver verwendet werden. Wenn diese Funktion aktiviert ist, wird das vorhandene Web-Server-Zertifikat durch ein neues Zertifikat ersetzt.

ANMERKUNG:

- Die automatische Zertifikatregistrierung ist eine lizenzierte Funktion und erfordert eine Datacenter-Lizenz.
- Für die Ausgabe des Serverzertifikats ist eine gültige NDES-Einrichtung (Network Device Enrollment Service) erforderlich.

Im Folgenden finden Sie die Konfigurationsparameter für die automatische Zertifikatregistrierung:

- Aktivieren/Deaktivieren
- SCEP-Server-URL
- Anfragekennwort

ANMERKUNG: Weitere Informationen zu diesen Parametern finden Sie in der *iDRAC-Online-Hilfe*.

Nachfolgend finden Sie die verfügbaren Status-Optionen für die automatische Zertifikatregistrierung.

- Registriert – Die automatische Zertifikatregistrierung ist aktiviert. Das Zertifikat wird überwacht und ein neues Zertifikat kann nach Ablauf der Lizenz ausgestellt werden.
- Anmeldung – Zwischenzustand nach der automatischen Zertifikatregistrierung ist aktiviert.
- Fehler – Problem mit dem NDES-Server.
- Keine – Standardeinstellung.

ANMERKUNG: Wenn Sie die automatische Zertifikatsregistrierung aktivieren, wird der Web-Server neu gestartet und alle vorhandenen Web-Sitzungen werden abgemeldet.

Serverzertifikat hochladen

Nach dem Generierung einer Zertifikatsignierungsanforderung (CSR) können Sie das signierte SSL-Serverzertifikat in die iDRAC-Firmware hochladen. iDRAC muss zurückgesetzt werden, damit das Zertifikat angewendet wird. iDRAC akzeptiert nur X509, Base 64-kodierte Webserverzertifikate. SHA-2-Zertifikate werden ebenfalls unterstützt.

VORSICHT: Während des Resets ist iDRAC für einige Minuten nicht verfügbar.

Serverzertifikat über die Web-Schnittstelle hochladen

So laden Sie das SSL-Serverzertifikat hoch:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Connectivity (Konnektivität)** > **SSL** > **SSL certificate (SSL-Zertifikat)**, wählen Sie **Serverzertifikat hochladen (Upload Server Certificate)** aus, und klicken Sie auf **Next** (Weiter).
   Die Seite **Zertifikat hochladen** wird angezeigt.
2. Klicken Sie unter **Dateipfad** auf **Durchsuchen**, und wählen Sie dann das Zertifikat auf der Management Station aus.
3. Klicken Sie auf **Anwenden**.
   Das SSL-Serverzertifikat wird auf iDRAC hochgeladen.
4. Es wird eine Popup-Meldung angezeigt, in der Sie aufgefordert werden, iDRAC sofort oder zu einem späteren Zeitpunkt zurückzusetzen. Klicken Sie nach Bedarf auf **Reset iDRAC** (iDRAC zurücksetzen) oder **Reset iDRAC Later** (iDRAC später zurücksetzen).
   iDRAC wird zurückgesetzt, und das neue Zertifikat wird angewendet. Während des Resets ist iDRAC für einige Minuten nicht verfügbar.
   ANMERKUNG: Sie müssen iDRAC zurücksetzen, um das neue Zertifikat anzuwenden. Bis iDRAC zurückgesetzt wird, ist das vorhandene Zertifikat aktiv.

Serverzertifikat über RACADM hochladen

Um das SSL-Serverzertifikat hochzuladen, verwenden Sie den Befehl `sslcertupload`. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Wenn die CSR außerhalb von iDRAC mit einem verfügbaren privaten Schlüssel erstellt wird, laden Sie das Zertifikat wie folgt auf iDRAC hoch:

1. Senden Sie die CSR an eine bekannte Zertifizierungsstelle. Diese unterzeichnet die CSR, wodurch aus der CSR ein gültiges Zertifikat wird.
2. Laden Sie den privaten Schlüssel mithilfe des Remote-RACADM-Befehls `sslkeyupload` hoch.
3. Laden Sie das signierte Zertifikat mithilfe des Remote-RACADM-Befehls `sslcertupload` auf iDRAC hoch.
   Das neue Zertifikat wird zum iDRAC hochgeladen. Eine Meldung wird angezeigt, in der Sie aufgefordert werden, iDRAC zurückzusetzen.
4. Führen Sie den Befehl racadm `racreset` aus, um iDRAC zurückzusetzen.
   iDRAC wird zurückgesetzt, und das neue Zertifikat wird angewendet. Während des Resets ist iDRAC für einige Minuten nicht verfügbar.
   ANMERKUNG: Sie müssen iDRAC zurücksetzen, um das neue Zertifikat anzuwenden. Bis iDRAC zurückgesetzt ist, bleibt das bestehende Zertifikat aktiv.

Serverzertifikat anzeigen

Sie können das SSL-Serverzertifikat, das derzeit in iDRAC verwendet wird, anzeigen.

Serverzertifikat über die Web-Schnittstelle anzeigen

Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC Einstellungen** > **Services** > **Webserver** > **SSL-Zertifikat**. Die Seite **SSL** zeigt das SSL-Serverzertifikat an, das derzeit am oberen Rand der Seite verwendet wird.

Serverzertifikat über RACADM anzeigen

Um das SSL-Serverzertifikat anzuzeigen, verwenden Sie den Befehl `sslcertview`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Hochladen eines benutzerdefinierten Signaturzertifikats

Sie können ein benutzerdefiniertes Signaturzertifikat hochladen, um das SSL-Zertifikat zu signieren. SHA-2-Zertifikate werden ebenfalls unterstützt.

Uploading custom signing certificate using web interface

To upload the custom signing certificate using iDRAC web interface:

1. Go to **iDRAC Settings** > **Services** > **Web Server** > **SSL/TLS Custom Signing Certificate**.
   The **SSL** page is displayed.
2. Under **SSL/TLS Custom Signing Certificate**, click **Upload Signing Certificate**.
   The **Upload Custom SSL Certificate Signing Certificate** page is displayed.
3. Click **Choose File** and select the custom SSL certificate signing certificate file.
   Only Public-Key Cryptography Standards #12 (PKCS #12) compliant certificate is supported.
4. If the certificate is password protected, in the **PKCS#12 Password** field, enter the password.
5. Click **Apply**.
   The certificate is uploaded to iDRAC.
6. A pop-up message is displayed asking you to reset iDRAC immediately or at a later time. Click **Reset iDRAC** or **Reset iDRAC Later** as required.
   After iDRAC resets, the new certificate is applied. The iDRAC is not available for a few minutes during the reset.
   NOTE: You must reset iDRAC to apply the new certificate. Until iDRAC is reset, the existing certificate is active.

Hochladen eines benutzerdefinierten SSL-Zeritfikatssignaturzertifikats unter Verwendung von RACADM

Um das benutzerdefinierte SSL-Zertifikatsignaturzertifikat mit RACADM hochzuladen, verwenden Sie den Befehl `sslcertupload` und dann den Befehl `racreset`, um iDRAC zurückzusetzen.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat herunterladen

Sie können das benutzerdefinierte Signaturzertifikat mithilfe der iDRAC-Webschnittstelle oder RACADM herunterladen.

Benutzerdefiniertes Signierungszertifikat herunterladen

So laden Sie Benutzerdefinierte Signierungszertifikate unter Verwendung der iDRAC Webschnittstelle herunter:

1. Gehen Sie zu **iDRAC Settings (iDRAC-Einstellungen)** > **Connectivity (Konnektivität)** > **SSL**.
   Die Seite **SSL** wird angezeigt.
2. Wählen Sie unter **Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat** die Option **Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat herunterladen** und klicken Sie auf **Weiter**.
   Ein Fenster öffnet sich, über das Sie das benutzerdefinierte Signierungszertifikat an den Speicherort Ihrer Wahl speichern können.

Herunterladen eines benutzerdefinierten SSL-Zeritfikatssignaturzertifikats unter Verwendung von RACADM

Um das benutzerdefinierte SSL-Zertifikatssignaturzertifikat herunterzuladen, verwenden Sie den Unterbefehl `sslcertdownload`.
Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat löschen

Sie können ein bestehendes benutzerdefiniertes Signierungszertifikat auch unter Verwendung der iDRAC Webschnittstelle oder RACADM löschen.

Löschen von benutzerdefinierten Signaturzertifikaten mithilfe der iDRAC-Webschnittstelle

So löschen Sie ein benutzerdefiniertes Signaturzertifikat mithilfe der iDRAC-Webschnittstelle:

1. Gehen Sie zu **iDRAC Settings (iDRAC-Einstellungen)** > **Connectivity (Verbindungen)** > **SSL**.
   Die Seite **SSL** wird angezeigt.
2. Wählen Sie unter **Benutzerdefiniertes SSL-Zeritfikatssignaturzertifikat Benutzerdefiniertes SSL-Zeritfikatssignaturzertifikat löschen** aus und klicken Sie auf **Weiter**.
3. Es wird eine Popup-Meldung angezeigt, in der Sie aufgefordert werden, iDRAC sofort oder zu einem späteren Zeitpunkt zurückzusetzen. Klicken Sie auf **Reset iDRAC** (iDRAC zurücksetzen) bzw. **Reset iDRAC Later** (iDRAC später zurücksetzen). Nachdem iDRAC zurückgesetzt wird, wird ein neues selbstsigniertes Zertifikat generiert.

Löschen eines benutzerdefinierten SSL-Zeritfikatssignaturzertifikats unter Verwendung von RACADM

Um das benutzerdefinierte SSL-Zertifikatsignaturzertifikat mit RACADM zu löschen, verwenden Sie den Unterbefehl `sslcertdelete`. Führen Sie den Befehl `racreset` aus, um iDRAC zurückzusetzen.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Mehrere iDRACs über RACADM konfigurieren

Mit RACADM können Sie einen oder mehrere iDRACs mit identischen Eigenschaften konfigurieren. Wenn Sie einen bestimmten iDRAC mit seiner Gruppen-ID und seiner Objekt-ID abfragen, erstellt RACADM eine Konfigurationsdatei aus den abgerufenen Informationen. Importieren Sie die Datei in andere iDRACs, um sie identisch zu konfigurieren.

ANMERKUNG:

- Die Konfigurationsdatei enthält Informationen, die für den jeweiligen Server gelten. Die Informationen sind nach verschiedenen Objektgruppen organisiert.
- Einige Konfigurationsdateien enthalten eindeutige iDRAC-Informationen (z. B. die statische IP-Adresse), die Sie ändern müssen, bevor Sie die Datei auf andere iDRACs importieren.

Sie können das System Configuration Profile (SCP) auch verwenden, um mehrere iDRACs mithilfe von RACADM zu konfigurieren. Die SCP-Datei enthält die Informationen zur Komponentenkonfiguration. Sie können diese Datei verwenden, um die Konfiguration für BIOS, iDRAC, RAID und NIC anzuwenden, indem Sie die Datei in ein Zielsystem importieren. Weitere Informationen finden Sie im Whitepaper *XML Configuration Workflow* unter https://www.dell.com/manuals.

So konfigurieren Sie mehrere iDRACs unter Verwendung der Konfigurationsdatei:

1. Rufen Sie den Ziel-iDRAC ab, der die erforderliche Konfiguration enthält, indem Sie den folgenden Befehl verwenden:

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

   Der Befehl fordert die iDRAC-Konfiguration an und generiert die Konfigurationsdatei.

   ANMERKUNG: Das Umleiten der iDRAC-Konfiguration zu einer Datei unter Verwendung von `get -f` wird nur bei den lokalen und Remote-RACADM-Schnittstellen unterstützt.

   ANMERKUNG: Die erstellte Konfigurationsdatei enthält keine Benutzerkennwörter.

   Der Befehl `get` zeigt alle Konfigurationseigenschaften in einer Gruppe (angegeben nach Gruppenname und Index) und alle Konfigurationseigenschaften für einen Benutzer an.

2. Ändern Sie falls erforderlich die Konfigurationsdatei mit einem einfachen Texteditor.

ANMERKUNG: Es wird empfohlen, diese Datei mit einem einfachen Texteditor zu bearbeiten. Das RACADAM-Dienstprogramm verwendet einen ASCII-Textparser. Formatierung verwirrt den Parser, wodurch die RACADAM-Datenbank beschädigt werden kann.

3. Auf dem Ziel-iDRAC verwenden Sie den folgenden Befehl zum Ändern der Einstellungen:

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

   Durch diesen Befehl werden die Informationen in den anderen iDRAC geladen. Sie können mit dem Befehl `set` die Benutzer- und Kennwortdatenbank über Server Administrator synchronisieren.
4. Setzen Sie den Ziel-iDRAC über den folgenden Befehl zurück: `racadm racreset`

Zugriff zum Ändern der iDRAC-Konfigurationseinstellungen auf einem Host-System deaktivieren

Sie können den Zugriff zum Ändern der iDRAC-Konfigurationseinstellungen über die lokale RACADM-Schnittstelle oder ein Dienstprogramm für iDRAC-Einstellungen deaktivieren. Sie können diese Konfigurationseinstellungen jedoch anzeigen. Führen Sie dazu folgende Schritte durch:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Services (Dienste)** > **Local Configurations (Lokale Konfigurationen)**.
2. Wählen eine oder beide der folgenden Maßnahmen aus:
   - **Lokale iDRAC-Konfiguration unter Verwendung der iDRAC-Einstellungen deaktivieren** – Deaktiviert den Zugriff zum Ändern der Konfigurationseinstellungen im Dienstprogramm für die iDRAC-Einstellungen.
   - **Lokale iDRAC-Konfiguration unter Verwendung von RACADM deaktivieren** – Deaktiviert den Zugriff zum Ändern der Konfigurationseinstellungen im lokalen RACADM.
3. Klicken Sie auf **Anwenden**.

   ANMERKUNG: Wenn der Zugriff deaktiviert ist, können Sie Server Administrator oder IPMITool nicht für iDRAC-Konfigurationen verwenden. Sie können jedoch IPMI über LAN verwenden

6

Delegierte Autorisierung mithilfe von OAuth 2.0

Die Funktion für die delegierte Autorisierung ermöglicht einem Nutzer oder einer Konsole den Zugriff auf die iDRAC-API mithilfe von OAuth 2.0 JSON Web Token (JWT), die der Nutzer oder die Konsole zuerst von einem Autorisierungsserver erhält. Sobald ein OAuth-JWT abgerufen wurde, kann der Nutzer oder die Konsole es verwenden, um die iDRAC-API aufzurufen. Damit ist die Angabe von Nutzername und Kennwort für den Zugriff auf die API nicht mehr notwendig.

ANMERKUNG: Diese Funktion ist nur mit einer Datacenter-Lizenz verfügbar. Sie müssen über die Berechtigung zum Konfigurieren von iDRAC oder zum Konfigurieren von Nutzern verfügen, um diese Funktion verwenden zu können.

iDRAC unterstützt die Konfiguration von bis zu 2 Autorisierungsservern. Für die Konfiguration muss ein Nutzer die folgenden Autorisierungsserver-Informationen angeben:

- **Name**: eine Zeichenfolge zur Identifizierung des Autorisierungsservers auf dem iDRAC
- **Metadaten-URL**: die OpenID-Connect-konforme URL, die vom Server ausgegeben wird
- **HTTPS-Zertifikat**: der öffentliche Serverschlüssel, den der iDRAC für die Kommunikation mit dem Server verwenden soll
- **Offline-Schlüssel**: das von JWK festgelegte Dokument für den Autorisierungsserver
- **Offline-Aussteller**: die Ausstellerzeichenfolge, die in den vom Autorisierungsserver ausgegebenen Token verwendet wird

Für die Online-Konfiguration:

- Beim Konfigurieren eines Autorisierungsservers muss der iDRAC-Administrator sicherstellen, dass der iDRAC über ein Online-Netzwerk auf den Autorisierungsserver zugreifen kann.
- Wenn iDRAC nicht auf den Autorisierungsserver zugreifen kann, schlägt die Konfiguration fehl und ein späterer Versuch, auf die iDRAC-API zuzugreifen, schlägt ebenfalls fehl, selbst wenn ein gültiges Token vorhanden ist.

Für die Offline-Konfiguration:

- Der iDRAC muss nicht mit dem Autorisierungsserver kommunizieren, sondern wird mit den Metadaten-Details konfiguriert, die er offline heruntergeladen hat. Bei der Offline-Konfiguration kann iDRAC auf einen öffentlichen Teil der Signierungsschlüssel zugreifen und das Token ohne eine Netzwerkverbindung zum Autorisierungsserver validieren.

7

Anzeigen von Informationen zu iDRAC und zum Managed System

Sie können den Zustand und die Eigenschaften für iDRAC und das verwaltete System sowie die Bestandsliste zu Hardware und Firmware, den Zustand des Sensors, die Speichergeräte und die Netzwerkgeräte anzeigen. Darüber hinaus können Sie Benutzersitzungen anzeigen und beenden. Bei Blade-Servern können Sie auch die Flex-Adresse oder Remote-zugewiesene Adresse (gilt nur für MX-Plattformen) anzeigen.

Themen:

- Zustand und Eigenschaften des Managed System anzeigen
- Konfigurieren der Assetnachverfolgung
- Viewing system inventory
- Sensorinformationen anzeigen
- Überwachen des Leistungsindex für CPU, Arbeitsspeicher und Eingabe-/Ausgabemodule
- Erkennung inaktiver Server
- GPU-Verwaltung (Beschleuniger)
- Das System auf Frischlufttauglichkeit überprüfen
- Temperaturverlaufsdaten anzeigen
- Anzeigen der auf dem Host-Betriebssystem verfügbaren Netzwerkschnittstellen
- Anzeigen der auf dem Host-Betriebssystem verfügbaren Netzwerke über RACADM
- Verbindungen der FlexAddress-Mezzanine-Kartenarchitektur anzeigen
- Anzeigen und Beenden von iDRAC-Sitzungen

Zustand und Eigenschaften des Managed System anzeigen

Wenn Sie sich bei der iDRAC-Webschnittstelle anmelden, können Sie auf der Seite **Systemzusammenfassung** den Zustand des Managed System und Basis-iDRAC-Informationen anzeigen, eine Vorschau auf die virtuelle Konsole abrufen, Arbeitsnotizen hinzufügen und anzeigen und Aufgaben schnell starten, wie z. B. Aus- und Einschalten, Protokolle anzeigen, Firmware aktualisieren und Firmware-Rollback durchführen, die LED an der Frontblende ein- oder ausschalten und iDRAC zurücksetzen.

Um auf die Seite **Systemzusammenfassung** zuzugreifen, gehen Sie zu **System** > **Übersicht** > **Zusammenfassung**. Die Seite **Systemzusammenfassung** wird angezeigt. Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.

Außerdem können Sie die grundlegenden Systemzusammenfassungsinformationen über das Dienstprogramm für die iDRAC-Einstellungen anzeigen. Führen Sie dazu folgende Schritte durch: Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Systemzusammenfassung**. Daraufhin wird die Seite **iDRAC-Einstellungen – Systemzusammenfassung** angezeigt. Weitere Informationen finden Sie in der *iDRAC-Dienstprogramm-Online-Hilfe*.

Konfigurieren der Assetnachverfolgung

Die Assetnachverfolgungsfunktion in iDRAC bietet Ihnen die Möglichkeit zum Konfigurieren verschiedener Attribute, die in einer Beziehung zu Ihrem Server stehen. Hierzu gehören Informationen wie Erwerb, Garantie, Service usw.

ANMERKUNG: Die Assetnachverfolgung in iDRAC ist vergleichbar mit der Systemkennnummerfunktion in OpenManage-Serveradministrator. Die Attributinformationen müssen jedoch getrennt voneinander in beide Extras eingegeben werden, damit sie die relevanten Assetdaten aufführen.

So konfigurieren Sie die Assetnachverfolgung:

1. Navigieren Sie in der iDRAC-Schnittstelle zu **Konfiguration** > **Assetnachverfolgung**.

2. Klicken Sie auf **Benutzerdefinierte Assets hinzufügen**, um weitere Attribute hinzuzufügen, die nicht standardmäßig auf dieser Seite angezeigt werden.
3. Geben Sie alle relevanten Informationen zu Ihrem Server-Asset ein und klicken Sie auf **Anwenden**.
4. Navigieren Sie zum Anzeigen Ihres Assetnachverfolgungsberichts zu **System** > **Details** > **Assetnachverfolgung**.

Viewing system inventory

You can view information about the hardware and firmware components installed on the managed system. To do this, in iDRAC web interface, go to **System** > **Inventory**. For information about the displayed properties, see the *iDRAC Online Help*.

The Hardware Inventory section displays the information for the following components available on the managed system:

- iDRAC
- RAID controller
- Batteries
- CPUs
- DIMMs
- HDDs
- Backplanes
- Network Interface Cards (integrated and embedded)
- Video card
- SD card
- Power Supply Units (PSUs)
- Fans
- Fibre Channel HBAs
- USB
- NVMe PCIe SSD devices

The Firmware Inventory section displays the firmware version for the following components:

- BIOS
- Lifecycle Controller
- iDRAC
- OS driver pack
- 32-bit diagnostics
- System CPLD
- PERC controllers
- Batteries
- Physical disks
- Power supply
- NIC
- Fibre Channel
- Backplane
- Enclosure
- PCIe SSDs

NOTE:

- Software inventory displays only the last 4 bytes of the firmware version and the Release date information. For example, if the firmware version is FLVDL06, the firmware inventory displays DL06.
- When collecting software inventory using Redfish interface, the Release date information is displayed only for components which support rollback.

NOTE:

- If any device (Example: TPM) is in OFF state, then software inventory displays the version as **Not Available** or **0**. And if the application is not installed, then it shows the version as **Not Installed**.
- The default initial system date and time is shown as Installed date/ time in software inventory until a new device firmware version is installed using the DUP. Also, BIOS and iDRAC date/ time should be synchronized for components whose inventory details are obtained from BIOS (Example: BIOS, TPM).
- Installation date do not change if the updated version is same as the installed version.

NOTE: On the Dell PowerEdge FX2/FX2s servers, the naming convention of the CMC version displayed in the iDRAC GUI differs from that on the CMC GUI. However, the version remains the same.

When you replace any hardware component or update the firmware versions, make sure to enable and run the **Collect System Inventory on Reboot** (CSIOR) option to collect the system inventory on reboot. After a few minutes, log in to iDRAC, and navigate to the **System Inventory** page to view the details. It may take up to 5 minutes for the information to be available depending on the hardware installed on the server.

NOTE: CSIOR option is enabled by default.

NOTE: Configuration changes and firmware updates that are made within the operating system may not reflect properly in the inventory until you perform a server restart.

Click **Export** to export the hardware inventory in an XML format and save it to a location of your choice.

Sensorinformationen anzeigen

Die folgenden Sensoren unterstützen Sie bei der Überwachung des Zustands des verwalteten Systems:

- **Batterien** – Bietet Informationen zu den Batterien auf dem Hauptplatinen-CMOS und dem Speicher-RAID auf der Hauptplatine (ROMB).
  ANMERKUNG: Die Einstellungen für Speicher-ROMB-Batterien sind nur verfügbar, wenn das System einen ROMB mit einer Batterie aufweist.
- **Lüfter** (nur für Rack- und Tower-Server verfügbar) – Bietet Informationen zu Lüftern in Systemen – Lüfterredundanz und Lüfterliste, in der die Lüftergeschwindigkeit und die Schwellenwerte angezeigt werden.
- **CPU** – Zeigt den Funktionszustand und den Status der CPUs im verwalteten System an. Meldet außerdem automatische Prozessordrosselung und vorhergesagte Fehler.
- **Speicher** – Zeigt den Funktionszustand und den allgemeinen Zustand der im Managed System vorhandenen Speichermodule mit zwei Kontaktanschlussreihen (Dual In-line Memory Module, DIMM) an.
- **Eingriff** – Zeigt Informationen über das Gehäuse an.
- **Netzteil** (nur für Tack- und Tower-Server) – Bietet Informationen zu den Netzteilen und dem Status der Netzteilredundanz.
  ANMERKUNG: Wenn das System nur ein Netzteil aufweist, ist die Netzteilredundanz **deaktiviert**.
- **Entfernbarer Flash-Datenträger** – Bietet Informationen zu den internen SD-Modulen, vFlash und Internal Dual SD Module (IDSDM).
  - Wenn IDSDM-Redundanz aktiviert ist, werden die folgenden IDSDM-Sensorstatus angezeigt: IDSDM-Redundanzstatus, IDSDM SD1 und IDSDM SD2. Wenn Redundanz deaktiviert ist, wird nur IDSDM SD1 angezeigt.
  - Wenn IDSDM-Redundanz beim Einschalten des Systems oder nach dem Zurücksetzen von iDRAC deaktiviert wird, wird der IDSDM SD1-Sensorstatus nur angezeigt, wenn eine Karte eingesetzt wird.
  - Wenn die IDSDM-Redundanz bei zwei im IDSDM vorhandenen SD-Karten aktiviert ist und der Status einer SD-Karte online ist, während der Status der anderen Karte offline ist. Ein Systemneustart ist erforderlich, um die Redundanz zwischen den beiden SD-Karten im IDSDM wiederherzustellen. Nachdem die Redundanz wiederhergestellt ist, ist der Status der beiden SD-Karten im IDSDM online.
  - Während der Wiederherstellung der Redundanz zwischen zwei SD-Karten, die sich im IDSDM befinden, wird der IDSDM-Status nicht angezeigt, da die IDSDM-Sensoren ausgeschaltet sind.
    ANMERKUNG: Wenn das Hostsystem während des IDSDM-Wiederherstellungsvorgangs neu gestartet wird, zeigt der iDRAC die IDSDM-Informationen nicht an. Um dieses Problem zu beheben, erstellen Sie das IDSDM neu, oder setzen Sie den iDRAC zurück.
  - Die Systemereignisprotokolle (SEL) für eine schreibgeschützte oder beschädigte SD-Karte im IDSDM-Modul werden erst wiederholt, nachdem sie durch das Ersetzen der SD-Karte durch eine beschreibbare und funktionsfähige SD-Karte gelöscht wurden.

  ANMERKUNG: Wenn die iDRAC-Firmware von Versionen vor 3.30.30.30 aktualisiert wird, muss der iDRAC auf die Standardwerte zurückgesetzt werden, damit die IDSDM-Einstellungen im Plattformereignisfilter des Serveradministrators angezeigt werden.
- **Temperatur** – Bietet Informationen zu den Lufteintritts- und Luftaustrittstemperaturen auf der Systemplatine (nur bei Rack-Servern). Die Temperatursonde zeigt an, ob der Status der Sonde innerhalb der voreingestellten Warn- und Grenzwerte liegt.
- **Spannung** – Zeigt den Status und die Messwerte des Spannungssensors für verschiedene Systemkomponenten an.

Die folgende Tabelle enthält Informationen zum Anzeigen der Sensorinformationen über die iDRAC-Webschnittstelle und RACADM. Informationen zu den Eigenschaften, die auf der Weboberfläche angezeigt werden, finden Sie in der *iDRAC-Onlinehilfe*.

ANMERKUNG: Die Seite „Hardware-Übersicht“ zeigt nur Daten für Sensoren an, die auf Ihrem System vorhanden sind.

Tabelle 17. Abrufen von Sensorinformationen über die Web-Schnittstelle und RACADM

Sensorinformationen anzeigen für	über die Web-Schnittstelle	RACADM verwenden
Batterien	**Dashboard** > **Systemzustand** > **Akkus**	Verwenden Sie den Befehl `getsensorinfo`. Bei Netzteilen können Sie außerdem den Befehl `System.Power.Supply` mit dem Unterbefehl `get` verwenden. Weitere Informationen finden Sie unter *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.
Lüfter	**Dashboard** > > **Systemzustand** > **Lüfter**	
CPU	**Dashboard** > **Systemzustand** > **CPU**	
Speicher	**Dashboard** > **Systemzustand** > **Arbeitsspeicher**	
Eingriff	**Dashboard** > **Systemzustand** > **Eingriff**	
Netzteile	> **Hardware** > **Netzteile**	
Wechselbarer Flash-Datenträger	**Dashboard** > **Systemzustand** > **Wechselbarer Flash-Datenträger**	
Temperatur	**Dashboard** > **Systemzustand** > **Strom und Temperatur** > **Temperaturen**	
Spannung	**Dashboard** > **Systemzustand** > **Strom und Temperatur** > **Spannungen**	

Überwachen des Leistungsindex für CPU, Arbeitsspeicher und Eingabe-/Ausgabemodule

In der 14. Generation der Dell PowerEdge-Server bietet Intel ME Unterstützung für die Funktion „Datenverarbeitungsauslastung pro Sekunde“ (Compute Usage Per Second, CUPS). Die CUPS-Funktion bietet eine Echtzeitüberwachung der CPU-, Arbeitsspeicher- und I/O-Auslastung sowie einen Auslastungsindex für das gesamte System. Intel ME erlaubt das Out-of-band-Performancemonitoring und beansprucht keine CPU-Ressourcen. Intel ME verfügt über einen System-CUPS-Sensor, der Auslastungswerte für die Datenverarbeitung, den Arbeitsspeicher und die I/O-Ressourcen als CUPS-Index bereitstellt. iDRAC überwacht den CUPS-Index für die Systemauslastung und auch die momentanen Werte des CPU-, Arbeitsspeicher- und I/O-Auslastungsindex.

ANMERKUNG: Die CUPS-Funktion wird auf den folgenden Servern nicht unterstützt:

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

Die CPU und der Chipsatz verfügen über dedizierte Ressourcenüberwachungsindikatoren (RMC). Die Daten aus diesen RMCs werden abgefragt, um Auslastungsinformationen der Systemressourcen zu erhalten. Die Daten von den RMCs werden vom Node-Manager aggregiert, um die kumulative Auslastung der einzelnen Systemressourcen zu ermitteln, die vom iDRAC über die vorhandenen Interkommunikationsverfahren gelesen werden, um diese Daten über Out-of-band-Managementschnittstellen bereitzustellen.

Die Darstellung von Intel Sensoren für Leistungsparameter und Indexwerte bezieht sich auf das gesamte physische System. Daher bezieht sich die Darstellung der Leistungsdaten auf den Schnittstellen ebenfalls auf das gesamte physische System, selbst wenn das System virtualisiert ist und mehrere virtuelle Hosts enthält.

Zum Anzeigen der Leistungsparameter müssen die unterstützten Sensoren auf dem Server vorhanden sein.

Die vier Systemauslastungsparameter sind:

- **CPU-Auslastung** – Die Daten der RMCs für jeden CPU-Kern werden zusammengefasst, um eine kumulative Auslastung aller Kerne im System bereitzustellen. Diese Auslastung basiert auf der jeweiligen Zeit im aktiven und inaktiven Zustand. Alle sechs Sekunden wird eine RMC-Probe genommen.
- **Speicherauslastung** – Die RMCs messen den Speicherdatenverkehr, der in den einzelnen Speicherkanälen oder Speicher-Controller-Instanzen auftritt. Die Daten von den RMCs werden kombiniert, um den gesamten Speicherdatenverkehr über alle Speicherkanäle im System zu messen. Dies ist eine Messung des Speicherbandbreitenverbrauchs und nicht der Auslastung des Arbeitsspeichers. iDRAC sammelt die Daten eine Minute lang, so dass sie eventuell nicht der von Tools in anderen Betriebssystemen, z. B. TOP in Linux, angezeigten Speicherauslastung entsprechen. Die Auslastung der Speicherbandbreite, die vom iDRAC angezeigt wird, ist ein Hinweis darauf, ob ein Workload arbeitsspeicherintensiv ist oder nicht.
- **I/O-Auslastung** – Es gibt einen RMC für jeden Root-Anschluss im PCI Express-Root-Komplex, um den PCI Express-Datenverkehr zu messen, der von bzw. zu diesem Root-Anschluss und dem unteren Segment fließt. Die Daten der RMCs werden aggregiert, um den PCI Express-Datenverkehr für alle PCI Express-Segmente des Pakets zu messen. Dies ist eine Messung der I/O-Bandbreitennutzung für das System.
- **CUPS-Index auf Systemebene** – Der CUPS-Index wird berechnet, indem CPU-, Arbeitsspeicher- und I/O-Index unter Berücksichtigung eines vordefinierten Auslastungsfaktors für jede Systemressource kombiniert werden. Der Auslastungsfaktor hängt von der Art des Workloads auf dem System ab. Der CUPS-Index stellt den Wert der Computing-Kapazitäten auf dem Server dar. Wenn das System über einen hohen CUPS-Index verfügt, steht nur wenig Kapazität für zusätzliche Workloads auf dem System zur Verfügung. Mit abnehmendem Ressourcenverbrauch reduziert sich auch der CUPS-Index des Systems. Ein niedriger CUPS-Index gibt an, dass eine hohe Computing-Kapazität verfügbar ist und der Server neue Workloads empfangen kann. Der Server befindet sich zudem in einem niedrigeren Energiezustand, um den Energieverbrauch zu reduzieren. Die Workload-Überwachung kann dann auf das gesamte Rechenzentrum angewendet werden, um eine ganzheitliche Übersicht über die Auslastung des Rechenzentrums zu erhalten und damit eine dynamische Rechenzentrumslösung bereitstellen zu können.

ANMERKUNG: Die CPU-, Arbeitsspeicher- und I/O-Auslastungsindizes werden über einen Zeitraum von einer Minute aggregiert. Wenn es unmittelbare Spitzen in diesen Indizes gibt, werden diese möglicherweise unterdrückt. Diese sind ein Anzeichen für Workload-Muster, nicht für die Menge der Ressourcenauslastung.

Die IPMI-, SEL- und SNMP-Traps werden generiert, wenn die Grenzwerte für die Auslastungsindizes erreicht und die Sensorereignisse aktiviert sind. Die Sensorereigniskennzeichnungen sind standardmäßig deaktiviert. Sie können jedoch über die Standard-IPMI-Schnittstelle aktiviert werden.

Im Folgenden werden die erforderlichen Berechtigungen aufgeführt:

- Anmeldeberechtigung für die Überwachung der Leistungsdaten
- Konfigurationsberechtigung für das Einstellen der Warnungsschwellenwerte und das Zurücksetzen der Verlaufsspitzen
- Anmeldeberechtigung und eine Enterprise-Lizenz sind erforderlich, um historische Statistikdaten zu lesen.

Überwachen des Leistungsindex von CPU, Speicher und E/A-Modulen über die Webschnittstelle

Um den Leistungsindex von CPU, Speicher und E/A-Modulen zu überwachen, gehen Sie in der iDRAC-Webschnittstelle zu **System** > **Performance (Leistung)**.

- Abschnitt **Systemleistung** – Zeigt den aktuellen Messwert und den Warnungsmesswert für den CPU-, Speicher- und E/A-Auslastungsindex sowie den CUPS-Index auf Systemebene in einer grafischen Ansicht an.
- Abschnitt **Historische Daten der Systemleistung**:
  - Enthält die Statistiken zu CPU, Arbeitsspeicher und E/A-Auslastung sowie den CUPS-Index auf Systemebene. Wenn das Host-System ausgeschaltet ist, zeigt das Diagramm die Ausschaltungslinie unter 0 %.
  - Sie können die maximale Auslastung für einen bestimmten Sensor zurücksetzen. Klicken Sie auf **Reset Historical Peak** (Historischen Spitzenwert zurücksetzen). Sie müssen über die Berechtigung zur Konfiguration verfügen, um den Spitzenwert zurückzusetzen.
- Abschnitt **Leistungskennzahlen**:
  - Zeigt den Status an und präsentiert Messwerte .
  - Zeigt den Warnungsschwellenwerte für die Auslastung an oder legt ihn fest. Sie müssen über Berechtigungen zum Konfigurieren des Servers verfügen, um die Schwellenwerte festlegen zu können.

Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der *iDRAC-Online-Hilfe*.

Überwachen des Leistungsindex für CPU-, Speicher- und E/A-Module über RACADM

Verwenden Sie den Unterbefehl **SystemPerfStatistics** zur Überwachung des Leistungsindex für CPU, Arbeitsspeicher und E/A-Module. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Erkennung inaktiver Server

Der iDRAC bietet einen bandexternen Leistungsüberwachungsindex der Server-Komponenten wie CPU, Speicher und E/A.

Die Verlaufsdaten für des CUPS-Index auf Server-Ebene werden verwendet, um zu überwachen, ob der Server für lange Zeit genutzt wird oder inaktiv ist. Wenn der Server für eine definierte Zeitspanne (in Stunden) unter einem bestimmten Schwellenwert ausgelastet ist, wird er als inaktiver Server gemeldet.

Diese Funktion wird nur auf Intel-Plattformen mit CUPS-Fähigkeit unterstützt. AMD- und Intel-Plattformen ohne CUPS-Funktion unterstützen diese Funktion nicht.

ANMERKUNG:

- Für diese Funktion wird eine Datacenter-Lizenz benötigt.
- Zum Lesen der Konfigurationen der Parameter inaktiver Server benötigen Sie Anmeldeberechtigungen und zum Ändern der Parameter benötigen Sie iDRAC-Konfigurationsberechtigungen.

Um die Parameter anzuzeigen oder zu ändern, navigieren Sie zu **Konfiguration** > **Systemeinstellungen**.

Die Erkennung inaktiver Server wird basierend auf den folgenden Parametern gemeldet:

- Schwellenwert für inaktive Server (%) – Dieser Wert ist standardmäßig auf 20 % eingestellt und kann von 0 bis 50 % konfiguriert werden. Der Reset-Vorgang setzt den Schwellenwert auf 20 %.
- Prüfintervall für inaktive Server (in Stunden): Dies ist der Zeitraum, in dem die stündlichen Stichproben erfasst werden, um inaktive Server zu bestimmen. Standardmäßig ist dieser Wert auf 240 Stunden festgelegt und kann von 1 bis 9000 Stunden konfiguriert werden. Der Reset-Vorgang setzt das Intervall auf 240 Stunden.
- Prozentwert für Server-Auslastung (%) – Der Wert für die Auslastung in Prozent kann von 80 bis 100 % eingestellt werden. Der Standardwert ist 80 %. Wenn 80 % der stündlichen Stichproben unter den Auslastungsgrenzwert fallen, gilt ein Server als inaktiv.

Ändern der Parameter für die Erkennung inaktiver Server mit RACADM

```
racadm get system.idleServerDetection
```

Ändern der Parameter für die Erkennung inaktiver Server mit Redfish

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

Ändern der Parameter für die Erkennung inaktiver Server mit WSMAN

```
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
```

ANMERKUNG: Die iDRAC-Benutzeroberfläche unterstützt nicht das Anzeigen oder Ändern der Attribute.

GPU-Verwaltung (Beschleuniger)

Dell PowerEdge Server werden mit Graphics Processing Unit (GPU) ausgeliefert. Mithilfe der GPU-Verwaltung können Sie die verschiedenen GPUs anzeigen, die mit dem System verbunden sind, und außerdem die Strom-, Temperatur- und Wärme Informationen für die GPUs überwachen.

ANMERKUNG: Dies ist eine lizenzierte Funktion und im Rahmen einer iDRAC Datacenter oder Enterprise Lizenz verfügbar. Nachfolgend sind die Eigenschaften aufgeführt, die mit der Datacenter/Enterprise Lizenz zur Verfügung stehen. Andere Eigenschaften werden auch ohne diese Lizenzen aufgeführt:

GPU-Eigenschaften	Datacenter Lizenz	Enterprise-Lizenz
Temperaturkennzahlen		
GPU-Zieltemperatur	Ja	Nein
Min. GPU-HW-Drosselungstemperatur	Ja	Nein
GPU-Temperatur beim Herunterfahren	Ja	Nein
Max. Speicher-Betriebstemperatur	Ja	Nein
Max. GPU-Betriebstemperatur	Ja	Nein
Temperatur-Warnmeldungsstatus	Ja	Nein
Strombremsstatus	Ja	Nein
Stromkennzahlen		
Netzteilstatus	Ja	Nein
Stromversorgungsstatus der Platine	Ja	Nein
Telemetrie		
Alle Telemetrie-Berichtsdaten	Ja	Nein

ANMERKUNG: GPU-Eigenschaften werden nicht für integrierte GPU-Karten aufgelistet und der Status wird als **Unbekannt** gekennzeichnet.

Die GPU muss sich im Zustand „Bereit“ befinden, bevor der Befehl die Daten abruft. Das Feld GPU-Status im Bestand zeigt die Verfügbarkeit der GPU an und ob das GPU-Gerät reagiert oder nicht. Wenn der GPU-Status „Bereit“ lautet, zeigt GPUStatus „OK“ an, andernfalls wird der Status „Nicht verfügbar“ angezeigt.

Die GPU bietet mehrere Integritätsparameter, die über die SMBPB-Schnittstelle der NVIDIA-Controller abgerufen werden können. Diese Funktion ist nur auf NVIDIA-Karten beschränkt. Es folgen die Integritätsparameter, die vom GPU-Gerät abgerufen werden:

- Stromversorgung
- Temperatur
- Thermisch

ANMERKUNG: Diese Funktion ist nur auf NVIDIA-Karten beschränkt. Diese Informationen sind für keine andere GPU verfügbar, die der Server möglicherweise unterstützt. Das Intervall, in dem die GPU-Karten über die PBI abgefragt werden, beträgt 5 Sekunden.

Auf dem Hostsystem muss der NVIDIA-Treiber installiert sein und ausgeführt werden, damit die Funktionen Stromverbrauch, GPU-Zieltemperatur, Min. GPU-Drosselungstemperatur, GPU-Temperatur beim Herunterfahren, Max. Speicher-Betriebstemperatur und Max. Speicher-Betriebstemperatur verfügbar sind. Diese Werte werden als **N/A** angezeigt, wenn der GPU-Treiber nicht installiert ist.

Wenn in Linux die Karte nicht verwendet wird, trainiert der Treiber die Karte nach unten und wird entladen, um Energie zu sparen. In solchen Fällen sind die Funktionen Stromverbrauch, GPU-Zieltemperatur, Min. GPU-Drosselungstemperatur, GPU-Temperatur beim Herunterfahren, Max. Speicher-Betriebstemperatur und Max. Speicher-Betriebstemperatur nicht verfügbar. Der persistente Modus sollte für das Gerät aktiviert werden, um eine Entladung zu vermeiden. Sie können das NVIDIA-SMI-Tool verwenden, um dies mithilfe `nvidia-smi -pm 1` zu aktivieren.

Sie können GPU-Berichte mithilfe von Telemetrie erzeugen. Weitere Informationen zur Telemetriefunktion finden Sie unter Telemetry Streaming auf Seite 220

ANMERKUNG: In RACADM werden möglicherweise Dummy-GPU-Einträge mit leeren Werten angezeigt. Dies kann der Fall sein, wenn das Gerät nicht bereit ist zu reagieren, wenn der iDRAC die Informationen vom GPU-Gerät abfragt. Führen Sie den iDRAC-Vorgang `racrest` durch, um dieses Problem zu beheben.

FPGA-Monitoring

Field-Programmable Gate Array-Geräte (FPGA) benötigen eine Echtzeitüberwachung des Temperatursensors, da sie bei Verwendung erhebliche Wärme erzeugen. Führen Sie die folgenden Schritte aus, um FPGA-Bestandsinformationen abzurufen:

- Schalten Sie den Server aus.
- Installieren Sie das FPGA-Gerät auf der Riser-Karte.
- Schalten Sie den Server ein.
- Warten Sie, bis der POST abgeschlossen ist.
- Melden Sie sich in der iDRAC-GUI an.
- Navigieren Sie zu **System** > **Übersicht** > **Beschleuniger**. Es werden sowohl der GPU- als auch der FPGA-Abschnitt angezeigt.
- Erweitern Sie die spezifische FPGA-Komponente, um die folgenden Sensorinformationen anzuzeigen:
  - Stromverbrauch
  - Temperaturdetails

ANMERKUNG: Sie müssen über die iDRAC-Anmeldeberechtigung verfügen, um auf FPGA-Informationen zugreifen zu können.

ANMERKUNG: Stromverbrauchssensoren stehen nur für die unterstützten FPGA-Karten zur Verfügung und sind nur mit einer Datacenter-Lizenz verfügbar.

Das System auf Frischlufttauglichkeit überprüfen

Die Frischluftkühlung kühlt die Systeme im Datenzentrum direkt mit Außenluft. Frischlufttaugliche Systeme können oberhalb ihres normalen Betriebstemperaturbereichs (Temperaturen bis zu 45 °C (113 °F)) betrieben werden.

ANMERKUNG: Manche Server oder bestimmte Konfigurationen eines Servers sind möglicherweise nicht frischlufttauglich. Weitere Informationen zur Frischluftkompatibilität finden Sie im jeweiligen Serverhandbuch. Alternativ können Sie sich an Dell wenden, um weitere Informationen zu erhalten.

So prüfen Sie das System auf Frischlufttauglichkeit:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **System** > **Overview (Übersicht)** > **Cooling (Kühlung)** > **Temperature overview (Temperaturübersicht)**.
   Die Seite **Temperature overview** (Temperaturübersicht) wird angezeigt.
2. Im Bereich **Frischluft** wird angezeigt, ob das System frischlufttauglich ist oder nicht.

Temperaturverlaufsdaten anzeigen

Sie können die Zeit in Prozent überwachen, die das System bei Umgebungstemperaturen oberhalb des normalerweise unterstützten Temperaturschwellenwertes für Frischluftkühlung in Betrieb war. Der Temperatursensormesswert der Systemplatine wird über einen gewissen Zeitraum erfasst, um die Temperatur zu überwachen. Die Datenerfassung beginnt beim ersten Einschalten nach dem Versand aus dem Werk. Die Daten werden erfasst und angezeigt, während das System eingeschaltet ist. Sie können die überwachte Temperatur für die letzten sieben Jahre verfolgen und speichern.

ANMERKUNG: Sie können den Verlauf der Temperatur auch für Systeme verfolgen, die nicht Fresh-Air-kompatibel sind. Die Schwellenwerte und die Frischluft-bezogenen generierten Warnungen basieren auf den Grenzwerten für Frischluftkühlung. Die Grenzwerte liegen bei 42 °C für Warnung und bei 47 °C für kritisch. Diese Werte entsprechen Frischluftgrenzwerten von 40 °C und 45 °C mit 2 °C Genauigkeitsgrenze.

Es werden zwei feste Temperaturbereiche erfasst, die mit Grenzwerten für Frischluftkühlung verknüpft sind:

- Warnbereich – besteht aus der Dauer, die das System oberhalb des Warnschwellenwerts für den Temperatursensor (42 °C) in Betrieb war. Das System darf innerhalb von zwölf Monaten 10 % der Zeit im Warnbereich betrieben werden.
- Kritischer Bereich – besteht aus der Dauer, die das System oberhalb des kritischen Schwellenwerts für den Temperatursensor (47 °C) in Betrieb war. Das System darf innerhalb von zwölf Monaten 1 % der Zeit im kritischen Bereich betrieben werden, was auch die Zeit im Warnbereich erhöht.

Die erfassten Daten werden grafisch dargestellt, damit Sie die Zeitdauer in den Bereichen von 10 % und 1 % verfolgen können. Die protokollierten Temperaturdaten können nur vor dem Versand vom Werk gelöscht werden.

Es wird ein Ereignis generiert, wenn das System weiterhin oberhalb des normalerweise unterstützten Temperaturschwellwerts während einer angegebenen Betriebszeit in Betrieb ist. Liegt die Durchschnittstemperatur während der angegebenen Betriebszeit über oder auf der Warnungsebene (> = 8 %) oder über oder auf der kritischen Ebene (> = 0,8 %), wird in dem Lifecycle-Protokoll ein Ereignis protokolliert und der entsprechende SNMP-Trap erstellt. Es werden die folgenden Ereignisse angezeigt:

- Warnereignis, wenn die Temperatur während 8 % oder mehr der vergangenen zwölf Monate oberhalb des Warnschwellenwertes lag.
- Kritisches Ereignis, wenn die Temperatur während 10 % oder mehr der vergangenen zwölf Monate oberhalb des Warnschwellenwertes lag.
- Warnereignis, wenn die Temperatur während 0,8 % oder mehr der vergangenen zwölf Monate oberhalb des kritischen Schwellenwertes lag.
- Kritisches Ereignis, wenn die Einlasstemperatur während 1 % oder mehr der vergangenen zwölf Monate oberhalb des kritischen Schwellenwertes lag.

Sie können iDRAC auch so konfigurieren, dass weitere kritische Ereignisse generiert werden. Weitere Informationen finden Sie im Abschnitt Alarmwiederholungsereignis einrichten auf Seite 185.

Anzeigen der Temperaturverlaufsdaten über die iDRAC-Webschnittstelle

So zeigen Sie den Verlauf der Temperaturdaten an:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **System** > **Übersicht** > **Kühlung** > **Temperaturübersicht**.
   Die Seite **Temperaturübersicht** wird angezeigt.
2. Im Bereich **Verlauf der Systemplatinentemperatur** wird in einem grafischen Schaubild die gespeicherte Temperatur (Durchschnitts- und Spitzenwerte) für den letzten Tag, die letzten 30 Tage und das letzte Jahr angezeigt.

   Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.

   ANMERKUNG: Nach einer Aktualisierung der iDRAC-Firmware oder einem Reset des iDRAC werden manche Temperaturdaten möglicherweise nicht mehr im Schaubild angezeigt.

   ANMERKUNG: Die WX3200 AMD GPU-Karte unterstützt derzeit nicht die I2C-Schnittstelle für Temperatursensoren. Daher sind für diese Karte keine Temperaturmesswerte über iDRAC-Schnittstellen verfügbar.

Temperaturverlaufsdaten über RACADM anzeigen

Um den Datenverlauf unter Verwendung von RACADM anzuzeigen, verwenden Sie den Befehl `inlettemphistory`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Konfigurieren des Warnungsschwellenwerts für die Einlasstemperatur

Sie können die minimalen und maximalen Warnungsschwellenwerte für den Einlasstemperatursensor der Systemplatine ändern. Wenn Sie den Vorgang zum Zurücksetzen auf die Standardwerte ausführen, werden die Temperaturschwellenwerte auf die Standardwerte eingestellt. Sie müssen über Benutzerberechtigungen zum Konfigurieren verfügen, um die Warnungsschwellenwerte für den Einlasstemperatursensor festzulegen.

Konfigurieren der Warnschwelle für die Einlasstemperatur über die Webschnittstelle

So konfigurieren Sie den Warnungsschwellenwert für die Einlasstemperatur:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **System** > **Übersicht** > **Kühlung** > **Temperaturübersicht**.
   Die Seite **Temperaturübersicht** wird angezeigt.
2. Geben Sie im Abschnitt **Temperatursonden** für die **Systemplatinen-Eingangstemperatur** den minimalen und den maximalen Wert für den **Warnschwellenwert** in Grad Celsius oder Fahrenheit ein. Wenn Sie den Wert in Celsius eingeben, berechnet das System automatisch den Wert in Fahrenheit und zeigt ihn an. Wenn Sie die Werte in Fahrenheit eingeben, werden die Werte in Celsius angezeigt.

3. Klicken Sie auf **Anwenden**.

   Die Werte werden konfiguriert.

   ANMERKUNG: Änderungen an den Standardschwellenwerten werden im Diagramm mit den Verlaufsdaten nicht berücksichtigt, da die Diagrammgrenzen nur für Frischluftgrenzwerte gelten. Warnmeldungen zum Überschreiten der benutzerdefinierten Schwellenwerte unterscheiden sich von der Warnmeldung, die mit der Überschreitung der Schwellenwerte für Frischluft verbunden ist.

Anzeigen der auf dem Host-Betriebssystem verfügbaren Netzwerkschnittstellen

Sie können Informationen über alle auf dem Host-Betriebssystem verfügbaren Netzwerkschnittstellen anzeigen, z. B. die IP-Adressen, die dem Server zugewiesen wurden. Das iDRAC Service Module gibt diese Informationen an den iDRAC weiter. Die Informationen zur Betriebssystem-IP-Adresse umfassen die IPv4- und IPv6-Adressen, die MAC-Adresse, die Subnetzmaske oder Präfixlänge, die FQDD des Netzwerkgeräts, den Namen der Netzwerkschnittstelle, die Beschreibung der Netzwerkschnittstelle, den Status der Netzwerkschnittstelle, den Netzwerkschnittstellentyp (Ethernet, Tunnel, Loopback usw.), die Gateway-Adresse, die DNS-Serveradresse und die Adresse des DHCP-Servers.

ANMERKUNG: Diese Funktion ist mit den iDRAC Express und Enterprise/Datacenter Lizenzen erhältlich.

Zum Anzeigen der Informationen zum Betriebssystem, stellen Sie Folgendes sicher:

- Sie verfügen über die Berechtigung zur Anmeldung.
- Das iDRAC-Service-Modul ist auf dem Host-Betriebssystem installiert und wird ausgeführt.
- Die Option zur Anzeige der Betriebssysteminformationen ist auf der Seite **iDRAC-Einstellungen** > **Übersicht** > **iDRAC Servicemodul** aktiviert.

iDRAC kann die IPv4- und IPv6-Adressen für alle Schnittstellen anzeigen, die auf dem Host-Betriebssystem konfiguriert sind.

Je nach vom Host-Betriebssystem für die Ermittlung des DHCP-Servers verwendeter Methode kann die zugehörige IPv4- oder IPv6-DHCP-Server-Adresse möglicherweise nicht angezeigt werden.

Anzeigen von verfügbaren Netzwerkschnittstellen auf dem Host-Betriebssystem über die Webschnittstelle

So zeigen Sie die Netzwerkschnittstellen auf dem Host-Betriebssystem über die Webschnittstelle an:

1. Wechseln Sie zu **System** > **Host OS (Host-Betriebssystem)** > **Network Interfaces (Netzwerkschnittstellen)**.
   Die Seite **Netzwerkschnittstellen** zeigt alle Netzwerkschnittstellen an, die auf dem Host-Betriebssystem verfügbar sind.
2. Um die Liste der Netzwerkschnittstellen anzuzeigen, die mit einem Netzwerkgerät verknüpft sind, wählen Sie ein Netzwerkgerät aus dem Drop-Down-Menü **Netzwerkgeräte-FQDD** aus, und klicken Sie dann auf **Anwenden**.
   Die Betriebssystem-IP-Details werden im Abschnitt **Host-BS-Netzwerkschnittstellen** angezeigt.
3. Klicken Sie in der Spalte **Geräte-FQDD** auf den Link für das Netzwerkgerät.

   Die entsprechende Geräteseite wird im Abschnitt **Hardware** > **Network Devices (Netzwerkgeräte)** angezeigt, in dem Sie die Gerätedetails einsehen können. Weitere Informationen zu den Eigenschaften finden Sie in der *iDRAC Online-Hilfe*.
4. Klicken Sie auf das Symbol +, um weitere Informationen zu erhalten.

   In ähnlicher Weise können Sie die Informationen zur Host-Betriebssystem-Netzwerkschnittstelle anzeigen, die mit einem Netzwerkgerät verknüpft sind. Diese Informationen befinden sich auf der Seite **Hardware** > **Network Devices (Netzwerkgeräte)**. Klicken Sie auf **View Host OS Network Interfaces** (Host-BS-Netzwerkschnittstellen anzeigen).

   ANMERKUNG: Ab Version 2.3.0 des iDRAC-Servicemoduls wird für das ESXi-Host-BS die Spalte **Beschreibung** in der Liste **Zusätzliche Details** in folgendem Format angezeigt:

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

Anzeigen der auf dem Host-Betriebssystem verfügbaren Netzwerke über RACADM

Verwenden Sie den Befehl `gethostnetworkinterfaces`, um die Netzwerkschnittstellen auf Host-Betriebssystemen über RACADM anzuzeigen. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Verbindungen der FlexAddress-Mezzanine-Kartenarchitektur anzeigen

In Blade Servern ermöglicht FlexAddress die Verwendung von beständigen, dem Gehäuse zugewiesenen World-Wide-Namen und MAC-Adressen (WWN/MAC) für jede verwaltete Server-Anschlussverbindung.

Sie können die folgenden Informationen für jede installierte eingebettete Ethernet- und optionalen Mezzanine-Kartenschnittstelle anzeigen:

- Strukturen, mit denen die Karten verbunden sind
- Strukturtyp
- MAC-Adressen, die Servern, Gehäusen oder remote zugewiesen sind

Um die Flex-Adressinformationen im iDRAC anzuzeigen, konfigurieren und aktivieren Sie die Flex-Adressfunktion im CMC (Chassis Management Controller). Weitere Informationen finden Sie im *Chassis Management Controller – Handbuch* verfügbar unter https://www.dell.com/cmcmanuals. Jede vorhandene virtuelle Konsolen- oder virtuelle Datenträger-Sitzung wird beendet, wenn die FlexAddress-Einstellung aktiviert oder deaktiviert wird.

ANMERKUNG: Um Fehler zu vermeiden, die zu einer Stromunterversorgung auf dem verwalteten System führen können, *muss* der richtige Mezzanine-Kartentyp für jede Anschluss- und Architekturverbindung installiert sein.

Die FlexAddress-Funktion ersetzt die vom Server zugewiesenen MAC-Adressen durch Gehäuse-zugewiesene MAC-Adressen und wird für den iDRAC zusammen mit Blade-LOMs, Zusatzkarten und I/O-Modulen implementiert. Die iDRAC FlexAddress-Funktion unterstützt die Beibehaltung der Steckplatz-spezifischen MAC-Adresse für iDRACs in einem Gehäuse. Die Gehäuse-zugewiesene MAC-Adresse wird im nichtflüchtigen CMC-Speicher abgelegt und während eines iDRAC-Bootvorgangs oder bei aktivierter CMC FlexAddress an den iDRAC gesendet.

Wenn CMC Gehäusen zugewiesene MAC-Adressen aktiviert, zeigt iDRAC die **MAC-Adresse** auf den folgenden Seiten an:

- **System Details iDRAC-Informationen**.
- **System Server WWN/MAC-**.
- **iDRAC-Einstellungen** > **Übersicht** > **Aktuelle Netzwerkeinstellungen**.

VORSICHT: Wenn Sie bei aktivierter FlexAddress zwischen Server-zugewiesener MAC-Adresse und Gehäuse-zugewiesener MAC-Adresse umschalten oder umgekehrt, ändert sich auch die iDRAC-IP-Adresse.

Anzeigen und Beenden von iDRAC-Sitzungen

Sie können die Anzahl der Benutzer anzeigen, die derzeit bei iDRAC angemeldet sind, und die Benutzersitzungen beenden.

Beenden der iDRAC-Sitzungen über die Webschnittstelle

Benutzer ohne Administratorberechtigungen benötigen eine Berechtigung zum Konfigurieren von iDRAC, um iDRAC-Sitzungen über die iDRAC-Webschnittstelle beenden zu können.

So zeigen Sie die iDRAC-Sitzungen an und beenden sie:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Users (Benutzer)** > **Sessions (Sitzungen)**.
   Auf der Seite **Sessions** (Sitzungen) werden die Sitzungs-ID, der Benutzername, die IP-Adresse und der Sitzungstyp angezeigt. Weitere Informationen zu diesen Eigenschaften finden Sie in der *iDRAC-Online-Hilfe*.
2. Klicken Sie zum Beenden der Sitzung in der Spalte **Beenden** auf das Papierkorbsymbol für eine Sitzung.

Beenden von iDRAC-Sitzungen über RACADM

Sie benötigen Administratorberechtigungen, um iDRAC-Sitzungen über RACADM beenden zu können.

Verwenden Sie zum Anzeigen der aktuellen Benutzersitzungen den Befehl `getssninfo`.

Verwenden Sie zum Beenden einer Benutzersitzung den Befehl `closessn`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

8

Einrichten der iDRAC-Kommunikation

Sie können über eine der folgenden Modi mit iDRAC kommunizieren:

- iDRAC-Weboberfläche
- Serielle Verbindung mithilfe eines DB9-Kabels (serielle RAC-Verbindung oder serielle IPMI-Verbindung) – nur für Rack- und Tower-Server
- Serielle IPMI-Verbindung über LAN
- IPMI über LAN
- Remote-RACADM
- Lokaler RACADM
- Remote-Dienste

ANMERKUNG: Um sicherzustellen, dass lokale RACADM Import- oder Exportbefehle ordnungsgemäß funktionieren, vergewissern Sie sich, dass der USB-Massenspeicherhost im Betriebssystem aktiviert ist. Informationen zum Aktivieren des USB-Speicherhosts finden Sie in der Dokumentation Ihres Betriebssystems.

Die folgende Tabelle enthält eine Übersicht der unterstützten Protokolle und Befehle sowie die Voraussetzungen:

Tabelle 18. Kommunikationsmodi – Übersicht

Kommunikationsmodus	Unterstütztes Protokoll	Unterstützte Befehle	Voraussetzung
iDRAC-Weboberfläche	Internet-Protokolle (https)	k. A.	Webserver
Serielle Verbindung über Null-Modem-DB9-Kabel	Protokoll für serielle Verbindung	RACADM IPMI	Teil der iDRAC-Firmware Serielle RAC- oder IPMI-Verbindungen ist aktiviert
Serielle IPMI-Verbindung über LAN	Intelligent Platform Management Bus-Protokoll SSH	IPMI	IPMITool ist installiert, und die serielle IPMI-Verbindung über LAN ist aktiviert
IPMI über LAN	Intelligent Platform Management Bus-Protokoll	IPMI	IPMITool ist installiert und die IPMI-Einstellungen sind aktiviert
Remote-RACADM	HTTPS	Remote-RACADM	Remote-RACADM ist installiert und aktiviert
Firmware RACADM	SSH	Firmware RACADM	Firmware-RACADM ist installiert und aktiviert.
Lokaler RACADM	IPMI	Lokaler RACADM	Lokaler RACADM ist installiert
Remote-Dienste [1]	WSMan	WinRM (Windows) OpenWSMan (Linux)	WinRM ist installiert (Windows) oder OpenWSMan ist installiert (Linux)
	Redfish	Verschiedene Browser-Plug-ins, CURL (Windows und Linux), Python-Aufforderung und JSON-Module	Plug-ins, CURL, Python Module sind installiert
[1] Weitere Informationen finden Sie unter *Benutzerhandbuch für den Lifecycle Controller* verfügbar unter https://www.dell.com/idracmanuals.			

Themen:

- Mit iDRAC über eine serielle Verbindung über ein DB9-Kabel kommunizieren
- Von der seriellen RAC-Verbindung auf die serielle Konsolenverbindung bei Verwendung eines DB9-Kabels umschalten

- Mit iDRAC über IPMI SOL kommunizieren
- Mit iDRAC über IPMI über LAN kommunizieren
- Remote-RACADM aktivieren oder deaktivieren
- Lokalen RACADM deaktivieren
- IPMI auf Managed System aktivieren
- Linux während des Starts in RHEL 6 für die serielle Konsole konfigurieren
- Konfigurieren des seriellen Terminals in RHEL 7
- Unterstützte SSH-Verschlüsselungssysteme

Mit iDRAC über eine serielle Verbindung über ein DB9-Kabel kommunizieren

Sie können jede der folgenden Kommunikationsmethoden verwenden, um Systemverwaltungsaufgaben über eine serielle Verbindung auf den Rack- und Tower-Servern durchzuführen:

- Serielle RAC-Verbindung
- Serielle IPMI-Verbindung – Grundlegender Modus „Direktverbindung“ und Terminalmodus „Direktverbindung“

ANMERKUNG: Bei Blade-Servern wird die serielle Verbindung über das Gehäuse hergestellt. Weitere Informationen finden Sie unter *Chassis Management Controller – Handbuch* verfügbar unter https://www.dell.com/cmcmanuals (gilt nicht für MX-Plattformen) *OME - Modular für PowerEdge MX7000-Gehäuse – Benutzerhandbuch* verfügbar unter https://www.dell.com/openmanagemanuals (gilt für MX-Plattformen).

So bauen Sie eine serielle Verbindung auf:

1. Konfigurieren Sie das BIOS, um die serielle Verbindung zu aktivieren.
2. Verbinden Sie das Null-Modem-DB9-Kabel von der seriellen Schnittstelle auf der Management Station mit dem externen seriellen Konnektor auf dem verwalteten System.

   ANMERKUNG: Aus- und Einschalten des Servers ist bei vConsole oder GUI für jede Änderung der Baudrate erforderlich.

   ANMERKUNG: Wenn die serielle iDRAC-Verbindungsauthentifizierung deaktiviert ist, ist ein Neustart von iDRAC erforderlich, damit die Baudrate geändert werden kann.

3. Stellen Sie sicher, dass die Terminal-Emulations-Software der Management Station für jede serielle Verbindung über eine der folgenden Methoden konfiguriert ist:
   - Linux Minicom in einem Xterm
   - Hilgraeve HyperTerminal Private Edition (Version 6.3)

   Je nachdem, wo sich das verwaltete System in seinem Bootprozess befindet, wird entweder der POST-Bildschirm oder der Betriebssystem-Bildschirm angezeigt. Dies basiert auf der Konfiguration: SAC für Windows und Linux Textmodus-Bildschirme für Linux.

4. Aktivieren Sie serielle RAC- oder IPMI-Verbindungen auf iDRAC.

BIOS für serielle Verbindung konfigurieren

So konfigurieren Sie das BIOS für serielle Verbindungen:

ANMERKUNG: Dies gilt nur für iDRAC auf Rack- und Tower-Servern.

1. Schalten Sie das System ein oder starten Sie es neu.
2. Klicken Sie auf F2.
3. Gehen Sie zu **System-BIOS-Einstellungen** > **Serielle Kommunikation**.
4. Wählen Sie **Externer serieller Konnektor** auf **Remote-Zugriffsgerät** aus.
5. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
6. Drücken Sie auf die Esc-Taste, um das **System-Setup**-Programm zu beenden.

Serielle RAC-Verbindung aktivieren

Nach der Konfiguration der seriellen Verbindung im BIOS aktivieren Sie die serielle RAC-Verbindung in iDRAC.

ANMERKUNG: Dies gilt nur für iDRAC auf Rack- und Tower-Servern.

Serielle RAC-Verbindungen über die Web-Schnittstelle aktivieren

So aktivieren Sie die serielle RAC-Verbindung:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Network (Netzwerk)** > **Serial (Seriell)**.
   Die Seite **Serielle Verbindung** wird angezeigt.
2. Wählen Sie unter **Serielle RAC-Verbindung** die Option **Aktiviert** aus, und legen Sie die Attributwerte fest.
3. Klicken Sie auf **Anwenden**.
   Damit werden die seriellen RAC-Einstellungen konfiguriert.

Serielle RAC-Verbindung über RACADM aktivieren

Um die serielle RAC-Verbindung über RACADM zu aktivieren, verwenden Sie den Befehl `set` mit dem Objekt in der Gruppe `iDRAC.Serial`.

Grundlegenden seriellen IPMI-Verbindungs- und -Terminalmodus aktivieren

Konfigurieren Sie zum Aktivieren der seriellen IPMI-Weiterleitung des BIOS an iDRAC die serielle IPMI-Verbindung in den folgenden iDRAC-Modi:

ANMERKUNG: Dies gilt nur für iDRAC auf Rack- und Tower-Servern.

- Grundlegender IPMI-Modus – Unterstützt eine binäre Schnittstelle für den Programmzugriff, z. B. die IPMI Shell (ipmish), die im Baseboard Management-Dienstprogramm (BMU) enthalten ist. Um beispielsweise das Systemereignisprotokoll über ipmish im grundlegenden IPMI-Modus zu drucken, führen Sie den folgenden Befehl aus:

  ```
  ipmish -com 1 -baud 57600 -flow cts -u <username> -p <password> sel get
  ```

  ANMERKUNG: Der standardmäßige iDRAC-Nutzername und das Standard-iDRAC-Kennwort werden auf dem System-Badge bereitgestellt.
- IPMI-Terminalmodus – Unterstützt ASCII-Befehle, die von einem seriellen Terminal gesendet werden. Dieser Modus unterstützt eine begrenzte Anzahl von Befehlen (einschließlich Stromregelung) und RAW-IPMI-Befehlen, die als hexadezimale ASCII-Zeichen eingegeben werden. Mit dieser Funktion können Sie die Startreihenfolge des Betriebssystems bis zum BIOS anzeigen, wenn Sie sich über SSH bei iDRAC anmelden. Sie müssen sich vom IPMI-Terminal mit `[sys pwd -x]` abmelden. Im Folgenden finden Sie ein Beispiel für IPMI-Terminalmodus-Befehle.
  - `[sys tmode]`
  - `[sys pwd -u root calvin]`
  - `[sys health query -v]`
  - `[18 00 01]`
  - `[sys pwd -x]`

Serielle Verbindung über die Web-Schnittstelle aktivieren

Stellen Sie sicher, dass Sie die serielle RAC-Schnittstelle für die Aktivierung der seriellen IPMI-Verbindung deaktivieren.

So konfigurieren Sie die Einstellungen für serielle IPMI-Verbindungen:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Connectivity (Konnektivität)** > **Serial (Seriell)**.

2. Geben Sie unter **IPMI Serial** (Serielle IPMI-Verbindung) die Attributwerte an. Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.
3. Klicken Sie auf **Anwenden**.

IPMI-Modus für die serielle Verbindung über RACADM aktivieren

Um den IPMI-Modus zu konfigurieren, deaktivieren Sie die serielle RAC-Schnittstelle und aktivieren dann den IPMI-Modus.

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

n=0 - Terminalmodus

n=1 - Grundlegender Modus

Einstellungen für serielle IPMI-Verbindung über RACADM aktivieren

1. Ändern Sie den Modus für die serielle IPMI-Verbindung über den folgenden Befehl auf die gewünschte Einstellung.

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

2. Stellen Sie die serielle Baudrate für IPMI über den folgenden Befehl ein.

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

Parameter	Zulässige Werte (in bps)
<baud_rate>	9600, 19200, 57600 und 115200.

3. Aktivieren Sie die Hardware-Datenflusssteuerung der seriellen IPMI-Hardware über den folgenden Befehl.

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

4. Stellen Sie die Mindestberechtigungsebene des seriellen IPMI-Kanals unter Verwendung des Befehls ein.

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

Parameter	Berechtigungsstufe
<level> = 2	Benutzer
<level> = 3	Operator
<level> = 4	Administratorkennwort

5. Stellen Sie sicher, dass der serielle MUX (externer serieller Konnektor) über das BIOS-Setup-Programm ordnungsgemäß für das Remote-Zugriffsgerät eingestellt ist, um das BIOS für die serielle Verbindung zu konfigurieren.

Weitere Informationen über diese Eigenschaften finden Sie in der IPMI 2.0-Spezifikation.

Zusätzliche Einstellungen für den seriellen IPMI-Terminalmodus

In diesem Abschnitt finden Sie zusätzliche Konfigurationseinstellungen für den seriellen IPMI-Terminalmodus.

Zusätzliche Einstellungen für den seriellen IPMI-Terminalmodus über die Web-Schnittstelle konfigurieren

So legen Sie die Terminalmoduseinstellungen fest:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Connectivity (Konnektivität)** > **Serial (Seriell)**.
   Die Seite **Serial** wird angezeigt.
2. Aktivieren Sie „Serielle IPMI-Verbindung“.
3. Klicken Sie auf **Terminalmoduseinstellungen**.
   Daraufhin wird die Seite **Terminalmoduseinstellungen** angezeigt.
4. Legen Sie die folgenden Werte fest:
   - Zeilenbearbeitung
   - Löschsteuerung
   - Echo-Steuerung
   - Handshaking-Steuerung
   - Neue Zeilenreihenfolge
   - Neue Zeilenfolgen eingeben

   Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.
5. Klicken Sie auf **Anwenden**.
   Die Terminalmoduseinstellungen werden konfiguriert.
6. Stellen Sie sicher, dass der serielle MUX (externer serieller Konnektor) über das BIOS-Setup-Programm ordnungsgemäß für das Remote-Zugriffsgerät eingestellt ist, um das BIOS für die serielle Verbindung zu konfigurieren.

Zusätzliche Einstellungen für den seriellen IPMI-Terminalmodus über RACADM konfigurieren

Um die Terminalmoduseinstellungen zu konfigurieren, verwenden Sie den Befehl `set` mit den Objekten in der Gruppe `idrac.ipmiserial`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Von der seriellen RAC-Verbindung auf die serielle Konsolenverbindung bei Verwendung eines DB9-Kabels umschalten

iDRAC unterstützt Escape-Tastensequenzen, mit denen Sie zwischen der seriellen RAC-Schnittstellenkommunikation und der seriellen Konsole auf den Rack- und Tower-Servern umschalten können.

Von der seriellen Konsole auf die serielle RAC-Verbindung umschalten

Um zum Kommunikationsmodus „Serielle RAC-Schnittstelle“ umzuschalten, wenn Sie sich im Modus „Serielle Konsole“ befinden, betätigen Sie Esc+Umschalttaste, 9.

Mit der obigen Tastenfolge rufen Sie entweder die `iDRAC Login`-Eingabeaufforderung auf (wenn der iDRAC auf den seriellen RAC-Modus gesetzt ist) oder den seriellen Anschlussmodus, in dem Terminalbefehle abgeben werden können (wenn der iDRAC auf den seriellen IPMI-Terminalmodus bei Direktverbindung eingestellt ist).

Von der seriellen RAC-Verbindung auf die serielle Konsole umschalten

Um auf den Modus „Serielle Konsole“ umzuschalten, wenn Sie sich im Kommunikationsmodus „Serielle RAC-Schnittstelle“ befinden, betätigen Sie Esc+Umschalttaste, Q.

Betätigen Sie im Terminalmodus zum Umschalten der Verbindung zum Modus „Serielle Konsole“ Esc+Umschalttaste, Q.

Um zum Terminalmodus zurückzukehren, wenn Sie über den Modus „Serielle Konsole“ verbunden sind, betätigen sie Esc+Umschalttaste, 9.:

Mit iDRAC über IPMI SOL kommunizieren

Mit der seriellen IPMI über LAN-Verbindung (SOL) kann die textbasierte Konsole eines verwalteten Systems serielle Daten über das dedizierte oder freigegebene Out-of-band-Ethernet-Managementnetzwerk von iDRAC umleiten. Mithilfe von SOL können Sie Folgendes tun:

- Ohne zeitliche Beschränkung remote auf Betriebssysteme zugreifen.
- Hostsysteme auf Emergency Management Services (EMS) oder Special Administrator Console (SAC) für Windows oder Linux-Shell diagnostizieren.
- Fortschritt eines Servers während des POST (Einschalt-Selbsttest) anzeigen und das BIOS-Setup-Programm neu konfigurieren

So richten Sie den SOL-Kommunikationsmodus ein:

1. Konfigurieren Sie das BIOS für die serielle Verbindung.
2. Konfigurieren Sie iDRAC für die Verwendung von SOL.
3. Aktivieren Sie ein unterstütztes Protokoll (SSH, IPMI-Tool).

BIOS für serielle Verbindung konfigurieren

ANMERKUNG: Dies gilt nur für iDRAC auf Rack- und Tower-Servern.

1. Schalten Sie das System ein oder starten Sie es neu.
2. Klicken Sie auf F2.
3. Gehen Sie zu **System-BIOS-Einstellungen** > **Serielle Kommunikation**.
4. Legen Sie die folgenden Werte fest:
   - Serielle Kommunikation – Eingeschaltet mit Konsolenumleitung
   - Adresse der seriellen Schnittstelle – COM2
     ANMERKUNG: Sie können die **serielle Kommunikation** auf **Eingeschaltet mit serieller Umleitung über COM1** einstellen, wenn das **Adressfeld des seriellen Anschlusses**, **Serielles Gerät2**, auch auf COM1 eingestellt ist.
   - Externer serieller Anschluss - Serielles Gerät2
   - Failsafe-Baud-Rate – 115.200
   - Remote-Terminaltyp... vt100/vt220
   - Umleitung nach Start – Aktiviert
5. Klicken Sie auf **Zurück** und dann auf **Fertigstellen**.
6. Klicken Sie auf **Ja**, um die Änderungen zu speichern.
7. Drücken Sie auf die Esc-Taste, um das **System-Setup**-Programm zu beenden.

   ANMERKUNG: BIOS sendet dem Bildschirm serielle Daten im 25 x 80-Format. Das SSH-Fenster, das zum Aufruf des Befehls `console com2` verwendet wird, muss auf 25 x 80 eingestellt sein. Dann wird der umgeleitete Bildschirm korrekt angezeigt.

   ANMERKUNG: Wenn der Bootloader oder das Betriebssystem eine serielle Umleitung ermöglicht, wie etwa GRUB oder Linux, muss die BIOS-Einstellung **Redirection After Boot** (Umleitung nach Start) deaktiviert werden. Damit sollen potenzielle Konkurrenzsituationen vermieden werden, in denen mehrere Komponenten auf die serielle Schnittstelle zugreifen.

iDRAC für die Verwendung von SOL konfigurieren

Sie können die SOL-Einstellungen in iDRAC über die Webschnittstelle, über RACADM oder über das Dienstprogramm für die iDRAC-Einstellungen festlegen.

iDRAC für die Verwendung von SOL über die iDRAC-Webschnittstelle konfigurieren

Um IPMI Seriell über LAN (SOL) zu konfigurieren:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Connectivity (Konnektivität)** > **Serial Over LAN (Seriell über LAN)**.

Die Seite **Seriell über LAN** wird angezeigt.

2. Aktivieren Sie SOL, geben Sie die Werte ein, und klicken Sie dann auf **Anwenden**.
   Die IPMI-SOL-Einstellungen werden konfiguriert.
3. Um das Intervall der Zeichenakkumulation und den Schwellenwert für die gesendeten Zeichen festzulegen, wählen Sie **Erweiterte Einstellungen** aus.
   Die Seite **Seriell über LAN - Erweiterte Einstellungen** wird angezeigt.
4. Geben Sie die Werte für die Attribute ein, und klicken Sie auf **Anwenden**.

   Die erweiterten IPMI-SOL-Einstellungen werden konfiguriert. Diese Werte tragen dazu bei, die Leistung zu verbessern.

   Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

iDRAC für die Verwendung von SOL über RACADM konfigurieren

Um IPMI Seriell über LAN (SOL) zu konfigurieren:

1. Aktivieren Sie unter Verwendung des Befehls „Seriell über LAN“.

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

2. Aktualisieren Sie die IPMI-SOL-Mindestberechtigungsebene unter Verwendung des Befehls.

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

Parameter	Berechtigungsstufe
<level> = 2	Benutzer
<level> = 3	Operator
<level> = 4	Administratorkennwort

ANMERKUNG: Für die Aktivierung von IPMI SOL müssen Sie über die in IPMI SOL definierten Mindestberechtigungen verfügen. Weitere Informationen finden Sie in der IPMI 2.0-Spezifikation.

3. Aktualisieren Sie die IPMI-SOL-Baudrate unter Verwendung des Befehls.

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

ANMERKUNG: Um die serielle Konsole über LAN umzuleiten, stellen Sie sicher, dass die SOL-Baudrate mit der Baudrate des verwalteten Systems übereinstimmt.

Parameter	Zulässige Werte (in bps)
<baud_rate>	9600, 19200, 57600 und 115200.

4. Aktivieren Sie SOL für jeden Benutzer unter Verwendung des Befehls.

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

Parameter	Beschreibung
<id>	Eindeutige ID des Benutzers

ANMERKUNG: Um die serielle Konsole über LAN umzuleiten, ist sicherzustellen, dass die SOL-Baudrate mit der Baudrate des Managed System identisch ist.

Unterstütztes Protokoll aktivieren

Die unterstützten Protokolle sind IPMI und SSH.

Unterstütztes Protokoll über die Weboberfläche aktivieren

Um SSH zu aktivieren, gehen Sie zu **iDRAC-Einstellungen** > **Dienste** und wählen Sie **Aktiviert** für SSH aus.

Um IPMI zu aktivieren, gehen Sie zu **iDRAC-Einstellungen** > **Konnektivität** und wählen Sie **IPMI-Einstellungen** aus. Stellen Sie sicher, dass der Wert für den **Verschlüsselungsschlüssel** nur aus Nullen besteht oder drücken Sie die Rücktaste, um den Wert zu löschen und Nullzeichen einzugeben.

Unterstütztes Protokoll über RACADM aktivieren

Um SSH zu aktivieren, geben Sie den folgenden Befehl ein.

SSH

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

So ändern Sie den SSH-Port

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

Sie können u. a. die folgenden Tools verwenden:

- IPMItool zur Verwendung des IPMI-Protokolls
- Putty/OpenSSH zur Verwendung des SSH-Protokolls

SOL über das IPMI-Protokoll

Das IPMI-basierte SOL-Dienstprogramm und IPMItool verwenden RMCP+, bereitgestellt über UDP-Datagramme an Port 623. RMCP+ bietet verbesserte Authentifizierung, Datenintegritätsprüfungen, Verschlüsselung sowie die Möglichkeit, verschiedene Arten von Nutzlasten bei Verwendung von IPMI 2.0 zu verwenden. Weitere Informationen finden Sie unter **http://ipmitool.sourceforge.net/manpage.html**.

RMCP+ verwendet für die Authentifizierung einen Verschlüsselungsschlüssel mit einer Hexadezimal-Zeichenkette aus 40 Zeichen (mit den Zeichen 0-9, a-f und A-F). Der Standardwert ist eine Zeichenfolge mit 40 Nullen.

Eine RMCP+-Verbindung zum iDRAC muss mit dem Verschlüsselungsschlüssel (Key Generator Key) verschlüsselt werden. Sie können den Verschlüsselungsschlüssel über die iDRAC-Weboberfläche oder das Dienstprogramm iDRAC-Einstellungen konfigurieren.

So starten Sie eine SOL-Sitzung mithilfe von IPMItool von einer Management Station aus:

ANMERKUNG: Falls erforderlich, können Sie das Standard-Timeout für SOL-Sitzungen über **iDRAC-Einstellungen** > **Dienste** ändern.

1. Installieren Sie IPMITool über die *Dell Systems Management Tools and Documentation*-DVD.
   Weitere Anweisungen finden Sie im *Software-Schnellinstallationshandbuch*.
2. In der Eingabeaufforderung (Windows oder Linux) führen Sie den folgenden Befehl aus, um SOL über iDRAC zu starten:

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

   Mit diesem Befehl wurde eine Verbindung von der Management Station zum seriellen Anschluss des Managed System hergestellt.
3. Zum Beenden einer SOL-Sitzung über IPMITool drücken Sie „~“ und anschließend „.“ (Punkt).

   ANMERKUNG: Wenn sich eine SOL-Sitzung nicht beenden lässt, setzen Sie iDRAC zurück, und warten Sie etwa zwei Minuten, bis der Startvorgang vollständig abgeschlossen ist.

ANMERKUNG: Die IPMI SOL-Sitzung kann beendet werden, wenn ein großer Text von einem Client mit Windows-Betriebssystem auf einen Host mit Linux-Betriebssystem kopiert wird. Um ein abruptes Beenden der Sitzung zu vermeiden, konvertieren Sie jeden großen Text in ein UNIX-basiertes Zeilenende.

ANMERKUNG: Wenn eine mit dem RACADM-Tool erstellte SOL-Sitzung existiert, werden beim Starten einer weiteren SOL-Sitzung mit dem IPMI-Tool keine Benachrichtigungen oder Fehler über die vorhandenen Sitzungen angezeigt.

ANMERKUNG: Aufgrund der Einstellungen des Windows-Betriebssystems wird für die SOL-Sitzung über SSH und das IPMI-Tool nach dem Start möglicherweise ein leerer Bildschirm angezeigt. Trennen Sie die SOL-Sitzung und stellen Sie eine neue Verbindung her, um die SAC-Eingabeaufforderung erneut anzuzeigen.

SOL über SSH

Secure Shell (SSH) ist ein Netzwerkprotokoll, das für die Kommunikation über Befehlszeilen mit iDRAC verwendet wird. Sie können Remote-RACADM-Befehle über diese Schnittstelle parsen.

SSH bietet verbesserte Sicherheit. iDRAC unterstützt SSH Version 2 mit Kennwortauthentifizierung und ist standardmäßig aktiviert. iDRAC unterstützt zwei bis vier SSH-Sitzungen gleichzeitig.

ANMERKUNG: Ab iDRAC-Version 4.40.00.00 wurde die Telnet-Funktion aus iDRAC entfernt, sodass die Registrierungseigenschaften der zugehörigen Attribute veraltet sind. Einige dieser Eigenschaften sind zwar noch in iDRAC verfügbar, um die Abwärtskompatibilität mit vorhandenen Konsolenanwendungen und -Skripten aufrechtzuerhalten. Die entsprechenden Einstellungen werden von der iDRAC-Firmware jedoch ignoriert.

ANMERKUNG: Beim Herstellen einer SSH Verbindung wird die Sicherheitsmeldung „Weitere Authentifizierung erforderlich“ angezeigt. Obwohl die 2FA deaktiviert ist.

ANMERKUNG: Für MX-Plattformen wird eine SSH-Sitzung für die iDRAC-Kommunikation verwendet. Wenn alle Sitzungen verwendet werden, wird iDRAC erst gestartet, wenn eine Sitzung frei ist.

Verwenden Sie Open Source-Programme, wie z. B. PuTTY oder OpenSSH, die SSH auf einer Managementstation unterstützen, um die Verbindung zu iDRAC herzustellen.

ANMERKUNG: Führen Sie `OpenSSH` über einen VT100- oder ANSI-Terminalemulator auf Windows aus. Wenn Sie `OpenSSH` an der Windows-Befehlseingabe ausführen, können Sie nicht auf den vollen Funktionsumfang zugreifen (einige Tasten reagieren nicht, und einige Grafiken werden nicht angezeigt).

Bevor Sie SSH für die Kommunikation mit iDRAC verwenden, müssen Sie die folgenden Schritte ausführen:

1. BIOS für die Aktivierung der seriellen Konsole konfigurieren
2. SOL in iDRAC konfigurieren
3. SSH über die iDRAC-Weboberfläche oder RACADM aktivieren.

   Client für SSH (Schnittstelle 22) <--> WAN-Verbindung <--> iDRAC

   Durch das IPMI-basierte SOL, das das SSH-Protokoll verwendet, ist kein zusätzliches Dienstprogramm nötig, da die Umwandlung von „seriell“ zu „Netzwerk“ innerhalb von iDRAC erfolgt. Die verwendete SSH-Konsole muss die Daten, die von dem seriellen Anschluss des verwalteten Systems eingehen, interpretieren und darauf reagieren können. Der serielle Abschluss wird normalerweise mit einer Shell verbunden, die ein ANSI- oder VT100/VT220-Terminal emuliert. Die serielle Konsole wird automatisch an die SSH-Konsole umgeleitet.

SOL über PuTTY auf Windows verwenden

ANMERKUNG: Falls erforderlich, können Sie das Standard-Timeout für SSH-Sitzungen über **iDRAC-Einstellungen** > **Services** ändern.

So starten Sie IPMI SOL über PuTTY auf einer Windows-Management Station:

1. Führen Sie den folgenden Befehl aus, um eine Verbindung zu iDRAC herzustellen

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

   ANMERKUNG: Die Portnummer ist optional. Sie ist nur erforderlich, wenn die Portnummer neu zugewiesen wird.

2. Führen Sie den Befehl `console com2` oder `connect` aus, um SOL und das verwaltete System zu starten.

   Es wird eine SOL-Sitzung von der Managementstation zum verwalteten System unter Verwendung des SSH-Protokolls geöffnet. Um auf die iDRAC-Befehlszeilenkonsole zuzugreifen, befolgen Sie die ESC-Tastensequenz. Verhalten von PuTTY- und SOL-Verbindungen:

   - Während Sie im Rahmen des POST auf das verwaltete System zugreifen, falls die Funktionstasten und Tastenfeld-Option unter PuTTY wie folgt eingestellt sind:
     - VT100+ – F2 erfolgreich, F12 nicht erfolgreich

- ESC[n~ – F12 erfolgreich, F2 jedoch nicht erfolgreich
- Wenn in Windows die Emergency Management System (EMS)-Konsole unmittelbar nach einem Host-Neustart geöffnet wird, kann das Special Admin Console (SAC)-Terminal möglicherweise beschädigt sein. Beenden Sie die SOL-Sitzung, schließen Sie das Terminal, öffnen Sie ein anderes Terminal und starten Sie die SOL-Sitzung mit demselben Befehl.

ANMERKUNG: Aufgrund der Einstellungen des Windows-Betriebssystems wird für die SOL-Sitzung über SSH und das IPMI-Tool nach dem Start möglicherweise ein leerer Bildschirm angezeigt. Trennen Sie die SOL-Sitzung und stellen Sie eine neue Verbindung her, um die SAC-Eingabeaufforderung erneut anzuzeigen.

Verwenden von SOL über OpenSSH auf Linux

So verwenden Sie SOL über OpenSSH auf einer Linux-Managementstation:

ANMERKUNG: Falls erforderlich, können Sie das Standard-Timeout für SSH-Sitzungen über **iDRAC-Einstellungen** > **Services** ändern.

1. Starten Sie eine Shell.
2. Stellen Sie eine Verbindung zum iDRAC über den folgenden Befehl her: ssh *<iDRAC-IP-Adresse>* -l *<Anmeldename>*.
3. Geben Sie zum Starten von SOL an der Befehlseingabeaufforderung einen der folgenden Befehle ein:
   - `connect`
   - `console com2`

   Dies verbindet den iDRAC mit dem SOL-Port des verwalteten Systems. Sobald eine SOL-Sitzung eingerichtet wurde, ist die iDRAC-Befehlszeilenkonsole nicht verfügbar. Führen Sie die Escape-Sequenz ordnungsgemäß aus, um die iDRAC-Befehlszeilenkonsole zu öffnen. Die Escape-Sequenz wird auch auf dem Bildschirm angezeigt, sobald eine SOL-Sitzung verbunden ist. Wenn das verwaltete System deaktiviert ist, dauert es einige Zeit, bis die SOL-Sitzung eingerichtet ist.

   ANMERKUNG: Sie können die Konsolen com1 oder com2 zum Starten von SOL verwenden. Starten Sie den Server neu, um die Verbindung herzustellen.

   Der Befehl `console -h com2` zeigt den Inhalt des seriellen Verlaufspuffers an, bevor er auf Eingaben über die Tastatur oder neue Zeichen vom seriellen Anschluss wartet.

   Die Standard- (und maximale) Größe des Verlaufspuffers beträgt 8192 Zeichen. Sie können diese Zahl mithilfe des folgenden Befehls auf einen niedrigeren Wert setzen:

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

4. Beenden Sie die SOL-Sitzung, um eine aktive SOL-Sitzung zu schließen.

Trennen der Verbindung zur SOL-Sitzung in der iDRAC-Befehlszeilenkonsole

Die Befehle zum Trennen einer SOL-Sitzung hängen vom Dienstprogramm ab. Sie können das Dienstprogramm nur dann beenden, wenn eine SOL-Sitzung vollständig beendet wurde.

Beenden Sie zum Abbrechen einer SOL-Sitzung die SOL-Sitzung über die iDRAC-Befehlszeilenkonsole.

- Um die SOL-Umleitung zu beenden, betätigen Sie Eingabetaste, Esc, T.
  Die SOL-Sitzung wird geschlossen.

Wenn eine SOL-Sitzung nicht vollständig im Dienstprogramm beendet wird, sind andere SOL-Sitzungen möglicherweise nicht verfügbar. Um dieses Problem zu beheben, beenden Sie die Befehlszeilenkonsole in der Weboberfläche über **iDRAC-Einstellungen** > **Konnektivität** > **Seriell über LAN**.

Mit iDRAC über IPMI über LAN kommunizieren

Sie müssen IPMI über LAN für iDRAC konfigurieren, um IPMI-Befehle über LAN-Kanäle auf beliebigen externen Systemen zu aktivieren oder zu deaktivieren. Wenn IPMI über LAN nicht konfiguriert ist, können die externen Systeme nicht über die IPMI-Befehle mit dem iDRAC-Server kommunizieren.

ANMERKUNG: IPMI unterstützt auch das IPv6-Adressprotokoll für Linux-basierte Betriebssysteme.

IPMI über LAN mithilfe der Web-Schnittstelle konfigurieren

So konfigurieren Sie IPMI über LAN:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Connectivity (Konnektivität)**.
   Die Seite **Netzwerk** wird angezeigt.
2. Geben Sie unter **IPMI-Einstellungen** die Attributwerte an, und klicken Sie dann auf **Anwenden**.

   Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

   Die IPMI über LAN-Einstellungen werden konfiguriert.

IPMI über LAN mithilfe des Dienstprogramms für die iDRAC-Einstellungen konfigurieren

So konfigurieren Sie IPMI über LAN:

1. Gehen Sie im **Dienstprogramm für die iDRAC-Einstellungen** zu **Netzwerk**.
   Die Seite **iDRAC-Netzwerkeinstellungen** wird angezeigt.
2. Geben Sie die erforderlichen Werte für die **IPMI-Einstellungen** ein.

   Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
   Die IPMI über LAN-Einstellungen werden konfiguriert.

IPMI über LAN mithilfe von RACADM konfigurieren

1. IPMI-über-LAN aktivieren

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

   ANMERKUNG: Diese Einstellung legt die IPMI-Befehle fest, die über die IPMI-über-LAN-Schnittstelle ausgeführt werden können. Weitere Informationen finden Sie in der IPMI 2.0-Spezifikation unter **intel.com**.

2. Aktualisieren Sie die IPMI-Kanalberechtigungen.

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

Parameter	Berechtigungsstufe
<level> = 2	Benutzer
<level> = 3	Operator
<level> = 4	Administratorkennwort

3. Stellen Sie den IPMI-LAN-Kanalverschlüsselungsschlüssel ein, falls erforderlich.

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

Parameter	Beschreibung
<key>	20-Zeichen-Verschlüsselungsschlüssel in einem gültigen Hexadezimalformat.

ANMERKUNG: iDRAC IPMI unterstützt das RMCP+-Protokoll. Weitere Informationen finden Sie in der IPMI 2.0-Spezifikation unter **intel.com**.

Remote-RACADM aktivieren oder deaktivieren

Remote-RACADM kann über die iDRAC-Webschnittstelle oder RACADM aktiviert oder deaktiviert werden. Sie können bis zu fünf Remote-RACADM-Sitzungen gleichzeitig ausführen.

ANMERKUNG: Remote-RACADM ist standardmäßig aktiviert.

Remote-RACADM über die Web-Schnittstelle aktivieren oder deaktivieren

1. Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Services (Dienste)**.
2. Wählen Sie unter **Remote-RACADM** die gewünschte Option aus und klicken Sie auf **Anwenden**.
   Entsprechend Ihrer Auswahl ist Remote-RACADM damit aktiviert oder deaktiviert.

Remote-RACADM über RACADM aktivieren oder deaktivieren

ANMERKUNG: Es wird empfohlen, diese Befehle unter Verwendung der lokalen RACADM- oder Firmware-RACADM-Schnittstelle auszuführen.

- So deaktivieren Sie Remote-RACADM:

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

- So aktivieren Sie Remote-RACADM:

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

Lokalen RACADM deaktivieren

Der lokale RACADM ist standardmäßig aktiviert. Weitere Informationen zum Deaktivieren finden Sie unter Zugriff zum Ändern der iDRAC-Konfigurationseinstellungen auf einem Host-System deaktivieren auf Seite 118.

IPMI auf Managed System aktivieren

Verwenden Sie auf einem verwalteten System den Dell Open Manage Server Administrator, um IPMI zu aktivieren oder zu deaktivieren. Weitere Informationen finden Sie im *OpenManage Server Administrator – Benutzerhandbuch* verfügbar unter https://www.dell.com/openmanagemanuals.

ANMERKUNG: Ab iDRAC-Version 2.30.30.30 unterstützt IPMI das IPv6-Adressprotokoll für Linux-basierte Betriebssysteme.

Linux während des Starts in RHEL 6 für die serielle Konsole konfigurieren

Die folgenden Schritte beziehen sich speziell auf den Linux GRand Unified Bootloader (GRUB). Wenn ein anderer Bootloader verwendet wird, sind ähnliche Änderungen erforderlich.

ANMERKUNG: Beim Konfigurieren des Client-VT100-Emulationsfensters stellen Sie das Fenster bzw. die Anwendung, die die umgeleitete virtuelle Konsole anzeigt, auf 25 Reihen x 80 Spalten ein, um eine ordnungsgemäße Textanzeige sicherzustellen. Andernfalls werden einige Textanzeigen möglicherweise nicht richtig dargestellt.

Bearbeiten Sie die Datei **/etc/grub.conf** wie folgt:

1. Suchen Sie in der Datei die Abschnitte zur allgemeinen Einstellung und fügen Sie Folgendes hinzu:

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

2. Hängen Sie zwei Optionen an die Kernel-Zeile an:

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

3. Deaktivieren Sie die grafische GRUB-Schnittstelle und verwenden Sie die textbasierte Schnittstelle. Andernfalls wird der GRUB-Bildschirm nicht in der virtuellen RAC-Konsole angezeigt. Zum Deaktivieren der grafischen Schnittstelle kommentieren Sie die Zeile aus, die mit `splashimage` beginnt.

   Das folgende Beispiel enthält ein Beispiel einer **/etc/grub.conf**-Datei, die die in diesem Verfahren beschriebenen Änderungen zeigt.

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

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

title Red Hat Linux Advanced Server (2.4.9-e.3smp) root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0
console=ttyS1,115200n8r
initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3) root (hd0,00)
kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
initrd /boot/initrd-2.4.9-e.3.im
```

4. Um mehreren GRUB-Optionen das Starten von Sitzungen der virtuellen Konsole über die serielle RAC-Verbindung zu ermöglichen, fügen Sie die folgende Zeile allen Optionen hinzu:

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

   Das Beispiel zeigt, dass `console=ttyS1,57600` zur ersten Option hinzugefügt wurde.

   ANMERKUNG: Wenn der Bootloader oder das Betriebssystem eine serielle Umleitung ermöglicht, wie etwa GRUB oder Linux, muss die BIOS-Einstellung **Redirection After Boot** (Umleitung nach Start) deaktiviert werden. Damit sollen potenzielle Konkurrenzsituationen vermieden werden, in denen mehrere Komponenten auf die serielle Schnittstelle zugreifen.

Anmeldung an der virtuellen Konsole nach dem Start aktivieren

Fügen Sie in der Datei **/etc/inittab** eine neue Zeile hinzu, um `agetty` auf der seriellen COM2-Schnittstelle zu konfigurieren:

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

Das folgende Beispiel zeigt eine Beispieldatei mit der neuen Zeile.

```
#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
```

Fügen Sie in der Datei **/etc/securetty** eine neue Zeile mit dem Namen der seriellen tty für COM2 hinzu:

```
ttyS1
```

Das folgende Beispiel zeigt eine Beispieldatei mit der neuen Zeile.

ANMERKUNG: Verwenden Sie die Sequenz der Untbr-Taste (~B), um auf einer seriellen Konsole mithilfe des IPMI-Hilfsprogramms die Befehle der magischen Linux **S-Abf**-Taste auszuführen.

```
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
```

Konfigurieren des seriellen Terminals in RHEL 7

So konfigurieren Sie das serielle Terminal in RHEL 7:

1. Fügen Sie die folgenden Zeilen zu `/etc/default/grub` hinzu, oder aktualisieren Sie sie:

   ```
   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` wendet diese Konfiguration nur auf den Standardmenüeintrag an, mit `GRUB_CMDLINE_LINUX` wird sie auf alle Menüeinträge angewendet.

   Jede Zeile sollte nur einmal innerhalb von `/etc/default/grub` auftreten. Wenn die Zeile bereits existiert, dann ändern Sie sie, um eine weitere Kopie zu vermeiden. Es ist daher nur eine Zeile `GRUB_CMDLINE_LINUX_DEFAULT` zulässig.

2. Erstellen Sie die Konfigurationsdatei `/boot/grub2/grub.cfg` neu, indem Sie den Befehl `grub2-mkconfig -o` wie folgt ausführen:
   - auf BIOS-basierten Systemen:

     ```
     ~]# grub2-mkconfig -o /boot/grub2/grub.cfg
     ```

   - auf UEFI-basierten Systemen:

     ```
     ~]# grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
     ```

Weitere Informationen finden Sie im RHEL 7 System Administrator's Guide (Administratorhandbuch für Systemadministratoren) unter redhat.com.

Steuern von GRUB von der seriellen Konsole

Sie können GRUB so konfigurieren, dass die serielle Konsole anstelle der VGA-Konsole verwendet wird. Dadurch können Sie den Bootvorgang unterbrechen und einen anderen Kernel wählen oder Kernelparameter hinzufügen, um z. B. in den Single-User-Modus zu booten.

Um GRUB für die Verwendung der seriellen Konsole zu konfigurieren, kommentieren Sie das Splash-Image aus, und fügen Sie die Optionen `serial` und `terminal` zu `grub.conf` hinzu:

```
[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
```

ANMERKUNG: Starten Sie das System neu, damit die Einstellungen in Kraft treten.

Unterstützte SSH-Verschlüsselungssysteme

Um mit iDRAC über das SSH-Protokoll zu kommunizieren, unterstützt es verschiedene Verschlüsselungsschemas, die in der folgenden Tabelle aufgelistet sind.

Tabelle 19. SSH-Verschlüsselungsschemas

Schematyp	Algorithmen
Asymmetrische Verschlüsselung	
Öffentlicher Schlüssel	ssh-rsa ecdsa-sha2-nistp256
Symmetrische Verschlüsselung	
Schlüsselaustausch	curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521

Tabelle 19. SSH-Verschlüsselungsschemas (fortgesetzt)

Schematyp	Algorithmen
	diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha1
Verschlüsselung	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 (Komprimierung)	Keine

ANMERKUNG: Wenn Sie OpenSSH 7.0 oder höher aktivieren, wird die Unterstützung für öffentliche DSA-Schlüssel deaktiviert. Für höhere Sicherheit für iDRAC empfiehlt Dell, die Unterstützung für öffentliche DSA-Schlüssel nicht zu aktivieren.

Authentifizierung von öffentlichen Schlüsseln für SSH verwenden

iDRAC unterstützt die Authentifizierung mit öffentlichem Schlüssel (Public Key Authentification, PKA) über SSH. Hierbei handelt es sich um eine lizenzierte Funktion. Wenn die PKA über SSH eingerichtet ist und korrekt verwendet wird, müssen Sie bei der Anmeldung am iDRAC den Benutzernamen eingeben. Beim Einrichten von automatisierten Skripts zur Durchführung verschiedener Funktionen ist dies hilfreich. Die hochgeladenen Schlüssel müssen im RFC 4716- oder OpenSSH-Format vorliegen. Wenn sie dieses Format nicht aufweisen, müssen die Schlüssel in dieses Format konvertiert werden.

In allen Szenarios muss ein Paar, das aus einem privaten und einem öffentlichen Schlüssel besteht, auf der Management Station generiert werden. Der öffentliche Schlüssel wird in den lokalen iDRAC-Benutzer hochgeladen und der private Schlüssel wird vom SSH-Client verwendet, um die Vertrauensstellung zwischen der Management Station und dem iDRAC herzustellen.

Sie können das Paar aus einem öffentlichen und einem privaten Schlüssel über die folgenden Verfahren generieren:

- *PuTTY-Schlüsselgenerator*-Anwendung für Clients, die auf Windows ausgeführt werden
- *ssh-keygen*-Befehlszeilenschnittstelle für Clients, die unter Linux ausgeführt werden

VORSICHT: Diese Berechtigung ist normalerweise Benutzern vorbehalten, die Mitglied der Administratorbenutzergruppe auf iDRAC sind. Diese Berechtigung kann jedoch auch Benutzern der Gruppe „Custom“ (Benutzerdefiniert) zugewiesen werden. Ein Benutzer mit dieser Berechtigung kann die Konfiguration beliebiger Benutzer modifizieren. Hierzu zählen das Erstellen oder Löschen beliebiger Benutzer, SSH-Schlüssel-Verwaltung für Benutzer usw. Weisen Sie diese Berechtigung daher mit Bedacht zu.

VORSICHT: Die Möglichkeit, SSH-Schlüssel hochzuladen, anzuzeigen und/oder zu löschen basiert auf der Benutzerberechtigung „Configure Users“ (Benutzer konfigurieren). Diese Berechtigung ermöglicht es Benutzern, den SSH-Schlüssel eines anderen Benutzers zu konfigurieren. Erteilen Sie diese Berechtigung mit Bedacht.

Generieren öffentlicher Schlüssel für Windows

So verwenden Sie die Anwendung *PuTTY-Schlüsselgenerator* zum Erstellen des Grundschlüssels:

1. Starten Sie die Anwendung und wählen Sie RSA als den Schlüsseltyp.
2. Geben Sie die Anzahl Bits für den Schlüssel ein. Die Anzahl an Bits muss zwischen 2048 und 4096 Bits betragen.
3. Klicken Sie auf **Generieren** und bewegen Sie die Maus gemäß Anleitung im Fenster.
   Die Schlüssel wurden erstellt.

4. Sie können das Schlüsselanmerkungsfeld ändern.
5. Geben Sie eine Passphrase zur Sicherung des Schlüssels ein.
6. Speichern Sie den öffentlichen und den privaten Schlüssel.

Generieren öffentlicher Schlüssel für Linux

Um die Anwendung *ssh-keygen* für die Erstellung des Basisschlüssels zu verwenden, öffnen Sie ein Terminalfenster, und geben Sie an der Shell-Eingabeaufforderung den Befehl `ssh-keygen -t rsa -b 2048 -C testing` ein,

wobei:

- `-t` der Zeichenfolge *rsa* entspricht.
- `-b` die Bit-Verschlüsselungsgröße zwischen 2048 und 4096 angibt.
- `-C` das Ändern der Anmerkung zum öffentlichen Schlüssel ermöglicht und optional ist.

ANMERKUNG: Bei den Optionen wird zwischen Groß- und Kleinschreibung unterschieden.

Folgen Sie den Anweisungen. Laden Sie nach der Ausführung des Befehls die öffentliche Datei hoch.

VORSICHT: Schlüssel, die von der Linux-Management Station unter Verwendung des Befehls „ssh-keygen“ erstellt wurden, weisen ein anderes Format als 4716 auf. Konvertieren Sie die Schlüssel mit dem Befehl `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub` in das 4716-Format. An den Berechtigungen für die Schlüsseldatei dürfen keine Änderungen vorgenommen werden. Die Konvertierung muss über Standardberechtigungen erfolgen.

ANMERKUNG: iDRAC unterstützt nicht die ssh-agent-Weiterleitung von Schlüsseln.

SSH-Schlüssel hochladen

Sie können bis zu vier öffentliche Schlüssel *pro Benutzer* zur Verwendung über eine SSH-Schnittstelle hochladen. Bevor Sie die öffentlichen Schlüssel hinzufügen, müssen Sie sicherstellen, dass Sie die Schlüssel anzeigen, wenn sie eingerichtet sind, so dass ein Schlüssel nicht versehentlich überschrieben wird.

Beim Hinzufügen neuer öffentlicher Schlüssel müssen Sie sicherstellen, dass bestehende Schlüssel nicht den Index belegen, zu dem der neue Schlüssel hinzugefügt werden soll. iDRAC prüft nicht, ob vorherige Schlüssel gelöscht wurden, bevor neue Schlüssel hinzugefügt werden. Wenn ein neuer Schlüssel hinzugefügt wird, kann dieser verwendet werden, wenn die SSH-Schnittstelle aktiviert ist.

SSH-Schlüssel über die Web-Schnittstelle hochladen

So laden Sie SSH-Schlüssel hoch:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Users (Benutzer)** > **Local Users (Lokale Benutzer)**.
   Die Seite **Lokale Benutzer** wird angezeigt.
2. In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.
   Die Seite **Benutzer-Hauptmenü** wird angezeigt.
3. Wählen Sie unter **SSH-Schlüsselkonfigurationen SSH-Schlüssel hochladen** aus, und klicken Sie dann auf **Weiter**.
   Daraufhin wird die Seite **SSH-Schlüssel hochladen** angezeigt.
4. Laden Sie die SSH-Schlüssel über eines der folgenden Verfahren hoch:
   - Schlüsseldatei hochladen
   - Inhalte der Schlüsseldatei in das Textfeld kopieren

   Weitere Informationen finden Sie in der iDRAC Online-Hilfe.
5. Klicken Sie auf **Anwenden**.

SSH-Schlüssel über RACADM hochladen

Um die SSH-Schlüssel hochzuladen, führen Sie den folgenden Befehl aus:

ANMERKUNG: Sie können einen Schlüssel nicht gleichzeitig hochladen und kopieren.

- Für lokales RACADM: `racadm sshpkauth -i <2 to 16> -k <1 to 4> -f <filename>`

- Über Remote-RACADM mit SSH: `racadm sshpkauth -i <2 to 16> -k <1 to 4> -t <key-text>`

Beispiel: Um einen gültigen Schlüssel für die Nutzer-ID 2 auf iDRAC für den ersten Schlüsselsektor mithilfe einer Datei hochzuladen, führen Sie den folgenden Befehl aus:

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

ANMERKUNG: Die Option `-f` wird für ssh/serielles RACADM nicht unterstützt.

SSH-Schlüssel anzeigen

Sie können die Schlüssel anzeigen, die nach iDRAC hochgeladen wurden.

SSH-Schlüssel über die Web-Schnittstelle anzeigen

So zeigen Sie die SSH-Schlüssel an:

1. Wechseln Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Users (Benutzer)**.
   Die Seite **Lokale Benutzer** wird angezeigt.
2. In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.
   Die Seite **Benutzer-Hauptmenü** wird angezeigt.
3. Wählen Sie unter **SSH-Schlüsselkonfiguration** die Option **SSH-Schlüssel anzeigen/entfernen** aus, und klicken Sie dann auf **Weiter**.
   Daraufhin wird die Seite **SSH-Schlüssel anzeigen/entfernen** mit den Schlüsseldetails angezeigt.

SSH-Schlüssel löschen

Bevor Sie die öffentlichen Schlüssel löschen, müssen Sie sicherstellen, dass Sie die Schlüssel anzeigen, wenn sie eingerichtet sind, so dass ein Schlüssel nicht versehentlich gelöscht werden kann.

SSH-Schlüssel über die Web-Schnittstelle löschen

So löschen Sie SSH-Schlüssel:

1. Gehen Sie in der Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Users (Benutzer)**.
   Die Seite **Lokale Benutzer** wird angezeigt.
2. Wählen Sie in der Spalte **ID** eine Benutzer-ID-Nummer aus, und klicken Sie auf **Edit** (Bearbeiten).
   Der Bildschirm **Benutzer bearbeiten** wird angezeigt.
3. Wählen Sie unter **SSH Key Configurations** (SSH-Schlüsselkonfigurationen) einen SSH-Schlüssel aus, und klicken Sie dann auf **Edit** (Bearbeiten).
   Die Seite **SSH Key** (SSH-Schlüssel) zeigt die Details für **Edit From** (Bearbeiten von) an.
4. Wählen Sie **Remove** (Entfernen) für die Schlüssel aus, die gelöscht werden sollen, und klicken Sie dann auf **Apply** (Anwenden).
   Die ausgewählten Schlüssel werden daraufhin gelöscht.

SSH-Schlüssel über RACADM löschen

Führen Sie zum Löschen der SSH-Schlüssel die folgenden Befehle aus:

- Spezifischer Schlüssel – `racadm sshpkauth -i <2 to 16> -d -k <1 to 4>`
- Alle Schlüssel – `racadm sshpkauth -i <2 to 16> -d -k all`

9

Benutzerkonten und Berechtigungen konfigurieren

Sie können Benutzerkonten mit spezifischen Berechtigungen (*rollenbasierte Autorität*) einrichten, um Ihr System über den iDRAC zu verwalten und die Systemsicherheit zu gewährleisten. Standardmäßig ist der iDRAC mit einem lokalen Administratorkonto konfiguriert. Der standardmäßige iDRAC-Benutzername und das Standard-iDRAC-Kennwort werden mit der Systemkennzeichnung bereitgestellt. Als Administrator können Sie Benutzerkonten einrichten, damit andere Benutzer auf den iDRAC zugreifen können. Weitere Informationen finden Sie in der Dokumentation für den Server.

Sie können lokale Benutzer einrichten oder Verzeichnisdienste wie Microsoft Active Directory oder LDAP verwenden, um Benutzerkonten einzurichten. Die Verwendung eines Verzeichnisdiensts stellt einen zentralen Standort für die Verwaltung berechtigter Benutzerkonten bereit.

Der iDRAC unterstützt den rollenbasierten Zugriff auf Benutzer mit einer Reihe von zugehörigen Berechtigungen. Die Rollen sind Administrator, Operator, schreibgeschützt oder keine. Die Rolle definiert die maximal verfügbaren Berechtigungen.

Themen:

- iDRAC-Benutzerrollen und -Berechtigungen
- Empfohlene Zeichen in Benutzernamen und Kennwörtern
- Lokale Benutzer konfigurieren
- Konfigurieren von Active Directory-Nutzern
- Generische LDAP-Benutzer konfigurieren

iDRAC-Benutzerrollen und -Berechtigungen

Die iDRAC-Rolle und Berechtigungsnamen haben sich seit einer früheren Generation von Servern geändert. Die Rollennamen sind:

Tabelle 20. iDRAC-Rollen

Aktuelle Generation	Vorherige Generation	Benutzerberechtigungen
Administrator	Administrator	Anmelden, Konfigurieren, Benutzer konfigurieren, Protokolle, Systemsteuerung, Auf virtuelle Konsole zugreifen, Auf virtuelle Datenträger zugreifen, Systemvorgänge, Debug
Operator	Hauptbenutzer	Anmelden, Konfigurieren, Systemsteuerung, Auf virtuelle Konsole zugreifen, Auf virtuelle Datenträger zugreifen, Systemvorgänge, Debug
Read Only (Nur-Lesen)	Gastbenutzer	Anmelden
Keine	Keine	Keine

In der folgenden Tabelle sind die IPMI-Benutzerberechtigungen beschrieben:

Tabelle 21. DRAC/iDRAC-Benutzerberechtigungen

Aktuelle Generation	Vorherige Generation	Beschreibung
Anmelden	Am iDRAC anmelden	Ermöglicht dem Benutzer, sich am iDRAC anzumelden.
Konfigurieren	iDRAC konfigurieren	Ermöglicht dem Benutzer, den iDRAC zu konfigurieren. Mit dieser Berechtigung kann ein Benutzer auch Energieverwaltung, virtuelle Konsole, virtuelle Medien, Lizenzen, Systemeinstellungen, Speichergeräte, BIOS-Einstellungen, SCP usw. konfigurieren.

Tabelle 21. DRAC/iDRAC-Benutzerberechtigungen (fortgesetzt)

Aktuelle Generation	Vorherige Generation	Beschreibung
ANMERKUNG: Die Administratorrolle übersteuert alle Privilegien der anderen Komponenten wie z.B. das BIOS-Setup-Passwort.		
Benutzer konfigurieren	Benutzer konfigurieren	Ermöglicht dem Benutzer, bestimmten Benutzern den Zugriff auf das System zu erlauben.
Protokolle	Protokolle löschen	Ermöglicht dem Benutzer, lediglich das Systemereignisprotokoll (SEL) zu löschen.
Systemsteuerung	System steuern und konfigurieren	Ermöglicht Aus- und Einschalten des Host-Systems.
Auf die virtuelle Konsole zugreifen	Auf die Umleitung der virtuellen Konsole zugreifen (bei Blade-Servern) Auf die virtuelle Konsole zugreifen (bei Rack- oder Tower-Servern)	Ermöglicht dem Benutzer, die virtuelle Konsole auszuführen.
Auf virtuelle Datenträger zugreifen	Auf virtuelle Datenträger zugreifen	Ermöglicht dem Benutzer, virtuelle Datenträger auszuführen und zu verwenden.
Systemvorgänge	Testwarnungen	Ermöglicht vom Benutzer initiierte und erzeugte Ereignisse und die Informationen werden als asychnrone Benachrichtigung versendet und protokolliert.
Debug	Diagnosebefehle ausführen	Ermöglicht dem Benutzer, Diagnosebefehle auszuführen.

Empfohlene Zeichen in Benutzernamen und Kennwörtern

Dieser Abschnitt enthält Details zu den empfohlenen Zeichen beim Erstellen und Verwenden von Benutzernamen und Kennwörtern.

ANMERKUNG: Das Passwort muss einen Großbuchstaben und einen Kleinbuchstaben, eine Zahl und ein Sonderzeichen enthalten.

Verwenden Sie beim Erstellen von Benutzernamen und Kennwörtern die folgenden Zeichen:

Tabelle 22. Empfohlene Zeichen für Benutzernamen

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

Tabelle 23. Empfohlene Zeichen für Kennwörter

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

ANMERKUNG: Sie können möglicherweise Benutzernamen und Passwörter erstellen, die andere Zeichen enthalten. Um allerdings die Kompatibilität mit allen Schnittstellen zu gewährleisten, empfiehlt Dell, nur die hier aufgeführten Zeichen zu verwenden.

ANMERKUNG: Die zulässigen Zeichen in Benutzernamen und Kennwörter für Netzwerkfreigaben ergeben sich aus der Netzwerkfreigabe. iDRAC unterstützt zulässige Zeichen in Anmeldeinformationen für die Netzwerkfreigabe dem Freigabetyp, außer < ,> und , (Komma).

ANMERKUNG: Zur Erhöhung der Sicherheit wird empfohlen, komplexe Kennwörter zu verwenden, die acht oder mehr Zeichen sowie Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen enthalten. Es wird außerdem empfohlen, die Kennwörter regelmäßig zu ändern (sofern möglich).

Lokale Benutzer konfigurieren

Sie können in iDRAC bis zu 16 lokale Benutzer mit spezifischen Zugriffsberechtigungen konfigurieren. Bevor Sie einen iDRAC-Benutzer erstellen, müssen Sie überprüfen, ob etwaige aktuelle Benutzer vorhanden sind. Sie können Benutzernamen, Kennwörter und Rollen mit den Berechtigungen für diese Benutzer festlegen. Die Benutzernamen und Kennwörter können über sichere iDRAC-Schnittstellen geändert werden (also über die Webschnittstelle, RACADM oder WSMan). Außerdem können Sie die SNMPv3-Authentifizierung für jeden Benutzer aktivieren oder deaktivieren.

Lokale Benutzer über die iDRAC-Webschnittstelle konfigurieren

So fügen Sie lokale iDRAC-Benutzer hinzu und konfigurieren sie:

ANMERKUNG: Sie müssen die Berechtigung „Benutzer konfigurieren“ besitzen, um einen iDRAC-Benutzer zu erstellen.

1. Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **User (Benutzer)**.
   Die Seite **Lokale Benutzer** wird angezeigt.
2. Wählen Sie in der Spalte **ID** des Benutzers eine Benutzer-ID-Nummer, und klicken Sie auf **Edit** (Bearbeiten).

   ANMERKUNG: Benutzer 1 ist für den anonymen IPMI-Benutzer reserviert; diese Konfiguration kann nicht geändert werden.

   Die Seite **User Configuration** (Benutzerkonfiguration) wird angezeigt.
3. Fügen Sie Angaben zu **User Account Settings** (Benutzerkontoeinstellungen) und **Advanced Settings** (Erweiterte Einstellungen) hinzu, um das Benutzerkonto zu konfigurieren.

   ANMERKUNG: Aktivieren Sie die Benutzer-ID, und geben Sie den Benutzernamen, das Kennwort und die Benutzerrolle (Zugangsberechtigungen) für den Benutzer an. Sie können auch die LAN-Berechtigungsebene, die Berechtigungsebene für serielle Schnittstellen, den Seriell-über-LAN-Status, die SNMPv3-Authentifizierung, den Authentifizierungstyp und den Datenschutztyp für den Benutzer aktivieren. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.
4. Klicken Sie auf **Save (Speichern)**. Der Benutzer wird mit den erforderlichen Berechtigungen erstellt.

Lokale Benutzer über RACADM konfigurieren

ANMERKUNG: Sie müssen als Benutzer **root** angemeldet sein, um RACADM-Befehle auf einem Remote-Linux-System ausführen zu können.

Sie können einen oder mehrere iDRAC-Benutzer über RACADM konfigurieren.

Um mehrere iDRAC-Benutzer mit identischen Konfigurationseinstellungen zu konfigurieren, führen Sie folgende Schritte durch:

- Erstellen Sie mit Hilfe der RACADM-Beispiele in diesem Abschnitt eine Batchdatei mit RACADM-Befehlen, und führen Sie diese Batchdatei dann auf jedem verwalteten System aus.
- Erstellen Sie die iDRAC-Konfigurationsdatei und führen Sie unter Verwendung derselben Konfigurationsdatei den Befehl `racadm set` auf den einzelnen verwalteten Systemen aus.

Wenn Sie einen neuen iDRAC konfigurieren oder wenn Sie den Befehl `racadm racresetcfg` verwendet haben, überprüfen Sie den Standard-iDRAC-Nutzernamen und das Standardkennwort auf dem System-Badge. Der Befehl `racadm racresetcfg` setzt den iDRAC auf die Standardwerte zurück.

ANMERKUNG: Wenn SEKM auf dem Server aktiviert ist, deaktivieren Sie SEKM mithilfe des Befehls `racadm sekm disable`, bevor Sie diesen Befehl verwenden. Somit kann verhindert werden, dass Storage-Geräte gesperrt werden, die durch iDRAC gesichert sind, wenn SEKM-Einstellungen aus iDRAC gelöscht werden, indem Sie den Befehl ausführen.

ANMERKUNG: Benutzer können im Laufe der Zeit aktiviert und deaktiviert werden. Infolgedessen kann ein Benutzer auf jedem iDRAC eine unterschiedliche Indexnummer besitzen.

Um zu überprüfen, ob ein Benutzer existiert, geben Sie den folgenden Befehl einmal für jeden Index (1-16) ein:

```
racadm get iDRAC.Users.<index>.UserName
```

Mehrere Parameter und Objekt-IDs werden mit ihren aktuellen Werten angezeigt. Das Schlüsselfeld ist `iDRAC.Users.UserName=`. Wenn nach = ein Nutzername angezeigt wird, wird diese Indexnummer verwendet.

ANMERKUNG: Sie können die Datei nutzen

```
racadm get -f <myfile.cfg>
```

und anzeigen oder bearbeiten,

```
myfile.cfg
```

die alle iDRAC-Konfigurationsparameter enthält.

Zur Aktivierung der SNMP v3-Authentifizierung für einen Benutzer verwenden Sie die Objekte **SNMPv3AuthenticationType**, **SNMPv3Enable**, **SNMPv3PrivacyType**. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Wenn Sie die Serverkonfigurationsprofildatei zur Benutzerkonfiguration verwenden, dann verwenden Sie die Attribute **AuthenticationProtocol, ProtocolEnable,** und **PrivacyProtocol**, um die SNMPv3-Authentifizierung zu aktivieren.

iDRAC-Benutzer über RACADM hinzufügen

1. Stellen Sie den Index und den Benutzernamen ein.

   ```
   racadm set idrac.users.<index>.username <user_name>
   ```

Parameter	Beschreibung
<index>	Eindeutiger Index des Benutzers
<user_name>	Benutzername

2. Legen Sie das Kennwort fest.

   ```
   racadm set idrac.users.<index>.password <password>
   ```

3. Legen Sie die Benutzerberechtigungen fest.

   Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

4. Aktivieren Sie den Benutzer.

   ```
   racadm set.idrac.users.<index>.enable 1
   ```

Für eine Überprüfung verwenden Sie den folgenden Befehl:

```
racadm get idrac.users.<index>
```

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Aktivieren des iDRAC-Benutzers mit Berechtigungen

Um einen Benutzer mit spezifischen administrativen Berechtigungen (rollenbasierte Autorität) zu aktivieren:

1. Lokalisieren Sie einen verfügbaren Benutzerindex.

```
racadm get iDRAC.Users <index>
```

2. Geben Sie die folgenden Befehle mit dem neuen Benutzernamen und dem neuen Kennwort ein.

```
racadm set iDRAC.Users.<index>.Privilege <user privilege bit mask value>
```

ANMERKUNG: Der Standardberechtigungswert ist 0, was bedeutet, dass der Benutzer über keine Berechtigungen verfügt. Eine Liste der gültigen Bitmaskenwerte für bestimmte Benutzerberechtigungen finden Sie unter *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Konfigurieren von Active Directory-Nutzern

Wenn Ihre Firma die Microsoft Active Directory-Software verwendet, kann die Software so konfiguriert werden, dass sie Zugriff auf iDRAC bietet. Sie können dann bestehenden Nutzern im Verzeichnisdienst iDRAC-Nutzerberechtigungen erteilen und diese steuern. Hierbei handelt es sich um eine lizenzierte Funktion.

Sie können die Nutzerauthentifizierung über Active Directory für die Anmeldung bei iDRAC konfigurieren. Sie können zudem rollenbasierte Autorität bereitstellen, die es einem Administrator ermöglicht, spezifische Berechtigungen für jeden Nutzer zu konfigurieren.

ANMERKUNG: Bei jeder Bereitstellung, die über eine MX-Vorlage erfolgt und bei der die CA-Validierung innerhalb der Vorlage aktiviert ist, muss der Nutzer CA-Zertifikate bei der ersten Anmeldung oder vor dem Wechsel des Authentifizierungsdienstes von LDAP zu Active Directory oder umgekehrt hochladen.

Voraussetzungen für die Verwendung der Active Directory-Authentifizierung für iDRAC

Um die Active Directory-Authentifizierungsfunktion auf dem iDRAC verwenden zu können, stellen Sie sicher, dass Sie:

- eine Active Directory-Infrastruktur bereitgestellt haben. Weitere Informationen finden Sie auf der Microsoft-Website.
- PKI in die Active Directory-Infrastruktur integriert ist. iDRAC verwendet die standardmäßigen PKI-Methode (Public-Key-Infrastruktur), um eine sichere Authentifizierung in Active Directory zu gewährleisten. Weitere Informationen finden Sie auf der Microsoft-Website.
- das Secure Socket Layer (SSL) auf allen Domänen-Controllern aktiviert haben, mit denen sich iDRAC zur Authentifizierung mit allen Domänen-Controllern verbindet.

SSL auf Domänen-Controller aktivieren

Wenn iDRAC Benutzer mit einem Active Directory-Domänen-Controller authentifiziert, wird eine SSL-Sitzung mit dem Domänen-Controller gestartet. Der Domänen-Controller muss dann ein von der Zertifizierungsstelle (CA) signiertes Zertifikat veröffentlichen – das Stammzertifikat, das auch in das iDRAC geladen wird. Für die iDRAC-Authentifizierung an einem *beliebigen* Domänen-Controller – ob Stamm- oder untergeordnete Domänen-Controller – muss dieser Domänen-Controller über ein SSL-fähiges Zertifikat verfügen, das von der Zertifizierungsstelle signiert wurde.

Wenn Sie die Microsoft Enterprise Stamm-CA verwenden, um alle Domänen-Controller-SSL-Zertifikate *automatisch* zuzuweisen, müssen Sie:

1. SSL-Zertifikat auf jedem Domain-Controller installieren.
2. Das CA-Stammzertifikat des Domänen-Controllers zu iDRAC exportieren.
3. Das SSL-Zertifikat der iDRAC-Firmware importieren.

SSL-Zertifikat für jeden Domänen-Controller installieren

So installieren Sie das SSL-Zertifikat für jeden Controller:

1. Klicken Sie auf **Start** > **Verwaltung** > **Domänensicherheitsrichtlinie**.
2. Erweitern Sie den Ordner **Richtlinien öffentlicher Schlüssel,** klicken Sie mit der rechten Maustaste auf **Automatische Zertifikatanforderungs-Einstellungen** und klicken Sie auf **Automatische Zertifikatanforderung**.
   Daraufhin wird der **Assistent für die Einrichtung der automatischen Zertifikatanforderung** angezeigt.
3. Klicken Sie auf **Weiter**, und wählen Sie dann **Domänen-Controller** aus.
4. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**. Das SSL-Zertifikat wird installiert.

Exportieren des CA-Stammzertifikats des Domänen-Controllers zu iDRAC

So exportieren Sie das Stamm-Zertifizierungsstellenzertifikat des Domänen-Controllers nach iDRAC:

1. Suchen Sie den Domänen-Controller, der den Microsoft Enterprise-CA-Dienst ausführt.
2. Klicken Sie auf **Start** > **Ausführen**.
3. Geben Sie `mmc` ein und klicken Sie auf **OK**.
4. Klicken Sie im Fenster **Konsole 1** (MMC) auf **Datei** (oder auf **Konsole)** und wählen Sie **Snap-in hinzufügen/entfernen**.
5. Klicken Sie im Fenster **Snap-In hinzufügen/entfernen** auf **Hinzufügen**.
6. Wählen Sie im Fenster **Eigenständiges Snap-In** die Option **Zertifikate** aus und klicken Sie auf **Hinzufügen**.
7. Wählen Sie **Computer** und klicken Sie auf **Weiter.**
8. Wählen Sie **Arbeitsplatz** aus, klicken Sie auf **Fertig stellen**, und klicken Sie schließlich auf **OK**.
9. Gehen Sie im Fenster **Konsole 1** zum Ordner **Zertifikate Persönliche Zertifikate**.
10. Suchen Sie das CA-Stammzertifikat, klicken Sie mit der rechten Maustaste darauf, wählen Sie **Alle Aufgaben** aus, und klicken Sie auf **Exportieren...**
11. Klicken Sie im **Zertifikate exportieren-Assistenten** auf **Weiter** und wählen Sie **Privaten Schlüssel nicht exportieren** aus.
12. Klicken Sie auf **Weiter** und wählen Sie **Base-64-kodiert X.509 (.cer)** als Format.
13. Klicken Sie auf **Weiter**, um das Zertifikat in einem Verzeichnis auf dem System zu speichern.
14. Laden Sie das in Schritt 13 gespeicherte Zertifikat auf das iDRAC.

Importieren des SSL-Zertifikats der iDRAC-Firmware

Das iDRAC-SSL-Zertifikat ist mit dem für iDRAC-Webserver verwendeten Zertifikat identisch. Alle iDRAC-Controller werden mit einem selbstsignierten Standardzertifikat geliefert.

Wenn der Active Directory-Server für die Authentifizierung des Clients während der Initialisierung einer SSL-Sitzung konfiguriert ist, müssen Sie das iDRAC-Serverzertifikat auf dem Active Directory-Domänen-Controller hochladen. Dieser zusätzliche Schritt ist nicht erforderlich, wenn Active Directory während der Initialisierung einer SSL-Sitzung keine Clientauthentifizierung ausführt.

ANMERKUNG: Wenn das SSL-Zertifikat der iDRAC-Firmware von einer Zertifizierungsstelle signiert wurde und das Zertifikat dieser Zertifizierungsstelle bereits in der Liste der vertrauenswürdigen Stammzertifizierungsstellen des Domänen-Controllers verzeichnet ist, müssen die Schritte in diesem Abschnitt nicht ausgeführt werden.

So importieren Sie das SSL-Zertifikat der iDRAC-Firmware in alle Listen vertrauenswürdiger Zertifikate der Domänen-Controller:

1. Laden Sie das iDRAC SSL-Zertifikat unter Verwendung des folgenden RACADM-Befehls herunter:

   ```
   racadm sslcertdownload -t 1 -f <RAC SSL certificate>
   ```

2. Öffnen Sie am Domänen-Controller ein Fenster der **MMC-Konsole** und wählen Sie **Zertifikate** > **Vertrauenswürdige Stammzertifizierungsstellen** aus.
3. Klicken Sie mit der rechten Maustaste auf **Zertifikate**, wählen Sie **Alle Aufgaben** aus, und klicken Sie auf **Importieren**.
4. Klicken Sie auf **Weiter** und suchen Sie die SSL-Zertifikatdatei.
5. Installieren Sie das iDRAC-SSL-Zertifikat in der **vertrauenswürdigen Stammzertifizierungsstelle** der einzelnen Domänen-Controller.

   Wenn Sie ein eigenes Zertifikat installiert haben, stellen Sie sicher, dass die Zertifizierungsstelle, die das Zertifikat signiert, in der Liste **Vertrauenswürdige Stammzertifizierungsstelle** aufgeführt wird. Wenn die Zertifizierungsstelle nicht in der Liste enthalten ist, müssen sie es auf allen Domänen-Controllern installieren.

6. Klicken Sie auf **Weiter** und wählen Sie aus, ob Windows den Zertifikatspeicher automatisch aufgrund des Zertifikattyps auswählen soll, oder suchen Sie selbst nach einem Speicher.

7. Klicken Sie auf **Fertig stellen** und klicken Sie auf **OK**. Das SSL-Zertifikat für die iDRAC-Firmware wird in alle Listen mit vertrauenswürdigen Zertifikaten für Domänen-Controller importiert.

Unterstützte Active Directory-Authentifizierungsmechanismen

Sie können mit Active Directory den Benutzerzugriff auf iDRAC mittels zweier Methoden definieren:

- Die *Standardschemalösung*, die nur Microsoft-Standard-Active Directory-Gruppenobjekte verwendet.
- *Erweiterte Schemalösung*, die über benutzerdefinierte Active Directory-Objekte verfügt. Alle Zugriffssteuerungsobjekte werden in Active Directory verwaltet. Bei der Konfiguration des Benutzerzugriffs auf verschiedenen iDRACs mit unterschiedlichen Berechtigungsebenen besteht maximale Flexibilität.

Übersicht des Standardschema-Active Directory

Wie in der folgenden Abbildung dargestellt, erfordert die Verwendung des Standardschemas für die Active Directory-Integration die Konfiguration unter Active Directory und unter iDRAC.

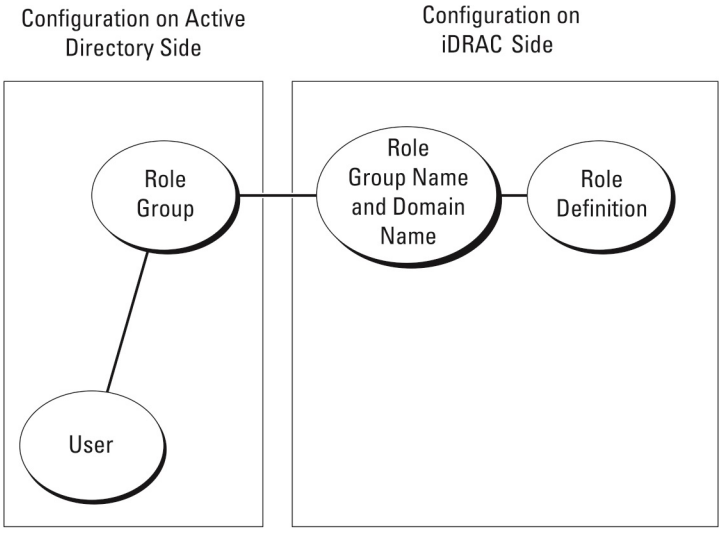


Abbildung 1. Konfiguration von iDRAC mit Active Directory-Standardschema

In Active Directory wird ein Standardgruppenobjekt als Rollengruppe verwendet. Ein Benutzer, der iDRAC-Zugriff hat, ist ein Mitglied der Rollengruppe. Um diesem Benutzer Zugang zu einem bestimmten iDRAC zu gewähren, müssen der Rollengruppenname und sein Domänenname für den bestimmten iDRAC konfiguriert werden. Die Rolle und Berechtigungsebene werden in jedem iDRAC definiert und nicht in Active Directory. In jedem iDRAC können Sie bis zu fünf Rollengruppen konfigurieren und definieren. Tabellenreferenznummer zeigt die standardmäßigen Rollengruppen-Berechtigungen.

Tabelle 24. Standardeinstellungsberechtigungen der Rollengruppe

Rollengruppen	Standard-Berechtigungsebene	Gewährte Berechtigungen	Bitmaske
Rollengruppe 1	Keine	Am iDRAC anmelden, iDRAC konfigurieren, Benutzer konfigurieren, Protokolle löschen, Serversteuerungsbefehle ausführen, auf virtuelle Konsole zugreifen, auf virtuellen Datenträger zugreifen, Warnungen testen, Diagnosebefehle ausführen	0x000001ff
Rollengruppe 2	Keine	Am iDRAC anmelden, iDRAC konfigurieren,	0x000000f9

Tabelle 24. Standardeinstellungsberechtigungen der Rollengruppe (fortgesetzt)

Rollengruppen	Standard-Berechtigungsebene	Gewährte Berechtigungen	Bitmaske
		Serversteuerungsbefehle ausführen, auf virtuelle Konsole zugreifen, auf virtuellen Datenträger zugreifen, Warnungen testen, Diagnosebefehle ausführen	
Rollengruppe 3	Keine	Melden Sie sich bei iDRAC an.	0x00000001
Rollengruppe 4	Keine	Keine zugewiesenen Berechtigungen	0x00000000
Rollengruppe 5	Keine	Keine zugewiesenen Berechtigungen	0x00000000

ANMERKUNG: Die Bitmasken-Werte werden nur verwendet, wenn das Standardschema mit RACADM eingerichtet wird.

Einfache Domänen (Single Domains) und mehrfache Domänen (Multiple Domains)

Wenn sich alle Anmeldebenutzer und Rollengruppen sowie die verschachtelten Gruppen in derselben Domäne befinden, müssen lediglich die Adressen der Domänen-Controller auf dem iDRAC konfiguriert werden. In diesem Szenario einer einfachen Domäne wird jede Art von Gruppe unterstützt.

Wenn sich alle Anmeldebenutzer und Rollengruppen sowie die verschachtelten Gruppen in mehreren Domäne befinden, müssen die Adressen des globalen Katalogs auf dem iDRAC konfiguriert werden. In diesem Szenario mit mehreren Domänen müssen alle Rollengruppen und verschachtelten Gruppen, falls vorhanden, vom Typ eine Universalgruppe sein.

Active Directory-Standardschema konfigurieren

Bevor Sie das Standardschema Active Directory konfigurieren, stellen Sie Folgendes sicher:

- Sie haben eine iDRAC Enterprise oder Datacenter Lizenz.
- Die Konfiguration erfolgt auf einem Server, der als Domain Controller verwendet wird.
- Datum, Uhrzeit und Zeitzone auf dem Server sind korrekt.
- Die iDRAC-Netzwerkeinstellungen sind konfiguriert. Falls nicht, gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC-Einstellungen > Konnektivität > Netzwerk > Allgemeine Einstellungen**, um die Netzwerkeinstellungen zu konfigurieren.

So konfigurieren Sie CMC für den Zugriff auf eine Active Directory-Anmeldung:

1. Öffnen Sie auf einem Active Directory-Server (Domänen-Controller) das Active Directory-Benutzer- und -Computer-Snap-In.
2. Erstellen Sie die iDRAC-Gruppen und -Benutzer.
3. Konfigurieren Sie den Gruppennamen, den Domänennamen und die Rollenberechtigungen auf iDRAC über die iDRAC-Web-Schnittstelle oder RACADM.

Active Directory mit Standardschema unter Verwendung der CMC-Webschnittstelle konfigurieren

ANMERKUNG: Weitere Informationen zu den verschiedenen Feldern finden Sie in der *iDRAC-Online-Hilfe*.

1. Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Users (Benutzer)** > **Directory Services (Verzeichnisdienste)**.
   Die Seite **Verzeichnisdienste** wird angezeigt.
2. Wählen Sie die Option **Microsoft Active Directory** und klicken Sie dann auf **Edit** (Bearbeiten).

Die Seite **Active Directory-Konfiguration und Verwaltung** wird angezeigt.

3. Klicken Sie auf **Active Directory konfigurieren**.
   Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 1 von 4 wird angezeigt.
4. Aktivieren Sie optional die Zertifikatvalidierung, und laden Sie das durch die Zertifikatstelle signierte digitale Zertifikat hoch, das im Rahmen der Initiierung von SSL-Verbindungen während der Kommunikation mit dem Active Directory (AD)-Server verwendet wird. Aus diesem Grund müssen die Domänen-Controller und die FQDN des globalen Katalogs angegeben werden. Dies erfolgt im nächsten Schritt. Folglich sollte das DNS in den Netzwerkeinstellungen ordnungsgemäß konfiguriert werden.
5. Klicken Sie auf **Next** (Weiter).

   Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 2 von 4 wird angezeigt.
6. Aktivieren Sie Active Directory und geben Sie Informationen zum Ort der Active Directory-Server und -Benutzerkonten an. Geben Sie außerdem die Zeit an, die iDRAC auf Antworten von Active Directory während des iDRAC-Anmeldevorgangs warten muss.

   ANMERKUNG: Wenn die Zertifikatüberprüfung aktiviert ist, geben Sie die Adressen des Domänen-Controller-Servers und den FQDN des globalen Katalogs an. Stellen Sie unter **iDRAC Settings (iDRAC-Einstellungen)** > **Network (Netzwerk)** sicher, dass DNS korrekt konfiguriert ist.
7. Klicken Sie auf **Next** (Weiter). Die Seite **Active Directory Configuration and Management Step 3 of 4** (Active Directory-Konfiguration und -Verwaltung Schritt 3 von 4) wird angezeigt.
8. Wählen Sie **Standardschema** aus, und klicken Sie auf „Weiter“.
   Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 4a von 4 wird angezeigt.
9. Geben Sie den Standort der globalen Katalogservers für Active Directory an, und geben Sie außerdem die Berechtigungsgruppen an, die für die Autorisierung von Benutzern verwendet werden.
10. Klicken Sie auf eine **Rollengruppe**, um die Steuerungsauthentifizierungsrichtlinie für Benutzer unter dem Standardschemacode zu konfigurieren.
    Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 4b von 4** wird angezeigt.
11. Geben Sie die Berechtigungen an, und klicken Sie auf **Anwenden**.

    Die Einstellungen werden angewendet, und die Seite **Active Directory – Konfiguration und Verwaltung – Schritt 4a von 4** wird angezeigt.
12. Klicken Sie auf **Fertigstellen**. Daraufhin werden die Active Directory-Einstellungen für das Standardschema konfiguriert.

Konfiguration des Active Directory mit Standardschema unter Verwendung von RACADM

1. Verwenden Sie die folgenden Befehle:

```
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>
```

- Geben Sie unbedingt den vollständig qualifizierten Domänennamen (FQDN) des Domänen-Controllers ein, nicht den FQDN der Domäne selbst. Geben Sie z. B. `servername.dell.com` statt `dell.com` ein.
- Informationen zu Bitmaskenwerten für spezifische Rollengruppenberechtigungen finden Sie unter Standardeinstellungsberechtigungen der Rollengruppe.
- Sie müssen mindestens eine der drei Domänen-Controller-Adressen angeben. Der iDRAC versucht so lange, nacheinander mit jeder der konfigurierten Adressen eine Verbindung herzustellen, bis eine Verbindung hergestellt werden konnte. Beim Standardschema sind dies die Adressen der Domänen-Controller, auf denen sich die Benutzerkonten und Rollengruppen befinden.

- Der globale Katalogserver ist nur für das Standardschema erforderlich, wenn sich die Benutzerkonten und Rollengruppen in verschiedenen Domänen befinden. Im Falle mehrerer Domänen kann nur die Universalgruppe verwendet werden.
- Wenn die Zertifikatsüberprüfung aktiviert ist, muss der vollständig qualifizierte Domänenname (FQDN) oder die IP-Adresse, die Sie in diesem Feld angeben, mit dem Feld „Servername“ oder „Alternativer Servername“ Ihres Domänen-Controller-Zertifikats übereinstimmen.
- Um die Zertifikatvalidierung während eines SSL-Handshake zu deaktivieren, verwenden Sie den folgenden Befehl:

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 0
  ```

  In diesem Fall brauchen Sie kein CA-Zertifikat zu laden.
- Um die Zertifikatvalidierung während eines SSL-Handshake (optional) durchzusetzen, verwenden Sie den folgenden Befehl:

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 1
  ```

  In diesem Fall müssen Sie mit dem folgenden RACADM-Befehl das CA-Zertifikat hochladen:

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

  ANMERKUNG: Wenn die Zertifikatüberprüfung aktiviert ist, geben Sie die Adressen des Domänen-Controller-Servers und die FQDN des globalen Katalogs an. Stellen Sie unter **Overview (Übersicht)** > **iDRAC Settings (iDRAC-Einstellungen)** > **Network (Netzwerk)** sicher, dass DNS korrekt konfiguriert ist.

  Die Verwendung des folgenden RACADM-Befehls kann optional sein.

  ```
  racadm sslcertdownload -t 1 -f <RAC SSL certificate>
  ```

2. Wenn DHCP auf dem iDRAC aktiviert ist und Sie den vom DHCP-Server bereitgestellten DNS verwenden möchten, geben Sie folgenden Befehl ein:

   ```
   racadm set iDRAC.IPv4.DNSFromDHCP 1
   ```

3. Wenn DHCP auf dem iDRAC deaktiviert ist oder Sie die DNS IP-Adresse manuell eingeben möchten, geben Sie den folgenden RACADM-Befehl ein:

   ```
   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. Wenn Sie eine Liste von Benutzerdomänen konfigurieren möchten, sodass für die Anmeldung an der Webschnittstelle nur der Benutzername eingegeben werden muss, verwenden Sie den folgenden Befehl:

   ```
   racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address of the
   domain controller>
   ```

   Sie können bis zu 40 Benutzerdomänen mit Indexzahlen zwischen 1 und 40 konfigurieren.

Übersicht über Active Directory mit erweitertem Schema

Für die Verwendung der Lösung mit dem erweiterten Schema benötigen Sie die Active Directory-Schema-Erweiterung.

Optimale Verfahren für das erweiterte Schema

Das erweiterte Schema verwendet Dell Zuordnungsobjekte zum Verknüpfen von iDRAC und der Berechtigung. So können Sie iDRAC basierend auf den allgemein erteilten Berechtigungen nutzen. Mithilfe der standardmäßigen Zugriffssteuerungsliste (Access Control List, ACL) von Dell Zuordnungsobjekten können Selbst- und Domänenadministratoren die Berechtigungen und den Umfang von iDRAC-Objekten verwalten.

Standardmäßig übernehmen die Dell Zuordnungsobjekte nicht alle Berechtigungen von den übergeordneten Active Directory-Objekten. Wenn Sie die Übernahme für das Dell Zuordnungsobjekt aktivieren, werden die übernommenen Berechtigungen für dieses Zuordnungsobjekt für die ausgewählten Benutzer und Gruppen gewährt. Dies kann dazu führen, dass dem iDRAC unbeabsichtigte Berechtigungen gewährt werden.

Um das erweiterte Schema sicher zu verwenden, empfiehlt Dell, dass Sie die Vererbung von Dell-Zuordnungsobjekten innerhalb der erweiterten Schemaimplementierung nicht aktivieren.

Active Directory-Schemaerweiterungen

Bei den Active Directory-Daten handelt es sich um eine verteilte Datenbank von *Attributen* und *Klassen*. Das Active Directory-Schema enthält die Regeln, die den Typ der Daten bestimmen, die der Datenbank hinzugefügt bzw. darin gespeichert werden können. Die Benutzerklasse ist ein Beispiel für eine *Klasse*, die in der Datenbank gespeichert wird. Attribute der Benutzerklasse können beispielsweise Vornamen, Nachnamen und Telefonnummern der Benutzer enthalten. Sie können die Active Directory-Datenbank erweitern, indem Sie eigene eindeutige *Attribute* und *Klassen* für spezifische Anforderungen hinzufügen. Dell hat das Schema um die erforderlichen Änderungen zur Unterstützung von Remote-Verwaltungsauthentifizierung mit Active Directory und -Autorisierung erweitert.

Attribute oder *Klassen*, die zu einem vorhandenen Active Directory-Schema hinzugefügt werden, müssen mit einer eindeutigen ID definiert werden. Um branchenweit eindeutige IDs zu gewährleisten, unterhält Microsoft eine Datenbank von Active Directory-Objektbezeichnern (OIDs). Wenn also Unternehmen das Schema erweitern, sind diese Erweiterungen eindeutig und ergeben keine Konflikte. Um das Schema in Active Directory von Microsoft zu erweitern, hat Dell eindeutige OIDs, eindeutige Namenserweiterungen und eindeutig verknüpfte IDs für die Attribute und Klassen erhalten, die dem Verzeichnisdienst hinzugefügt werden:

- Erweiterung lautet: `dell`
- Basis-OID lautet: `1.2.840.113556.1.8000.1280`
- RAC-LinkID-Bereich ist: `12070 to 12079`

Übersicht über die iDRAC-Schemaerweiterungen

Dell hat das Schema um die *Association*-, *Device*- und *Privilege*-Eigenschaft erweitert. Die *Association*-Eigenschaft dient zum Verknüpfen von Benutzern oder Gruppen mit einem bestimmten Satz an Berechtigungen für ein oder mehrere iDRAC-Geräte. Dieses Modell ist einfach und sorgt mit verschiedenen Kombinationen an Benutzern, iDRAC-Berechtigungen und iDRAC-Geräten im Netzwerk für höchste Flexibilität von Administratoren.

Für jedes physische iDRAC-Gerät im Netzwerk, das Sie für die Authentifizierung und Autorisierung in Active Directory integrieren möchten, müssen Sie mindestens ein Zuordnungsobjekt und ein iDRAC-Geräteobjekt erstellen. Sie können mehrere Zuordnungsobjekte erstellen, wobei jedes Zuordnungsobjekt nach Bedarf mit beliebig vielen Benutzern, Benutzergruppen, oder iDRAC-Geräteobjekten verknüpft werden kann. Die Benutzer und iDRAC-Benutzergruppen können Mitglieder beliebiger Domänen im Unternehmen sein.

Jedes Zuordnungsobjekt darf jedoch nur mit einem Berechtigungsobjekt verknüpft sein (bzw. Benutzer, Benutzergruppen oder iDRAC-Geräteobjekte verbinden). In diesem Beispiel kann der Administrator die Berechtigungen jedes Benutzers für bestimmte iDRAC-Geräte steuern.

Das iDRAC-Geräteobjekt ist die Verknüpfung mit der iDRAC-Firmware für die Abfrage von Active Directory für die Authentifizierung und Autorisierung. Wenn iDRAC dem Netzwerk hinzugefügt wird, muss der Administrator iDRAC und das Geräteobjekt mit dem Active Directory-Namen so konfigurieren, dass Benutzer die Authentifizierung und Autorisierung mit Active Directory durchführen können. Der Administrator muss außerdem iDRAC mindestens einem Zuordnungsobjekt hinzufügen, damit Benutzer Authentifizierungen vornehmen können.

Die folgende Abbildung zeigt, dass das Zuordnungsobjekt die Verbindung bereitstellt, die für die gesamte Authentifizierung und Genehmigung erforderlich ist.

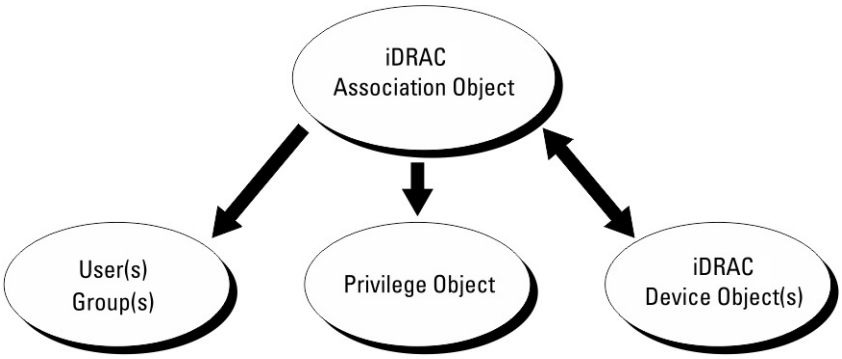


Abbildung 2. Typisches Setup für Active Directory-Objekte

Sie können eine beliebige Anzahl an Zuordnungsobjekten erstellen. Es ist jedoch erforderlich, dass Sie mindestens ein Zuordnungsobjekt erstellen, und Sie müssen ein iDRAC-Geräteobjekt für jedes iDRAC-Gerät im Netzwerk haben, das zum Zweck der Authentifizierung und Autorisierung mit iDRAC in Active Directory integriert werden soll.

Für das Zuordnungsobjekt sind beliebig viele Benutzer und/oder Gruppen und iDRAC-Geräteobjekte zulässig. Das Zuordnungsobjekt enthält jedoch nur ein Berechtigungsobjekt pro Zuordnungsobjekt. Das Zuordnungsobjekt verbindet die Benutzer, die über Berechtigungen für iDRAC-Geräte verfügen.

Über die Dell Erweiterung zum ADUC MMC Snap-In können nur Berechtigungsobjekte und iDRAC-Objekte derselben Domäne dem Zuordnungsobjekt zugewiesen werden. Mit der Dell Erweiterung können keine Gruppen oder iDRAC-Objekte aus anderen Domänen als Produktmitglied des Zuordnungsobjekts hinzugefügt werden.

Wenn Sie Universalgruppen aus unterschiedlichen Domänen hinzufügen, müssen Sie ein Zuordnungsobjekt mit Universalbereich erstellen. Die mit dem Dell Schema Extender-Dienstprogramm erstellten Standardzuordnungsobjekte sind lokale Domänengruppen und funktionieren nicht mit Universalgruppen anderer Domänen.

Dem Zuordnungsobjekt können Benutzer, Benutzergruppen oder verschachtelte Benutzergruppen beliebiger Domänen hinzugefügt werden. Erweiterte Schemalösungen unterstützen jede Art von Benutzergruppe sowie jede Benutzergruppe, die über mehrere Domänen verschachtelt und von Microsoft Active Directory zugelassen ist.

Unter Verwendung des erweiterten Schemas Berechtigungen ansammeln

Die Methode zur Authentifizierung des erweiterten Schemas unterstützt das Ansammeln von Berechtigungen über unterschiedliche Berechtigungsobjekte, die mit demselben Benutzer über verschiedene Zuordnungsobjekte in Verbindung stehen. Anders gesagt: Die Authentifizierung des erweiterten Schemas sammelt Berechtigungen an, um dem Benutzer den Supersatz aller zugewiesener Berechtigungen zu ermöglichen, die den verschiedenen, demselben Benutzer zugeordneten Berechtigungsobjekten entsprechen.

Die folgende Abbildung enthält ein Beispiel für das Ansammeln von Berechtigungen unter Verwendung des erweiterten Schemas.

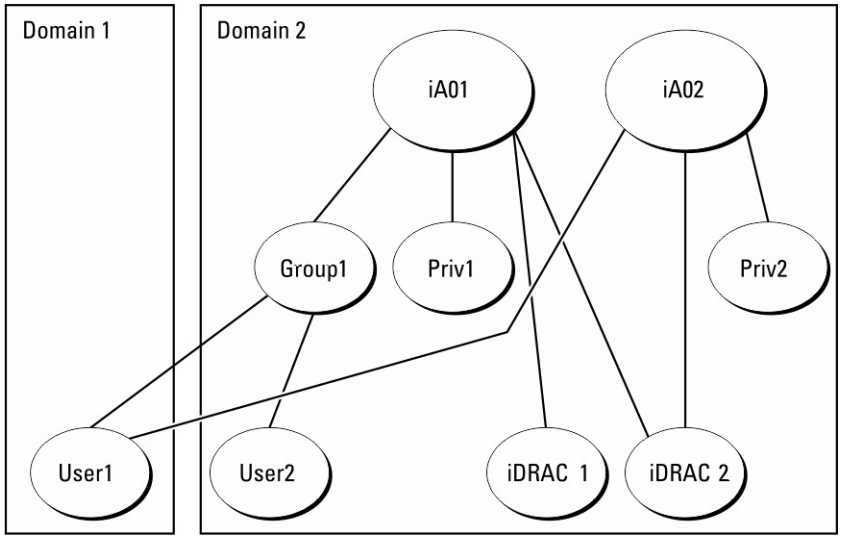


Abbildung 3. Ansammeln von Berechtigungen für einen Benutzer

Die Abbildung zeigt zwei Zuordnungsobjekte: A01 und A02. Benutzer1 ist über beide Zuordnungsobjekte mit iDRAC2 verbunden.

Die Authentifizierung des erweiterten Schemas sammelt Berechtigungen an, um dem Benutzer den maximalen Satz aller möglichen Berechtigungen zur Verfügung zu stellen, und berücksichtigt dabei die zugewiesenen Berechtigungen der verschiedenen Berechtigungsobjekte für den gleichen Benutzer.

In diesem Beispiel verfügt Benutzer1 auf iDRAC2 über die Berechtigungen von Priv1 und Priv2. Benutzer1 verfügt auf iDRAC1 ausschließlich über Priv1-Berechtigungen. Benutzer2 verfügt sowohl auf iDRAC1 als auch auf iDRAC2 über Priv1-Berechtigungen. Diese Darstellung zeigt außerdem, dass Benutzer1 einer anderen Domäne und auch einer Gruppe angehören kann.

Active Directory mit erweitertem Schema konfigurieren

So konfigurieren Sie Active Directory für den Zugriff auf iDRAC:

1. Erweitern des Active Directory-Schemas.
2. Active Directory-Benutzer und Computer-Snap-In erweitern.
3. iDRAC-Benutzer mit Berechtigungen zum Active Directory hinzufügen.
4. Konfigurieren Sie die iDRAC Active Directory-Eigenschaften über die iDRAC-Web-Schnittstelle oder RACADM.

Erweitern des Active Directory-Schemas

Bei der Erweiterung des Active Directory-Schemas werden dem Active Directory-Schema eine Dell Organisationseinheit, Schemaklassen und -attribute sowie Beispielberechtigungen und Zuordnungsobjekte hinzugefügt. Bevor Sie das Schema erweitern, müssen Sie sicherstellen, dass Sie die Schema-Admin-Berechtigungen für den Schema-Master FSMO-Role-Owner der Domänengesamtstruktur besitzen.

ANMERKUNG: Die Schema-Erweiterung für dieses Produkt unterscheidet sich von den Vorgängergenerationen. Das vorherige Schema kann bei diesem Produkt nicht verwendet werden.

ANMERKUNG: Eine Erweiterung des neuen Schemas ändert nichts an den Vorgängerversionen des Produktes.

Sie können das Schema mit einer der folgenden Methoden erweitern:

- Dell Schema Extender-Dienstprogramm
- LDIF-Script-Datei

Die Dell-Organisationseinheit wird dem Schema nicht hinzugefügt, wenn Sie die LDIF-Skriptdatei verwenden.

Die LDIF-Dateien und Dell Schema Extender befinden sich auf der DVD *Dell Systems Management Tools and Documentation* in den folgenden jeweiligen Verzeichnissen:

- DVD-Laufwerk `:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files`
- <DVDdrive>: `\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender`

Lesen Sie zur Verwendung der LDIF-Dateien die Anleitungen in der Infodatei im Verzeichnis **LDIF_Files**.

Sie können Schema Extender oder die LDIF-Dateien an einem beliebigen Standort kopieren und ausführen.

Dell Schema Extender verwenden

VORSICHT: Dell Schema Extender verwendet die Datei SchemaExtenderOem.ini. Um sicherzustellen, dass das Dell Schema Extender-Dienstprogramm richtig funktioniert, ändern Sie nicht den Namen dieser Datei.

1. Klicken Sie im **Begrüßungsbildschirm** auf **Weiter**.
2. Lesen Sie die Warnung und vergewissern Sie sich, dass Sie sie verstehen und klicken Sie dann auf **Weiter**.
3. Wählen Sie **Aktuelle Anmeldeinformationen Verwenden** aus, oder geben Sie einen Benutzernamen und ein Kennwort mit Schema-Administratorrechten ein.
4. Klicken Sie auf **Weiter,** um Dell Schema Extender auszuführen.
5. Klicken Sie auf **Fertigstellen**.

   Das Schema wird erweitert. Um die Schema-Erweiterung zu überprüfen, verwenden Sie MMC und das Active Directory-Schema-Snap-In, um sicherzustellen, dass Klassen und Attribute auf Seite 163 vorhanden sind. Weitere Informationen zum Verwenden von MMC und des Active Directory-Schema-Snap-In finden Sie in der Microsoft-Dokumentation.

Klassen und Attribute

Tabelle 25. Klassendefinitionen für Klassen, die zum Active Directory-Schema hinzugefügt wurden

Klassenname	Zugewiesene Objekt-Identifikationsnummer (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

Tabelle 26. DelliDRACdevice-Klasse

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Beschreibung	Repräsentiert das Dell iDRAC-Gerät. iDRAC muss im Active Directory als delliDRACDevice konfiguriert sein. Mit dieser Konfiguration kann der iDRAC Lightweight Directory Access Protocol (LDAP)-Abfragen an Active Directory senden.
Klassentyp	Strukturklasse
SuperClasses	dellProduct
Attribute	dellSchemaVersion dellRacType

Tabelle 27. delliDRACAssociationObject Class

OID	1.2.840.113556.1.8000.1280.1.7.1.2
Beschreibung	Repräsentiert das Dell-Zuordnungsobjekt. Das Zuordnungsobjekt ist die Verbindung zwischen Benutzern und Geräten.
Klassentyp	Strukturklasse
SuperClasses	Gruppe
Attribute	dellProductMembers dellPrivilegeMember

Tabelle 28. dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Beschreibung	Legt die Berechtigungen für iDRAC fest (Autorisierungsrechte)
Klassentyp	Erweiterungsklasse
SuperClasses	Keine
Attribute	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

Tabelle 29. dellPrivileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Beschreibung	Wird als Container-Klasse für die Dell-Berechtigungen (Autorisierungsrechte) verwendet.

Tabelle 29. dellPrivileges Class (fortgesetzt)

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Klassentyp	Strukturklasse
SuperClasses	Benutzer
Attribute	dellRAC4Privileges

Tabelle 30. dellProduct Class

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Beschreibung	Die Hauptklasse, von der alle Dell-Produkte abgeleitet werden.
Klassentyp	Strukturklasse
SuperClasses	Computer
Attribute	dellAssociationMembers

Tabelle 31. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden

Attributname/Beschreibung	Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
dellPrivilegeMember Die Liste von dellPrivilege-Objekten, die zu diesem Attribut gehören.	1.2.840.113556.1.8000.1280.1.1.2.1 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Die Liste von dellRacDevice- und DelliDRACDevice-Objekten, die zu dieser Rolle gehören. Dieses Attribut ist die Vorwärtsverbindung zur dellAssociationMembers-Rückwärtsverbindung. Link-ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser TRUE, wenn der Benutzer Anmeldungsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.3 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin TRUE, wenn der Benutzer Kartenkonfigurationsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.4 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin TRUE, wenn der Benutzer Benutzerkonfigurationsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.5 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin TRUE, wenn der Benutzer Protokolllöschungsrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.6 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE

Tabelle 31. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden (fortgesetzt)

Attributname/Beschreibung	Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
dellIsServerResetUser TRUE, wenn der Benutzer Server-Reset-Rechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.7 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE, wenn der Benutzer über Virtuelle-Konsole-Rechte auf dem Gerät verfügt.	1.2.840.113556.1.8000.1280.1.1.2.8 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE, wenn der Benutzer Rechte für den virtuellen Datenträger auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.9 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE, wenn der Benutzer Testwarnungsbenutzerrechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.10 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE, wenn der Benutzer Debug-Befehl-Admin-Rechte auf dem Gerät hat.	1.2.840.113556.1.8000.1280.1.1.2.11 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion Die aktuelle Schemaversion wird verwendet, um das Schema zu aktualisieren.	1.2.840.113556.1.8000.1280.1.1.2.12 Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Dieses Attribut ist der aktuelle RAC-Typ für das dellRacDevice-Objekt und der Rückwärtslink zum dellAssociationObjectMembers-Vorwärtslink.	1.2.840.113556.1.8000.1280.1.1.2.13 Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Liste der dellAssociationObjectMembers, die zu diesem Produkt gehören. Dieses Attribut ist die Rückwärtsverbindung zum verknüpften dellProductMembers-Attribut. Link-ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Dell-Erweiterung zu Active Directory Benutzer- und Computer-Snap-In installieren

Wenn Sie das Schema im Active Directory erweitern, müssen Sie auch das Active Directory-Benutzer- und -Computer-Snap-In erweitern, so dass der Administrator iDRAC-Geräte, Benutzer und Benutzergruppen, iDRAC-Zuordnungen und iDRAC-Berechtigungen verwalten kann.

Wenn Sie die Systemverwaltungssoftware mit der *Dell Systems Management Tools and Documentation*-DVD installieren, können Sie das Snap-In installieren, indem Sie während des Installationsverfahrens die Option **Active Directory Users and Computers Snap-in**

(Active Directory-Benutzer und Computer-Snap-In) auswählen. Weitere Anleitungen zur Installation der Systemverwaltungssoftware finden Sie im Schnellinstallationshandbuch zu Dell OpenManage Software. Das Snap-In-Installationsprogramm für 64-Bit-Versionen von Windows-Betriebssystemen finden Sie unter:

<DVD-Laufwerk>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

Weitere Informationen über Active Directory-Benutzer- und -Computer-Snap-In finden Sie in der Microsoft-Dokumentation.

iDRAC-Benutzer und -Berechtigungen zu Active Directory hinzufügen

Mit dem von Dell erweiterten Active Directory-Benutzer- und -Computer-Snap-In können Sie iDRAC-Benutzer und -Berechtigungen hinzufügen, indem Sie Gerät-, Zuordnungs- und Berechtigungsobjekte erstellen. Um die einzelnen Objekte hinzuzufügen, führen Sie die folgenden Schritte durch:

- Erstellen eines iDRAC-Geräteobjekts
- Erstellen eines Berechtigungsobjekts
- Erstellen eines Zuordnungsobjekts
- Einem Zuordnungsobjekt Objekte hinzufügen

Erstellen von iDRAC-Geräteobjekten

So erstellen Sie ein iDRAC-Geräteobjekt:

1. Klicken Sie im Fenster **Console Root** (MCC) mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu** > **Dell Remote Management Object Advanced** aus.
   Das Fenster **Neues Objekt** wird angezeigt.
3. Geben Sie einen Namen für das neue Objekt ein. Der Name muss mit dem iDRAC-Namen identisch sein, den Sie im Rahmen der Konfiguration der Active Directory-Eigenschaften über die iDRAC-Webschnittstelle eingegeben haben.
4. Wählen Sie **iDRAC-Geräteobjekt** und klicken Sie auf OK.

Berechtigungsobjekt erstellen

So erstellen Sie ein Berechtigungsobjekt:

ANMERKUNG: Sie müssen ein Berechtigungsobjekt in der gleichen Domäne erstellen, in der auch das verknüpfte Zuordnungsobjekt vorhanden ist.

1. Klicken Sie im Fenster **Console Root** (MMC) mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu** > **Dell Remote Management Object Advanced** aus.
   Das Fenster **Neues Objekt** wird angezeigt.
3. Geben Sie einen Namen für das neue Objekt ein.
4. Wählen Sie **Berechtigungsobjekt** und klicken Sie auf OK.
5. Klicken Sie mit der rechten Maustaste auf das Berechtigungsobjekt, das Sie erstellt haben, und wählen Sie **Eigenschaften** aus.
6. Klicken Sie auf die Registerkarte **Remote-Verwaltungsberechtigungen**, und weisen Sie die Berechtigungen für den Benutzer oder die Gruppe zu.

Zuordnungsobjekt erstellen

So erstellen Sie ein Zuordnungsobjekt:

ANMERKUNG: Das iDRAC-Zuordnungsobjekt wird von der Gruppe abgeleitet und hat einen Wirkungsbereich in einer lokalen Domäne.

1. Klicken Sie im Fenster **Console Root** (MMC) mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu** > **Dell Remote Management Object Advanced** aus.
   Das Fenster **Neues Objekt** wird angezeigt.
3. Geben Sie einen Namen für das neue Objekt ein, und wählen Sie **Zuordnungsobjekt** aus.
4. Wählen Sie den Bereich für das **Zuordnungsobjekt** und klicken Sie auf OK.
5. Geben Sie den authentifizierten Benutzern Zugriffsberechtigungen für den Zugriff auf die angelegten Zuordnungsobjekte.

Benutzerzugriffsberechtigungen für verknüpfte Objekte bereitstellen

Um den authentifizierten Benutzern Zugriffsberechtigungen für den Zugriff auf die angelegten Zuordnungsobjekte zu geben:

1. Navigieren Sie zu **Administrative Tools (Verwaltung)** > **ADSI Edit (ADSI-Bearbeitung)**. Die Konsole **ADSI Edit (ADSI-Bearbeitung)** wird angezeigt.
2. Wechseln Sie im rechten Bereich zum angelegten Zuordnungsobjekt, klicken Sie auf die rechte Maustaste und wählen Sie **Eigenschaften**.
3. Klicken Sie auf Registerkarte **Sicherheit** auf **Hinzufügen**.
4. Geben Sie `Authenticated Users` ein, klicken Sie auf **Check Names** (Namen prüfen) und klicken Sie auf **OK**. Die authentifizierten Benutzer werden der Liste **Groups and user names** (Gruppen- oder Benutzernamen) hinzugefügt.
5. Klicken Sie auf **OK**.

Objekte zu einem Zuordnungsobjekt hinzufügen

Durch die Verwendung des Fensters **Zuordnungsobjekt-Eigenschaften** können Sie Benutzer oder Benutzergruppen, Berechtigungsobjekte und iDRAC-Geräte oder iDRAC-Gerätegruppen zuordnen.

Sie können Benutzergruppen und iDRAC-Geräte hinzufügen.

Benutzer oder Benutzergruppen hinzufügen

So fügen Sie Benutzer oder Benutzergruppen hinzu:

1. Klicken Sie mit der rechten Maustaste auf das **Zuordnungsobjekt** und wählen Sie **Eigenschaften** aus.
2. Wählen Sie das Register **Benutzer** und klicken Sie auf **Hinzufügen.**
3. Geben Sie den Namen des Benutzers oder der Benutzergruppe ein und klicken Sie auf **OK**.

Berechtigungen hinzufügen

So fügen Sie Berechtigungen hinzu:

Klicken Sie auf die Registerkarte **Privilege Object** (Berechtigungsobjekt), um das Berechtigungsobjekt der Zuordnung hinzuzufügen, die die Berechtigungen der Benutzer oder Benutzergruppe bei Authentifizierung eines iDRAC-Geräts definiert. Sie können einem Zuordnungsobjekt nur ein Berechtigungsobjekt hinzufügen.

1. Wählen Sie das Register **Berechtigungsobjekt** und klicken Sie auf **Hinzufügen**.
2. Geben Sie den Namen des Berechtigungsobjekts ein und klicken Sie auf **OK**.
3. Klicken Sie auf die Registerkarte **Privilege Object** (Berechtigungsobjekt), um das Berechtigungsobjekt der Zuordnung hinzuzufügen, die die Berechtigungen der Benutzer oder Benutzergruppe bei Authentifizierung eines iDRAC-Geräts definiert. Sie können einem Zuordnungsobjekt nur ein Berechtigungsobjekt hinzufügen.

Hinzufügen von iDRAC-Geräten oder iDRAC-Gerätegruppen

So fügen Sie iDRAC-Geräte oder iDRAC-Gerätegruppen hinzu:

1. Wählen Sie die Registerkarte **Produkte** und klicken Sie auf **Hinzufügen**.
2. Geben Sie die Namen der iDRAC-Geräte oder iDRAC-Gerätegruppen ein und klicken Sie auf **OK**.
3. Im Fenster **Eigenschaften** klicken Sie auf **Anwenden** und dann auf **OK**.
4. Klicken Sie auf die Registerkarte **Products** (Produkte) und fügen Sie ein iDRAC-Gerät hinzu, das mit dem Netzwerk verbunden ist, das den definierten Benutzern oder Benutzergruppen zur Verfügung steht. Einem Zuordnungsobjekt können mehrere iDRAC-Geräte hinzugefügt werden.

Active Directory mit erweitertem Schema unter Verwendung der iDRAC-Webschnittstelle konfigurieren

So konfigurieren Sie Active Directory mit erweitertem Schema über die Web-Schnittstelle:

ANMERKUNG: Weitere Informationen zu den verschiedenen Feldern finden Sie in der *iDRAC-Online-Hilfe*.

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Users (Benutzer)** > **Directory Services (Verzeichnisdienste)** > **Microsoft Active Directory**. Klicken Sie auf **Edit** (Bearbeiten).
   Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 1 von 4 wird angezeigt.
2. Aktivieren Sie optional die Zertifikatvalidierung, und laden Sie das durch die Zertifikatstelle signierte digitale Zertifikat hoch, das im Rahmen der Initiierung von SSL-Verbindungen während der Kommunikation mit dem Active Directory (AD)-Server verwendet wird.
3. Klicken Sie auf **Next** (Weiter).
   Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 2 von 4 wird angezeigt.
4. Geben Sie Informationen zum Ort der Active Directory(AD)-Server und -Benutzerkonten an. Geben Sie außerdem die Zeit an, die iDRAC auf Antworten von AD während des Anmeldevorgangs warten muss.

   ANMERKUNG:
   - Wenn die Zertifikatvalidierung aktiviert ist, geben Sie die Serveradressen des Domänen-Controllers und den FQDN an. Stellen Sie unter **iDRAC Settings (iDRAC-Einstellungen)** > **Network (Netzwerk)** sicher, dass DNS korrekt konfiguriert ist.
   - Wenn sich Benutzer und iDRAC-Objekte in unterschiedlichen Domänen befinden, sollten Sie nicht die Option **User Domain from Login** (Benutzerdomäne von Anmeldung) wählen. Wählen Sie stattdessen die Option **Specify a Domain** (Domäne angeben) aus und geben Sie den Namen der Domäne ein, in der das iDRAC-Objekt verfügbar ist.

5. Klicken Sie auf **Next** (Weiter). Die Seite **Active Directory Configuration and Management Step 3 of 4** (Active Directory-Konfiguration und -Verwaltung Schritt 3 von 4) wird angezeigt.
6. Wählen Sie **Erweitertes Schema** aus, und klicken Sie auf **Weiter**.
   Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 4 von 4 wird angezeigt.
7. Geben Sie den Namen und den Speicherort des iDRAC-Geräteobjekts unter Active Directory (AD) an, und klicken Sie auf **Fertigstellen**.
   Die Active Directory-Einstellungen für den Modus „Erweitertes Schema“ wird konfiguriert.

Konfiguration des Active Directory mit erweitertem Schema unter Verwendung von RACADM

So konfigurieren Sie Active Directory mit erweitertem Schema unter Verwendung von RACADM:

1. Verwenden Sie die folgenden Befehle:

```
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>
```

   - Geben Sie unbedingt den vollständig qualifizierten Domänennamen (FQDN) des Domänen-Controllers ein, nicht den FQDN der Domäne selbst. Geben Sie z. B. `servername.dell.com` statt `dell.com` ein.
   - Sie müssen mindestens eine der drei Adressen angeben. Der iDRAC versucht so lange, nacheinander mit jeder der konfigurierten Adressen eine Verbindung herzustellen, bis eine Verbindung hergestellt werden konnte. Mit erweitertem Schema sind diese der FQDN oder die IP-Adresse des Domänen-Controllers, auf dem sich das iDRAC-Gerät befindet.
   - Um die Zertifikatvalidierung während eines SSL-Handshake zu deaktivieren, verwenden Sie den folgenden Befehl:

     ```
     racadm set iDRAC.ActiveDirectory.CertValidationEnable 0
     ```

     In diesem Fall brauchen Sie kein CA-Zertifikat zu laden.
   - So erzwingen Sie die Zertifikatvalidierung während eines SSL-Handshake (optional):

     ```
     racadm set iDRAC.ActiveDirectory.CertValidationEnable 1
     ```

     In diesem Fall müssen Sie mit dem folgenden Befehl ein CA-Zertifikat laden:

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

ANMERKUNG: Wenn die Zertifikatvalidierung aktiviert ist, geben Sie die Serveradressen des Domänen-Controllers und den FQDN an. Stellen Sie sicher, dass DNS unter **iDRAC-Einstellungen** > **Netzwerk** korrekt konfiguriert ist.

Die Verwendung des folgenden RACADM-Befehls kann optional sein.

```
racadm sslcertdownload -t 1 -f <RAC SSL certificate>
```

2. Wenn DHCP auf dem iDRAC aktiviert ist und Sie den vom DHCP-Server bereitgestellten DNS verwenden möchten, geben Sie folgenden Befehl ein:

```
racadm set iDRAC.IPv4.DNSFromDHCP 1
```

3. Wenn DHCP auf dem iDRAC deaktiviert ist oder Sie ihre DNS IP-Adresse manuell eingeben möchten, arbeiten Sie mit den folgenden Befehlen:

```
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. Möchten Sie eine Liste mit Benutzerdomänen konfigurieren, sodass für die Anmeldung an der iDRAC-Webschnittstelle nur der Benutzername eingegeben werden muss, verwenden Sie dazu den folgenden Befehl:

```
racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address of the
domain controller>
```

Sie können bis zu 40 Benutzerdomänen mit Indexzahlen zwischen 1 und 40 konfigurieren.

Active Directory-Einstellungen testen

Sie können die Active Directory-Einstellungen testen, um zu überprüfen, ob Ihre Konfiguration korrekt ist oder um Fehler bei der Active Directory-Anmeldung zu analysieren.

Active Directory-Einstellungen über die iDRAC-Webschnittstelle testen

So testen Sie die Active Directory-Einstellungen:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Users (Benutzer)** > **Directory Services (Verzeichnisdienste)** > **Microsoft Active Directory**, und klicken Sie auf **Test** (Testen).
   Die Seite **Test Active Directory Settings** (Active Directory-Einstellungen testen) wird angezeigt.
2. Klicken Sie auf **Testen**.
3. Geben Sie einen Test-Benutzernamen (z. B. **benutzername@domain.com**) sowie ein Kennwort ein und klicken Sie auf **Start Test** (Test starten). Es werden ausführliche Testergebnisse und das Testprotokoll angezeigt.

   Überprüfen Sie gegebenenfalls die einzelnen Fehlermeldungen und mögliche Lösungen im Testprotokoll.

   ANMERKUNG: Wenn beim Testen der Active Directory-Einstellungen die Zertifikatsüberprüfung aktiviert ist, verlangt iDRAC, dass der Active Directory-Server über den FQDN und nicht über eine IP-Adresse identifiziert wird. Wenn der Active Directory-Server über eine IP-Adresse identifiziert wird, schlägt die Zertifikatsvalidierung fehl, da iDRAC nicht mit dem Active Directory-Server kommunizieren kann.

Active Directory-Einstellungen über RACADM testen

Um die Active-Directory-Einstellungen zu testen, verwenden Sie den Befehl `testfeature`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Generische LDAP-Benutzer konfigurieren

Der iDRAC bietet eine allgemeine Lösung zur Unterstützung Lightweight Directory Access Protocol(LDAP)-basierter Authentifizierung. Für diese Funktion ist keine Schemaerweiterung in Ihren Verzeichnisdiensten erforderlich.

Um die iDRAC-LDAP-Implementierung generisch zu gestalten, werden die Gemeinsamkeiten der verschiedenen Verzeichnisdienste dazu genutzt, Benutzer in Gruppen zusammenzufassen und danach die Beziehung zwischen Benutzer und Gruppe festzulegen. Die verzeichnisdienstspezifische Maßnahme ist hierbei das Schema. Es können beispielsweise verschiedene Attributnamen für Gruppe, Benutzer und Verbindung zwischen dem Benutzer und der Gruppe vergeben werden. Diese Maßnahmen kann im iDRAC konfiguriert werden.

ANMERKUNG: Die Smart Card-basierte Zweifaktor-Authentifizierung (TFA) und einfache Anmeldung (SSO) werden nicht für den allgemeinen LDAP-Verzeichnisdienst unterstützt.

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mit der iDRAC-Webschnittstelle

So konfigurieren Sie den generischen LDAP-Verzeichnisdienst über die Web-Schnittstelle:

ANMERKUNG: Weitere Informationen zu den verschiedenen Feldern finden Sie in der *iDRAC-Online-Hilfe*.

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Users (Benutzer)** > **Directory Services (Verzeichnisdienste)** > **Generic LDAP Directory Service (Allgemeiner LDAP-Verzeichnisdienst)**, klicken Sie auf **Edit** (Bearbeiten).
   Die Seite **Generic LDAP Configuration and Management Step 1 of 3** (Generisches LDAP – Konfiguration und Verwaltung – Schritt 1 von 3) zeigt die aktuellen Einstellungen für das generische LDAP an.
2. Aktivieren Sie optional Zertifikatsvalidierung und laden Sie das digitale Zertifikat hoch, das Sie zum Aufbau von SSL-Verbindungen bei der Kommunikation mit einem generischen LDAP-Server verwendet haben.

   ANMERKUNG: Bei dieser Version wird eine LDAP-Bindung, die nicht auf einem SSL-Anschluss basiert, nicht unterstützt. Nur LDAP über SSL wird unterstützt.

3. Klicken Sie auf **Next** (Weiter).
   Die Seite **Allgemeines LDAP – Konfiguration und Verwaltung** Schritt 2 von 3 wird angezeigt.
4. Aktivieren Sie die generische LDAP-Authentifizierung, und geben Sie die Speicherortinformationen zu den generischen LDAP-Servern und -Benutzerkonten an.

   ANMERKUNG: Wenn die Zertifikatvalidierung aktiviert ist, geben Sie die FQDN des LDAP-Servers an und stellen Sie sicher, dass DNS unter **iDRAC Settings (iDRAC-Einstellungen)** > **Network (Netzwerk)** korrekt konfiguriert ist.

   ANMERKUNG: In dieser Version werden verschachtelte Gruppen nicht unterstützt. Die Firmware sucht nach dem direkten Mitglied der Gruppe, das dem Benutzer-DN entspricht. Weiterhin werden nur Einzeldomänen unterstützt. Übergreifende Domänen werden nicht unterstützt.

5. Klicken Sie auf **Next** (Weiter).
   Die Seite **Allgemeines LDAP – Konfiguration und Verwaltung** Schritt 3a von 3 wird angezeigt.
6. Klicken Sie auf **Rollengruppe**.
   Die Seite **Allgemeines LDAP – Konfiguration und Verwaltung** Schritt 3b von 3 wird angezeigt.
7. Geben Sie den abgegrenzten Namen für die Gruppe und die mit dieser Gruppe verbundenen Berechtigungen ein, und klicken Sie dann auf **Anwenden**.

   ANMERKUNG: Wenn Sie Novell eDirectory verwenden und die folgenden Zeichen für den Gruppen-Domänennamen verwendet haben, müssen diese Zeichen umgeschrieben werden: # (Hash-Zeichen), " (doppelte Anführungszeichen), ; (Semikolon), > (größer als), , (Komma) oder < (kleiner als).

   Die Einstellungen für die Rollengruppe werden gespeichert. Diese werden auf der Seite **Generic LDAP Configuration and Management Step 3a of 3** (Allgemeines LDAP – Konfiguration und Verwaltung – Schritt 3a von 3) angezeigt.
8. Wenn Sie weitere Rollengruppen konfigurieren möchten, wiederholen Sie die Schritte 7 und 8.
9. Klicken Sie auf **Fertigstellen**. Der allgemeine LDAP-Verzeichnisdienst ist damit konfiguriert.

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mittels RACADM

Um den LDAP-Verzeichnisdienst zu konfigurieren, verwenden Sie die Objekte in den Gruppen `iDRAC.LDAP` und `iDRAC.LDAPRole`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Einstellungen für LDAP-Verzeichnisdienst testen

Sie können die Einstellungen für LDAP-Verzeichnisdienste testen, um zu überprüfen, ob Ihre Konfiguration korrekt ist oder um Fehler bei der Active Directory-Anmeldung zu analysieren.

Testen der Einstellungen des LDAP-Verzeichnisdienstes über die iDRAC-Webschnittstelle

So testen Sie die Einstellungen für den LDAP-Verzeichnisdienst:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Users (Benutzer)** > **Directory Services (Verzeichnisdienste)** > **Generic LDAP Directory Service (Generische LDAP-Verzeichnisdienste)**.
   Die Seite **Generisches LDAP - Konfiguration und Verwaltung** zeigt die aktuellen Einstellungen für das generische LDAP an.
2. Klicken Sie auf **Testen**.
3. Geben Sie den Benutzernamen und das Kennwort eines Verzeichnisbenutzers ein, der zur Überprüfung der LDAP-Einstellungen ausgewählt wurde. Das Format hängt vom verwendeten *Attribut der Benutzeranmeldung* ab und der eingegebene Benutzername muss dem Wert des gewählten Attributs entsprechen.

   ANMERKUNG: Wenn beim Testen der LDAP-Einstellungen **Enable Certificate Validation** (Zertifikatsüberprüfung aktivieren) ausgewählt ist, verlangt iDRAC, dass der LDAP-Server über den FQDN und nicht über eine IP-Adresse identifiziert wird. Wenn der LDAP-Server über eine IP-Adresse identifiziert wird, schlägt die Zertifikatsvalidierung fehl, da iDRAC nicht mit dem LDAP-Server kommunizieren kann.

   ANMERKUNG: Wenn generisches LDAP aktiviert ist, versucht iDRAC zunächst, den Benutzer als Verzeichnisbenutzer anzumelden. Schlägt dies fehl, wird die Suche nach lokalen Benutzern aktiviert.

   Die Testergebnisse und das Testprotokoll werden angezeigt.

LDAP-Verzeichnisdiensteinstellungen über RACADM testen

Um die Einstellungen des LDAP-Verzeichnisdiensts zu testen, verwenden Sie den Befehl `testfeature`. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

10

Systemkonfigurations-Sperrmodus

Der Systemkonfigurations-Sperrmodus hilft, unbeabsichtigte Änderungen nach der Bereitstellung eines Systems zu verhindern. Der Sperrmodus gilt sowohl für Konfigurations- als auch für Firmware-Updates. Wenn das System gesperrt ist, wird jeder Versuch, die Systemkonfiguration zu ändern, blockiert. Wenn versucht wird, die kritischen Systemeinstellungen zu ändern, wird eine Fehlermeldung angezeigt. Das Aktivieren des Systemsperrmodus sperrt die Firmwareupdates von Drittanbieter-E/A-Karten über die Anbieter-Tools.

Der Systemsperrmodus ist nur für Kunden mit Enterprise-Lizenz verfügbar.

In der Version 4.40.00.00 wird die Systemsperrfunktion auch auf den NIC erweitert.

ANMERKUNG: Die verbesserte Sperrung für NICs umfasst nur die Firmwaresperrung, um Firmwareupdates zu verhindern. Die Sperrung der Konfiguration (x-UEFI) wird nicht unterstützt.

ANMERKUNG: Wenn der Sperrmodus des Systems aktiviert ist, können Sie keine Konfigurationseinstellungen mehr ändern. Die Felder unter Systemeinstellungen sind deaktiviert.

Der Sperrmodus kann über die folgenden Schnittstellen aktiviert oder deaktiviert werden:

- iDRAC-Weboberfläche
- RACADM
- WSMan
- SCP (Systemkonfigurationsprofil)
- Redfish
- Verwendung von F2 beim POST und Auswahl der iDRAC-Einstellungen
- Löschen des werkseitigen Systems

ANMERKUNG: Um den Sperrmodus zu aktivieren, müssen Sie über eine iDRAC Datacenter-Lizenz und Berechtigungen zur Steuerung und Konfiguration des Systems verfügen.

ANMERKUNG: Sie können möglicherweise auf vMedia zugreifen, während sich das System im Sperrmodus befindet, doch das Konfigurieren der Remote-Dateifreigabe nicht aktiviert ist.

ANMERKUNG: Die Schnittstellen, wie z. B. OMSA, SysCfg und USC, können die Einstellungen nur überprüfen, aber keine Änderungen an den Konfigurationen vornehmen.

Die folgende Tabelle listet die funktionalen und nicht-funktionalen Funktionen, Schnittstellen und Dienstprogramme auf, die vom Sperrmodus betroffen sind:

ANMERKUNG: Das Ändern der Bootreihenfolge mittels iDRAC wird nicht unterstützt, wenn der Sperrmodus aktiviert ist. Die Boot-Control-Option ist jedoch im vConsole-Menü verfügbar, was keine Auswirkung hat, wenn sich der iDRAC im Sperrmodus befindet.

Tabelle 32. Vom Sperrmodus betroffene Elemente

Deaktiviert	Weiterhin funktionsfähig
• Lizenzen löschen • DUP-Updates • SCP-Import • Auf Standardeinstellung zurücksetzen • OMSA/OMSS • IPMI • DRAC/LC • DTK-Dienstprogramm SYSCFG • Redfish • OpenManage Essentials • BIOS (F2-Einstellungen werden schreibgeschützt) • Group Manager • Auswählen von Netzwerkkarten	• Betriebsvorgänge – Einschalten/Ausschalten, Zurücksetzen • Einstellung der Stromobergrenze • Leistungspriorität • Identifizierung von Geräten (Gehäuse oder PERC) • Teileaustausch, Easy Restore (Einfache Wiederherstellung) und Austausch der Hauptplatine • Ausführen von Diagnosen • Modulare Vorgänge (FlexAddress- oder Remote-zugewiesene Adresse) • Group Manager-Passcode • Alle Anbieterhilfsprogramme mit direktem Zugriff auf das Gerät (ausgewählte NICs ausgeschlossen) • Lizenzexport

Tabelle 32. Vom Sperrmodus betroffene Elemente

Deaktiviert	Weiterhin funktionsfähig

	• PERC
	  ○ PERC CLI
	  ○ DTK-RAIDCFG
	  ○ F2/Strg+R
	• Alle Herstellerhilfsprogramme mit direktem Zugriff auf das Gerät
	• NVMe
	  ○ DTK-RAIDCFG
	  ○ F2/Strg+R
	• BOSS-S1
	  ○ Marvell CLI
	  ○ F2/Strg+R
	• ISM-/OMSA-Einstellungen (BS BMC-Aktivierung, Watchdog ping, BS-Name, BS-Version)

ANMERKUNG: Wenn der Sperrmodus aktiviert ist, wird die OpenID Connect-Anmeldeoption nicht auf der iDRAC-Anmeldeseite angezeigt.

11

iDRAC für die einfache Anmeldung oder Smart Card-Anmeldung konfigurieren

In diesem Abschnitt erhalten Sie Informationen zur Konfiguration von iDRAC für die Smart Card-Anmeldung (für lokale und Active Directory-Benutzer) und die einmalige Anmeldung (SSO, für Active Directory-Benutzer.) Die SSO- und Smart Card-Anmeldungen sind lizenzierte Funktionen.

Der iDRAC unterstützt die Kerberos-basierte Active Directory-Authentifizierung zur Unterstützung von Smart Card- und SSO-Anmeldungen. Weitere Informationen über Kerberos finden Sie auf der Microsoft-Website.

Themen:

- Voraussetzungen für die einmalige Active Directory-Anmeldung oder die Smart Card-Anmeldung
- iDRAC-SSO-Anmeldung für Active Directory-Benutzer konfigurieren
- Smartcard-Anmeldung aktivieren oder deaktivieren
- Konfigurieren von Smart Card-Anmeldung
- Anmelden mit Smart Card

Voraussetzungen für die einmalige Active Directory-Anmeldung oder die Smart Card-Anmeldung

Die Voraussetzungen für die Active Directory-basierten SSO- oder Smart Card-Anmeldungen lauten wie folgt:

- Synchronisieren Sie die iDRAC-Zeit mit der Zeit des Active Directory-Domänen-Controllers. Andernfalls schlägt die Kerberos-Authentifizierung auf dem iDRAC fehl. Sie können die Funktion für Zeitzone und NTP verwenden, um die Zeit zu synchronisieren. Informieren Sie sich dazu unter Das Konfigurieren von Zeitzone und NTP auf Seite 106.
- Registrieren Sie den iDRAC als Computer in der Active Directory-Root-Domäne.
- Generieren Sie eine Keytab-Datei über das Ktpass-Tool.
- Um die einmalige Anmeldung für das erweiterte Schema zu aktivieren, stellen Sie sicher, dass die Option **Trust this user for delegation to any service (Kerberos only) (Diesem Benutzer für die Delegierung zu einem beliebigen Dienst vertrauen (nur Kerberos))** auf der Registerkarte **Delegation (Delegierung)** für den Keytab-Benutzer ausgewählt ist. Diese Registerkarte ist erst verfügbar, nachdem die Keytab-Datei über das ktpass-Dienstprogramm erstellt wurde.
- Konfigurieren Sie den Browser für die Aktivierung der SSO-Anmeldung.
- Erstellen Sie die Active Directory-Objekte, und stellen Sie die erforderlichen Berechtigungen bereit.
- Konfigurieren Sie für SSO auf den DNS-Servern die Zone für die Rückwärtssuche für das Subnetz, auf dem sich iDRAC befindet.

  ANMERKUNG: Wenn der Host-Name mit der DNS-Rückwärtssuche nicht übereinstimmt, schlägt die Kerberos-Authentifizierung fehl.
- Konfigurieren Sie den Browser für die Unterstützung der SSO-Anmeldung. Weitere Informationen finden Sie unter Einmaliges Anmelden auf Seite 367.

  ANMERKUNG: Google Chrome und Safari unterstützen Active Directory für die SSO-Anmeldung nicht.

iDRAC im Domänennamensystem registrieren

So registrieren Sie iDRAC in der Active Directory-Stammdomäne:

1. Klicken Sie auf **iDRAC Einstellungen** > **Konnektivität** > **Netzwerk**.
   Die Seite **Netzwerk** wird angezeigt.
2. Wählen Sie **IPv4-Einstellungen** oder **IPv6-Einstellungen** basierend auf den IP-Einstellungen.
3. Geben Sie eine gültige IP-Adresse für den **Bevorzugten/Alternativen DNS Server** an. Dieser Wert ist eine gültige DNS-Server-IP-Adresse, die Teil der Root-Domäne ist.
4. Wählen Sie **iDRAC auf DNS registrieren** aus.

5. Geben Sie einen gültigen **DNS-Domänennamen an**.
6. Stellen Sie sicher, dass die Netzwerk-DNS-Konfiguration mit den Active Directory-DNS-Informationen übereinstimmt.
   Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

Active Directory-Objekte erstellen und Berechtigungen bereitstellen

Anmelden bei Active Directory mit Standardschema-SSO

Führen Sie die folgenden Schritte für die SSO-Anmeldung bei Active Directory mit dem Standardschema aus:
1. Erstellen Sie eine Benutzergruppe.
2. Erstellen Sie einen Benutzer für das Standardschema.

ANMERKUNG: Verwenden Sie die vorhandene AD-Benutzergruppe und den AD-Benutzer.

Anmelden bei Active Directory mit erweitertem SSO-Schema

Führen Sie die folgenden Schritte für das erweiterte Active Directory-Schema auf der Basis der SSO-Anmeldung aus:

1. Erstellen Sie das Geräteobjekt, Berechtigungsobjekt und das Zuordnungsobjekts im Active Directory-Server.
2. Stellen Sie die Zugriffsrechte auf das angelegte Berechtigungsobjekt ein.
   ANMERKUNG: Es wird empfohlen, keine Administratorberechtigungen zu vergeben, da hiermit einige Sicherheitsprüfungen umgangen werden könnten.
3. Ordnen Sie das Geräteobjekt und das Berechtigungsobjekt mit dem Zuordnungsobjekt zu.
4. Fügen Sie dem Geräteobjekt den vorherigen SSO-Benutzer (anmeldender Benutzer) zu.
5. Vergeben Sie die Zugangsberechtigung zum Zugriff auf das angelegte Zuordnungsobjekt an *authentifizierte Benutzer*.

Anmelden bei Active Directory-SSO

Führen Sie die folgenden Schritte für die Active Directory-SSO-Anmeldung aus:
1. Erstellen Sie einen Kerberos-Schlüssel-Registerkarten-Benutzer, der für die Erstellung der Schüssel-Registerkarten-Datei verwendet wird.

ANMERKUNG: Erstellen Sie einen neuen KERBROS-Schlüssel für jede iDRAC-IP.

iDRAC-SSO-Anmeldung für Active Directory-Benutzer konfigurieren

Stellen Sie vor der Konfiguration von iDRAC für die Active Directory-SSO-Anmeldung sicher, dass alle Voraussetzungen erfüllt sind.

Sie können iDRAC für Active Directory-SSO konfigurieren, wenn Sie ein Benutzerkonto auf der Basis von Active Directory einrichten.

Erstellen eines Nutzers in Active Directory für SSO

So erstellen Sie einen Nutzer in Active Directory für SSO:

1. Erstellen Sie einen neuen Nutzer in der Organisationseinheit.
2. Gehen Sie zu **Kerberos-Nutzer>Eigenschaften>Konto>Kerberos-AES-Verschlüsselungstypen für dieses Konto verwenden**
3. Verwenden Sie den folgenden Befehl, um eine Kerberos-Keytab auf dem Active Directory-Server zu erstellen:

```
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
```

Hinweis für erweitertes Schema

- Ändern Sie die Delegierungseinstellung des Kerberos-Nutzers.
- Gehen Sie zu **Kerberos-Nutzer>Eigenschaften>Delegierung>Diesem Nutzer für die Delegierung zu einem beliebigen Dienst vertrauen (nur Kerberos)**

ANMERKUNG: Abmelden und anmelden über den Management Station-Active Directory-Nutzer nach dem Ändern der Einstellung oben.

Kerberos Keytab-Datei generieren

Zur Unterstützung der SSO- und Smartcard-Authentifizierung bei der Anmeldung unterstützt iDRAC die Konfiguration, um sich selbst als kerberisierter Dienst in einem Windows Kerberos-Netzwerk zu aktivieren. Die Kerberos-Konfiguration auf iDRAC umfasst die gleichen Schritte wie die Konfiguration eines Kerberos-Dienstes auf einem Nicht-Windows Server als Sicherheitsprinzipal in Windows Server Active Directory.

Das Tool ktpass (von Microsoft als Teil der Server-Installations-CD/DVD erhältlich) wird verwendet, um die SPN-Bindungen (Service Principal Name) zu einem Nutzerkonto zu erstellen und die Vertrauensinformationen in eine Kerberos-Schlüsselregisterdatei im MIT-Stil zu exportieren, die eine Vertrauensbeziehung zwischen einem externen Nutzer oder System und dem Key Distribution Centre (KDC) ermöglicht. Die Datei keytab enthält einen kryptografischen Schlüssel, der zur Verschlüsselung der Informationen zwischen dem Server und dem KDC verwendet wird. Das Tool ktpass ermöglicht es UNIX-basierten Diensten, die die Kerberos-Authentifizierung unterstützen, die Interoperabilitätsfunktionen zu nutzen, die von einem Windows Server Kerberos KDC-Dienst bereitgestellt werden. Weitere Informationen zum Dienstprogramm **ktpass** auf der Microsoft Website unter: **technet.microsoft.com/en-us/library/cc779157(WS.10).aspx**

Vor der Erzeugung einer keytab-Datei müssen Sie ein Active Directory-Nutzerkonto zur Verwendung mit der Option -mapuser des Befehls `ktpass` erstellen. Darüber hinaus müssen Sie den gleichen Namen wie der iDRAC-DNS-Name haben, auf den Sie die generierte keytab-Datei hochladen.

So generieren Sie eine Keytab-Datei mithilfe des ktpass-Tools:

1. Führen Sie das Dienstprogramm *ktpass* auf dem Domain Controller (Active Directory-Server) aus, auf dem Sie den iDRAC einem Nutzerkonto in Active Directory zuordnen möchten.
2. Verwenden Sie den folgenden ktpass-Befehl, um die Kerberos-Keytab-Datei zu erstellen:

```
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
```

Der Verschlüsselungstyp lautetAES256-SHA1. Der Prinzipaltyp lautet KRB5_NT_PRINCIPAL. Die Eigenschaften des Nutzerkontos, dem der Dienstprinzipalname zugeordnet ist, muss „**AES 256“-Verschlüsselungstypen für dieses Konto verwenden** ordnungsgemäß aktiviert haben.

ANMERKUNG: Verwenden Sie Kleinbuchstaben für den **iDRACname** und den **Service Principal Name**. Verwenden Sie Großbuchstaben für den Domänennamen, wie im Beispiel gezeigt.

Es wird eine Keytab-Datei generiert.

ANMERKUNG: Falls Probleme mit dem iDRAC-Nutzer auftreten, für den die keytab-Datei erstellt wird, erstellen Sie einen neuen Nutzer und eine neue keytab-Datei. Wenn dieselbe keytab-Datei, die ursprünglich erstellt wurde, erneut ausgeführt wird, wird sie nicht korrekt konfiguriert.

iDRAC-SSO-Anmeldung für Active Directory-Benutzer über die Webschnittstelle konfigurieren

So konfigurieren Sie iDRAC für die Active Directory-SSO-Anmeldung:

ANMERKUNG: Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

1. Überprüfen Sie, ob der iDRAC-DNS-Name mit dem vollqualifizierten iDRAC-Domänennamen übereinstimmt. Gehen Sie dazu in der iDRAC-Webschnittstelle zu **iDRAC-Einstellungen** > **Netzwerk** > **Allgemeine Einstellungen** und beziehen Sie sich auf die Eigenschaft**DNS-iDRAC-Name**.
2. Während Sie Active Directory für die Einrichtung eines Benutzerkontos auf der Basis eines Standardschemas oder eines erweiterten Schemas konfigurieren, führen Sie die folgenden zwei zusätzlichen Schritte für die Konfiguration von SSO aus:

- Laden Sie die Keytab-Datei auf die Seite **Active Directory-Konfiguration und Verwaltung – Schritt 1 von 4** hoch.
- Wählen Sie die Option **Einmaliges Anmelden aktivieren** auf der Seite **Active Directory-Konfiguration und Verwaltung – Schritt 2 von 4** aus.

iDRAC SSO-Anmeldung für Active Directory-Benutzer über RACADM konfigurieren

Um SSO zu aktivieren, führen Sie die Schritte zum Konfigurieren von Active Directory und den folgenden Befehl aus:

```
racadm set iDRAC.ActiveDirectory.SSOEnable 1
```

Management Station-Einstellungen

Führen Sie die folgenden Schritte nach der Konfiguration der SSO-Anmeldung für Active Directory-Nutzer durch:

1. Legen Sie die DNS-Server-IP-Adresse in den Netzwerkeigenschaften fest und geben Sie die bevorzugte DNS-Server-IP-Adresse an.
2. Öffnen Sie den Arbeitsplatz und fügen Sie die ***domain.tld**-Domäne hinzu.
3. Fügen Sie den Active Directory-Nutzer zum Administrator hinzu, indem Sie zu **Arbeitsplatz** > **Verwalten** > **Lokale Nutzer und Gruppen** > **Gruppen** > **Administrator** navigieren und den Active Directory-Nutzer hinzufügen.
4. Melden Sie sich vom System ab und melden Sie sich unter Verwendung der Active Directory-Nutzeranmeldeinformationen an.
5. Fügen Sie in der Internet Explorer-Einstellung die *domain.tld-Domäne wie folgt hinzu:
   a. Gehen Sie zu **Extras** > **Internetoptionen** > **Sicherheit** > **Lokale Internet** > **sites** und entfernen Sie die Markierung bei der Auswahl **Intranet-Netzwerkeinstellungen automatisch ermitteln**. Wählen Sie die verbleibenden drei Optionen aus und klicken Sie auf **Erweitert**, um *domain.com hinzuzufügen.
   b. Öffnen Sie ein neues Fenster im IE und verwenden Sie den iDRAC-Hostnamen zum Starten der iDRAC-GUI.
6. Fügen Sie in der Mozilla Firefox-Einstellung die *domain.tld-Domäne hinzu:
   - Starten Sie den Firefox-Browser und geben Sie „about:config“ in die URL ein.
   - Verwenden Sie im „Filter“-Textfeld „Verhandlung“. Doppelklicken Sie auf das Ergebnis *auth.trusted.uris*. Geben Sie die Domäne ein, speichern Sie die Einstellungen und schließen Sie den Browser.
   - Öffnen Sie ein neues Fenster in Firefox und verwenden Sie den iDRAC-Hostnamen zum Starten der iDRAC-GUI.

Smartcard-Anmeldung aktivieren oder deaktivieren

Vor der Aktivierung oder Deaktivierung der Smartcard-Anmeldung für iDRAC müssen Sie Folgendes sicherstellen:

- Die iDRAC-Berechtigungen sind konfiguriert.
- Die lokale iDRAC-Benutzerkonfiguration oder die Active Directory-Benutzerkonfiguration mit den entsprechenden Zertifikaten ist abgeschlossen.

ANMERKUNG: Wenn die Smartcard-Anmeldung aktiviert ist, werden SSH, IPMI über LAN, Seriell über LAN und Remote-RACADM deaktiviert. Wenn Sie die Smartcard-Anmeldung deaktivieren, werden die Schnittstellen nicht automatisch wieder aktiviert.

Smart Card-Anmeldung über die Web-Schnittstelle aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die Smart Card-Anmeldefunktion:

1. Gehen Sie in der iDRAC-Web-Schnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **User (Benutzer)** > **Smart Card**. Daraufhin wird die Seite **Smart Card** angezeigt.
2. Wählen Sie in der Dropdown-Liste **Configure Smart Card Logon (Smart Card-Anmeldung konfigurieren)** die Option **Enabled (Aktiviert)** aus, um die Smart Card-Anmeldung zu aktivieren, oder wählen Sie **Enabled With Remote RACADM (Mit Remote-RACADM aktiviert)** aus. Wählen Sie ansonsten die Option **Disabled (Deaktiviert)** aus.

   Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.
3. Klicken Sie auf **Anwenden**, um die Einstellungen zu übernehmen.
   Bei nachfolgenden Anmeldeversuchen über die iDRAC-Web-Schnittstelle werden Sie dazu aufgefordert, eine Smart Card-Anmeldung auszuführen.

Smart Card-Anmeldung über RACADM aktivieren oder deaktivieren

Um die Smart Card-Anmeldung zu aktivieren, verwenden Sie den Befehl `set` mit Objekten in der Gruppe `iDRAC.SmartCard`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Smart Card-Anmeldung über das Dienstprogramm für die iDRAC-Einstellungen aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die Smart Card-Anmeldefunktion:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen nach **Smart Card**.
   Daraufhin wird die Seite **iDRAC-Einstellungen – Smart Card** angezeigt
2. Wählen Sie **Enabled** (Aktiviert), um die Smart Card-Anmeldung zu aktivieren. Andernfalls wählen Sie **Disabled** (Deaktiviert). Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
   Die Smart Card-Anmeldefunktion wird entsprechend Ihrer Auswahl entweder aktiviert oder deaktiviert.

Konfigurieren von Smart Card-Anmeldung

ANMERKUNG: Für die Active Directory Smart Card-Konfiguration, muss iDRAC entweder mit der Standardanmeldung oder dem erweiterten SSO-Anmeldungsschema konfiguriert werden.

iDRAC-Smart-Card-Anmeldung für Active Directory-Benutzer konfigurieren

Vor der Konfiguration der iDRAC-Smart-Card-Anmeldung für Active Directory-Benutzer müssen Sie sicherstellen, dass die erforderlichen Voraussetzungen erfüllt sind.

So konfigurieren Sie iDRAC für die Smart Card-Anmeldung:

1. Führen Sie über die iDRAC-Webschnittstelle, während Sie Active Directory für die Einrichtung eines Benutzerkontos auf der Basis eines Standard- oder eines erweiterten Schemas konfigurieren, auf der Seite **Active Directory-Konfiguration und Verwaltung – Schritt 1 von 4** die folgenden Aktivitäten aus:
   - Aktivieren Sie die Zertifikatüberprüfung.
   - Laden Sie ein vertrauenswürdiges, von einer Zertifikatzertifizierungsstelle signiertes Zertifikat hoch.
   - Laden Sie die Keytab-Datei hoch.
2. Smart Card-Anmeldung aktivieren Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

iDRAC-Smart Card-Anmeldung für lokale Benutzer konfigurieren

So konfigurieren Sie einen lokalen iDRAC-Benutzer für die Smart Card-Anmeldung:

1. Laden Sie das Smart Card-Benutzerzertifikat und das vertrauenswürdige Zertifizierungsstellenzertifikat nach iDRAC noch.
2. Smart Card-Anmeldung aktivieren

Smart Card-Benutzerzertifikat hochladen

Bevor Sie das Benutzerzertifikat hochladen, stellen Sie sicher, dass das Benutzerzertifikat des Smart Card-Anbieters im Base64-Format vorliegt. SHA-2-Zertifikate werden ebenfalls unterstützt.

Smart Card-Benutzerzertifikat über die Web-Schnittstelle hochladen

So laden Sie ein Smart Card-Benutzerzertifikat hoch:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **iDRAC-Einstellungen** > **Benutzer** > **Smart Card**.

   ANMERKUNG: Die Smart Card-Anmeldung erfordert die Konfiguration des lokalen und/oder die Konfiguration des Active Directory-Benutzerzertifikats.

2. Wählen Sie unter **Smart Card-Anmeldung konfigurieren Aktiviert mit Remote-RACADM** zum Aktivieren der Konfiguration aus.
3. Stellen Sie die Option auf **CRL-Prüfung für Smart Card-Anmeldung aktivieren** aus.
4. Klicken Sie auf **Anwenden**.

Smart Card-Benutzerzertifikat über RACADM hochladen

Um ein Smart Card-Benutzerzertifikat hochzuladen, verwenden Sie das Objekt **usercertupload**. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Anfordern von Zertifikat für Smart Card-Registrierung

Führen Sie die folgenden Schritte aus, um ein Zertifikat für die Smart Card Anmeldung anzufordern:

1. Verbinden Sie die Smart Card im Clientsystem und installieren Sie die erforderlichen Treiber und Software.
2. Überprüfen Sie den Treiberstatus im Geräte-Manager.
3. Starten Sie den Smart Card-Aktivierungsdienst im Browser.
4. Geben Sie den **Benutzernamen** und das **Kennwort** ein und klicken Sie auf **OK**.
5. Klicken Sie auf **Zertifikat anfordern**.
6. Klicken Sie auf **Erweiterte Zertifikatsanforderung**.
7. Klicken Sie auf **Ein Zertifikat anfordern** für eine Smart Card für einen anderen Benutzer über die Smart Card-Zertifikatsregistrierungsstation.
8. Wählen Sie den zu registrierenden Benutzer aus, indem Sie auf die Schaltfläche **Benutzer auswählen** klicken.
9. Klicken Sie auf **Registrieren** und geben Sie die Smart Card-Anmeldeinformationen ein.
10. Geben Sie die Smart Card-PIN ein und klicken Sie auf **Senden**.

Vertrauenswürdiges Zertifizierungsstellenzertifikat für Smart Card hochladen

Bevor Sie das Zertifizierungsstellenzertifikat hochladen, müssen Sie sicherstellen, dass Sie über ein Zertifikat verfügen, das von der Zertifizierungsstelle signiert wurde.

Vertrauenswürdiges Zertifizierungsstellenzertifikat für Smart Card über die Web-Schnittstelle hochladen

So laden Sie ein vertrauenswürdiges Zertifizierungsstellenzertifikat für die Smart Card-Anmeldung hoch:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **iDRAC Settings (iDRAC-Einstellungen)** > **Network (Netzwerk)** > **User Authentication (Benutzerauthentifizierung)** > **Local Users (Lokale Benutzer)**.
   Die Seite **Benutzer** wird angezeigt.
2. In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.
   Die Seite **Benutzer-Hauptmenü** wird angezeigt.
3. Wählen Sie unter **Smart Card-Konfiguration** die Option **Zertifikat einer vertrauenswürdigen Zertifizierungsstelle hochladen** aus, und klicken Sie dann auf **Weiter**.
   Daraufhin wird die Seite **Zertifikat einer vertrauenswürdigen Zertifizierungsstelle hochladen** angezeigt.
4. Suchen Sie das vertrauenswürdige Zertifizierungsstellenzertifikat, und klicken Sie auf **Anwenden**.

Vertrauenswürdiges Zertifizierungsstellenzertifikat für Smart Card über RACADM hochladen

Um ein vertrauenswürdiges Zertifikat einer vertrauenswürdigen Zertifizierungsstelle für die Smart Card-Anmeldung hochzuladen, verwenden Sie das Objekt **usercertupload**. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Anmelden mit Smart Card

ANMERKUNG: Die Smart Card-Anmeldung wird nur auf Internet Explorer unterstützt.

So melden Sie sich mit einer Smart Card an:

1. Melden Sie sich von der iDRAC-GUI nach der Aktivierung der Smart Card ab.
2. Starten Sie iDRAC über `http://IP/` oder starten Sie mit FQDN `http://FQDN/`
3. Klicken Sie nach dem Herunterladen des Smart Card Plug-ins auf **Installieren**.
4. Geben Sie die Smart Card-PIN ein und klicken Sie auf **Senden**.
5. iDRAC meldet sich erfolgreich mit der Smart Card an.

12

iDRAC für das Versenden von Warnungen konfigurieren

Sie können Warnungen und Maßnahmen für bestimmte Ereignisse festlegen, die auf dem verwalteten System auftreten. Dieser Fall tritt ein, wenn der Status einer Systemkomponente den vordefinierten Zustand überschreitet. Wenn ein Ereignis mit einem Ereignisfilter übereinstimmt und Sie diesen Filter für die Generierung einer Warnung konfiguriert haben (per E-Mail, SNMP-Trap, IPMI-Warnung, Remote-Systemprotokolle, Redfish-Ereignis oder WS-Ereignisse), wird eine Warnung an ein oder mehrere konfigurierte Ziele gesendet. Ist dieser Ereignisfilter zudem für die Durchführung einer Maßnahme konfiguriert (z. B. Neustart oder Aus- und Einschalten), wird diese Maßnahme durchgeführt. Sie können nur eine Maßnahme pro Ereignis einstellen.

So konfigurieren Sie iDRAC zum Versenden von Warnungen:

1. Aktivieren Sie Warnungen.
2. Optional können Sie die Warnungen auf der Basis der Kategorie oder des Schweregrads filtern.
3. Konfigurieren Sie E-Mail-Warnungen, IPMI-Warnungen, SNMP-Traps, Remote System-Protokolle, Redfish-Ereignisse, Betriebssystemprotokolle und/oder WS-Ereignis-Einstellungen.
4. Aktivieren Sie die folgenden Ereigniswarnungen und Maßnahmen:
   - Senden von E-Mail-Warnungen, IPMI-Warnungen, SNMP-Traps, Remote System-Protokollen, Redfish-Ereignissen, Betriebssystemprotokollen oder WS-Ereignissen an die konfigurierten Ziele.
   - Führen Sie einen Neustart aus, schalten Sie das Gerät aus, oder führen Sie einen Aus- und Einschaltvorgang auf dem Managed System durch.

Themen:

- Warnungen aktivieren und deaktivieren
- Warnungen filtern
- Ereigniswarnungen einrichten
- Alarmwiederholungsereignis einrichten
- Ereignismaßnahmen festlegen
- Einstellungen für E-Mail-Warnungs-SNMP-Trap oder IPMI-Trap konfigurieren
- Konfigurieren von WS-Ereignisauslösung
- Konfigurieren von Redfish-Ereignissen
- Überwachung von Gehäuseereignissen
- IDs für Warnungsmeldung

Warnungen aktivieren und deaktivieren

Zum Senden einer Warnung an konfigurierte Ziele oder zum Ausführen einer Ereignismaßnahme müssen Sie die globale Warnoption aktivieren. Diese Eigenschaft setzt individuelle Warnungen oder Ereignismaßnahmen außer Kraft.

Warnungen über die Web-Schnittstelle aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die Generierung von Warnungen:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Systemeinstellungen** > **Warnungskonfiguration**.
   Die Seite **Warnungen** wird angezeigt.
2. Im Abschnitt **Warnungen**:
   - Wählen Sie die Option **Aktivieren** aus, um die Generierung von Warnungen zu aktivieren oder um eine Ereignismaßnahme auszuführen.
   - Wählen Sie die Option **Deaktivieren** aus, um die Generierung von Warnungen zu deaktivieren oder um eine Ereignismaßnahme zu deaktivieren.
3. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Schnellkonfiguration von Warnungen

So konfigurieren Sie Warnungen auf einmal:

1. Gehen Sie zu **Schnellkonfiguration von Warnungen** unter der Seite **Warnungskonfiguration**.
2. Im Abschnitt **Schnellkonfiguration von Warnungen**:
   - Wählen Sie die Warnkategorie aus.
   - Wählen Sie die Problemschweregradbenachrichtigung aus.
   - Wählen Sie den Speicherort aus, an dem Sie diese Benachrichtigungen empfangen möchten.
3. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

ANMERKUNG: Sie müssen mindestens eine Kategorie, einen Schweregrad sowie einen Zieltyp auswählen, um die Konfiguration anzuwenden.

Alle Warnungen, die konfiguriert sind, werden vollständig unter **Warnungskonfiguration – Zusammenfassung** angezeigt.

Warnungen über RACADM aktivieren oder deaktivieren

Geben Sie folgenden Befehl ein:

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

n=0 – Deaktiviert

n=1 – Aktiviert

Warnungen über das Dienstprogramm für iDRAC-Einstellungen aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die Generierung von Warnungen oder Ereignismaßnahmen:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Warnungen**.
   Die Seite **Warnungen für iDRAC-Einstellungen** wird angezeigt.
2. Wählen Sie unter **Platform Events** (Plattformereignisse) die Option **Enabled** (Aktiviert) aus, um die Generierung von Warnungen oder Ereignismaßnahmen zu aktivieren. Wählen Sie andernfalls **Disabled** (Deaktiviert) aus. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
   Die Warnungseinstellungen sind damit konfiguriert.

Warnungen filtern

Sie können Warnungen auf der Basis der Kategorie und des Schweregrads filtern.

Filtern von Warnungen über die iDRAC-Webschnittstelle

So filtern Sie Warnungen auf der Basis der Kategorie und des Schweregrads:

ANMERKUNG: Selbst wenn Sie als Benutzer nur über Leseberechtigungen verfügen, können Sie die Warnungen filtern.

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Alerts and Remote System Log Configuration (Warnungen und Konfiguration von Remote-System-Protokollen)**.
2. Wählen Sie im Abschnitt **Alerts and Remote System Log Configuration** (Warnungen und Konfiguration von Remote-System-Protokollen) die Option **Filter**:
   - System Health (Systemzustand) – Die Kategorie „System Health“ (Systemzustand) umfasst alle Warnungen im Zusammenhang mit Hardware innerhalb des Systemgehäuses. Beispiele: Temperaturfehler, Spannungsfehler, Gerätefehler.
   - Storage Health (Speicherzustand) – Die Kategorie „Storage Health“ (Speicherzustand) umfasst Warnungen, die mit dem Speichersubsystem zusammenhängen. Beispiele: Controller-Fehler, Fehler der physischen und virtuellen Festplatten.

- Configuration (Konfiguration) – Die Kategorie „Configuration“ (Konfiguration) umfasst Warnungen, die mit Hardware-, Firmware- und Software-Konfigurationsänderungen zusammenhängen. Beispiele: PCI-e-Karte hinzugefügt/entfernt, RAID-Konfiguration geändert, iDRAC-Lizenz geändert.
- Audit – Die Kategorie „Audit“ umfasst das Prüfprotokoll. Beispiele: Informationen zu Benutzeranmeldungen/-abmeldungen, Kennwortauthentifizierungsfehler, Sitzungsinformationen, Betriebszustände.
- Updates (Aktualisierungen) – Die Kategorie „Updates“ (Aktualisierungen) umfasst Warnungen, die aufgrund von Firmware-/Treiber-Upgrades/-Downgrades generiert wurden.

  ANMERKUNG: Es handelt sich nicht um eine Firmware-Bestandsliste.
- Arbeitsanmerkungen

3. Wählen Sie eine oder mehrere der folgenden Schweregrade aus:
   - Informativ
   - Warnung
   - Kritisch
4. Klicken Sie auf **Anwenden**.
   Der Abschnitt **Warnungsergebnisse** zeigt die Ergebnisse auf der Basis der ausgewählten Kategorie und des Schweregrads an.

Warnungen über RACADM filtern

Verwenden Sie zum Filtern von Warnungen den Befehl **eventfilters**. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Ereigniswarnungen einrichten

Sie können Ereigniswarnungen, wie z. B. E-Mail-Warnungen, IPMI-Warnungen, SNMP-Traps, Remote-System-Protokolle, Betriebssystemprotokolle und WS-Ereignisse so einstellen, dass sie an die konfigurierten Ziele gesendet werden.

Ereigniswarnungen über die Web-Schnittstelle einrichten

So legen Sie eine Ereigniswarnung über die Web-Schnittstelle fest:

1. Stellen Sie sicher, dass Sie E-Mail-Warnung, IPMI-Warnung, SNMP-Trap-Einstellungen und/oder Einstellungen des Remote System-Protokolls konfiguriert haben.
2. Gehen Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Systemeinstellungen** > **Warnungen und Remote Systemprotokollkonfiguration**.
3. Wählen Sie unter **Kategorie** eine oder alle der folgenden Warnungen für die benötigten Ereignisse aus:
   - E-Mail
   - SNMP-Trap
   - IPMI-Warnung
   - Remote System-Protokoll
   - WS-Ereignisauslösung
   - BS-Protokoll
   - Redfish-Ereignis
4. Wählen Sie **Aktion**.
   Die Einstellung wird gespeichert.
5. Optional können Sie ein Testereignis versenden. Geben Sie im Feld **Meldungs-ID zum Testen des Ereignisses** die Meldungs-ID ein, um zu testen, ob die Warnung erzeugt wird, und klicken Sie auf **Testen**. Weitere Informationen zur Prüfung der Ereignis- und Fehlermeldungen, die von der System-Firmware und den Agenten, die die Systemkomponenten überwachen, generiert werden, finden Sie im Referenzhandbuch für Ereignis- und Fehlermeldungen *Referenzhandbuch zu Ereignis- und Fehlermeldungen* unter iDRACmanuals

Ereigniswarnungen über RACADM einrichten

Verwenden Sie zum Festlegen einer Ereigniswarnung den Befehl **eventfilters**. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Alarmwiederholungsereignis einrichten

Sie können iDRAC so konfigurieren, dass weitere Ereignisse in bestimmten Intervallen generiert werden, wenn das System weiterhin oberhalb eines Schwellenwertes für die Eintrittstemperatur betrieben wird. Das standardmäßige Intervall beträgt 30 Tage. Der gültige Bereich liegt zwischen 0 und 366 Tagen. Ein Wert von 0 zeigt an, dass die Ereigniswiederholung deaktiviert ist.

ANMERKUNG: Sie müssen die Berechtigung zum Konfiguirieren des iDRAC („Configure iDRAC“) besitzen, um den Wert für die Alarmwiederholung einzustellen.

Alarmwiederholungsereignis über RACADM einrichten

Um mit RACADM das Alarmwiederholungsereignis einzurichten, verwenden Sie den Befehl **eventfilters**. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Einrichten eines Alarmwiederholungsereignisses über die iDRAC-Webschnittstelle

So legen Sie einen Wert für die Alarmwiederholung fest:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Alert Recurrence (Alarmwiederholung)**.
2. Geben Sie in der Spalte **Wiederholung** einen Wert für die Alarmhäufigkeit für die gewünschte Kategorie, den Alarm und die Schweregrade ein.

   Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.
3. Klicken Sie auf **Anwenden**.
   Die Einstellungen für die Alarmwiederholung werden gespeichert.

Ereignismaßnahmen festlegen

Sie können Ereignismaßnahmen festlegen, z. B. das Ausführen eines Neustarts, Aus- und Einschalten und Ausschalten. Es ist auch möglich, keine Maßnahme auf dem System auszuführen.

Ereignismaßnahmen über die Web-Schnittstelle einrichten

So richten Sie eine Ereignismaßnahme ein:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Alert and Remote System Log Configuration (Warnung und Konfiguration von Remote-System-Protokollen)**.
2. Wählen Sie im Drop-Down-Menü **Actions (Maßnahmen)** für jedes Ereignis eine Maßnahme aus:
   - Neustart
   - Aus- und Einschalten
   - Ausschalten
   - Keine Maßnahme
3. Klicken Sie auf **Anwenden**.
   Die Einstellung wird gespeichert.

Ereignismaßnahmen über RACADM einrichten

Zum Konfigurieren einer Ereignismaßnahme verwenden Sie den Befehl `eventfilters`. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Einstellungen für E-Mail-Warnungs-SNMP-Trap oder IPMI-Trap konfigurieren

Die Management Station verwendet SNMP- (Simple Network Management Protocol) und IPMI-Traps (Intelligent Platform Management Interface) zum Empfangen von Daten von iDRAC. Bei Systemen mit einer größeren Anzahl an Knoten ist es möglicherweise nicht effizient, dass eine Management Station alle iDRACs zu jedem Zustand abfragt. Ereignis-Traps helfen beispielsweise einer Management Station beim Lastenausgleich zwischen Knoten oder durch Generieren einer Warnung, wenn ein Authentifizierungsfehler auftritt. SNMP v1-, v2- und v3-Formate werden unterstützt.

Sie können die IPv4- und IPv6-Warnungsziele, die E-Mail-Einstellungen und die SMTP-Server-Einstellungen konfigurieren und diese Einstellungen testen. Sie können auch den SNMP v3-Benutzer angeben, an den Sie SNMP-Traps senden möchten.

Vor der Konfigurierung der Einstellungen für E-Mails, SNMPs oder IPMI-Traps müssen Sie Folgendes sicherstellen:

- Sie verfügen über Berechtigungen zum Konfigurieren von RAC.
- Sie haben die Ereignisfilter konfiguriert.

IP-basierte Warnziele konfigurieren

Sie können die IPv6- oder IPv4-Adressen für den Empfang von IPMI-Warnungen oder SNMP-Traps konfigurieren.

Weitere Informationen zur Überwachung der Server mit iDRAC-MIB über SNMP finden Sie unter *Dell EMC OpenManage SNMP – Referenzhandbuch* verfügbar unter https://www.dell.com/openmanagemanuals.

IP-basierte Warnziele über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die Warnungszieleinstellungen unter Verwendung der Web-Schnittstelle:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **SNMP and E-mail Settings (SNMP- und E-Mail-Einstellungen)**.
2. Wählen Sie die Option **Zustand** aus, um ein Warnungsziel (IPv4-Adresse, IPv6-Adresse oder vollständig qualifizierter Domänenname (FQDN)) zum Empfang der Traps zu aktivieren.

   Sie können bis zu acht Zieladressen angeben. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.
3. Wählen Sie die SNMP-v3-Benutzer aus, an die Sie den SNMP-Trap senden möchten.
4. Geben Sie die iDRAC-SNMP-Community-Zeichenfolge (nur für SNMPv1- und v2) und die SNMP-Warnungsschnittstellennummer ein.

   Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

   ANMERKUNG: Der Wert für die Community-Zeichenfolge zeigt die Community-Zeichenfolge an, die für einen Warnungs-Trap der Art „Simple Network Management Protocol“ (SNMP) verwendet wird, der von iDRAC aus versendet wird. Stellen Sie sicher, dass die Ziel-Community-Zeichenfolge mit der iDRAC-Community-Zeichenfolge übereinstimmt. Der Standardwert ist „Public“ (Öffentlich).
5. Um zu testen, ob die IP-Adresse die IPMI- oder SNMP-Traps empfängt, klicken Sie auf die Option **Senden**, die sich entweder unter **IPMI-Trap testen** oder unter **SNMP-Trap testen** befindet.
6. Klicken Sie auf **Anwenden**.
   Die Warnungsziele sind damit konfiguriert.
7. Wählen Sie im Abschnitt **SNMP-Trap-Format** die Protokollversion aus, die zum Senden der Traps an die Trap-Ziele – **SNMP v1**, **SNMP v2** oder **SNMP v3** verwendet werden soll, und klicken Sie auf **Anwenden**.

   ANMERKUNG: Die Option **SNMP Trap Format** (SNMP-Trap-Format) gilt nur für SNMP-Traps und nicht für IPMI-Traps. IPMI-Traps werden immer im SNMP v1-Format gesendet und basieren nicht auf der konfigurierten Option **SNMP Trap Format**.

   Das SNMP-Trap-Format ist konfiguriert.

IP-Warnungsziele über RACADM konfigurieren

So konfigurieren Sie Trap-Warnungseinstellungen:

1. So aktivieren Sie Traps:

```
racadm set idrac.SNMP.Alert.<index>.Enable <n>
```

Parameter	Beschreibung
<index>	Zielindex. Zulässige Werte sind 1 bis 8.
<n>=0 **<n>**=1	Trap deaktivieren Trap aktivieren

2. So konfigurieren Sie die Adresse für das Trap-Ziel:

```
racadm set idrac.SNMP.Alert.<index>.DestAddr <Address>
```

Parameter	Beschreibung
<index>	Zielindex. Zulässige Werte sind 1 bis 8.
<Address>	Eine gültige IPv4-, IPv6- oder FQDN-Adresse

3. Konfigurieren Sie die SNMP-Community-Namen-Zeichenkette.

```
racadm set idrac.ipmilan.communityname <community_name>
```

Parameter	Beschreibung
<community_name>	Der SNMP-Community-Name.

4. So konfigurieren Sie das SNMP-Ziel:
   - Stellen Sie das SNMP-Trap-Ziel für SNMPv3 ein:

     ```
     racadm set idrac.SNMP.Alert.<index>.DestAddr <IP address>
     ```

   - Stellen Sie SNMPv3-Benutzer für die Trap-Ziele ein:

     ```
     racadm set idrac.SNMP.Alert.<index>.SNMPv3Username <user_name>
     ```

   - Aktivieren Sie SNMPv3 für einen Benutzer:

     ```
     racadm set idrac.users.<index>.SNMPv3Enable Enabled
     ```

5. So testen bei Bedarf Sie den Trap:

```
racadm testtrap -i <index>
```

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

IP-basierte Warnziele über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren

Sie können Warnungsziele (IPv4, IPv6 oder FQDN) unter Verwendung des Dienstprogramms für die iDRAC-Einstellungen konfigurieren. Führen Sie dazu folgende Schritte durch:

1. Gehen Sie im **Dienstprogramm für die iDRAC-Einstellungen** zu **Warnungen**.
   Die Seite **Warnungen für iDRAC-Einstellungen** wird angezeigt.
2. Aktivieren Sie unter **Trap Settings** (Trap-Einstellungen) die IP-Adresse(n) für den Empfang der Traps und geben Sie die IPv4-, IPv6- oder FQDN-Zieladresse(n) ein. Sie können bis zu acht Adressen angeben.
3. Geben Sie die Community-Namen-Zeichenkette ein.
   Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.
4. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

Die Warnungsziele sind damit konfiguriert.

Konfigurieren von E-Mail-Benachrichtigungen

Sie können die Absender-E-Mail-Adresse und die Empfänger-E-Mail-Adresse für den Empfang von E-Mail-Warnungen konfigurieren. Konfigurieren Sie auch die SMTP-Server-Adresseinstellungen:

ANMERKUNG: E-Mail-Warnungen unterstützen sowohl IPv4- als auch IPv6-Adressen. Der iDRAC DNS-Domänenname muss bei der Verwendung von IPv6 angegeben werden.

ANMERKUNG: Wenn Sie einen externen SMTP Server verwenden, stellen Sie sicher, dass der iDRAC mit diesem Server kommunizieren kann. Wenn der Server nicht erreichbar ist, wird der Fehler RAC0225 angezeigt, wenn versucht wird, eine Test-E-Mail zu senden.

E-Mail-Warnungseinstellungen über Weboberfläche konfigurieren

So konfigurieren Sie die E-Mail-Warnungseinstellungen über die Weboberfläche:

1. Gehen Sie in der iDRAC-Weboberfläche zu **Konfiguration** > **Systemeinstellungen** > **SMTP- (E-Mail-) Konfiguration**.
2. Geben Sie eine gültige E-Mail-Adresse ein.
3. Klicken Sie auf **Senden** bei **E-Mail testen**, um die konfigurierten E-Mail-Warnungseinstellungen zu testen.
4. Klicken Sie auf **Anwenden**.
5. Geben Sie für SMTP- (E-Mail-) Servereinstellungen die folgenden Informationen an:
   - SMTP (E-Mail) Server IP-Adresse oder FQDN/DNS-Name
   - Nutzerdefinierte Absenderadresse - Dieses Feld hat die folgenden Optionen:
     - **Standard** – Adressfeld ist nicht editierbar
     - **Beutzerdefiniert** – Sie können die E-Mail-ID eingeben, von der Sie die E-Mail-Benachrichtigungen erhalten können.
   - Nutzerdefinierter Betreff der Nachricht – Dieses Feld hat die folgenden Optionen:
     - **Standard** – Standardmeldung ist nicht editierbar
     - **Nutzerdefiniert** – Wählen Sie die Nachricht, die in der **Betreffzeile** der E-Mail angezeigt werden soll.
   - SMTP-Portnummer - Die Verbindung kann verschlüsselt werden und E-Mails können über sichere Ports gesendet werden:
     - **Keine Verschlüsselung** – Port 25 (Standard)
     - **SSL** – Port 465
   - Verbindungsverschlüsselung - Wenn Sie keinen E-Mail-Server in Ihren Räumlichkeiten haben, können Sie Cloud-basierte E-Mail-Server oder SMTP-Relays verwenden. Um den Cloud-E-Mail-Server zu konfigurieren, können Sie diese Funktion in der Dropdown-Liste auf einen der folgenden Werte einstellen:
     - **Keine** – Keine Verschlüsselung für die Verbindung mit dem SMTP-Server. Das ist der Standardwert.
     - **SSL** – Führt SMTP-Protokoll über SSL aus

     ANMERKUNG:
     - Diese Funktion ist nicht über Group Manager konfigurierbar.
     - Dies ist eine lizenzierte Funktion und nicht im Rahmen einer iDRAC Basislizenz verfügbar.
     - Um diese Funktion zu verwenden, müssen Sie über die Berechtigung zum Konfigurieren des iDRAC verfügen.
   - Authentifizierung
   - Nutzername

   Für Server-Einstellungen hängt die Port-Nutzung von `connectionencryptiontype` ab und kann nur über RACADM konfiguriert werden.
6. Klicken Sie auf **Anwenden**. Weitere Informationen zu den Optionen finden Sie in der *iDRAC-Online-Hilfe*.

E-Mail-Warnungseinstellungen mit RACADM konfigurieren

1. E-Mail-Warnung aktivieren:

```
racadm set iDRAC.EmailAlert.Enable.[index] [n]
```

Parameter	Beschreibung
index	E-Mail-Zielindex. Zulässige Werte sind 1 bis 4.
n=0 **n=1**	Deaktiviert E-Mail-Warnungen. Aktiviert E-Mail-Warnungen.

2. Konfigurieren der E-Mail-Einstellungen:

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

Parameter	Beschreibung
index	E-Mail-Zielindex. Zulässige Werte sind 1 bis 4.
email-address	Ziel-E-Mail-Adresse, die die Plattformereigniswarnungen empfängt.

3. Konfigurieren der E-Mail-Einstellungen des Absenders:

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

Parameter	Beschreibung
index	E-Mail-Index des Absenders
email-address	Sender-E-Mail-Adresse, die die Plattformereigniswarnungen sendet.

4. So konfigurieren Sie eine benutzerdefinierte Meldung:

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

Parameter	Beschreibung
index	E-Mail-Zielindex. Zulässige Werte sind 1 bis 4.
custom-message	Benutzerdefinierte Meldung

5. So testen Sie bei Bedarf die konfigurierte E-Mail-Warnung:

```
racadm testemail -i [index]
```

Parameter	Beschreibung
index	E-Mail-Zielindex, der getestet werden soll. Zulässige Werte sind 1 bis 4.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Konfigurieren der Adresseneinstellungen des SMTP-E-Mail-Servers

Sie müssen die SMTP-Server-Adresse für E-Mail-Warnungen konfigurieren, damit diese an bestimmte Ziele versendet werden können.

Konfigurieren von Adresseinstellungen für den SMTP-E-Mail-Server über die iDRAC-Webschnittstelle

So konfigurieren Sie die SMTP-Server-Adresse:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Alert Configuration (Konfiguration von Warnungen)** > **SNMP (E-mail Configuration) (SNMP (E-Mail-Konfiguration))**.
2. Geben Sie eine gültige IP-Adresse oder den voll qualifizierten Domänennamen (FQDN) des in der Konfiguration zu verwendenden SMTP-Servers ein.

3. Wählen Sie die Option **Authentifizierung aktivieren** aus, und geben Sie den Benutzernamen und das Kennwort (eines Benutzers mit Zugriff auf den SMTP-Server) ein.
4. Geben Sie die SMTP-Portnummer ein.

   Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.
5. Klicken Sie auf **Anwenden**.
   Die SMTP-Einstellungen sind damit konfiguriert.

Adresseinstellungen für den SMTP-E-Mail-Server über RACADM konfigurieren

So konfigurieren Sie den SMTP-E-Mail-Server:

```
racadm set iDRAC.RemoteHosts.SMTPServerIPAddress <SMTP E-mail Server IP Address>
```

Konfigurieren von WS-Ereignisauslösung

Das WS-Ereignisauslösungsprotokoll wird verwendet, damit ein Clientdienst (Abonnent) mit einem Server (Ereignisquelle) Interesse (Abonnement) an Meldungen zu Serverereignissen (Benachrichtigungen oder Ereignismeldungen) bekunden kann. Clients, die WS-Ereignisauslösungsmeldungen erhalten möchten, können mit iDRAC Lifecycle Controller-aufgabenbezogene Ereignisse abonnieren.

Die Schritte zur Konfiguration der WS-Ereignisauslösungsfunktion zum Erhalt von WS-Ereignisauslösungsmeldungen für Änderungen, die mit Lifecycle Controller-Aufgaben verknüpft sind, werden im Spezifikationsdokument „Web service Eventing Support for iDRAC 1.30.30“ beschrieben. Zusätzlich erhalten Sie im Dokument „DSP0226 (DMTF WS Management Specification), Section 10 Notifications (Eventing)“ umfassende Informationen zum WS-Ereignisauslösungsprotokoll. Die Lifecycle Controller-Aufgaben werden im Dokument „DCIM Job Control Profile“ beschrieben.

Konfigurieren von Redfish-Ereignissen

Das Redfish-Ereignisprotokoll wird verwendet, damit ein Clientdienst (Abonnent) mit einem Server (Ereignisquelle) Interesse (Abonnement) an Meldungen zu Redfish-Ereignissen (Benachrichtigungen oder Ereignismeldungen) bekunden kann. Clients, die Redfish-Ereignismeldungen erhalten möchten, können mit iDRAC Lifecycle Controller-aufgabenbezogene Ereignisse abonnieren.

Überwachung von Gehäuseereignissen

Beim Gehäuse des PowerEdge FX2/FX2s können Sie die Einstellung **Gehäuseverwaltung und -überwachung** in iDRAC aktivieren, um Gehäuseverwaltungs- und -überwachungsaufgaben durchzuführen, z. B. die Überwachung von Gehäusekomponenten, die Konfiguration von Warnmeldungen und die Weiterleitung von CMC RACADM-Befehle- und Aktualisierung der Gehäuseverwaltungs-Firmware mithilfe von iDRAC RACADM. Mit dieser Einstellung können Sie die Server im Gehäuse verwalten, selbst wenn sich der CMC nicht im Netzwerk befindet. Sie können den Wert auf **Deaktiviert** setzen, um die Gehäuseereignisse weiterzuleiten. Standardmäßig ist diese Option auf **Aktiviert** gesetzt.

ANMERKUNG: Damit sich diese Einstellung auswirkt, müssen Sie sicherstellen, dass in CMC die **Gehäuseverwaltung im Server** -Einstellung auf **Überwachen** oder **Verwalten und Überwachen** eingestellt ist.

Wenn die Option **Gehäuseverwaltung und -überwachung** auf **Aktiviert** gesetzt ist, erzeugt iDRAC Gehäuseereignisse und protokolliert diese. Die generierten Ereignisse werden in das iDRAC-Ereignis-Subsystem eingefügt und Warnmeldungen werden ähnlich den anderen Ereignissen erzeugt.

Darüber hinaus leitet CMC die generierten Ereignisse an iDRAC weiter. Für den Fall, dass der iDRAC auf dem Server nicht aktiviert ist, werden die ersten 16 Ereignisse von CMC in der Warteschlange gereiht und der Rest im CMC-Protokoll protokolliert. Diese 16 Ereignisse werden an iDRAC gesendet, sobald die **Gehäuseüberwachung** auf Aktiviert gesetzt ist.

In Fällen, in denen der iDRAC ermittelt, dass eine erforderliche CMC-Funktion nicht vorhanden ist, wird eine Warnmeldung angezeigt, die Sie darüber informiert, dass bestimmte Funktionen ohne eine CMC-Firmware-Aktualisierung möglicherweise nicht funktionsfähig sind.

ANMERKUNG: iDRAC unterstützt die folgenden Gehäuseattribute nicht:

- `ChassisBoardPartNumber`
- `ChassisBoardSerialNumber`

Überwachung von Gehäuseereignissen unter Verwendung der iDRAC-Webschnittstelle

Zur Überwachung von Gehäuseereignissen unter Verwendung der iDRAC-Webschnittstelle führen Sie die folgenden Schritte aus:

ANMERKUNG: Dieser Abschnitt wird nur für PowerEdge FX2-/FX2s-Gehäuse und bei Einstellung des **Gehäuseverwaltung im Servermodus** in CMC auf **Überwachen** oder **Verwalten und Überwachen** angezeigt.

1. Klicken Sie in der CMC-Oberfläche auf **Chassis Overview (Gehäuseübersicht)** > **Setup** > **General (Allgemein)**.
2. Wählen Sie aus dem Dropdown-Menü **Gehäuseverwaltung in Servermodus** den Eintrag **Verwalten und Überwachen** aus und klicken Sie auf **Anwenden**.
3. Starten Sie die iDRAC-Weboberfläche und klicken Sie auf **Overview (Übersicht)** > **iDRAC Settings (iDRAC-Einstellungen)** > **CMC**.
4. Stellen Sie im Abschnitt **Gehäuseverwaltung in Servermodus** sicher, dass im Drop-Down-Feld **Fähigkeit von iDRAC Aktiviert** eingestellt wurde.

Überwachung von Gehäuseereignissen unter Verwendung von RACADM

Diese Einstellung kann nur auf PowerEdge FX2-/FX2s-Servern angewendet werden und wenn der **Gehäuseverwaltung im Server-Modus** auf **Überwachung** oder **Verwalten und Überwachen** eingestellt wurde.

Zur Überwachung von Gehäuseereignissen unter Verwendung von iDRAC-RACADM:

```
racadm get system.chassiscontrol.chassismanagementmonitoring
```

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

IDs für Warnungsmeldung

Die folgende Tabelle enthält eine Liste mit Meldungs-IDs, die bei Warnungen angezeigt werden.

Tabelle 33. IDs für Warnungsmeldungen

Meldungs-ID	Beschreibung	Beschreibung (Für MX-Plattformen)
AMP	Stromstärke	Stromstärke
ASR	Automatische Systemrücksetzung	Automatische Systemrücksetzung
BAT	Akkuereignis	Akkuereignis
BIOS	BIOS Management	BIOS Management
Boot (Starten)	Boot-Steuerung	Boot-Steuerung
CBL	Kabel	Kabel
CPU	Prozessor	Prozessor
CPUA	Verfahren nicht vorhanden	Verfahren nicht vorhanden
CTL	Speicher-Controller	Speicher-Controller
DH	Zertifikatverwaltung	Zertifikatverwaltung
DIS	Automatische Ermittlung	Automatische Ermittlung

Tabelle 33. IDs für Warnungsmeldungen (fortgesetzt)

Meldungs-ID	Beschreibung	Beschreibung (Für MX-Plattformen)
ENC	Speichergehäuse	Speichergehäuse
Lüfter (FAN)	Lüfterereignis	Lüfterereignis
FSD	Debug	Debug
HWC	Hardware-Konfiguration	Hardware-Konfiguration
IPA	DRAC-IP-Änderung	DRAC-IP-Änderung
ITR	Eingriff	Eingriff
JCP	Auftragssteuerung	Auftragssteuerung
LC	Lifecycle Controller	Lifecycle Controller
LIC	Lizenzierung	Lizenzierung
Verbindung	Link-Status	Link-Status
Protokoll	Protokollereignis	Protokollereignis
MEM	Speicher	Speicher
NDR	NIC-Betriebssystemtreiber	NIC-Betriebssystemtreiber
Netzwerkadapter	NIC-Konfiguration	NIC-Konfiguration
OSD	BS-Bereitstellung	BS-Bereitstellung
OSE	BS-Ereignis	BS-Ereignis
PCI	PCI-Gerät	PCI-Gerät
PDR	Physisches Laufwerk	Physisches Laufwerk
PR	Teileaustausch	Teileaustausch
PST	BIOS POST	BIOS POST
Netzteil	Stromversorgung	Stromversorgung
PSUA	PSU nicht vorhanden	PSU nicht vorhanden
PWR	Stromverbrauch	Stromverbrauch
RAC	RAC-Ereignis	RAC-Ereignis
RDU	Redundanz	Redundanz
Rot	FW-Download	FW-Download
RFL	IDSDM-Datenträger	IDSDM-Datenträger
RFLA	IDSDM nicht vorhanden	IDSDM nicht vorhanden
RFM	FlexAddress-SD	Nicht anwendbar

Tabelle 33. IDs für Warnungsmeldungen (fortgesetzt)

Meldungs-ID	Beschreibung	Beschreibung (Für MX-Plattformen)
RRDU	IDSDM-Redundanz	IDSDM-Redundanz
RSI	Remote-Dienst	Remote-Dienst
SEC	Sicherheitsereignis	Sicherheitsereignis
Systemereignisprotokoll	System-Ereignisprotokoll	System-Ereignisprotokoll
SRD	Software-RAID	Software-RAID
SSD	PCIe-SSD-Festplatten	PCIe-SSD-Festplatten
STOR	Storage	Storage
SUP	FW-Aktualisierungsaufgabe	FW-Aktualisierungsaufgabe
SWC	Softwarekonfiguration	Softwarekonfiguration
SWU	Software-Änderung	Software-Änderung
[SYS]	System Info	System Info
tmp	Temperatur	Temperatur
TST	Test-Warnung	Test-Warnung
UEFI	UEFI-Ereignis	UEFI-Ereignis
usr	Benutzerverfolgung	Benutzerverfolgung
VDR	Virtuelles Laufwerk	Virtuelles Laufwerk
VF	vFlash-SD-Karte	vFlash-SD-Karte
VFL	vFlash-Ereignis	vFlash-Ereignis
VFLA	vFlash nicht vorhanden	vFlash nicht vorhanden
VLT	Spannung	Spannung
VME	Virtueller Datenträger	Virtueller Datenträger
VRM	Virtuelle Konsole	Virtuelle Konsole
WRK	Arbeitsanmerkung	Arbeitsanmerkung

13

iDRAC 9 Group Manager

Group Manager ermöglicht es dem Benutzer, mehrere Konsolen zu betreiben, und bietet eine vereinfachte grundlegende iDRAC-Verwaltung.

Die Funktion iDRAC Group Manager ist für Dell Server der 14. Generation verfügbar und ermöglicht mithilfe der iDRAC-GUI eine einfachere grundlegende Verwaltung der iDRACs und zugehöriger Server auf dem lokalen Netzwerk. Group Manager ermöglicht die Nutzung beliebig vieler Konsolen ohne Einsatz einer zusätzlichen Anwendung. Group Manager ermöglicht es Benutzern, Details zu einer Reihe von Servern einzusehen, da die Funktion eine leistungsstärkere Leistungsverwaltung bietet, als durch die Sichtprüfung der Server oder andere manuelle Methoden möglich ist.

Group Manager ist eine lizenzierte Funktion und Teil der Enterprise-Lizenz. Nur iDRAC-Admin-Benutzer können auf die Group Manager-Funktion zugreifen.

ANMERKUNG: Für eine bessere Benutzerfreundlichkeit unterstützt Group Manager bis zu 250 Serverknoten.

Themen:

- Group Manager
- Ansicht „Zusammenfassung“
- Konfigurationsanforderungen des Netzwerks
- Anmeldungen verwalten
- Warnungen konfigurieren
- Exportieren
- Ansicht „Discovered Servers“ (Ermittelte Server)
- Ansicht „Jobs“ (Aufgaben)
- Jobs-Export
- Gruppeninformationsbedienfeld
- Gruppeneinstellungen
- Aktionen für einen ausgewählten Server
- iDRAC-Gruppen-Firmwareupdates

Group Manager

Um die **Group Manager**-Funktion zu verwenden, müssen Sie den **Group Manager** auf der iDRAC-Indexseite oder auf dem Group Manager-Willkommensbildschirm aktivieren. Der Begrüßungsbildschirm von Group Manager enthält Optionen, die in der folgenden Tabelle aufgeführt sind.

Tabelle 34. Optionen in Group Manager

Option	Beschreibung
Vorhandener Gruppe beitreten	Ermöglicht das Beitreten zu einer vorhandenen Gruppe. Sie müssen den **Gruppennamen** und den **Passcode** kennen, um einer bestimmten Gruppe beitreten zu können. **ANMERKUNG:** Kennwörter werden iDRAC-Benutzeranmeldeinformationen zugeordnet. Ein Passcode ist einer Gruppe zugeordnet, um eine authentifizierte Gerätekommunikation zwischen verschiedenen iDRACs in derselben Gruppe herzustellen.
Neue Gruppe erstellen	Ermöglicht das Erstellen einer neuen Gruppe. Der spezifische iDRAC, der die Gruppe erstellt hat, wäre der Master (primärer Controller) der Gruppe.

Tabelle 34. Optionen in Group Manager (fortgesetzt)

Option	Beschreibung
Group Manager für dieses System deaktivieren	Sie können diese Option auswählen, wenn Sie von einem bestimmten System aus nicht einer Gruppe beitreten möchten. Sie können jedoch zu jedem beliebigen Zeitpunkt durch Auswahl von „Group Manager öffnen“ auf der iDRAC-Indexseite auf Group Manager zugreifen. Sobald Sie Group Manager deaktivieren, muss der Benutzer 60 Sekunden warten, bevor er weitere Vorgänge in Group Manager durchführen kann.

Wenn die Group Manager-Funktion aktiviert ist, können Sie mit diesem iDRAC die Option zum Erstellen oder Hinzufügen einer lokalen iDRAC-Gruppe auswählen. Es kann mehr als eine iDRAC-Gruppe im lokalen Netzwerk eingerichtet werden, aber einzelne iDRAC können jeweils nur Mitglied einer Gruppe sein. Um die Gruppe zu wechseln (einer neuen Gruppe beizutreten), muss der iDRAC zuerst die aktuelle Gruppe verlassen und dann der neuen Gruppe hinzugefügt werden. Der iDRAC, von dem aus die Gruppe erstellt wurde, wird standardmäßig als primärer Controller der Gruppe ausgewählt. Der Benutzer definiert keinen dedizierten primären Group Manager-Controller, um diese Gruppe zu steuern. Der primäre Controller hostet die Group Manager-Webschnittstelle und stellt die GUI-basierten Workflows bereit. Die iDRAC-Mitglieder wählen selbst einen neuen primären Controller für die Gruppe aus, wenn der aktuelle primäre Controller über einen längeren Zeitraum offline geschaltet wird. Dies hat aber keine Auswirkungen auf den Endbenutzer. Sie können in der Regel von allen iDRAC-Mitgliedern auf Group Manager zugreifen, indem Sie auf der iDRAC-Indexseite auf Group Manager klicken.

Ansicht „Zusammenfassung“

Sie müssen über Administratorrechte verfügen, um auf Group Manager-Seiten zugreifen zu können. Wenn sich ein Nicht-Administrator bei iDRAC anmeldet, wird der Abschnitt „Group Manager“ für die entsprechenden Anmeldeinformationen nicht angezeigt. Die Group Manager-Startseite (Übersicht) ist in drei Abschnitte unterteilt. Im ersten Abschnitt wird die Rollup-Zusammenfassung mit zusammengefassten Details dargestellt.

- Gesamtzahl der Server in der lokalen Gruppe
- Diagramm mit der Anzahl der Server pro Servermodell
- Ringdiagramm, das die Server mit ihrem Funktionsstatus anzeigt (durch Klicken auf einen Diagrammabschnitt wird die Serverliste gefiltert, sodass nur die Server mit dem gewählten Funktionsstatus angezeigt werden)
- Warnmeldung, wenn im lokalen Netzwerk eine duplizierte Gruppe erkannt wurde. Eine duplizierte Gruppe ist in der Regel eine Gruppe mit demselben Namen, aber einem anderen Passcode. Diese Warnmeldung wird nicht angezeigt, wenn es keine duplizierte Gruppe gibt.
- Zeigt die iDRACs, die die Gruppe steuern (primärer und sekundärer Controller)

Der zweite Abschnitt enthält Schaltflächen für Maßnahmen, die für die gesamte Gruppe ergriffen werden, und der dritte Abschnitt enthält die Liste aller iDRACs in der Gruppe.

Er zeigt alle Systeme in der Gruppe mit ihrem aktuellen Funktionsstatus an und ermöglicht es dem Benutzer, nach Bedarf Korrekturmaßnahmen zu ergreifen. Serverspezifische Attribute werden in der Tabelle unten beschrieben.

Tabelle 35. Serverattribute

Serverattribut	Beschreibung
Funktionszustand	Zeigt den Integritätsstatus dieses bestimmten Servers an.
Host Name (Hostname)	Zeigt den Servernamen an.
iDRAC-IP-Adresse	Zeigt die genaue IPV4- und IPV6-Adresse an.
Service-Tag	Zeigt die Service-Tag-Informationen an.
Modell	Zeigt die Modellnummer des Dell Servers an.
iDRAC	Zeigt die iDRAC-Version an.
Letzte Zustandsaktualisierung	Zeigt per Zeitstempel an, wann der Serverstatus zuletzt aktualisiert wurde.

Das Systeminformationsfeld enthält weitere Angaben zum Server, beispielsweise iDRAC-Netzwerkverbindungsstatus, Server-Host-Stromzustand, Express-Servicecode, Betriebssystem, Systemkennnummer, Knoten-ID, iDRAC-DNS-Name, Server-BIOS-Version, Server-CPU-Informationen, Systemspeicher und Standortinformationen. Sie können auf eine Zeile doppelklicken oder auf die Schaltfläche zum Starten von iDRAC klicken, um eine Single-Sign-On-Umleitung auf die iDRAC-Indexseite durchzuführen. Auf dem ausgewählten Server

kann auf die virtuelle Konsole zugegriffen werden und über die Drop-Down-Liste „More Actions“ (Weitere Aktionen) können Server-Strommaßnahmen ausgeführt werden.

Die unterstützten Gruppenaktionen sind das Verwalten von iDRAC Benutzeranmeldungen, das Konfigurieren von Warnungen und das Exportieren von Gruppeninventar.

Konfigurationsanforderungen des Netzwerks

Group Manager verwendet IPv6 Link Local Networking für die Kommunikation zwischen iDRACs (mit Ausnahme der Webbrowser-GUI). Die Link Local-Kommunikation wird als nicht geroutete Pakete definiert, was bedeutet, dass alle iDRAC, die durch einen Router getrennt sind, nicht in einer lokalen Gruppe zusammengefügt werden können. Wenn der iDRAC-dedizierte Port oder ein freigegebenes LOM einem vLAN zugewiesen wird, wird das vLAN auch die Anzahl der iDRACs begrenzen, die in einer Gruppe zusammengefügt werden können (iDRACs müssen sich im selben vLAN befinden und der Datenverkehr darf keinen Router passieren).

Wenn Group Manager aktiviert ist, aktiviert der iDRAC eine IPv6 Link-Local-Adresse unabhängig von der aktuellen benutzerdefinierten Netzwerkkonfiguration des iDRAC. Group Manager kann verwendet werden, wenn iDRAC für IPv4- oder IPv6 IP-Adressen konfiguriert ist.

Group Manager verwendet mDNS, um andere iDRACs im Netzwerk zu ermitteln, und sendet verschlüsselte Pakete für die normale Bestandsaufnahme, Überwachung und Verwaltung der Gruppe mithilfe der lokalen IP-Link-Adresse. Durch die Verwendung von IPv6 Link Local Networking werden die Group Manager-Ports und -Pakete nie das lokale Netzwerk verlassen oder für externe Netzwerke zugänglich sein.

Die Ports (spezifisch für eindeutige Group Manager-Funktion, umfasst nicht alle iDRAC-Ports) sind:

- 5353 (mDNS)
- 443 (Webserver) – konfigurierbar
- 5670 (Multicast-Gruppenkommunikation)
- C000- > F000 identifiziert dynamisch einen freien Port für jedes Mitglied, das in der Gruppe kommuniziert.

Bewährte Netzwerk-Praktiken

- Die Gruppen sind so konzipiert, dass sie klein sind und sich auf demselben physischen Link im lokalen Netzwerk befinden.
- Es wird empfohlen, den dedizierten iDRAC-Netzwerkport für eine erhöhte Sicherheit zu verwenden. Gemeinsam genutzte LOM werden ebenfalls unterstützt.

Weitere Überlegungen zum Netzwerk

Zwei iDRACs, die durch einen Router in der Netzwerktopologie getrennt sind, werden als in separaten lokalen Netzwerken betrachtet und können nicht zur selben lokalen iDRAC-Gruppe hinzugefügt werden. Wenn der iDRAC für dedizierte NIC-Einstellungen konfiguriert ist, muss das Netzwerkkabel, das mit dem iDRAC-dedizierten Port auf der Rückseite des Servers verbunden ist, zu einem lokalen Netzwerk für alle relevanten Server gehören.

Wenn der iDRAC für freigegebene LOM-Netzwerkeinstellungen konfiguriert ist, muss die von Server-Host und iDRAC gemeinsam genutzte Netzwerkverbindung unter einem lokalen Netzwerk angeschlossen sein, damit Group Manager diese Server erkennen und in einer gemeinsamen Gruppe eingliedern kann. IDRACs, die mit einer Kombination aus dedizierten und freigegebenen LOM-Modus-NIC-Einstellungen konfiguriert sind, können auch in einer gemeinsamen Gruppe integriert werden, wenn keine der Netzwerkverbindungen einen Router passiert.

Auswirkungen von MLD Snooping in VLAN Umgebungen bei der Group Manager-Ermittlung

Da Group Manager eine IPv6-Multicast-Adressierung für Node-initiierte Ermittlungen verwendet, kann eine Funktion, die als MLD Snooping bezeichnet wird, verhindern, dass Group-Manager-fähige Geräte einander erkennen, wenn sie nicht ordnungsgemäß konfiguriert ist. MLD Snooping ist eine gängige Ethernetswitch-Funktion, die die Menge des unnötigen IPv6-Multicast-Datenverkehrs in einem Netzwerk reduzieren soll.

Wenn MLD Snooping in einem Netzwerk aktiv ist, stellen sie sicher, dass ein MLD-Abfrager aktiviert ist, damit die Ethernetswitches mit den aktiven Group-Manager-Geräten im Netzwerk auf dem neuesten Stand gehalten werden. Wenn MLD Snooping nicht benötigt wird, kann es auch deaktiviert werden. Beachten Sie, dass einige Netzwerkswitches MLD Snooping standardmäßig aktiviert haben. Das gleiche gilt für das Wechseln von Modulen im MX7000-Gehäuse.

ANMERKUNG:

Zum Beispiel:

- So deaktivieren Sie MLD Snooping für das VLAN auf einem MX5108n-IOM:

  MX5108N-B1# configure terminal

  MX5108N-B1(config)# interface vlan 194

  MX5108N-B1(conf-if-vl-194)#no ipv6 mld snooping

- So aktivieren Sie einen MLD-Abfrager für das VLAN auf einem MX5108n-IOM:

  MX5108N-B1# configure terminal

  MX5108N-B1(config)# interface vlan 194

  MX5108N-B1(conf-if-vl-194)#ipv6 mld snooping querier

Anmeldungen verwalten

Verwenden Sie diesen Abschnitt zum **Hinzufügen neuer Benutzer**, **Ändern des Benutzerkennworts** und **Löschen von Benutzern** aus der Gruppe.

Gruppenaufgaben einschließlich Verwalten von Anmeldungen sind einmalige Konfigurationen auf den Servern. Group Manager verwendet SCP und Aufgaben, um Änderungen vorzunehmen. Alle iDRACs in der Gruppe verfügen über eine einzelne Aufgabe in der Warteschlange für jede Group Manager-Aufgabe. Group Manager erkennt keine Änderungen an Mitglied-iDRACs oder Konfigurationen gesperrter Mitglieder.

ANMERKUNG: Gruppenaufgaben konfigurieren nicht und setzen den Lockdown-Modus für iDRACs nicht außer Kraft.

Durch das Verlassen einer Gruppe ändern sich nicht der lokale Benutzer und die Einstellungen auf einem Mitglieds-iDRAC.

Einen neuen Benutzer hinzufügen

In diesem Abschnitt können Sie ein neues Benutzerprofil für alle Server in dieser Gruppe erstellen und hinzufügen. Eine Gruppenaufgabe wird zum Hinzufügen des Benutzers zu allen Servern in dieser Gruppe erstellt. Der Status einer Gruppenaufgabe ist auf der Seite **GroupManager** > **Jobs (Aufgaben)** zu finden.

ANMERKUNG: Standardmäßig ist iDRAC mit einem lokalen Administratorkonto konfiguriert. Sie können mit einem lokalen Administratorkonto auf weitere Informationen für jeden Parameter zugreifen.

Weitere Informationen finden Sie unter Benutzerkonten und Berechtigungen konfigurieren.

Tabelle 36. Optionen für neue Benutzer

Option	Beschreibung
Informationen zum neuen Benutzer	Ermöglicht Ihnen die Angabe von Informationsdetails zum neuen Benutzer.
iDRAC-Berechtigungen	Ermöglicht Ihnen die Festlegung der Rolle des Benutzer für die zukünftige Verwendung.
Erweiterte Benutzereinstellungen	Ermöglicht Ihnen die Festlegung von (IPMI) Benutzerberechtigungen und hilft Ihnen, SNMP zu aktivieren.

ANMERKUNG: Jeder Mitglieds-iDRAC mit aktivierter Systemsperre, der Teil derselben Gruppe ist, gibt einen Fehler zurück, dass das Benutzerkennwort nicht aktualisiert wurde.

Benutzerkennwort ändern

Verwenden Sie diesen Abschnitt zum Ändern des Kennworts für den Benutzer. Sie können die Angaben zum **Benutzer**, **Benutzernamen** zur **Rolle** und **Domäne** für einzelne Benutzer anzeigen. Eine Gruppenaufgabe wird zum Ändern des Benutzerkennworts auf allen Servern in dieser Gruppe erstellt. Der Status einer Gruppenaufgabe ist auf der Seite **GroupManager** > **Jobs (Aufgaben)** zu finden.

Wenn der Benutzer bereits existiert, kann das Kennwort aktualisiert werden. Jeder Mitglieds-iDRAC mit aktivierter Systemsperre, der Teil der Gruppe ist, gibt einen Fehler zurück, dass das Benutzerkennwort nicht aktualisiert wurde. Wenn der Benutzer nicht vorhanden ist, wird ein Fehler in Group Manager ein Fehler zurückgegeben, dass der Benutzer nicht auf dem System vorhanden ist. Die Liste der Benutzer, die in der Group Manager-GUI angezeigt werden, basiert auf der aktuellen Benutzerliste im iDRAC, der als primärer Controller fungiert. Es werden nicht alle Benutzer für alle iDRACs angezeigt.

Benutzer löschen

In diesem Abschnitt können Sie Benutzer aus Group Manager entfernen. Eine Gruppenaufgabe wird zum Löschen von Benutzern aus allen Gruppenservern erstellt. Der Status einer Gruppenaufgabe ist auf der Seite **GroupManager** > **Jobs (Aufgaben)** zu finden.

Wenn der Benutzer für einen Mitglieds-iDRAC bereits vorhanden ist, kann der Benutzer gelöscht werden. Jeder Mitglieds-iDRAC mit aktivierter Systemsperre, der Teil der Gruppe ist, gibt einen Fehler zurück, dass der Benutzer nicht gelöscht wurde. Wenn der Benutzer nicht vorhanden ist, wird angezeigt, dass der Löschvorgang für diesen iDRAC erfolgreich war. Die Liste der Benutzer, die in der Group Manager-GUI angezeigt werden, basiert auf der aktuellen Benutzerliste im iDRAC, der als primärer Controller fungiert. Es werden nicht alle Benutzer für alle iDRACs angezeigt.

Warnungen konfigurieren

In diesem Bereich können Sie E-Mail-Warnungen konfigurieren. Warnungen sind standardmäßig deaktiviert. Sie können sie jedoch jederzeit aktivieren. Dann wird ein Gruppenauftrag erstellt, um die E-Mail-Warnungskonfiguration auf alle Gruppenserver anzuwenden. Der Status des Gruppenauftrags kann auf der Seite **GroupManager** > **Jobs (Aufträge)** überwacht werden. Über die Group Manager-E-Mail-Warnung werden E-Mail-Warnungen für alle Mitglieder konfiguriert. Es werden die SMTP-Servereinstellungen für alle Mitglieder in derselben Gruppe festgelegt. Jeder iDRAC wird separat konfiguriert. Die E-Mail-Konfiguration wird nicht global gespeichert. Die aktuellen Werte basieren auf dem iDRAC, der als primärer Controller fungiert. Durch Verlassen einer Gruppe werden E-Mail-Warnungen nicht neu konfiguriert.

Weitere Informationen zum Konfigurieren von Warnungen finden Sie unter iDRAC für das Versenden von Warnungen konfigurieren.

Tabelle 37. Optionen zum Konfigurieren von Benachrichtigungen

Option	Beschreibung
Konfigurieren der Adresseneinstellungen des SMTP (E-Mail)-Servers	Ermöglicht Ihnen das Konfigurieren von Server-IP-Adresse und SMTP-Portnummer sowie das Aktivieren der Authentifizierung. Wenn Sie die Authentifizierung aktivieren, müssen Sie Benutzername und Passwort angeben.
E-Mail-Adressen	Ermöglicht Ihnen das Konfigurieren mehrerer E-Mail-IDs für den Empfang von E-Mail-Benachrichtigungen zu Systemstatusänderungen. Sie können eine Test-E-Mail an das konfigurierte Konto vom System senden.
Warnungskategorien	Ermöglicht Ihnen die Auswahl mehrerer Warnungskategorien, um E-Mail-Benachrichtigungen zu erhalten.

ANMERKUNG: Jeder Mitglieds-iDRAC mit aktivierter Systemsperre, der Teil derselben Gruppe ist, gibt einen Fehler zurück, dass das Benutzerpasswort nicht aktualisiert wurde.

Exportieren

Verwenden Sie diesen Abschnitt, um die Group Summary (Gruppenzusammenfassung) auf das lokale System zu exportieren. Die Informationen können im CSV-Dateiformat exportiert werden. Sie enthält Daten zu jedem einzelnen System in der Gruppe. Der Export enthält die folgenden Informationen im CSV-Format. Details zum Server:

- Funktionszustand

- Host Name (Hostname)
- iDRAC-IPV4-Adresse
- iDRAC-IPV6-Adresse
- Systemkennnummer
- Modell
- iDRAC-Firmware-Version
- Letzte Zustandsaktualisierung
- Eildienstcode
- iDRAC-Konnektivität
- Stromstatus
- Betriebssystem
- Service-Tag
- Knoten-ID
- iDRAC-DNS-Name
- BIOS Version
- CPU-Details
- Systemspeicher (MB)
- Standortdetails

ANMERKUNG: Falls Sie Internet Explorer verwenden, deaktivieren Sie die erweiterten Sicherheitseinstellungen, damit die CSV-Datei heruntergeladen werden kann.

Ansicht „Discovered Servers“ (Ermittelte Server)

Nach der Erstellung der lokalen Gruppe benachrichtigt iDRAC Group Manager alle anderen iDRACs im lokalen Netzwerk, dass eine neue Gruppe erstellt wurde. Damit iDRACs unter „Discovered Servers“ (Ermittelte Server) angezeigt werden, sollte die Funktion „Group Manager“ für jeden iDRAC aktiviert werden. Die Ansicht „Discovered Servers“ (Ermittelte Server) zeigt die Liste der iDRACs an, die in demselben Netzwerk, das Teil einer beliebigen Gruppe sein kann, ermittelt wurden. Wenn ein iDRAC nicht in der Liste der ermittelten Systeme angezeigt wird, muss sich der Benutzer an dem betreffenden iDRAC anmelden und der Gruppe beitreten. Der iDRAC, der die Gruppe erstellt hat, wird als einziges Mitglied in der Essentials-Ansicht angezeigt, bis mehrere iDRACs mit der Gruppe verbunden sind.

ANMERKUNG: Die Ansicht „Discovered Servers“ (Ermittelte Server) in der Group Manager-Konsole ermöglicht es Ihnen, einen oder mehrere in der Ansicht aufgeführte Server in diese Gruppe zu integrieren. Der Fortschritt der Aktivität kann unter **GroupManager** > **Jobs (Aufträge)** nachverfolgt werden. Alternativ dazu können Sie sich am iDRAC anmelden und die Gruppe in der Drop-Down-Liste auswählen, die Sie zu dieser Gruppe hinzufügen möchten. Sie können auf den GroupManager-Begrüßungsbildschirm von der iDRAC-Indexseite aus zugreifen.

Tabelle 38. Gruppe integrierter Optionen

Option	Beschreibung
Aufnehmen und Anmeldedaten ändern	Wählen Sie eine spezifische Zeile aus und wählen Sie die Option „Onboard and Change Login“ (Aufnehmen und Anmeldedaten ändern), um die neu ermittelten Systeme in die Gruppe aufzunehmen. Sie müssen die Administrator-Anmeldeinformationen für die neuen Systeme bereitstellen, die der Gruppe beitreten sollen. Wenn das System das Standardkennwort hat, müssen Sie es während der Aufnahme in eine Gruppe ändern. Bei der Aufnahme von Gruppen können Sie dieselben Gruppenalarmeinstellungen auf die neuen Systeme anwenden.
Ignorieren	Ermöglicht es Ihnen, die Systeme aus der Liste ermittelter Server zu ignorieren, falls Sie diese nicht zu einer Gruppe hinzufügen möchten.
Ignorieren aufheben	Ermöglicht Ihnen die Auswahl der Systeme, die Sie in der Liste der ermittelten Server reaktivieren möchten.
Erneute Suche	Ermöglicht es Ihnen, die Liste der ermittelten Server jederzeit zu durchsuchen und zu generieren.

Ansicht „Jobs“ (Aufgaben)

Die Ansicht „Jobs“ (Aufgaben) ermöglicht es dem Benutzer, den Fortschritt einer Gruppenaufgabe nachzuverfolgen, und unterstützt bei einfachen Wiederherstellungsschritten zur Korrektur von Ausfällen durch mangelnde Konnektivität. Sie zeigt ferner den Verlauf der letzten Gruppenaktionen, die als Prüfprotokoll durchgeführt wurden. Der Benutzer kann die Ansicht „Jobs“ (Aufgaben) verwenden, um den Fortschritt der Aktion in der Gruppe nachzuverfolgen oder eine zukünftige Aktion abzubrechen. Die Auftragsansicht ermöglicht es dem Benutzer, den Status der letzten 50 Aufträge anzuzeigen, die ausgeführt wurden, sowie alle aufgetretenen Erfolge und Ausfälle.

Tabelle 39. Ansicht „Jobs“ (Aufgaben)

Option	Beschreibung
Status	Zeigt den Auftragsstatus und den Status des laufenden Auftrags an.
Aufträge	Zeigt den Auftragsnamen an.
ID	Zeigt die Auftrags-ID an.
Startzeit	Zeigt die Startzeit an.
Endzeit	Zeigt die Endzeit an.
Maßnahmen	• Abbrechen – Ein geplanter Auftrag kann abgebrochen werden, bevor er ausgeführt wird. Ein ausgeführter Auftrag kann über die Schaltfläche „Stop“ (Anhalten) angehalten werden. • Erneut ausführen – Ermöglicht es dem Benutzer, die Aufgabe erneut auszuführen, falls die Aufgabe einen Fehlerstatus aufweist. • Entfernen – Ermöglicht es dem Benutzer, die abgeschlossenen alten Aufgaben zu entfernen.
Exportieren	Die können die Gruppenaufgabeninformationen auf das lokale System als zukünftige Referenz exportieren. Die Auftragsliste kann in das CSV-Dateiformat exportiert werden. Sie enthält Daten zu einzelnen Aufträgen.

ANMERKUNG: Für jeden Auftragseintrag bietet die Liste der Systeme Details zu bis zu 100 Systemen. Jeder Systemeintrag enthält Hostname, Service-Tag, Mitgliedsauftragsstatus und Meldung, wenn der Auftrag fehlschlägt.

Alle Gruppenaktionen, die Aufträge erstellen, werden für alle Gruppenmitglieder direkt durchgeführt. Sie können folgende Aufgaben ausführen:

- Benutzer hinzufügen/bearbeiten/entfernen
- E-Mail-Warnmeldungen konfigurieren
- Gruppenpasscode und -name ändern

ANMERKUNG: Gruppenaufgaben werden schnell durchgeführt, solange alle Mitglieder online und zugänglich sind. Es kann 10 Minuten vom Starten bis zum Abschließen der Aufgabe dauern. Eine Aufgabe wartet und wiederholt den Vorgang bis zu 10 Stunden für Systeme, die nicht zugänglich sind.

ANMERKUNG: Während eine Onboarding-Aufgabe ausgeführt wird, kann keine andere Aufgabe geplant werden. Aufträge umfassen:

- Neuen Benutzer hinzufügen
- Benutzerkennwort ändern
- Benutzer löschen
- Warnungen konfigurieren
- Zusätzliche Systeme aufnehmen
- Gruppenpasscode ändern
- Gruppenname ändern

Wenn Sie versuchen, eine andere Aufgabe aufzurufen, während eine Onboarding-Aufgabe aktiv ist, wird der Fehlercode GMGR0039 ausgegeben. Nach dem ersten Versuch der Onboarding-Aufgabe, alle neuen Systeme aufzunehmen, können jederzeit Aufgaben erstellt werden.

Jobs-Export

Sie können das Protokoll auf dem lokalen System für weitere Referenzen exportieren. Die Aufgabenliste kann im CSV-Format exportiert werden. Sie enthält alle aufgabenbezogenen Daten.

ANMERKUNG: Exportierte CSV-Dateien sind nur in englischer Sprache verfügbar.

Gruppeninformationsbedienfeld

Das Gruppeninformationsbedienfeld oben rechts in der Group Manager-Zusammenfassungsansicht zeigt eine konsolidierte Gruppenzusammenfassung. Die aktuelle Gruppenkonfiguration kann auf der Seite „Group Settings“ (Gruppeneinstellungen) bearbeitet werden, die durch Klicken auf die Schaltfläche „Group Settings“ (Gruppeneinstellungen) zugänglich ist. Sie zeigt, wie viele Systeme es in der Gruppe gibt. Sie bietet außerdem Informationen über den primären und sekundären Controller in der Gruppe.

Gruppeneinstellungen

Auf der Seite „Group settings“ (Gruppeneinstellungen) werden alle ausgewählten Gruppenattribute angezeigt.

Tabelle 40. Gruppeneinstellungen – Attribute

Gruppenattribut	Beschreibung
Gruppenname	Zeigt den Namen dieser Gruppe an.
Anzahl der Systeme	Zeigt die Gesamtanzahl der Systeme in dieser Gruppe an.
Erstellt am	Zeigt die Zeitstempelinformationen an.
Erstellt von	Zeigt die Details des Gruppenadministrators an.
Kontrollierendes System	Zeigt die Service-Tag-Nummer des Systems an, das als kontrollierendes System fungiert und die Gruppenverwaltungsaufgaben koordiniert.
Backup-System	Zeigt die Service-Tag-Nummer des Systems an, das als Backup-System fungiert. Für den Fall, dass das kontrollierende System nicht verfügbar ist, nimmt es die Rolle des kontrollierenden Systems ein.

Ermöglicht dem Benutzer die Ausführung der in der folgenden Tabelle aufgeführten Aktionen für die Gruppe. Eine Gruppenkonfigurationsaufgabe wird für diese Aktionen erstellt (Ändern des Gruppennamens, Ändern des Gruppenpasscodes, Entfernen der Mitglieder und Löschen der Gruppe). Der Status einer Gruppenaufgabe ist auf der Seite **GroupManager** > **Jobs (Aufgaben)** zu finden und kann dort geändert werden.

Tabelle 41. Gruppeneinstellungen – Aktionen

Maßnahmen	Beschreibung
Namen ändern	Ermöglicht Ihnen die Änderung des **aktuellen Gruppennamens** in einen **neuen Gruppennamen**.
Change Passcode (Passcode ändern)	Ermöglicht Ihnen die Änderung des derzeitigen Gruppenkennworts durch Eingeben eines **neuen Gruppenpasscodes** sowie die Validierung dieses Kennworts durch die **erneute Eingabe des Gruppenpasscodes**.
Systeme entfernen	Ermöglicht Ihnen das gleichzeitige Entfernen mehrerer Systeme aus der Gruppe.
Gruppe löschen	Löscht die Gruppe. Für die Verwendung von Group Manager-Funktionen müssen Sie über Administratorrechte verfügen. Alle ausstehenden Aufgaben werden angehalten, wenn die Gruppe gelöscht wird.

Aktionen für einen ausgewählten Server

Auf der Seite „Summary“ (Zusammenfassung) können Sie auf eine Zeile doppelklicken, um den iDRAC für diesen Server über eine Single Sign On-Umleitung zu starten. Stellen Sie sicher, dass der Popup-Blocker in den Browsereinstellungen deaktiviert ist. Sie können die folgenden Maßnahmen auf dem ausgewählten Server durchführen, indem Sie auf das entsprechende Element in der Drop-Down-Liste **More Actions (Weitere Aktionen)** klicken.

Tabelle 42. Aktionen für einen ausgewählten Server

Option	Beschreibung
Ordentliches Herunterfahren	Fährt das Betriebssystem ordnungsgemäß herunter und schaltet dann die Systemstromversorgung ab.
Kalt-Neustart	Schaltet das System aus und startet es dann erneut.
Virtuelle Konsole	Startet die virtuelle Konsole mit einmaligem Anmelden in einem neuen Browserfenster. **ANMERKUNG:** Deaktivieren Sie den Popup-Blocker im Browser, um diese Funktion zu verwenden.

Group Manager – einmaliges Anmelden

Alle iDRACs in der Gruppe vertrauen einander basierend auf dem gemeinsamen Passcode-Geheimschlüssel und dem gemeinsamen Gruppennamen. Als Ergebnis werden einem Administrator für ein Gruppenmitglieds-IDRAC Administratorberechtigungen für ein beliebiges Gruppenmitglieds-iDRAC gewährt (bei Zugriff über die Group Manager-Web-Schnittstelle per Single Sign On). Der iDRAC protokolliert <user>-<SVCTAG> als Benutzer, der sich bei Peer-Mitgliedern angemeldet hat. <SVCTAG> ist das Service-Tag des iDRAC, bei dem sich der Benutzer zum ersten Mal angemeldet hat.

Group Manager-Konzepte – Steuersystem

- Automatisch ausgewählt – standardmäßig der erste für Group Manager konfigurierte iDRAC.
- Stellt Group Manager-GUI-Workflow bereit.
- Verfolgt alle Mitglieder nach.
- Koordiniert Aufgaben.
- Wenn sich ein Benutzer bei einem beliebigen Mitglied anmeldet und auf „Open Group Manager“ (Group Manager öffnen) klickt, wird der Browser zum primären Controller umgeleitet.

Group Manager-Konzepte – Sicherungssystem

- Der primäre Controller wählt automatisch einen sekundären Controller aus, der übernimmt, wenn der primäre Controller für einen längeren Zeitraum (10 Minuten oder mehr) offline ist.
- Wenn der primäre und der sekundäre Controller länger offline sind (mehr als 14 Minuten), werden ein neuer primärer und sekundärer Controller ausgewählt.
- Behält eine Kopie des Group Manager-Cache aller Gruppenmitglieder und Aufgaben bei.
- Steuersystem und Sicherungssystem werden automatisch von Group Manager ermittelt.
- Benutzerkonfiguration oder -eingriffe sind nicht erforderlich.

iDRAC-Gruppen-Firmwareupdates

Führen Sie für iDRAC-Gruppen-Firmwareupdates aus der DUP-Datei in einem lokalen Verzeichnis die folgenden Schritte aus:

1. Greifen Sie auf die Essential-Ansicht der Group Manager-Konsole zu und klicken Sie in der Ansicht Zusammenfassung auf **iDRAC-Firmware aktualisieren**.
2. Suchen Sie im angezeigten Dialogfeld für das Firmwareupdate die lokale iDRAC-DUP-Datei, die Sie installieren möchten, und wählen Sie sie aus. Klicken Sie auf **Hochladen**.
3. Die Datei wird in iDRAC hochgeladen und auf Integrität überprüft.

4. Bestätigen Sie das Firmwareupdate. Der Job für das iDRAC-Gruppen-Firmwareupdate wird für die sofortige Ausführung geplant. Wenn von Group Manager andere Gruppen-Jobs ausgeführt werden, wird das Update ausgeführt, nachdem der vorherige Job abgeschlossen ist.
5. Sie können die Ausführung des iDRAC-Update-Jobs über die Ansicht Gruppen-Jobs nachverfolgen.

ANMERKUNG: Diese Funktion wird nur auf iDRAC-Version 3.50.50.50 und höher unterstützt.

14

Protokolle verwalten

iDRAC stellt ein Lifecycle-Protokoll bereit, das Ereignisse zum System, zu Speichergeräten, Netzwerkgeräten, Firmware-Aktualisierungen, Konfigurationsänderungen, Lizenzmeldungen und mehr enthält. Die Systemereignisse sind jedoch auch als separates Protokoll mit der Bezeichnung „Systemereignisprotokoll“ (SEL) verfügbar. Auf das Lifecycle-Protokoll kann über die iDRAC- Webschnittstelle, RACADM und die WSMan-Schnittstelle zugegriffen werden.

Wenn das Lifecycle-Protokoll eine Größe von 800 KB erreicht, werden die Protokolle komprimiert und archiviert. Sie können nur die nicht archivierten Protokolleinträge anzeigen und Filter und Kommentare auf nicht archivierte Protokolle anwenden. Um die archivierten Protokolle anzuzeigen, müssen Sie das gesamte Lifecycle-Protokoll an einem Speicherort auf Ihrem System exportieren.

Themen:

- Systemereignisprotokoll anzeigen
- Lifecycle-Protokoll anzeigen
- Exportieren der Lifecycle Controller-Protokolle
- Arbeitsanmerkungen hinzufügen
- Remote-Systemprotokollierung konfigurieren

Systemereignisprotokoll anzeigen

Wenn ein Systemereignis auf einem verwalteten System auftritt, wird dies im Systemereignisprotokoll (SEL) aufgezeichnet. Derselbe SEL-Eintrag ist auch im LC-Protokoll verfügbar.

ANMERKUNG: SEL- und LC-Protokolle können unterschiedliche Zeitstempel aufweisen, wenn der iDRAC neu gestartet wird.

Systemereignisprotokoll über die Web-Schnittstelle anzeigen

Um das Systemereignisprotokoll (SEL) anzuzeigen, gehen Sie in der iDRAC-Webschnittstelle auf **Maintenance (Wartung)** > **System Event Log (Systemereignisprotokoll)**.

Auf der Seite **System Event Log (Systemereignisprotokoll)** wird eine Systemzustandsanzeige, ein Zeitstempel und eine Beschreibung für jedes protokollierte Ereignis angezeigt. Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.

Klicken Sie auf **Speichern unter**, um das **SEL** in einem Speicherort Ihrer Wahl zu speichern.

ANMERKUNG: Wenn Sie Internet Explorer verwenden und ein Problem beim Speichern auftritt, laden Sie das kumulative Sicherheitsupdate für Internet Explorer herunter. Sie können es auf der Microsoft Support-Website unter **support.microsoft.com** herunterladen.

Klicken Sie zum Löschen aller Protokolle auf **Protokoll löschen**.

ANMERKUNG: Die Schaltfläche **Protokoll löschen** wird nur angezeigt, wenn Sie über die Berechtigung Protokolle löschen verfügen.

Sobald SEL gelöscht ist, wird ein Eintrag im Lifecycle Controller-Protokoll erfasst. Der Protokolleintrag enthält den Benutzernamen und die IP-Adresse, von der SEL gelöscht wurde.

Systemereignisprotokoll über RACADM anzeigen

So zeigen Sie das Systemereignisprotokoll (SEL) an:

```
racadm getsel <options>
```

Wenn keine Argumente vorgegeben werden, wird das gesamte Protokoll angezeigt.

So zeigen Sie die Anzahl der SEL-Einträge an: `racadm getsel -i`

Zum Löschen von SEL: `racadm clrsel`

Weitere Informationen finden Sie unter *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Anzeigen des Systemereignisprotokolls unter Verwendung des Dienstprogramms für die iDRAC-Einstellungen

Sie können die Gesamtzahl der Einträge im Systemereignisprotokoll (SEL) unter Verwendung des Dienstprogramms für die iDRAC-Einstellungen anzeigen und die Protokolle löschen. Führen Sie dazu folgende Schritte durch:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Systemereignisprotokoll**.
   Das **iDRAC- Settings.System Event Log** zeigt die **Gesamtzahl der Einträge** an.
2. Um die Einträge zu löschen, wählen Sie **Yes** (Ja). Andernfalls wählen Sie **No** (Nein).
3. Klicken Sie zum Anzeigen der Systemereignisse auf **Systemereignisprotokoll anzeigen**.
4. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

Lifecycle-Protokoll anzeigen

Die Lifecycle Controller-Protokolle enthalten die Änderungsverlaufsdaten in Bezug auf die Komponenten, die auf einem verwalteten System installiert sind. Sie können auch Arbeitsanmerkungen zu jedem Protokolleintrag hinzufügen.

Die folgenden Ereignisse und Aktivitäten werden protokolliert:

- Alle
- Systemzustand – Die Kategorie „Systemzustand“ umfasst alle Warnungen im Zusammenhang mit Hardware innerhalb des Systemgehäuses.
- Storage – Die Kategorie „Speicherzustand“ umfasst Warnmeldungen, die mit dem Speichersubsystem zusammenhängen.
- Aktualisierungen – Die Kategorie „Aktualisierungen“ umfasst Warnmeldungen, die aufgrund von Upgrades/Downgrades von Firmware/Treiber generiert wurden.
- Audit – Die Kategorie „Audit“ umfasst das Auditprotokoll.
- Konfiguration – Die Kategorie „Konfiguration“ umfasst Warnmeldungen, die mit Hardware-, Firmware- und Softwarekonfigurationsänderungen zusammenhängen.
- Arbeitsanmerkungen

Wenn Sie sich über eine der folgenden Schnittstellen bei iDRAC anmelden oder von iDRAC abmelden, werden die Anmelde- und Abmeldeereignisse bzw. Anmeldefehler in den Lifecycle-Protokollen aufgezeichnet:

- SSH
- Weboberfläche
- RACADM
- Redfish
- IPMI über LAN
- Seriell
- Virtuelle Konsole
- Virtueller Datenträger

Sie können Protokolle auf der Basis der Kategorie und des Schweregrads anzeigen und filtern. Sie können eine Arbeitsanmerkung auch exportieren und zu einem Protokollereignis hinzufügen.

ANMERKUNG: Lifecycle-Protokolle für Änderungen am Persönlichkeitsmodus werden nur während des Warmstarts des Hosts generiert.

Wenn Sie Konfigurationsaufträge mittels RACADM-CLI oder iDRAC-Weboberfläche initiieren, enthält das Lifecycle-Protokoll Informationen über den Benutzer, verwendete Schnittstelle und die IP-Adresse des Systems, von dem aus Sie den Job initiieren.

ANMERKUNG: Auf der MX-Plattform, erfasst Lifecycle Controller mehrere Job-IDs für Konfigurations- oder Installationsjobs, die mit OME – Modular erstellt wurden. Weitere Informationen über die durchgeführten Jobs finden Sie in den OME – Modular Protokollen.

Lifecycle-Protokoll über die Web-Schnittstelle anzeigen

Klicken Sie zum Anzeigen der Lifecycle-Protokolle auf **Maintenance (Wartung)** > **Lifecycle Log (Lifecycle-Protokoll)**. Die Seite **Lifecycle Log** (Lifecycle-Protokoll) wird angezeigt. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

Filtern der Lifecycle-Protokolle

Sie können Protokolle auf der Basis der Kategorie, des Schweregrads, des Schlüsselworts oder des Datumsbereichs filtern.

So filtern Sie die Lifecycle-Protokolle:

1. Führen Sie auf der Seite **Lifecycle-Protokoll** im Abschnitt **Protokollfilter** einen oder alle der folgenden Schritte aus:
   - Wählen Sie den **Protokolltyp** aus dem Dropdown-Menü.
   - Wählen Sie den Schweregrad aus der Drop-Down-Liste **Schweregrad** aus.
   - Geben Sie ein Schlüsselwort ein.
   - Legen Sie den Datumsbereich fest.
2. Klicken Sie auf **Anwenden**.
   Die gefilterten Protokolleinträge werden in den **Protokollergebnissen** angezeigt.

Anmerkungen zu Lifecycle-Protokollen hinzufügen

So fügen Sie Anmerkungen zu den Lifecycle-Protokollen hinzu:

1. Klicken Sie auf der Seite **Lifecycle-Protokoll** auf das Plus-Symbol (+) für den gewünschten Protokolleintrag.
   Daraufhin werden die Nachrichten-ID-Details angezeigt.
2. Geben Sie die gewünschten Anmerkungen für den Protokolleintrag in das Feld **Anmerkung** ein.
   Die Anmerkungen werden daraufhin im Feld **Anmerkung** angezeigt.

Lifecycle-Protokoll über RACADM anzeigen

Verwenden Sie zum Anzeigen von Lifecycle-Protokollen den Befehl `lclog`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Exportieren der Lifecycle Controller-Protokolle

Sie können das gesamte Lifecycle Controller-Protokoll (aktive und archivierte Einträge) in einer einzigen komprimierten XML-Datei in einer Netzwerkfreigabe oder auf dem lokalen System exportieren. Die Erweiterung der komprimierten XML-Datei lautet `.xml.gz`. Die Dateieinträge sind basierend auf den Sequenznummern in der Reihenfolge von der niedrigsten bis zur höchsten Sequenznummer sortiert.

Exportieren von Lifecycle Controller-Protokollen mithilfe der Webschnittstelle

So exportieren Sie Lifecycle Controller-Protokolle mithilfe der Webschnittstelle:

1. Klicken Sie auf der Seite **Lifecycle-Protokoll** auf **Exportieren**.
2. Wählen Sie aus den folgenden Optionen aus:
   - **Netzwerk** – Exportiert die Lifecycle-Controller-Protokolle an einen freigegebenen Speicherort im Netzwerk.
   - **Lokal** – Exportiert die Lifecycle-Controller-Protokolle an einen Speicherort auf dem lokalen System.

   ANMERKUNG: Beim Angeben der Netzwerkfreigabe wird empfohlen, für Benutzername und Kennwort Sonderzeichen zu vermeiden oder Prozent kodieren Sie diese Sonderzeichen.

   Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.
3. Klicken Sie auf **Exportieren**, um das Protokoll an den gewünschten Speicherort zu exportieren.

Exportieren von Lifecycle Controller-Protokollen mit RACADM

Verwenden Sie zum Exportieren von Lifecycle-Controller-Protokollen den Befehl `lclog export`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Arbeitsanmerkungen hinzufügen

Jeder Benutzer, der sich beim iDRAC anmeldet, kann Arbeitsanmerkungen hinzufügen. Diese werden im Lifecycle-Protokoll als Ereignis gespeichert. Allerdings sind hierfür die notwendigen Privilegien erforderlich. Für eine Arbeitsanmerkung sind jeweils maximal 255 Zeichen zulässig.

ANMERKUNG: Sie können keine Arbeitsanmerkungen löschen.

So fügen Sie eine Arbeitsanmerkung hinzu:

1. Gehen Sie in der iDRAC-Web-Schnittstelle zu **Dashboard** > **Notes (Anmerkungen)** > **Add Note (Anmerkung hinzufügen)**.
   Die Seite **Work Notes (Arbeitsanmerkungen)** wird angezeigt.
2. Geben Sie unter **Arbeitsanmerkungen** den gewünschten Test in das leere Textfeld ein.

   ANMERKUNG: Es wird empfohlen, nicht zu viele Sonderzeichen zu verwenden.

3. Klicken Sie auf **Save (Speichern)**.
   Die Arbeitsanmerkung wird zum Protokoll hinzugefügt. Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.

Remote-Systemprotokollierung konfigurieren

Sie können Lifecycle-Protokolle an ein Remote-System senden. Bevor Sie beginnen, stellen Sie Folgendes sicher:

- iDRAC und das Remote-System sind über eine Netzwerkkonnektivität verbunden.
- Das Remote-System und iDRAC befinden sich auf dem gleichen Netzwerk.

Remote-System-Protokollierung über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die Remote-Syslog-Server-Einstellungen:

1. Gehen Sie in der iDRAC-Weboberfläche zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Remote Syslog Settings (Remote-Syslog-Einstellungen)**.
   Die Seite **Remote-Syslog-Einstellungen** wird angezeigt.
2. Aktivieren Sie das Remote-Syslog und geben Sie die Serveradresse und Portnummer an. Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.
3. Klicken Sie auf **Anwenden**.
   Die Einstellungen werden gespeichert. Alle in das Lifecycle-Protokoll geschriebenen Protokolle werden ferner gleichzeitig auf die konfigurierten Remote-Server geschrieben.

Remote-Systemanmeldung über RACADM konfigurieren

Um die Remote-System-Protokollierungseinstellungen zu konfigurieren, verwenden Sie den Befehl `set` mit den Objekten in der Gruppe `iDRAC.SysLog`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

15

Stromversorgung im iDRAC überwachen und verwalten

Sie können den iDRAC verwenden, um die Stromanforderungen des verwalteten Systems zu überwachen und zu verwalten. Dies trägt dazu bei, das System vor Stromausfällen zu schützen, indem der Stromverbrauch des Systems angemessen verteilt und reguliert wird.

Zentrale Funktionen:

- **Stromverbrauchsüberwachung** – Zeigen Sie den Stromverbrauchsstatus, den Verlauf der Strommessungen, die aktuellen Durchschnittswerte, die Höchstwerte, usw. für das Managed System an.
- **Strombegrenzung** – Zeigen Sie die Strombegrenzung für das verwaltete System an und legen Sie sie fest, einschließlich der Anzeige des geringsten und maximalen potenziellen Stromverbrauchs. Hierbei handelt es sich um eine lizenzierte Funktion.
- **Stromsteuerung** – Über diese Funktion können Sie Stromsteuerungsvorgänge (z. B. Einschalten, Ausschalten, Systemrücksetzung, Aus- und einschalten und ordnungsgemäßes Herunterfahren) auf dem Managed System ausführen.
- **Netzteiloptionen** – Konfigurieren Sie die Netzteiloptionen, z. B. die Redundanzrichtlinie, das Austauschen von Laufwerken im laufenden Betrieb und die Korrektur des Leistungsfaktors.

Themen:

- Stromversorgung überwachen
- Festlegen des Warnungsschwellenwerts für den Stromverbrauch
- Stromsteuerungsvorgänge ausführen
- Strombegrenzung
- Netzteiloptionen konfigurieren
- Netzschalter aktivieren oder deaktivieren
- Multi-Vektor-Kühlung

Stromversorgung überwachen

iDRAC führt eine Dauerüberwachung des Stromverbrauchs im System durch und zeigt die folgenden Stromwerte an:

- Stromverbrauchswarnung und kritische Schwellenwerte.
- Kumulativer Stromverbrauch, Stromverbrauchshöchstwert und Ampere-Höchstwert.
- Stromverbrauch in der letzten Stunden, am vorherigen Tag oder in der abgelaufenen Woche.
- Durchschnittliche, Mindest- und Höchstleistungsaufnahme
- Verlaufshöchstwerte und Zeitstempel für Höchstwerte.
- Höchst-Aussteuerungsreserve und ummittelbare Aussteuerungsreserve-Werte (für Rack- und Tower-Server).

ANMERKUNG: Das Histogramm für die Stromverbrauchstrends des Systems (stündlich, täglich, wöchentlich) wird nur gespeichert, während iDRAC ausgeführt wird. Falls iDRAC neu gestartet wird, gehen die vorhandenen Daten zum Stromverbrauch verloren, und das Histogramm wird neu gestartet.

ANMERKUNG: Nach der Aktualisierung oder Zurücksetzung der iDRAC-Firmware wird das Diagramm zum Stromverbrauch gelöscht bzw. zurückgesetzt.

Überwachen des Leistungsindex von CPU, Speicher und E/A-Modulen über die Webschnittstelle

Um den Leistungsindex von CPU, Speicher und E/A-Modulen zu überwachen, gehen Sie in der iDRAC-Webschnittstelle zu **System** > **Performance (Leistung)**.

- Abschnitt **Systemleistung** – Zeigt den aktuellen Messwert und den Warnungsmesswert für den CPU-, Speicher- und E/A-Auslastungsindex sowie den CUPS-Index auf Systemebene in einer grafischen Ansicht an.
- Abschnitt **Historische Daten der Systemleistung**:
  - Enthält die Statistiken zu CPU, Arbeitsspeicher und E/A-Auslastung sowie den CUPS-Index auf Systemebene. Wenn das Host-System ausgeschaltet ist, zeigt das Diagramm die Ausschaltungslinie unter 0 %.
  - Sie können die maximale Auslastung für einen bestimmten Sensor zurücksetzen. Klicken Sie auf **Reset Historical Peak** (Historischen Spitzenwert zurücksetzen). Sie müssen über die Berechtigung zur Konfiguration verfügen, um den Spitzenwert zurückzusetzen.
- Abschnitt **Leistungskennzahlen**:
  - Zeigt den Status an und präsentiert Messwerte .
  - Zeigt den Warnungsschwellenwerte für die Auslastung an oder legt ihn fest. Sie müssen über Berechtigungen zum Konfigurieren des Servers verfügen, um die Schwellenwerte festlegen zu können.

Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der *iDRAC-Online-Hilfe*.

Überwachen des Leistungsindex für CPU-, Speicher- und E/A-Module über RACADM

Verwenden Sie den Unterbefehl **SystemPerfStatistics** zur Überwachung des Leistungsindex für CPU, Arbeitsspeicher und E/A-Module. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Festlegen des Warnungsschwellenwerts für den Stromverbrauch

Sie können den Warnschwellenwert für den Stromverbrauchssensor in den Rack- und Tower-Systemen einstellen. Der Warn-/kritische Stromschwellenwert für Rack- und Tower-Systeme kann sich je nach Kapazität des Netzteils und der Redundanzrichtlinie nach dem Aus- und Einschalten des Systems ändern. Der Warnschwellenwert darf jedoch auch dann den kritischen Schwellenwert nicht überschreiten, wenn die Kapazität des Netzteils in der Redundanzrichtlinie geändert wird.

Der Warnschwellenwert für die Stromversorgung für Blade-Systeme ist auf die Stromzuweisung von CMC (für Nicht-MX-Plattformen) oder OME –Modular (für MX-Plattformen) festgelegt.

Wenn ein Vorgang zum Zurücksetzen auf die Standardmaßnahme durchgeführt wird, werden die Stromversorgungsschwellenwerte auf den Standard festgelegt.

Sie müssen über Benutzerberechtigungen zum Konfigurieren verfügen, um den Warnungsschwellenwert für den Stromverbrauchssensor festzulegen.

ANMERKUNG: Der Warnungsschwellenwert wird nach Durchführung einer Aktualisierung von racreset oder iDRAC auf den Standardwert zurückgesetzt.

Einrichten der Warnschwelle für den Stromverbrauch über die Webschnittstelle

1. Gehen Sie in der iDRAC-Webschnittstelle zu **System** > **Overview (Übersicht)** > **Present Power Reading and Thresholds (Aktuelle Strommesswerte und -schwellenwerte)**.
2. Klicken Sie im Abschnitt **Present Power Reading and Thresholds (Aktuelle Strommesswerte und -schwellenwerte)** auf **Edit Warning Threshold (Warnungsschwellenwert bearbeiten)**.
   Die Seite **Edit Warning Threshold (Warnungsschwellenwert bearbeiten)** wird angezeigt.
3. Geben Sie in der Spalte **Warning Threshold (Warnungsschwellenwert)** den Wert in **Watt** oder **BTU/h** ein.

   Die Werte müssen niedriger sein als die Werte für den **Fehlerschwellenwert**. Die Werte werden auf den nächsten Wert abgerundet, der durch 14 teilbar ist. Wenn Sie den Wert in **Watt** eingeben, berechnet das System automatisch die Werte in **BTU/h** und zeigt sie an. Wenn Sie den Wert in BTU/h eingeben, werden die Werte in **Watt** angezeigt.
4. Klicken Sie auf **Save (Speichern)**. Die Werte werden konfiguriert.

Stromsteuerungsvorgänge ausführen

iDRAC ermöglicht, im Remote-Zugriff die Maßnahmen Einschalten, Ausschalten, Reset, ordentliches Herunterfahren, nicht maskierbarer Interrupt (NMI) oder Aus- und Einschalten mithilfe der Webschnittstelle oder RACADM auszuführen.

Sie können diese Vorgänge auch über die Lifecycle Controller-Remote-Dienste oder WSMan ausführen. Weitere Informationen finden Sie unter *Schnellstart-Benutzerhandbuch für Lifecycle Controller Remote Services* verfügbar unter https://www.dell.com/idracmanuals und im Dokument *Dell Energiezustandsverwaltungsprofil* unter https://www.dell.com/support.

Die vom iDRAC ausgelösten Stromversorgungs-Steuerungsvorgänge auf dem Server sind unabhängig von dem im BIOS konfigurierten Stromversorgungsverhalten. Sie können die PushPowerButton-Funktion verwenden, um das System ordnungsgemäß herunterzufahren oder einzuschalten, selbst wenn das BIOS so konfiguriert ist, dass es nichts tut, wenn der physische Netzschalter gedrückt wird.

Stromsteuerungsvorgänge über die Web-Schnittstelle ausführen

So führen Sie Stromsteuerungsvorgänge aus:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Energieverwaltung** > **Energiesteuerung**. Die Optionen für die **Energiesteuerung** werden angezeigt.
2. Wählen Sie die erforderliche Stromsteuerungsmaßnahme aus:
   - System einschalten
   - System ausschalten
   - NMI (Non-Masking Interrupt, nicht-maskierbare Unterbrechung)
   - Ordentliches Herunterfahren
   - System zurücksetzen (Softwareneustart)
   - System aus- und wieder einschalten (Hardwareneustart)
3. Klicken Sie auf **Anwenden**. Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.

Stromsteuerungsvorgänge über RACADM ausführen

Verwenden Sie zum Ausführen von Strommaßnahmen den Befehl **serveraction**.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Strombegrenzung

Sie können die Stromverbrauchs-Schwellenwerte anzeigen, die den Bereich des Gleich- und Drehstrom-Stromverbrauchs abdecken, den ein System unter schwerer Belastung gegenüber dem Rechenzentrum meldet. Hierbei handelt es sich um eine lizenzierte Funktion.

Strombegrenzung bei Blade-Servern

Bevor sich ein Blade-Server einschaltet, wenn begrenzter Hardware-Bestand vorhanden ist, versorgt iDRAC den Gehäuse-Manager mit den Leistungsanforderungen des Blade-Servers. Wenn sich der Stromverbrauch im Laufe der Zeit erhöht und wenn der Server die ihm maximal zugewiesene Strommenge verbraucht, weist iDRAC CMC (für Nicht-MX-Plattformen) oder OME-Modular (für MX-Plattformen) an, die maximale potenzielle Stromzufuhr zu erhöhen. Dies führt zu einer erhöhten Stromzuteilung, doch die Stromzuteilung wird nicht weniger, wenn der Verbrauch sinkt.

Nach dem Einschalten und Initialisieren des Systems berechnet iDRAC einen neuen Energiebedarf basierend auf der aktuellen Hardwarekonfiguration. Das System bleibt auch dann mit Strom versorgt, wenn CMC (nicht für MX-Plattformen) oder OME-Modular (nicht für MX-Plattformen) keine neue Stromanforderung zuweist.

CMC oder OME Modular fordern sämtliche ungenutzte Energie von Servern mit niedrigerer Priorität zurück und ordnen diese Energie einem Infrastrukturmodul mit höherer Priorität oder einem Server zu.

Strombegrenzungsrichtlinie anzeigen und konfigurieren

Wenn die Strombegrenzungsrichtlinie aktiviert ist, werden benutzerdefinierte Strombegrenzungen für das System durchgesetzt. Wenn Strombegrenzung nicht aktiviert ist, wird die standardmäßige Hardware-Stromschutzrichtlinie verwendet. Diese Stromschutzrichtlinie ist unabhängig von der benutzerdefinierten Richtlinie. Die Systemleistung wird dynamisch angepasst, um die Leistungsaufnahme am festgelegten Schwellenwert zu halten.

Der tatsächliche Stromverbrauch hängt von der Arbeitsauslastung ab. Dieser kann den Schwellenwert vorübergehend überschreiten, bis die Leistungsanpassungen vorgenommen sind. Betrachten Sie z. B. ein System mit einem minimalen und einem maximalen Stromverbrauch von 500 W bzw. 700 W. Sie können eine Strombudgetschwelle angeben, um den Verbrauch auf 525 W zu reduzieren. Wenn dieses Strombudget konfiguriert ist, wird die Leistung des Systems dynamisch angepasst, um eine Stromaufnahme von 525 W oder weniger aufrechtzuerhalten.

Wenn Sie eine sehr niedrige Stromaufnahme einstellen oder wenn die Umgebungstemperatur ungewöhnlich hoch ist, kann die Stromaufnahme während des Einschaltens oder Zurücksetzens des Systems vorübergehend die Stromaufnahme übersteigen.

Wenn der Wert für die Strombegrenzung auf einen Wert unterhalb des empfohlenen Schwellenwerts gesetzt ist, ist iDRAC möglicherweise nicht in der Lage, die angeforderte Strombegrenzung aufrecht zu erhalten.

Sie können den Wert in Watt, BTU/h oder als Prozentsatz der empfohlenen maximalen Strombegrenzung angeben.

Bei einer Stromobergrenze in BTU/h wird bei der Umrechung in Watt auf die nächste Ganzzahl abgerundet. Beim Auslesen der Strombegrenzungsschwelle aus dem System wird auch die Umrechnung von Watt auf BTU/h abgerundet. Aufgrund der Abrundung können die tatsächlichen Werte leicht abweichen.

Strombegrenzungsrichtlinie über die Web-Schnittstelle konfigurieren

So zeigen Sie die Stromrichtlinien an:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Energieverwaltung** > **Richtlinie für die Stromobergrenze**. Die aktuelle Stromobergrenze der Richtlinie wird im Bereich **Stromobergrenzwerte** angezeigt.
2. Wählen Sie unter **Stromobergrenze** die Option **Aktivieren**.
3. Geben Sie im Abschnitt **Stromobergrenzwerte** innerhalb des empfohlenen Bereichs die Stromobergrenze in Watt und BTU/h oder den maximalen Prozentsatz der empfohlenen Systembegrenzung an.
4. Klicken Sie auf **Anwenden**, um die Werte zu übernehmen.

Strombegrenzungsrichtlinie über RACADM konfigurieren

Um die Werte für die aktuelle Strombegrenzung anzuzeigen und zu konfigurieren, verwenden Sie die folgenden Objekte mit dem Befehl `set`:

- System.Power.Cap.Enable
- System.Power.Cap.Watts
- System.Power.Cap.Btuhr
- System.Power.Cap.Percent

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Strombegrenzungsrichtlinie über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren

So zeigen Sie die Stromrichtlinien an und konfigurieren sie:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Stromkonfiguration**.

   ANMERKUNG: Der Link **Stromkonfiguration** ist nur verfügbar, wenn die Netzteileinheit des Servers die Stromüberwachung unterstützt.

   Daraufhin wird die Seite **iDRAC-Einstellungen – Stromkonfiguration** angezeigt.
2. Wählen Sie **Aktiviert** aus, um die **Stromobergrenzenrichtlinie** zu aktivieren. Wählen Sie ansonsten **Deaktiviert** aus.
3. Verwenden Sie die empfohlenen Einstellungen, oder geben Sie unter **Benutzerdefinierte Richtlinie für Stromobergrenze** die gewünschten Grenzwerte ein.

   Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

4. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
   Damit sind die Strombegrenzungswerte konfiguriert.

Netzteiloptionen konfigurieren

Sie können die Netzteiloptionen konfigurieren, so z. B. die Redundanzrichtlinie, das Austauschen von Laufwerken im laufenden Betrieb und die Korrektur des Leistungsfaktors.

Das Hotspare ist eine Netzteilfunktion, über die die redundanten Netzteilgeräte (PSUs) je nach Server-Belastung ausgeschaltet werden können. Auf diese Weise können die übrigen PSUs mit einer höheren Auslastung und Effizienz laufen. Die PSUs müssen diese Funktion jedoch unterstützen, damit gewährleistet ist, dass sie bei Bedarf schnell eingeschaltet werden können.

In einem System mit zwei Netzteilen kann entweder PSU 1 oder PSU 2 als primäres Netzteil konfiguriert werden.

Nach der Aktivierung von Hot Spare können Netzteile je nach Belastung aktiv werden oder in den Standbymodus übergehen. Wenn Hot Spare aktiviert ist, wird die asymmetrische elektrische Leistungsaufteilung zwischen zwei Netzteilen aktiviert. Ein Netzteil ist *aktiv* und erbringt den Großteil der Leistung, während sich das andere Netzteil im Standbymodus befindet und eine geringe Leistungsmenge erbringt. Dies wird oft als 1+0 mit zwei Netzteilen und aktiviertem Hot Spare bezeichnet. Wenn sich alle PSU-1 in Stromkreis A und alle PSU-2 in Stromkreis B befinden, so ist bei aktiviertem Hot Spare (werkseitige Standardeinstellung) Stromkreis C weniger stark ausgelastet und löst die Warnmeldungen aus. Ist Hot Spare deaktiviert, so wird die Last gleichmäßig im Verhältnis 50:50 zwischen den beiden Netzteilen aufgeteilt und die Stromkreise A und B weisen in der Regel die gleiche Last auf.

Der Leistungsfaktor bezieht sich auf den tatsächlichen Stromverbrauch im Verhältnis zur Scheinleistung. Wenn die Korrektur des Leistungsfaktors aktiviert ist, verbraucht der Server eine geringe Menge Strom, wenn der Host AUSgeschaltet ist. Per Standardeinstellung ab Werk ist die Korrektur des Leistungsfaktors aktiviert.

Netzteiloptionen über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die Netzteiloptionen:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Configuration (Konfiguration)** > **Power Management (Energieverwaltung)** > **Power Configuration (Stromkonfiguration)**.
2. Wählen Sie unter **Power Redundancy Policy (Stromredundanzregel)** die gewünschten Optionen aus. Weitere Informationen finden Sie in der *iDRAC Online-Hilfe*.
3. Klicken Sie auf **Anwenden**. Die Netzteiloptionen sind damit konfiguriert.

Netzteiloptionen über RACADM konfigurieren

Verwenden Sie zum Konfigurieren der Netzteiloptionen die folgenden Objekte mit dem Befehl `get/set`:

- System.Power.RedundancyPolicy
- System.Power.Hotspare.Enable
- System.Power.Hotspare.PrimaryPSU
- System.Power.PFC.Enable

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Netzteiloptionen über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren

So konfigurieren Sie die Netzteiloptionen:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Stromkonfiguration**.

   ANMERKUNG: Der Link **Stromkonfiguration** ist nur verfügbar, wenn die Netzteileinheit des Servers die Stromüberwachung unterstützt.

   Daraufhin wird die Seite **iDRAC-Einstellungen – Stromkonfiguration** angezeigt.
2. Führen Sie unter **Netzteiloptionen** die folgenden Schritte aus:
   - Aktivieren oder deaktivieren Sie die Netzteilredundanz.
   - Aktivieren oder deaktivieren Sie das Hotspare.

- Legen Sie das primäre Netzteilgerät fest.
- Aktivieren oder Deaktivieren Sie die Korrektur des Leistungsfaktors. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
   Die Netzteiloptionen sind damit konfiguriert.

Netzschalter aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie den Netzschalter auf dem Managed System:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Frontblendensicherheit**.
   Die Seite **iDRAC-Einstellungen Frontblendensicherheit** wird angezeigt.
2. Wählen Sie **Aktiviert** zum Aktivieren des Betriebsschalters oder **Deaktiviert**, um ihn zu deaktivieren.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
   Die Einstellungen werden gespeichert.

Multi-Vektor-Kühlung

Die Multi-Vektor-Kühlung nutzt einen mehrschichtigen Ansatz zur thermischen Steuerung auf Dell EMC-Serverplattformen. Sie können Multi-Vektor-Kühloptionen über die iDRAC-Webschnittstelle konfigurieren, indem Sie zu **Konfiguration** > **Systemeinstellungen** > **Hardwareeinstellungen** > **Lüfterkonfiguration** navigieren. Multi-Vektor-Kühlung umfasst unter anderem Folgendes:

- Eine hohe Zahl von Sensoren (thermisch, Strom, Inventar usw.), die eine genaue Echtzeit-Erfassung des thermischen Systemzustands an verschiedenen Stellen innerhalb des Servers ermöglichen. Es wird nur eine kleine Teilmenge von Sensoren angezeigt, die je nach Konfiguration für den Benutzer relevant sind.
- Ein intelligenter und adaptiver geschlossener Regelalgorithmus optimiert das Lüfterverhalten, um die Temperaturen der Komponenten aufrechtzuerhalten. Außerdem werden Lüfterleistung und Luftstromverbrauch sowie die Lautstärke reduziert.
- Mit der Lüfterzonenzuordnung kann bei Bedarf eine Kühlung der Komponenten eingeleitet werden. So wird maximale Leistung erreicht und die Energienutzungseffizienz optimiert.
- Genaue Darstellung des PCIe-Luftstroms pro Steckplatz in Bezug auf die LFM-Metrik (Linear Feet per Minute, ein anerkannter Industriestandard für die Spezifikation der PCIe-Karten-Luftstromanforderungen). Durch die Anzeige dieser Metrik in verschiedenen iDRAC-Schnittstellen kann der Benutzer:
  1. die maximale LFM-Kapazität jedes Steckplatzes innerhalb des Servers sehen.
  2. feststellen, welcher Ansatz für die PCIe-Kühlung für jeden Slot zum Einsatz kommt (luftstromgesteuert, temperaturgesteuert).
  3. den Mindest-LFM-Wert jedes Steckplatzes sehen, wenn es sich bei der Karte um eine Drittanbieter-Karte (benutzerdefinierte Karte) handelt.
  4. einen benutzerdefinierten Mindest-LFM-Wert für die Drittanbieter-Karte festlegen, der eine genauere Definition des Kühlbedarfs ermöglicht, da der Kunde ein besseres Verständnis der benutzerdefinierten Spezifikation der Karte hat.
- Zeigt dem Benutzer in Echtzeit die System-Luftstrommetrik (CFM, Kubikfuß pro Minute) in verschiedenen iDRAC-Schnittstellen an, um einen Ausgleich des Luftstroms im Rechenzentrum basierend auf dem kumulierten CFM-Verbrauch pro Server zu ermöglichen.
- Ermöglicht benutzerdefinierte Temperatureinstellungen wie thermische Profile (Maximalleistung im Vgl. zu maximaler Leistung pro Watt, Sound-Obergrenze), benutzerdefinierte Lüfterdrehzahloptionen (minimale Lüfterdrehzahl, Offset für Lüftergeschwindigkeit) und benutzerdefinierte Ablufttemperatureinstellungen.
  1. Die meisten dieser Einstellungen ermöglichen eine zusätzliche Kühlung über die durch thermische Algorithmen erzeugte Grundlinienkühlung hinaus und lassen nicht zu, dass die Lüfterdrehzahlen unter die Systemkühlungsanforderungen fallen.
     ANMERKUNG: Eine Ausnahme von der obigen Aussage sind die Lüfterdrehzahlen, die für PCIe-Karten von Drittanbietern hinzugefügt werden. Der über den thermische Algorithmus gelieferte Luftstrom für Drittanbieterkarten kann den tatsächlichen Kühlbedarf der Karte unter- oder überschreiten. Der Kunde kann die Leistung für die Karte durch Eingabe des LFM-Wertes der Drittanbieterkarte feinabstimmen.
  2. Die benutzerdefinierte Ablufttemperatur-Option begrenzt die Ablufttemperatur auf die vom Kunden gewünschten Einstellungen.
     ANMERKUNG: Hinweis: Bei bestimmten Konfigurationen und Auslastungen ist es möglicherweise physikalisch nicht möglich, die Abluft bis unter einen gewünschten Sollwert zu reduzieren (z. B. benutzerdefinierte Ablufteinstellung von 45 °C mit hoher Einlasstemperatur {z. B. 30 °C} und bestimmter geladener Konfiguration {hoher System-Stromverbrauch, niedriger Luftstrom}).
  3. Die Option Sound-Obergrenze ist bei PowerEdge-Servern der 14. Generation neu. Hierdurch wird die CPU-Leistungsaufnahme begrenzt und die Lüfterdrehzahl sowie Lautstärkeobergrenze gesteuert. Dies ist speziell für akustische Anwendungen gedacht und kann zu einer verminderten Systemleistung führen.

- System-Layout und -design ermöglichen eine höhere Luftströmungskapazität (durch die Möglichkeit höherer Leistung) und dichte Systemkonfigurationen. Dies bietet weniger Systembeschränkungen und eine höhere Funktionsdichte.
  1. Der optimierte Luftstrom ermöglicht ein effizientes Verhältnis von Luftstrom zu Lüfterleistung.
- Kundenspezifische Lüfter sind für höhere Effizienz, bessere Leistung, längere Lebensdauer und geringere Vibration ausgelegt. Sie sind außerdem geräuschärmer.
  1. Lüfter sind potenziell langlebig (im Allgemeinen mehr als 5 Jahre), selbst wenn sie die ganze Zeit mit voller Drehzahl laufen.
- Kundenspezifische Kühlkörper wurden entwickelt, um die Komponentenkühlung für minimalen (erforderlichen) Luftstrom zu optimieren und unterstützen gleichzeitig Hochleistungs-CPUs.

16

iDRAC Direct Updates

iDRAC provides out of band ability to update the firmware of various components of a PowerEdge server. iDRAC direct update helps in eliminating staged jobs during updates. This is supported only for iDRAC releases 5.00.00.00 and above. Only SEP(passive) backplanes are supported for direct updates.

iDRAC used to have staged updates to initiate firmware update of the components. From this release, Direct updates have been applied to PSU and Backplane. With the use of Direct Updates and Backplane can have quicker updates. In case of PSU, one reboot (for initializing the updates) is avoided and the update can happen in single reboot.

With Direct update feature in iDRAC, you can eliminate the first reboot to initiate the updates. The second reboot will be controlled by the device itself and iDRAC notifies the user if there is need for a separate reset via job status.

17

Durchführen einer Bestandsaufnahme, Überwachung und Konfiguration von Netzwerkgeräten

Sie können den Bestand für die folgenden Netzwerkgeräte erfassen und diese überwachen und konfigurieren:

- Netzwerkadapter (NICs)
- Konvergente Netzwerkadapter (CNAs)
- LAN auf Hauptplatinen (LOMs)
- Netzwerktochterkarten (NDCs)
- Mezzanine-Karten (nur für Blade-Server)

Bevor Sie NPAR oder eine einzelne Partition auf CNA-Geräten deaktivieren, stellen Sie sicher, dass Sie alle E/A-Identitätsattribute (Beispiel: IP-Adresse, virtuelle Adressen, Initiator und Speicherziele) und Attribute auf Partitionsebene (Beispiel: Bandbreitenzuweisung) gelöscht haben. Sie können eine Partition entweder durch Ändern der Einstellung des „VirtualizationMode“-Attributs zu NPAR oder durch Deaktivieren aller Persönlichkeiten auf einer Partition deaktivieren.

Je nach Typ des installierten CNA-Geräts bleiben die Einstellungen von Partitionsattributen ggf. nicht erhalten, nachdem die Partition zuletzt aktiv war. Legen Sie alle E/A-Identitätsattribute und partitionsbezogenen Attribute beim Aktivieren einer Partition fest. Sie können eine Partition entweder durch Ändern der Einstellung des „VirtualizationMode“-Attributs zu NPAR oder durch Aktivieren einer Persönlichkeit (Beispiel: NicMode) auf der Partition aktivieren.

Themen:

- Bestandsaufnahme für Netzwerkgeräte erstellen und Netzwerkgeräte überwachen
- Inventorying and monitoring FC HBA devices
- Inventorying and monitoring SFP Transceiver devices
- Telemetry Streaming
- Serielle Datenerfassung
- Dynamische Konfiguration von virtuellen Adressen, Initiator- und Speicherziel-Einstellungen

Bestandsaufnahme für Netzwerkgeräte erstellen und Netzwerkgeräte überwachen

Sie können den Zustand remote überwachen und die Bestandsaufnahme für die Netzwerkgeräte im Managed System anzuzeigen:

Für jedes Gerät können Sie folgende Informationen zu den Schnittstellen und aktivierten Partitionen abrufen:

- Link-Status
- Eigenschaften
- Einstellungen und Funktionen
- Empfangs- und Übertragungsstatistiken
- iSCSI-, FCoE-Initiator- und Zielinformationen

Netzwerkgeräte über die Web-Schnittstelle überwachen

Um die Netzwerkgeräteinformationen über die Web-Schnittstelle anzuzeigen, gehen Sie zu **System** > **Overview (Übersicht)** > **Network Devices (Netzwerkgeräte)**. Die Seite **Netzwerkgeräte** wird angezeigt. Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der *iDRAC-Online-Hilfe*.

Netzwerkgeräte über RACADM überwachen

Um Informationen über Netzwerkgeräte anzuzeigen, verwenden Sie die Befehle `hwinventory` und `nicstatistics`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Zusätzliche Eigenschaften werden möglicherweise angezeigt, wenn Sie RACADM oder WSMan neben den auf der iDRAC-Web-Schnittstelle angezeigten Eigenschaften verwenden.

Verbindungsanzeige

Die manuelle Überprüfung und Fehlerbehebung der Netzwerkverbindungen der Server ist in einer Rechenzentrumsumgebung nicht durchführbar. iDRAC9 vereinfacht diese Aufgabe mit der iDRAC-Verbindungsanzeige. Mit dieser Funktion können Sie Netzwerkverbindungen von derselben zentralen GUI aus überprüfen und Fehler beheben, die Sie für die Bereitstellung, Aktualisierung, Überwachung und Wartung der Server verwenden. Die Verbindungsanzeige in iDRAC9 bietet Details zur physischen Zuordnung von Switch-Ports zu den Netzwerkports des Servers und zu dedizierten iDRAC-(Integrated Dell Remote Access Controller-)Portverbindungen. Alle unterstützten Netzwerkkarten sind unabhängig von der Marke in der Verbindungsanzeige sichtbar.

Anstatt die Netzwerkverbindungen des Servers manuell zu überprüfen und Fehler zu beheben, können Sie Netzwerkkabelverbindungen per Remote-Zugriff anzeigen und verwalten.

Die Verbindungsanzeige zeigt Informationen zu den Switch-Ports, die mit den Server-Ports verbunden sind, sowie zum dedizierten Port von iDRAC. Die Server-Netzwerkports beinhalten jene auf PowerEdge LOM-, NDC-, Mezz-Karten, PCIe-Add-In-Karten.

Um die Verbindungsanzeige für Netzwerkgeräte anzuzeigen, navigieren Sie zu **System** > **Übersicht** > **Netzwerkgerät** > **Verbindungsanzeige**, um die Verbindungsanzeige zu sehen.

Sie können die Verbindungsanzeige auch mit **iDRAC-Einstellungen** > **Konnektivität** > **Netzwerk** > **Allgemeine Einstellungen** > **Verbindungsanzeige** aktivieren oder deaktivieren.

Die Verbindungsanzeige kann mit dem RACADM-Befehl `SwitchConnection View` überprüft und mit dem Befehl angezeigt werden.

Feld oder Option	Beschreibung
Aktiviert	Wählen Sie **Aktiviert** aus, um die Verbindungsanzeige zu aktivieren. Standardmäßig ist die Option **Aktiviert** ausgewählt.
Zustand	Zeigt **Aktiviert** an, wenn Sie in der **Verbindungsanzeige** in den iDRAC-Einstellungen die Option „Verbindungsanzeige“ aktivieren.
Switch-Verbindungs-ID	Zeigt die LLDP-Gehäuse-ID des Switches an, über den der Geräte-Port verbunden ist.
Switch-Portverbindungs-ID	Zeigt die LLDP-Port-ID des Switch-Ports an, mit dem der Geräte-Port verbunden ist.

ANMERKUNG: Die Switch-Verbindungs-ID und Switch-Portverbindungs-ID sind verfügbar, sobald die Verbindungsanzeige aktiviert und die Verbindung hergestellt ist. Die zugeordnete Netzwerkkarte muss mit der Verbindungsanzeige kompatibel sein. Nur Nutzer mit iDRAC-Konfigurationsberechtigung können die Einstellungen für die Verbindungsanzeige ändern.

Ab iDRAC9 4.00.00.00 und späteren Versionen unterstützt iDRAC das Senden von Standard-LLDP-Paketen an externe Switches. Dies bietet Optionen zur Erkennung von iDRACs im Netzwerk. Der iDRAC sendet zwei Arten von LLDP-Paketen an das ausgehende Netzwerk:

- **Topology LLDP** – Bei dieser Funktion durchläuft das LLDP-Paket alle unterstützten NIC-Ports des Servers, so dass ein externer Switch den Ursprungsserver, den NDC-Port[NIC FQDD], die IOM-Position im Gehäuse, das Service-Tag des Blade-Gehäuses usw. lokalisieren kann. Ab iDRAC9 4.00.00.00 und späteren Versionen ist Topologie-LLDP als Option für alle PowerEdge-Server verfügbar. Die LLDP-Pakete enthalten Konnektivitätsinformationen zu Server-Netzwerkgeräten und werden von E/A-Modulen und externen Switches zur Aktualisierung ihrer Konfiguration verwendet.

  ANMERKUNG:
  - Die Topologie-LLDP muss aktiviert sein, damit die MX-Gehäusekonfiguration ordnungsgemäß funktioniert.
  - Die Topologie-LLDP wird auf 1-GbE-Controllern nicht unterstützt und wählt 10-GbE-Controller (Intel X520, QLogic 578xx) aus.
- **Ermittlungs-LLDP** – Bei dieser Funktion geht das LLDP-Paket nur durch den aktiven, verwendeten iDRAC-NIC-Port (dedizierte NIC oder gemeinsam genutztes LOM), so dass ein benachbarter Switch den iDRAC-Verbindungsport im Switch lokalisieren kann. Ermittlungs-LLDP ist nur für den aktiven iDRAC-Netzwerkanschluss spezifisch und wird nicht in allen Netzwerkanschlüssen des

Servers angezeigt. Ermittlungs-LLDP wird über einige Details des iDRAC wie IP-Adresse, MAC-Adresse, Service-Tag usw. verfügen, so dass ein Switch automatisch angeschlossene iDRAC-Geräte und einige Daten von iDRAC erkennen kann.

ANMERKUNG: Wenn die virtuelle MAC-Adresse auf einem Port/einer Partition gelöscht wird, dann ist die virtuelle MAC-Adresse gleich der MAC-Adresse.

Zum Aktivieren oder Deaktivieren der Topologie-LLDP navigieren Sie zu **iDRAC-Einstellungen** > **Konnektivität** > **Netzwerk** > **Allgemeine Einstellungen** > **Topologie-LLDP**, um die Topologie LLDP zu aktivieren oder zu deaktivieren. Standardmäßig ist sie für MX-Server aktiviert und für alle anderen Server deaktiviert.

Zum Aktivieren oder Deaktivieren der iDRAC Ermittlungs-LLDP navigieren Sie zu **iDRAC-Einstellungen** > **Verbindung** > **Netzwerk** > **Allgemeine Einstellungen** > **iDRAC Ermittlungs-LLDP**. Standardmäßig ist die Option Enable (Aktivieren) ausgewählt.

LLDP-Pakete, die von iDRAC stammen, können mit dem Befehl vom Switch aus eingesehen werden: `show lldp neighbors`.

Aktualisieren der Verbindungsanzeige

Verwenden Sie **Verbindungsanzeige aktualisieren**, um aktuelle Informationen zur Switch-Verbindungs-ID und Switch-Portverbindungs-ID einzusehen.

ANMERKUNG: Wenn iDRAC über Switch-Verbindungs- und Switch-Portverbindungsinformationen für den Server-Netzwerkport oder den iDRAC-Netzwerkport verfügt und die Switch-Verbindungs- und Switch-Portverbindungsinformationen aus irgendeinem Grund für 5 Minuten nicht aktualisiert werden, werden die Switch-Verbindungs- und Switch-Portverbindungsinformationen als veraltete (zuletzt als funktionierend bekannte) Daten für alle Nutzeroberflächen angezeigt. In der Nutzeroberfläche wird ein gelbes Symbol angezeigt. Dies ist jedoch normal und stellt keine Warnung dar.

Mögliche Werte für Verbindungsanzeige

Mögliche Daten der Verbindungsanzeige	Beschreibung
Funktion deaktiviert	Die Verbindungsanzeige-Funktion ist deaktiviert. Um die Daten der Verbindungsanzeige anzuzeigen, aktivieren Sie die Funktion.
Keine Verbindung	Zeigt an, dass die dem Netzwerk-Controller-Port zugeordnete Verbindung unterbrochen ist.
Nicht verfügbar	LLDP ist auf dem Switch nicht aktiviert. Überprüfen Sie, ob LLDP auf dem Switch-Port aktiviert ist.
Nicht unterstützt	Netzwerkcontroller unterstützt die Verbindungsanzeige-Funktion nicht.
Veraltete Daten	Die letzten als funktionierend bekannten Daten. Entweder ist die Verbindung mit dem Netzwerk-Controller-Port unterbrochen oder das System ist ausgeschaltet. Verwenden Sie die Aktualisierungsoption, um die Details der Verbindungsanzeige zu aktualisieren und die neuesten Daten zu erhalten.
Gültige Daten	Zeigt die gültige Switch-Verbindungs-ID und die Informationen zur Switch-Port-Verbindungs-ID an.

Netzwerk-Controller mit Verbindungsanzeige-Unterstützung

Folgende Karten oder Controller unterstützen die Verbindungsanzeige-Funktion.

Hersteller	Typ
Broadcom	• 57414 rNDC 25GE • 57416/5720 rNDC 10GbE • 57412/5720 rNDC 10GbE • 57414 PCIe FH/LP 25GE • 57412 PCIe FH/LP 10GbE • 57416 PCIe FH/LP 10GbE
Intel	• X710 bNDC 10Gb • X710 DP PCIe 10Gb

Hersteller	Typ
	• X710 QP PCIe 10Gb • X710 + I350 rNDC 10Gb+1Gb • X710 rNDC 10Gb • X710 bNDC 10Gb • XL710 PCIe 40Gb • XL710 OCP Mezz 10Gb • X710 PCIe 10Gb
Mellanox	• MT27710 rNDC 40Gb • MT27710 PCIe 40Gb • MT27700 PCIe 100Gb
QLogic	• QL41162 PCIe 10GE 2P • QL41112 PCIe 10GE 2P • QL41262 PCIe 25GE 2P

Inventorying and monitoring FC HBA devices

You can remotely monitor the health and view the inventory of the Fibre Channel Host Bus Adapters (FC HBA) devices in the managed system. The Emulex and QLogic FC HBAs are supported. For each FC HBA device, you can view the following information for the ports:

- FC storage target information
- NVMe storage target information
- Port Properties
- Receive and Transmit Statistics

NOTE: Emulex FC8 HBAs are not supported.

FC-HBA-Geräte mit der Webschnittstelle überwachen

Um Informationen zu FC-HBA-Geräten über die Web-Schnittstelle anzuzeigen, gehen Sie zu **System** > **Overview (Übersicht)** > **Network Devices (Netzwerkgeräte)** > **Fibre Channel**. Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der *iDRAC-Online-Hilfe*.

Im Seitennamen werden auch die Steckplatznummer, die angibt, wo das FC-HBA-Gerät verfügbar ist, und der Typ des FC-HBA-Geräts angezeigt.

Überwachung von FC-HBA-Geräten unter Verwendung von RACADM

Um die FC-HBA-Geräteinformationen unter Verwendung von RACADM anzuzeigen, verwenden Sie den Befehl `hwinventory`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Inventorying and monitoring SFP Transceiver devices

You can remotely monitor the health and view the inventory of SFP transceiver devices connected to the system. Following are the supported transceivers:

- SFP
- SFP+
- SFP28
- SFP-DD
- QSFP
- QSFP+
- QSFP28
- QSFP-DD

- Base-T modules
- AOC & DAC cables
- RJ-45 Base-T connected with Ethernet
- Fiber channel
- IB adapter ports

Most useful transceiver information are Serial number and Part number from transceiver EPROM. These would allow to verify the remotely installed transceivers, when troubleshooting connectivity issues. For each SFP Transceiver device, you can view the following information for the ports:

- Vendor Name
- Part Number
- Revision
- Serial Number
- Device Identifier
- Interface Type

Monitoring SFP Transceiver devices using web interface

To view the SFP Transceiver device information using Web interface, go to **System** > **Overview** > **Network Devices** and click on particular device. For more information about the displayed properties, see *iDRAC Online Help*.

The page name also displays the slot number where the transceiver device is available under Port statistics.

Monitoring data for SFP devices is only available for active SFPs. Following are the information displayed:

- TX Output Power
- TX Bias Current
- RX Input Power
- Vcc Voltage
- Temperature

Monitoring SFP Transceiver devices using RACADM

To view the SFP Transceiver device information using RACADM, use the `networktransceiverstatistics` command.

For more information, see the *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Telemetry Streaming

Telemetry enables users to collect and stream real-time device metrics, events, and data logs from a PowerEdge server to a subscribed external client or server application. Using Telemetry, you can set the type and frequency of reports that needs to be generated.

NOTE: The feature is supported on all the platforms and it requires iDRAC Datacenter license.

Telemetry is one-to-many solution for collecting and streaming the live system data from one or more PowerEdge servers (iDRAC) to a centralized 'Remote Server Monitoring, Analysis, and Alerting service'. The feature also supports on-demand data collection of the data.

The telemetry data includes metrics/inventory and logs/events. The data can be streamed (pushed out) or collected (pulled) from iDRAC to or by remote consumers like Redfish client and Remote Syslog Server. The telemetry data is also provided to the iDRAC SupportAssist data collector on demand. The data collection and report is based on predefined Redfish telemetry metrics, trigger, and report definitions. The telemetry streaming settings can be configured using iDRAC web interface, RACADM, Redfish, and Server Configuration Profile (SCP).

To configure Telemetry, enable or select the required device reports or logs that define the behavior and frequency of data streaming. Go to **Configuration** > **System Settings** page to configure Telemetry. Data streaming is automatic until the Telemetry is disabled.

Following table describes the metric reports that can be generated using telemetry:

Type	Metric Group	Inventory	Sensor	Statistics	Configuration	Metrics
I/O Devices	NICs	No	Yes	Yes	No	No

Type	Metric Group	Inventory	Sensor	Statistics	Configuration	Metrics
	FC HBAs	No	Yes	Yes	No	No
Server Devices	CPUs	No	Yes	No	No	Yes
	Memory	No	Yes	No	No	Yes
	Fans	No	Yes	No	No	No
	PSUs	No	No	No	No	Yes
	Sensors	No	Yes	No	No	No
Environmental	Thermal	No	Yes	No	No	Yes
	Power	No	No	Yes	No	Yes
	Performance	No	No	Yes	No	No
Accelerators	GPUs	No	No	Yes	No	Yes

To know about the field descriptions of Telemetry section, see *iDRAC Online Help*.

NOTE:

- StorageDiskSMARTDATA is only supported on SSD drives with SAS/SATA bus protocol and behind the BOSS controller.
- StorageSensor data is reported only for the drives in Ready / Online / Non-RAID mode and not behind the BOSS controller.
- NVMeSMARTData is only supported for SSD (PCIeSSD / NVMe Express) drives with PCIe bus protocol (not behind SWRAID).
- GPGPUStatistics data is only available in specific GPGPU models that support ECC memory capability.
- PSUMetrics is not available on modular platforms.
- Fan Power and PCIe Power Metrics may be displayed as 0 for some platforms.
- CUPS report has been renamed to SystemUsage in 4.40.00.00 release and it's supported on both INTEL and AMD platforms.

Telemetry Workflow:

1. Install Datacenter license, if not installed already.
2. Configure global Telemetry settings including Enabling the telemetry and Rsyslog server network address and port using RACADM, Redfish, SCP, or iDRAC GUI.
3. Configure the following Telemetry report streaming parameters on the required device report or log using either RACADM or Redfish interface:
   - EnableTelemetry
   - ReportInterval
   - ReportTriggers

   NOTE: Enable iDRAC Alerts and Redfish events for the specific hardware for which you need telemetry reports.
4. Redfish client makes subscription request to the Redfish EventService on iDRAC.
5. iDRAC generates and pushes the metric report or log/event data to the subscribed client when the predefined trigger conditions are met.

Feature Constraints:

1. For security reasons, iDRAC supports only HTTPS-based communication to the client.
2. For stability reasons, iDRAC supports up to eight subscriptions.
3. Deletion of subscriptions is supported through Redfish interface only, even for the manual deletion by the Admin.

Behavior of Telemetry feature:

- iDRAC generates and pushes (HTTP POST) the Metric Report or log/event data to all the subscribed clients to the destination specified in the subscription when the predefined trigger conditions are met. The clients receive new data only upon successful subscription creation.
- The metric data includes the timestamp in ISO format, UTC time (ends in 'Z'), at the time of data collection from source.
- Clients can terminate a subscription by sending an HTTP DELETE message to the URI of the subscription resource through the Redfish interface.
- If the subscription is deleted either by iDRAC or the client, then iDRAC does not send (HTTP POST) reports. If the number of delivery errors exceeds predefined thresholds, then iDRAC may delete a subscription.
- If a user has Admin privilege, they can delete the subscriptions but only through Redfish interface.
- Client is notified about the termination of a subscription by iDRAC by sending 'Subscription terminated' event as the last message.

- Subscriptions are persistent and can remain even after iDRAC restarts. But, they can be deleted either by performing `racresetcfg` or LCwipe operations.
- User interfaces like RACADM, Redfish, SCP, and iDRAC display the current status of the client subscriptions.

Serielle Datenerfassung

Der iDRAC ermöglicht die serielle Erfassung der Konsolenumleitung zum späteren Abrufen mithilfe der Funktion zur seriellen Datenerfassung. Für diese Funktion wird eine iDRAC Datacenter-Lizenz benötigt.

Der Zweck der Funktion der seriellen Datenerfassung besteht darin, die seriellen Daten des Systems zu erfassen und zu speichern, damit der Kunde Sie später zu Debugging-Zwecken abrufen kann.

Sie können eine serielle Datenerhebung mit den iDRAC-Schnittstellen RACADM oder Redfish aktivieren oder deaktivieren. Wenn dieses Attribut aktiviert ist, erfasst der iDRAC den seriellen Datenverkehr, der auf den seriellen Host-Gerät2 empfangen wird, unabhängig von den Einstellungen des seriellen MUX-Modus.

Um die serielle Datenerhebung mit der iDRAC-GUI zu aktivieren bzw. zu deaktivieren, gehen Sie zur Seite „**Wartung** > **Diagnose** > **Serielle Datenprotokolle**“ und aktivieren Sie das Kontrollkästchen, um die Funktion zu aktivieren oder zu deaktivieren.

ANMERKUNG:
- Dieses Attribut wird bei einem iDRAC-Neustart nicht zurückgesetzt.
- Durch Zurücksetzen der Firmware auf die Standardeinstellung wird diese Funktion deaktiviert.
- Solange die serielle Datenerhebung aktiviert ist, werden dem Puffer immer aktuelle Daten angehängt. Wenn der Nutzer die serielle Erfassung deaktiviert und erneut aktiviert, beginnt der iDRAC den Anhängevorgang ab des letzten Updates.

Die serielle Datenerhebung des Systems beginnt, wenn der Nutzer das Kennzeichen für die serielle Datenerhebung von einer beliebigen Schnittstelle aktiviert. Wenn die serielle Datenerfassung aktiviert ist, nachdem das System gestartet wurde, müssen Sie das System neu starten, sodass das BIOS die neue Einstellung sehen kann (Konsolenumleitung auf Anfrage von iDRAC aktiviert), um die seriellen Daten zu erhalten. Der iDRAC startet die Datenerhebung kontinuierlich und speichert sie in dem gemeinsam genutzten Speicher mit einer Begrenzung von 512 KB. Bei dem Puffer handelt es sich um einen Ringspeicher.

ANMERKUNG:
- Um diese Funktion zu nutzen, muss man über die Berechtigung zur Anmeldung und Systemsteuerung verfügen.
- Für diese Funktion wird eine iDRAC Enterprise-Lizenz benötigt.

Dynamische Konfiguration von virtuellen Adressen, Initiator- und Speicherziel-Einstellungen

Sie können die Einstellungen für virtuelle Adresse, Initiator und Speicherziel dynamisch anzeigen und konfigurieren und eine Persistenzrichtlinie anwenden. Dies ermöglicht es der Anwendung, die Einstellungen basierend auf den Stromzustandsänderungen (das heißt, Betriebssystem-Neustart, Softwareneustart, Hardwareneustart oder Aus- und Einschalten) und auch basierend auf der Persistenzrichtlinieneinstellung für diesen Stromzustand anzuwenden. Dies bietet mehr Flexibilität bei Bereitstellungen, die eine schnelle Neukonfiguration der Systemarbeitslasten auf einem anderen System erfordern.

Die virtuellen Adressen sind:
- Virtuelle MAC-Adresse
- Virtuelle iSCSI MAC-Adresse
- Virtuelle FIP-MAC-Adresse
- Virtuelle WWN
- Virtuelle WWPN

ANMERKUNG: Wenn Sie die Richtlinie für die Persistenz löschen, werden alle virtuellen Adressen auf die werkseitig eingestellte permanente Adresse zurückgesetzt.

ANMERKUNG: Bei einigen Karten mit virtuellen FIP-, virtuellen WWN- und virtuellen WWPN-MAC-Attributen werden die virtuellen WWN- und virtuellen WWPN-MAC-Attribute beim Konfigurieren der virtuellen FIP automatisch konfiguriert.

Durch die Verwendung der E/A-Identitätsfunktion können Sie:
- die virtuellen Adressen für Netzwerk- und Fibre Channel-Geräte (zum Beispiel NIC, CNA, FC HBA) anzeigen und konfigurieren.
- den Initiator (für iSCSI und FCoE) und die Speicher-Zieleinstellungen (für iSCSI, FCoE und FC) konfigurieren.

- die Beständigkeit oder das Löschen der konfigurierten Werte zu einem Stromausfall oder zu warmen oder kalten Systemrücksetzungen festlegen.

Die Werte für die virtuellen Adressen sowie Initiator und Speicherziele ändern sich möglicherweise je nach der Art und Weise, wie die Hauptstromversorgung beim Systemneustart durchgeführt wird und ob das NIC-, CNA- oder FC-HBA-Gerät über die Notstromversorgung mit Strom versorgt wird. Die Persistenz von E/A-Identitätseinstellungen kann auf Basis der Richtlinieneinstellung erreicht werden, die Sie unter Verwendung des iDRAC vorgenommen haben.

Nur wenn die E/A-Identitätsfunktion aktiviert ist, wird die Persistenzrichtlinie umgesetzt. Jedes Mal, wenn das System zurückgesetzt oder eingeschaltet wird, werden die Werte auf der Grundlage der Richtlinieneinstellungen beibehalten oder gelöscht.

ANMERKUNG: Nachdem die Werte gelöscht wurden, können sie erst wieder angewendet werden, nachdem der Konfigurationsjob ausgeführt wurde.

Unterstützte Karten für die E/A-Identitätsoptimierung

Die folgende Tabelle zeigt die Karten, die die E/A-Identitätsoptimierungsfunktion unterstützen.

Tabelle 43. Unterstützte Karten für die E/A-Identitätsoptimierung

Hersteller	Typ
Broadcom	• 5719 Mezz 1GB • 5720 PCIe 1 GB • 5720 bNDC 1 GB • 5720 rNDC 1 GB • 57414 PCIe 25GbE
Intel	• i350 DP FH PCIe 1GB • i350 QP PCIe 1GB • i350 QP rNDC 1GB • i350 Mezz 1GB • i350 bNDC 1GB • x520 PCIe 10GB • x520 bNDC 10GB • x520 Mezz 10GB • x520 + i350 rNDC 10GB+1GB • X710 bNDC 10GB • X710 QP bNDC 10GB • X710 PCIe 10 GB • X710 + I350 rNDC 10GB+1GB • X710 rNDC 10GB • XL710 QSFP DP LP PCIe 40GE • XL710 QSFP DP FH PCIe 40GE • X550 DP BT PCIe 2 x 10 Gb • X550 DP BT LP PCIe 2 x 10 Gb • XXV710 Fab A/B Mezz 25 Gb (*für MX-Plattformen*)
Mellanox	• ConnectX-3 Pro 10G Mezz 10GB • ConnectX-4 LX 25GE SFP DP rNDC 25GB • ConnectX-4 LX 25GE DP FH PCIe 25GB • ConnectX-4 LX 25GE DP LP PCIe 25GB • ConnectX-4 LX Fab A/B Mezz 25GB (*für MX-Plattformen*)
QLogic	• 57810 PCIe 10GB • 57810 bNDC 10GB • 57810 Mezz 10GB • 57800 rNDC 10GB+1GB • 57840 rNDC 10GB • 57840 bNDC 10GB • QME2662 Mezz FC16

Tabelle 43. Unterstützte Karten für die E/A-Identitätsoptimierung (fortgesetzt)

Hersteller	Typ
	• 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 (*für MX-Plattformen*) • QME2742-DEL Fab C Mezz FC32 (für MX-Plattformen) • QL41262HMKR-DE Fab A/B Mezz 25 Gb (*für MX-Plattformen*) • QL41232HMKR-DE Fab A/B Mezz 25 Gb (für MX-Plattformen) • QLogic 1x32Gb QLE2770 FC HBA • QLogic 2x32Gb 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 (*für MX-Plattformen*) • LPe32002-D Fab C Mezz FC32 (für MX-Plattformen) • LPe35002-M2 FC32 2-Port • LPe35000-M2 FC32 1-Port

Unterstützte NIC-Firmware-Versionen für die E/A-Identitätsoptimierung

Auf den Dell PowerEdge-Servern der 14. Generation ist die erforderliche NIC-Firmware standardmäßig verfügbar.

Die folgende Tabelle zeigt die NIC-Firmware-Versionen, die die E/A-Identitätsoptimierungsfunktion unterstützen.

Virtuelle oder Remote-zugewiesene Adresse und Persistenzrichtlinien-Verhalten, wenn iDRAC auf Remote-zugewiesenen Address-Modus oder Konsolenmodus eingestellt ist

Die folgende Tabelle beschreibt die VAM-Konfiguration (Virtual Address Management) und das Verhalten der Persistenzrichtlinie sowie die Abhängigkeiten.

Tabelle 44. Virtuelle/Remote-zugewiesene Adresse und Verhalten der Persistenzrichtlinie

Status der Remote-zugewiesenen Adressfunktion in OME Modular	In iDRAC festgelegter Modus	Funktionsstatus der E/A-Identität in iDRAC	SCP	Beständigkeitsrichtlinie	Beständigkeitsrichtlinie löschen – Virtuelle Adresse
Remote-zugewiesene Adresse aktiviert	RemoteAssignedAddress-Modus	Aktiviert	Virtuelle Adressverwaltung (VAM) ist konfiguriert.	Konfigurierte VAM besteht weiterhin	Auf Remote-zugewiesene Adresse eingestellt

Tabelle 44. Virtuelle/Remote-zugewiesene Adresse und Verhalten der Persistenzrichtlinie (fortgesetzt)

Status der Remote-zugewiesenen Adressfunktion in OME Modular	In iDRAC festgelegter Modus	Funktionsstatus der E/A-Identität in iDRAC	SCP	Beständigkeitsrichtlinie	Beständigkeitsrichtlinie löschen – Virtuelle Adresse
Remote-zugewiesene Adresse aktiviert	RemoteAssignedAddress-Modus	Aktiviert	VAM nicht konfiguriert	Auf Remote-zugewiesene Adresse eingestellt	Keine Persistenz – Hat Remote-zugewiesene Adresse
Remote-zugewiesene Adresse aktiviert	Remote-zugewiesener Adressmodus	Deaktiviert	Mit dem in Lifecycle Controller angegebenen Pfad konfiguriert	Einstellung auf Remote-zugewiesene Adresse für diesen Zyklus	Keine Persistenz – Hat Remote-zugewiesene Adresse
Remote-zugewiesene Adresse aktiviert	Remote-zugewiesener Adressmodus	Deaktiviert	VAM nicht konfiguriert	Auf Remote-zugewiesene Adresse eingestellt	Auf Remote-zugewiesene Adresse eingestellt
Remote-zugewiesene Adresse deaktiviert	Remote-zugewiesener Adressmodus	Aktiviert	VAM konfiguriert	Konfigurierte VAM besteht weiterhin	Nur Beständigkeit – Löschen ist nicht möglich.
Remote-zugewiesene Adresse deaktiviert	Remote-zugewiesener Adressmodus	Aktiviert	VAM nicht konfiguriert	Auf Hardware-MAC-Adresse eingestellt	Persistenz wird nicht unterstützt. Abhängig vom Kartenverhalten
Remote-zugewiesene Adresse deaktiviert	Remote-zugewiesener Adressmodus	Deaktiviert	Mit dem in Lifecycle Controller angegebenen Pfad konfiguriert	Lifecycle Controller-Konfiguration besteht für diesen Zyklus weiterhin	Persistenz wird nicht unterstützt. Abhängig vom Kartenverhalten
Remote-zugewiesene Adresse deaktiviert	Remote-zugewiesener Adressmodus	Deaktiviert	VAM nicht konfiguriert	Auf Hardware-MAC-Adresse eingestellt	Auf Hardware-MAC-Adresse eingestellt
Remote-zugewiesene Adresse aktiviert	Konsolenmodus	Aktiviert	VAM konfiguriert	Konfigurierte VAM besteht weiterhin	Beständigkeit und Löschen muss funktionieren
Remote-zugewiesene Adresse aktiviert	Konsolenmodus	Aktiviert	VAM nicht konfiguriert	Auf Hardware-MAC-Adresse eingestellt	Auf Hardware-MAC-Adresse eingestellt
Remote-zugewiesene Adresse aktiviert	Konsolenmodus	Deaktiviert	Mit dem in Lifecycle Controller angegebenen Pfad konfiguriert	Lifecycle Controller-Konfiguration besteht für diesen Zyklus weiterhin	Persistenz wird nicht unterstützt. Abhängig vom Kartenverhalten
Remote-zugewiesene Adresse deaktiviert	Konsolenmodus	Aktiviert	VAM konfiguriert	Konfigurierte VAM besteht weiterhin	Beständigkeit und Löschen muss funktionieren
Remote-zugewiesene Adresse deaktiviert	Konsolenmodus	Aktiviert	VAM nicht konfiguriert	Auf Hardware-MAC-Adresse eingestellt	Auf Hardware-MAC-Adresse eingestellt
Remote-zugewiesene Adresse deaktiviert	Konsolenmodus	Deaktiviert	Mit dem in Lifecycle Controller angegebenen Pfad konfiguriert	Lifecycle Controller-Konfiguration besteht für diesen Zyklus weiterhin	Persistenz wird nicht unterstützt. Abhängig vom Kartenverhalten
Remote-zugewiesene Adresse aktiviert	Konsolenmodus	Deaktiviert	VAM nicht konfiguriert	Auf Hardware-MAC-Adresse eingestellt	Auf Hardware-MAC-Adresse eingestellt

Systemverhalten für FlexAddress und E/A-Identität

Tabelle 45. System-Verhalten für FlexAddress und E/A-Identität

Typ	FlexAddress-Funktionsstatus im CMC	Funktionsstatus der E/A-Identität in iDRAC	Verfügbarkeit von Remote-Agent-VA für den Neustart-Zyklus	VA-Programmierungsquelle	Neustartzyklus-VA-Persistenzverhalten
Server mit FA-äquivalenter Persistenz	Aktiviert	Deaktiviert		FlexAddress von CMC	Gemäß FlexAddress-Spezifikation
	-, Aktiviert oder Deaktiviert	Aktiviert	Ja – Neu oder Beständig	Virtuelle Adresse des Remote-Agenten	Gemäß FlexAddress-Spezifikation
			Nein	Virtuelle Adresse gelöscht	
	Deaktiviert	Deaktiviert			
Server mit Richtlinienfunktion für VAM-Persistenz	Aktiviert	Deaktiviert		FlexAddress von CMC	Gemäß FlexAddress-Spezifikation
	Aktiviert	Aktiviert	Ja – Neu oder Beständig	Virtuelle Adresse des Remote-Agenten	Gemäß Remote-Agenten-Richtlinieneinstellung
			Nein	FlexAddress von CMC	Gemäß FlexAddress-Spezifikation
	Deaktiviert	Aktiviert	Ja – Neu oder Beständig	Virtuelle Adresse des Remote-Agenten	Gemäß Remote-Agenten-Richtlinieneinstellung
			Nein	Virtuelle Adresse gelöscht	
	Deaktiviert	Deaktiviert			

Aktivieren oder Deaktivieren der E/A-Identitätsoptimierung

Normalerweise werden die Geräte nach dem Systemstart konfiguriert und nach einem Neustart initialisiert. Sie können für einen optimierten Start die Funktion zur E/A-Identitätsoptimierung aktivieren. Wenn sie aktiviert ist, werden zwischen dem Zurücksetzen und dem Initialisieren des Geräts die virtuelle Adresse, der Initiator und die Speicherzielattribute eingestellt. Auf diese Weise wird ein zweiter BIOS-Neustart umgangen. Die Gerätekonfiguration und der Startvorgang finden im Rahmen eines einzigen Systemstarts statt, wodurch die Startzeitleistung optimiert wird.

Stellen Sie vor dem Aktivieren der E/A-Identitätsoptimierung Folgendes sicher:

- Sie verfügen über Anmelde-, Konfigurations- und Systemsteuerungsberechtigungen.
- BIOS, iDRAC und Netzwerk-Karten sind auf die neueste Firmware aktualisiert.

Nach dem Aktivieren der E/A-Identitätsoptimierungsfunktion exportieren Sie die XML-Konfigurationsprofil-Datei aus dem iDRAC, ändern Sie die erforderlichen E/A-Identitätsattribute in der SCP-Datei und importieren Sie die Datei zurück in den iDRAC.

Eine Liste der E/A-Identitätsoptimierungsattribute, die Sie in der SCP-Datei ändern können, finden Sie im Dokument *NIC-Profil* unter https://www.dell.com/support.

ANMERKUNG: Ändern Sie keine Attribute außerhalb der E/A-Identitätsoptimierung.

Aktivieren oder Deaktivieren der E/A-Identitätsoptimierung mithilfe der Webschnittstelle

So aktivieren oder deaktivieren Sie die E/A-Identitätsoptimierung:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Hardware Settings (Hardwareeinstellungen)** > **I/O Identity Optimization (E/A-Identitätsoptimierung)**.
   Die Seite **I/O Identity Optimization** (E/A-Identitätsoptimierung) wird angezeigt.

2. Klicken Sie auf die Registerkarte **I/O Identity Optimization** (E/A-Identitätsoptimierung) und wählen Sie die Option **Enable** (Aktivieren) aus, um diese Funktion zu aktivieren. Zum Deaktivieren müssen Sie diese Option deaktivieren.
3. Klicken Sie auf **Anwenden,** um die Einstellung zu übernehmen.

Aktivieren oder Deaktivieren der E/A-Identitätsoptimierung mithilfe von RACADM

Verwenden Sie zum Aktivieren der E/A-Identitätsoptimierung den folgenden Befehl:

```
racadm set idrac.ioidopt.IOIDOptEnable Enabled
```

Nach Aktivierung dieser Funktion müssen Sie das System neu starten, damit die Einstellungen wirksam werden.

Verwenden Sie zum Deaktivieren der E/A-Identitätsoptimierung den folgenden Befehl:

```
racadm set idrac.ioidopt.IOIDOptEnable Disabled
```

Verwenden Sie zum Anzeigen der Einstellungen für die E/A-Identitätsoptimierung den folgenden Befehl:

```
racadm get iDRAC.IOIDOpt
```

SSD-Verschleiß-Schwellenwerte

iDRAC bietet Ihnen die Möglichkeit, Schwellenwerte für die verbleibende Nennschreibdauer für alle SSDs und verfügbare Ersatz-NVMe PCIe SSDs zu konfigurieren.

Wenn die Werte für SSD Remaining Rated Write Endurance und NVMe PCIe SSD Available Spare unter dem Schwellenwert liegen, dann protokolliert iDRAC dieses Ereignis im LC-Protokoll und je nach Auswahl des Warnmeldungstyps führt iDRAC auch E-Mail-Warnmeldung, SNMP Trap, IPMI-Warnmeldung, Protokollierung im Remote Syslog, WS Eventing und Betriebssystemprotokoll durch.

iDRAC warnt den Nutzer, wenn die verbleibende Schreibdauer des SSD unter den festgelegten Schwellenwert fällt, so dass der Systemadministrator ein Backup des SSD erstellen oder es ersetzen kann.

Nur bei NVMe PCIe SSDs zeigt iDRAC **Available Spare** an und bietet einen Schwellenwert für die Warnung. Available Spare ist nicht verfügbar für SSDs, die hinter PERC und HBA angeschlossen sind.

Konfigurieren von SSD-Verschleißschwellenwert-Warnfunktionen über die Web-Schnittstelle

So konfigurieren Sie den Remaining Rated Write Endurance und Available Spare Alarm-Schwellenwert über die Web-Schnittstelle:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Systemeinstellungen** > **Hardwareeinstellungen** > **SSD-Verschleiß-Schwellenwerte**.
   Die Seite **SSD-Verschleiß-Schwellenwerte** wird angezeigt.
2. **Remaining Rated Write Endurance** – Sie können den Wert zwischen 1-99 % einstellen. Der Standardwert ist 10 %.
   Der Warntyp für diese Funktion ist **SSD Wear Write Endurance** und der Sicherheitswarntyp ist **Warnung** als Folge eines Schwellenereignisses.
3. **Available Spare Alert Threshold** – Sie können den Wert zwischen 1-99 % einstellen. Der Standardwert ist 10 %.
   Der Warntyp für diese Funktion ist **SSD Wear Available Spare** und der Sicherheitswarntyp ist **Warnung** als Folge eines Schwellenereignisses.

SSD-Verschleißschwellen-Alarmfunktionen mit RACADM konfigurieren

Um die verbleibende Nenn-Schreibdauer zu konfigurieren, verwenden Sie den Befehl:

```
racadm set System.Storage.RemainingRatedWriteEnduranceAlertThreshold n
```

, wobei n= 1 bis 99 %.

Um die verfügbare Reserveschwelle für den Alarm zu konfigurieren, verwenden Sie den Befehl:

```
racadm System.Storage.AvailableSpareAlertThreshold n
```

, wobei n= 1 bis 99 %.

Konfigurieren der Einstellungen für die Beständigkeitsrichtlinie

Mithilfe der E/A-Identität können Sie Richtlinien zum Verhalten für System Reset sowie Aus- und Wiedereinschalten festlegen, die die Persistenz oder Freigabe der Einstellungen für virtuelle Adresse, Initiator und Speicherziel bestimmen. Jedes einzelne Persistenzrichtlinienattribut gilt für alle Ports und Partitionen aller zutreffenden Geräte im System. Das Geräteverhalten für auxiliär-betriebene Geräte unterscheidet sich von demjenigen für nicht-auxiliär-betriebene Geräte:

ANMERKUNG: Die Funktion **Persistenzrichtlinie** kann nicht ausgeführt werden, wenn sie auf die Standardeinstellung festgelegt ist, wenn das Attribut **VirtualAddressManagement** auf **FlexAddress** (nicht für MX-Plattformen) festgelegt ist oder der Modus **RemoteAssignedAddress** (für MX-Plattformen) auf dem iDRAC festgelegt ist und wenn die FlexAddress oder die Funktion Remote-zugewiesene Adresse in CMC (nicht für MX-Plattformen) oder OME – Modular (für MX-Plattformen) deaktiviert ist, müssen Sie sicherstellen, dass Sie das Attribut **VirtualAddressManagement** auf den Modus **Konsole** im iDRAC festlegen oder Sie die FlexAddress oder die Funktion Remote-zugewiesene Adresse in CMC oder OME – Modular aktivieren.

Sie können die folgenden Beständigkeitsrichtlinien konfigurieren:

- Virtuelle Adresse: Auxiliär-betriebene Geräte
- Virtuelle Adresse: Nicht-auxiliär-betriebene Geräte
- Initiator
- Speicherziel

Stellen Sie vor dem Anwenden der Beständigkeitsrichtlinie sicher, dass:

- Sie mindestens einmal eine Bestandsaufnahme der Netzwerk-Hardware erstellen, also die Option für die System-Bestandsaufnahme beim Neustart (CSIOR) aktiviert ist.
- Sie die E/A-Identitätsoptimierung aktivieren.

Ereignisse im Lifecycle Controller-Protokoll protokolliert werden, wenn Folgendes zutrifft:

- Die E/A-Identitätsoptimierung ist aktiviert oder deaktiviert.
- Die Beständigkeitsrichtlinie wurde geändert.
- Virtuelle Adresse, Initiator- und Ziel-Werte werden basierend auf der Richtlinie eingestellt. Ein einzelner Protokolleintrag wird für die konfigurierten Geräte und die Werte protokolliert, die für diese Geräte eingestellt werden, wenn die Richtlinie angewendet wird.

Ereignismaßnahmen werden für SNMP-, E-Mail- oder WS-Ereignisbenachrichtigungen aktiviert. Protokolle sind ebenfalls in den Remote-Syslogs enthalten.

Standardwerte für die Beständigkeitsrichtlinie

Tabelle 46. Standardwerte für die Beständigkeitsrichtlinie

Beständigkeitsrichtlinie	Stromausfall	Hardwarestart	Softwareneustart
Virtuelle Adresse: Auxiliär-betriebene Geräte	Nicht ausgewählt	Ausgewählt	Ausgewählt
Virtuelle Adresse: Nicht-auxiliär-betriebene Geräte	Nicht ausgewählt	Nicht ausgewählt	Ausgewählt
Initiator	Ausgewählt	Ausgewählt	Ausgewählt
Speicherziel	Ausgewählt	Ausgewählt	Ausgewählt

ANMERKUNG: Wenn eine persistente Richtlinie deaktiviert ist und Sie die Aktion zum Verwerfen der virtuellen Adresse ausführen, wird bei der erneuten Aktivierung der persistenten Richtlinie die virtuelle Adresse nicht abgerufen. Sie müssen die virtuelle Adresse nach Aktivierung der persistenten Richtlinie erneut festlegen.

ANMERKUNG: Wenn eine Persistenzrichtlinie in Kraft ist und die virtuellen Adressen, Initiatoren oder Speicherziele auf einer CNA-Gerätepartition festgelegt sind, löschen Sie die für virtuelle Adressen, Initiatoren und Speicherziele konfigurierten Werte nicht bzw. setzen Sie sie nicht zurück, bevor Sie den Virtualisierungsmodus oder die Persönlichkeit der Partition ändern. Die Aktion wird

automatisch ausgeführt, wenn Sie die Persistenzrichtlinie deaktivieren. Sie können auch einen Konfigurationsauftrag verwenden, um die Attribute der virtuellen Adresse explizit auf null und die Werte der Initiator- und Speicherziele gemäß der Definition in Standardwerte für iSCSI-Initiator und Speicherziel auf Seite 229 zu setzen.

Konfigurieren der Richtlinieneinstellungen für die Persistenz über die iDRAC-Webschnittstelle

So konfigurieren Sie die Richtlinie für die Persistenz:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Systemeinstellungen** > **Hardwareeinstellungen** > **E/A-Identitätsoptimierung**.
2. Klicken Sie auf die Registerkarte **E/A-Identitätsoptimierung**.
3. Wählen Sie im Abschnitt **Richtlinie für die Persistenz** eine oder mehrere der folgenden Elemente für jede Persistenz-Richtlinie aus:
   - **Softwareneustart** – Die virtuelle Adresse oder die Zieleinstellungen bleiben erhalten, wenn ein Softwareneustart erforderlich ist.
   - **Hardwareneustart** – Die virtuelle Adresse oder die Zieleinstellungen bleiben erhalten, wenn ein Hardwareneustart erforderlich ist.
   - **Wechselstromverlust** – Die virtuelle Adresse oder die Zieleinstellungen bleiben erhalten, wenn ein Stromausfall eintritt.
4. Klicken Sie auf **Anwenden**.
   Die Persistenz-Richtlinien werden konfiguriert.

Konfigurieren der Persistenz-Richtlinieneinstellungen über RACADM

Um eine Richtlinie für die Persistenz festzulegen, verwenden Sie das folgende racadm-Objekt mit dem Unterbefehl **set**:

- Verwenden Sie für virtuelle Festplatten die Objekte **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyAuxPwrd** und **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyNonAuxPwrd**.
- Verwenden Sie für Initiatoren das Objekt **iDRAC.IOIDOPT.InitiatorPersistencePolicy**.
- Verwenden Sie für Speicherziele das Objekt **iDRAC.IOIDOpt.StorageTargetPersistencePolicy**.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Standardwerte für iSCSI-Initiator und Speicherziel

Die folgenden Tabellen enthalten die Liste der Standardwerte für die iSCSI-Initiator- und Speicherziele, wenn die Persistenzrichtlinien gelöscht werden.

Tabelle 47. iSCSI-Initiator – Standardwerte

iSCSI-Initiator	Standardeinstellungen im IPv4-Modus	Standardeinstellungen im IPv6-Modus
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

Tabelle 47. iSCSI-Initiator – Standardwerte (fortgesetzt)

iSCSI-Initiator	Standardeinstellungen im IPv4-Modus	Standardeinstellungen im IPv6-Modus
IscsiInitiatorIpv6PrimDns	::	::
IscsiInitiatorSecDns	0.0.0.0	::
IscsiInitiatorIpv4SecDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6SecDns	::	::
iscsiInitiatorName	Wert wurde gelöscht	Wert wurde gelöscht
IscsiInitiatorChapId	Wert wurde gelöscht	Wert wurde gelöscht
IscsiInitiatorChapPwd	Wert wurde gelöscht	Wert wurde gelöscht
IPVer	Ipv4	Ipv6

Tabelle 48. Attribute für iSCSI-Speicherziel – Standardwerte

Attribute für iSCSI-Speicherziel	Standardeinstellungen im IPv4-Modus	Standardeinstellungen im IPv6-Modus
ConnectFirstTgt	Deaktiviert	Deaktiviert
FirstTgtIpAddress	0.0.0.0	::
FirstTgtTcpPort	3260	3260
FirstTgtBootLun	0	0
FirstTgtIscsiName	Wert wurde gelöscht	Wert wurde gelöscht
FirstTgtChapId	Wert wurde gelöscht	Wert wurde gelöscht
FirstTgtChapPwd	Wert wurde gelöscht	Wert wurde gelöscht
FirstTgtIpVer	Ipv4	
ConnectSecondTgt	Deaktiviert	Deaktiviert
SecondTgtIpAddress	0.0.0.0	::
SecondTgtTcpPort	3260	3260
SecondTgtBootLun	0	0
SecondTgtIscsiName	Wert wurde gelöscht	Wert wurde gelöscht
SecondTgtChapId	Wert wurde gelöscht	Wert wurde gelöscht
SecondTgtChapPwd	Wert wurde gelöscht	Wert wurde gelöscht
SecondTgtIpVer	Ipv4	

18

Managing storage devices

Starting with iDRAC 3.15.15.15 release, iDRAC supports Boot Optimized Storage Solution (BOSS) controller in the 14th generation of PowerEdge servers. BOSS controllers are designed specifically for booting the operating system of the server. These controllers support limited RAID features and the configuration is staged.

Starting with iDRAC 4.30.30.30 release, iDRAC supports PERC 11, HBA 11, and BOSS 1.5 for AMD systems.

NOTE: BOSS controllers support only RAID level1.

NOTE: For BOSS Controllers, the complete VD information may not be available when both PD's are plugged-out and plugged-in back.

NOTE: PERC 11 and later controllers support Hardware Root of Trust (RoT).

iDRAC has expanded its agent-free management to include direct configuration of the PERC controllers. It enables you to remotely configure the storage components attached to your system at run-time. These components include RAID and non-RAID controllers and the channels, ports, enclosures, and disks attached to them. For the PowerEdge Rx4xx/Cx4xx servers, PERC 9 and PERC 10 controllers are supported. For PowerEdge Rx5xx/Cx5xx AMD platform servers, PERC 11 is supported.

The complete storage subsystem discovery, topology, health monitoring, and configuration are accomplished in the Comprehensive Embedded Management (CEM) framework by interfacing with the internal and external PERC controllers through the MCTP protocol over I2C interface. For real-time configuration, CEM supports PERC9 controllers and above. The firmware version for PERC9 controllers must be 9.1 or later.

NOTE: The Software RAID (SWRAID) is not supported by CEM and thus is not supported in the iDRAC GUI. SWRAID can be managed using either RACADM, WSMAN or Redfish.

Using iDRAC, you can perform most of the functions that are available in OpenManage Storage Management including real-time (no reboot) configuration commands (for example, create virtual disk). You can completely configure RAID before installing the operating system.

You can configure and manage the controller functions without accessing the BIOS. These functions include configuring virtual disks and applying RAID levels and hot spares for data protection. You can initiate many other controller functions such as rebuilds and troubleshooting. You can protect your data by configuring data-redundancy or assigning hot spares.

The storage devices are:

- Controllers — Most operating systems do not read and write data directly from the disks, but instead send read and write instructions to a controller. The controller is the hardware in your system that interacts directly with the disks to write and retrieve data. A controller has connectors (channels or ports) which are attached to one or more physical disks or an enclosure containing physical disks. RAID controllers can span the boundaries of the disks to create an extended amount of storage space— or a virtual disk — using the capacity of more than one disk. Controllers also perform other tasks, such as initiating rebuilds, initializing disks, and more. To complete their tasks, controllers require special software known as firmware and drivers. In order to function properly, the controller must have the minimum required version of the firmware and the drivers installed. Different controllers have different characteristics in the way they read and write data and execute tasks. It is helpful to understand these features to most efficiently manage the storage.
- Physical disks or physical devices — Reside within an enclosure or are attached to the controller. On a RAID controller, physical disks or devices are used to create virtual disks.
- Virtual disk — It is storage created by a RAID controller from one or more physical disks. Although a virtual disk may be created from several physical disks, it is viewed by the operating system as a single disk. Depending on the RAID level used, the virtual disk may retain redundant data if there is a disk failure or have particular performance attributes. Virtual disks can only be created on a RAID controller.
- Enclosure — It is attached to the system externally while the backplane and its physical disks are internal.
- Backplane — It is similar to an enclosure. In a Backplane, the controller connector and physical disks are attached to the enclosure, but it does not have the management features (temperature probes, alarms, and so on) associated with external enclosures. Physical disks can be contained in an enclosure or attached to the backplane of a system.

NOTE: In any MX chassis which contains storage sleds and compute sleds, iDRAC pertaining to any of the compute sleds in that chassis will report all storage sleds (both assigned and unassigned). If any one of the assigned or unassigned blades are in Warning or Critical heath state, the blade controller also reports the same status.

In addition to managing the physical disks contained in the enclosure, you can monitor the status of the fans, power supply, and temperature probes in an enclosure. You can hot-plug enclosures. Hot-plugging is defined as adding of a component to a system while the operating system is still running.

The physical devices connected to the controller must have the latest firmware. For the latest supported firmware, contact your service provider.

Storage events from PERC are mapped to SNMP traps and WSMan events as applicable. Any changes to the storage configurations are logged in the Lifecycle Log.

Table 49. PERC capability

PERC Capability	CEM configuration Capable Controller (PERC 9.1 or later)	CEM configuration Non-capable Controller (PERC 9.0 and lower)
Real-time	**NOTE:** For PowerEdge Rx5xx/Cx5xx servers, PERC 9, PERC 10, and PERC 11 controllers are supported. If there is no existing pending or scheduled jobs for the controller, then configuration is applied. If there are pending or scheduled jobs for that controller, then the jobs have to be cleared or you must wait for the jobs to be completed before applying the configuration at run-time. Run-time or real-time means, a reboot is not required.	Configuration is applied. An error message is displayed. Job creation is not successful and you cannot create real-time jobs using Web interface.
Staged	If all the set operations are staged, the configuration is staged and applied after reboot or it is applied at real-time.	Configuration is applied after reboot

Topics:

- Zum Verständnis von RAID-Konzepten
- Unterstützte Controller
- Unterstützte Gehäuse
- Übersicht über die unterstützten Funktionen für Speichergeräte
- Bestandsaufnahme für Speichergeräte erstellen und Speichergeräte überwachen
- Anzeigen der Speichergerätetopologie
- Verwalten von physischen Festplatten
- Verwalten von virtuellen Festplatten
- RAID-Konfigurationsfunktionen
- Verwalten von Controllern
- Managing PCIe SSDs
- Verwalten von Gehäusen oder Rückwandplatinen
- Auswählen des Betriebsmodus zum Anwenden von Einstellungen
- Anzeigen und Anwenden von ausstehenden Vorgängen
- Speicher-Geräte – Szenarien des Anwenden-Vorgangs
- Blinken oder Beenden des Blinkens der Komponenten-LEDs
- Softwareneustart

Zum Verständnis von RAID-Konzepten

Die Speicherverwaltung verwendet die Redundant Array of Independent Disks(RAID)-Technologie, um Speicherverwaltungsfunktionen bereitzustellen. Um die Speicherverwaltung verstehen zu können, müssen Sie die RAID-Konzepte verstehen sowie damit vertraut sein, wir die RAID-Controller und das Betriebssystem den Festplatten-Speicherplatz auf Ihrem System anzeigen.

Was ist RAID?

RAID ist eine Technologie zur Verwaltung der Datenspeicherung auf den physischen Festplatten, die sich in Ihrem System befinden oder damit verbunden sind. Ein Hauptaspekt von RAID ist die Fähigkeit, sich über physische Festplatten zu erstrecken, sodass die kombinierte Speicherkapazität mehrerer physischer Festplatten als ein erweiterter Festplattenspeicherplatz betrachtet werden kann. Ein anderer Hauptaspekt von RAID besteht in der Fähigkeit zur Erhaltung redundanter Daten, mit denen Daten bei einem Festplattenausfall wiederhergestellt werden können. RAID arbeitet beim Speichern und Wiederherstellen von Daten mit verschiedenen Methoden wie z. B. Striping, Datenspiegelung und Parität. Es gibt verschiedene RAID-Stufen, die jeweils unterschiedliche Methoden zur Speicherung und Wiederherstellung von Daten anwenden. Die RAID-Stufen besitzen verschiedene Eigenschaften in Bezug auf Lese-/Schreib-Leistung, Datenschutz und Speicherkapazität. Da nicht alle RAID-Stufen redundante Daten beibehalten, können einige RAID-Stufen verlorene Daten nicht wiederherstellen. Die von Ihnen ausgewählte RAID-Stufe hängt davon ab, ob Ihre Priorität bei Leistung, Schutz oder Speicherkapazität liegt.

ANMERKUNG: Die zur Implementierung von RAID verwendeten Angaben werden vom RAID Advisory Board (RAB) definiert. Obwohl das RAB die RAID-Stufen definiert, kann die kommerzielle Implementierung von RAID-Stufen durch unterschiedliche Hersteller von den tatsächlichen RAID-Spezifikationen abweichen. Die von einem bestimmten Hersteller verwendete Implementierung kann die Lese- bzw. Schreibleistung und den Grad der Datenredundanz beeinflussen.

Hardware- und Software-RAID

RAID kann entweder mit Hardware oder Software implementiert werden. Ein System, das Hardware-RAID verwendet, weist einen RAID-Controller auf, der die RAID-Stufen implementiert und Lese- bzw. Schreibvorgänge von Daten auf physischen Festplatten verarbeitet. Wenn über das Betriebssystem zur Verfügung gestelltes Software-RAID verwendet wird, implementiert das Betriebssystem die RAID-Stufen. Aus diesem Grund kann die ausschließliche Verwendung von Software-RAID die Systemleistung herabsetzen. Sie können jedoch Software-RAID zusätzlich zu Hardware-RAID-Volumes verwenden, um eine bessere Leistung und Vielseitigkeit bei der Konfiguration von RAID-Volumes bereitzustellen. Zum Beispiel kann ein Paar von Hardware-RAID 5-Volumes über zwei RAID-Controller gespiegelt werden, um RAID-Controller-Redundanz bereitzustellen.

RAID-Konzepte

RAID verwendet bestimmte Verfahren zum Schreiben von Daten auf Festplatten. Mit diesen Verfahren kann RAID für Datenredundanz oder eine höhere Leistung sorgen. Dazu gehören folgende Verfahren:

- Datenspiegelung – Duplizieren von Daten von einer physischen Festplatte auf eine andere physische Festplatte. Die Datenspiegelung sorgt für Datenredundanz, indem zwei Kopien derselben Daten auf verschiedenen physischen Festplatten gespeichert werden. Wenn eine der gespiegelten Festplatten ausfällt, kann das System weiterhin mit der intakten Festplatte betrieben werden. Beide Seiten der Spiegelung enthalten zu jeder Zeit die gleichen Daten. Eine Seite der Spiegelung kann als funktionsfähige Seite fungieren. Die Lesevorgänge einer gespiegelten RAID-Festplattengruppe sind leistungsmäßig mit einer RAID 5-Festplattengruppe vergleichbar, jedoch sind die Schreibvorgänge schneller.
- Striping – Beim Disk-Striping werden die Daten aller physischen Festplatten auf eine virtuelle Festplatte geschrieben. Jeder Stripe besteht aus fortlaufenden virtuellen Laufwerksdatenadressen, die jeder physikalischen Festplatte des virtuellen Laufwerks in gleich großen Einheiten und in einem bestimmten sequenziellen Muster zugewiesen werden. Beispiel: Wenn das virtuelle Laufwerk fünf physische Festplatten enthält, dann schreibt der Stripe Daten auf die physischen Festplatten eins bis fünf, ohne dabei eine physische Festplatte zu wiederholen. Jeder Stripe verwendet dabei auf den einzelnen physischen Festplatten die gleiche Menge an Speicherplatz. Der Teil eines Stripes, der sich auf einer einzelnen physischen Festplatte befindet, ist ein Stripe-Element. Mit Striping allein erhält man keine Datenredundanz. Wenn Striping jedoch mit Parität kombiniert wird, lässt sich Datenredundanz erzielen.
- Blockgröße – Der gesamte Speicherplatz, der von einem Stripe auf der Festplatte in Anspruch genommen wird, wobei kein Paritätslaufwerk eingeschlossen ist. Beispiel: Ein Stripe hat 64 KB Festplattenspeicherplatz und 16 KB Daten auf jeder Festplatte im Stripe. In diesem Fall beträgt die Blockgröße 64 KB und die Größe des Stripe-Elements 16 KB.
- Stripe-Element – Ein Stripe-Element ist ein Teil eines Stripes, welcher sich auf einer einzigen physischen Festplatte befindet.
- Größe des Stripe-Elements – Der Speicherplatz, den ein Stripe-Element auf der Festplatte in Anspruch nimmt. Beispiel: Ein Stripe hat 64 KB Festplattenspeicherplatz und 16 KB Daten auf jeder Festplatte im Stripe. In diesem Fall beträgt die Größe des Stripe-Elements 16 KB und die Blockgröße 64 KB.
- Parität – Parität bezeichnet redundante Daten, die unter Verwendung eines Algorithmus in Verbindung mit Striping aufrechterhalten werden. Wenn einer der gestripten Festplatten ausfällt, können die Daten mithilfe des Algorithmus anhand der Paritätsinformationen rekonstruiert werden.
- Bereich – Ein Bereich ist eine RAID-Technik, mit der Speicherplatz von Gruppen physischer Festplatten in einer virtuellen RAID 10, 50, oder 60 Festplatte kombiniert wird.

RAID-Level

Jede RAID-Stufe verwendet eine Kombination aus Datenspiegelung, Striping und Parität, um Datenredundanz oder eine verbesserte Lese- und Schreibleistung bereitzustellen. Details zu den einzelnen RAID-Stufen finden Sie unter Auswählen der RAID-Stufen.

Datenspeicher-Organisation zur erhöhten Verfügbarkeit und Leistung

RAID stellt verschiedene Methoden oder RAID-Stufen zur Organisation des Speichers bereit. Einige RAID-Stufen behalten redundante Daten aufrecht, sodass Sie Daten nach einem Laufwerkausfall wiederherstellen können. Verschiedene RAID-Stufen verbessern oder reduzieren die E/A-Leistung (Lesen und Schreiben) des Systems.

Die Aufrechterhaltung redundanter Daten erfordert die Verwendung zusätzlicher physischer Laufwerke. Die Wahrscheinlichkeit eines Laufwerkausfalls steigt mit der Anzahl von Laufwerken. Durch die Unterschiede bei der E/A-Leistung und Redundanz ist eine bestimmte RAID-Stufe je nach Anwendungen in der Betriebsumgebung und den gespeicherten Daten möglicherweise besser geeignet als alle anderen.

Wenn eine RAID-Stufe ausgewählt wird, treffen die folgenden Leistungs- und Kostenerwägungen zu:

- Verfügbarkeit oder Fehlertoleranz – Verfügbarkeit oder Fehlertoleranz beziehen sich auf die Fähigkeit eines Systems, den Betrieb aufrechtzuerhalten und Zugriff auf Daten bereitzustellen, selbst wenn eine der Systemkomponenten fehlerhaft ist. In RAID-Volumes wird Verfügbarkeit oder Fehlertoleranz durch die Beibehaltung von redundanten Daten erzielt. Redundante Daten umfassen Spiegelungen von Daten (duplizierte Daten) und Paritätsinformationen (Daten werden mit einem Algorithmus rekonstruiert).
- Leistung – Lese- und Schreibleistung kann je nach der ausgewählten RAID-Stufe erhöht oder reduziert werden. Einige RAID-Stufen eignen sich eventuell besser für bestimmte Anwendungen.
- Kosteneffizienz – Aufrechterhaltung der redundanten Daten oder Paritätsinformationen, die den RAID-Volumes zugeordnet sind, erfordert zusätzlichen Speicherplatz. Wenn die Daten temporär, leicht reproduzierbar oder nicht unbedingt notwendig sind, sind die höheren Kosten für die Datenredundanz möglicherweise nicht gerechtfertigt.
- MTBF (Mean Time Between Failure, mittlere Betriebsdauer zwischen Ausfällen) – Bei der Verwendung zusätzlicher Laufwerke zur Aufrechterhaltung von Datenredundanz ist auch die Wahrscheinlichkeit eines Laufwerkausfalls höher. Obwohl dies in Fällen, in denen redundante Daten erforderlich sind, nicht verhindert werden kann, hat es Auswirkungen auf die Arbeitsauslastung der Systemsupportmitarbeiter Ihrer Organisation.
- Volume – Volume bezieht sich auf ein einzelnes virtuelle Nicht-RAID-Laufwerk. Sie können Volumes mithilfe externer Dienstprogramme wie O-ROM <Strg> <r> erstellen. Storage Management bietet keine Unterstützung für die Erstellung von Volumes. Sie können jedoch Volumes anzeigen und Laufwerke dieser Volumens für die Erstellung neuer virtueller Laufwerke oder OCE (Online Capacity Expansion OCE) vorhandener virtueller Laufwerke verwenden, vorausgesetzt, es ist genügend freier Speicherplatz vorhanden.

Auswählen der RAID-Stufen

RAID kann zur Steuerung des Datenspeichers auf mehreren Laufwerken verwendet werden. Jede RAID-Stufe oder -Verkettung verfügt über unterschiedliche Leistungs- und Datenschutzeigenschaften.

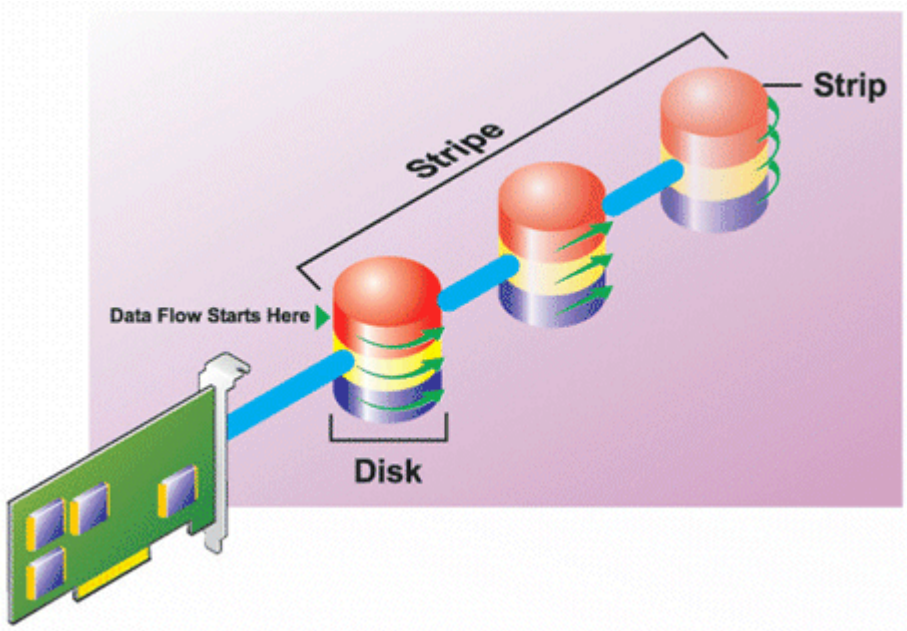
ANMERKUNG: Die H3xx-PERC-Controller bieten keine Unterstützung für die RAID-Stufen 6 und 60.

Die folgenden Themen enthalten spezifische Informationen zur Art und Weise wie jede RAID-Stufe Daten speichert, sowie als auch deren spezifische Leistungs- und Schutzeigenschaften:

- RAID-Stufe 0 (Striping)
- RAID-Stufe 1 (Datenspiegelung)
- RAID-Stufe 5 (Striping mit verteilter Parität)
- RAID-Stufe 6 (Striping mit zusätzlicher verteilter Parität)
- RAID-Stufe 50 (Striping über RAID 5-Sets)
- RAID-Stufe 60 (Striping über RAID 6-Sets)
- RAID-Stufe 10 (Striping über gespiegelte Sets)

RAID-Stufe 0 - Striping

RAID 0 verwendet Daten-Striping, wobei Daten in gleich großen Segmenten über die physischen Festplatten geschrieben werden. RAID 0 bietet keine Datenredundanz.

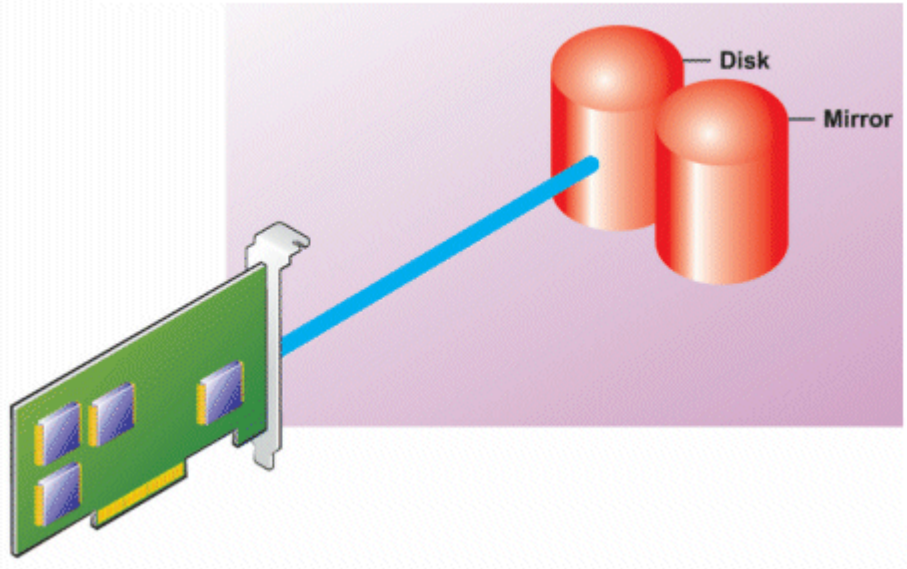


RAID 0-Eigenschaften:

- Gruppiert *n* Festplatten als eine große virtuelle Festplatte mit einer Kapazität von (kleinste Festplattengröße) **n* Festplatten.
- Daten werden auf den Festplatten abwechselnd gespeichert.
- Es werden keine redundanten Daten gespeichert. Wenn eine Festplatte fehlerhaft wird, fällt die große virtuelle Festplatte, ohne eine Möglichkeit zur Neuerstellung der Daten, aus.
- Bessere Lese- und Schreibleistung.

RAID-Stufe 1 (Spiegelung)

RAID 1 stellt die einfachste Art und Weise dar, redundante Daten aufrechtzuerhalten. Mit RAID 1 werden Daten auf eine oder mehrere physische Festplatten gespiegelt oder dupliziert. Wenn eine physische Festplatte ausfällt, werden die Daten unter Verwendung der Daten der anderen Seite der Spiegelung wiederhergestellt.



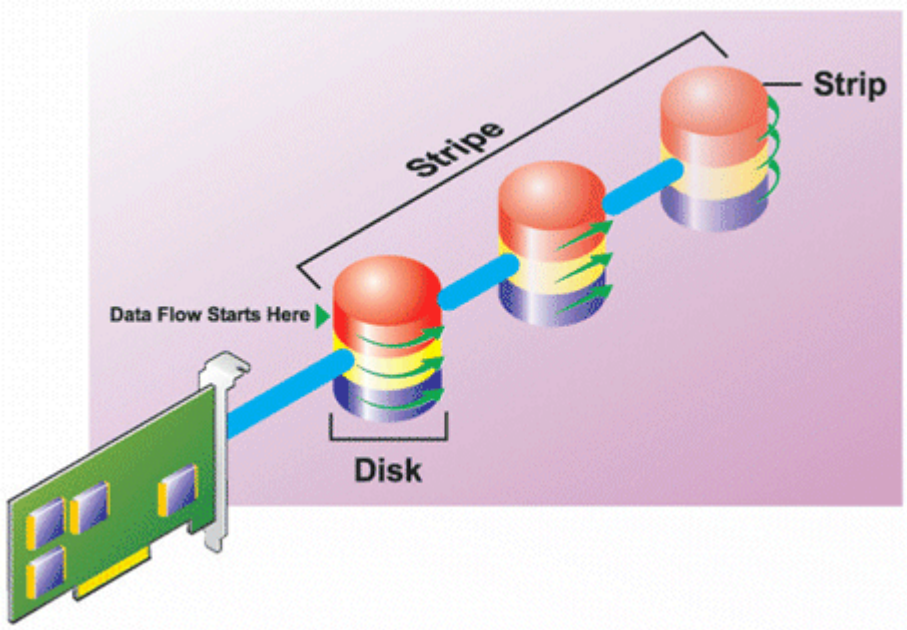
RAID 1-Eigenschaften:

- Gruppiert *n* + *n* Festplatten zu einer großen virtuellen Festplatte mit einer Kapazität von *n* Festplatten. Controller, die derzeit von Storage Management unterstützt werden, erlauben bei der Erstellung von RAID 1 die Auswahl von zwei Festplatten. Da diese Festplatten gespiegelt werden, ist die Gesamtspeicherkapazität gleich der einer Festplatte.
- Die Daten werden auf den beiden Festplatten repliziert.

- Wenn eine Festplatte ausfällt, funktioniert die virtuelle Festplatte weiterhin. Die Daten werden von der verbleibenden gespiegelten Festplatte gelesen.
- Bessere Leseleistung, aber etwas langsamere Schreibleistung.
- Redundanz zum Schutz der Daten.
- RAID 1 ist in Bezug auf Festplattenspeicherplatz teurer, da die doppelte Anzahl von Festplatten verwendet wird, die zum Speichern der Daten ohne Redundanz erforderlich wären.

RAID-Stufe 5 (Striping mit verteilter Parität)

RAID 5 ermöglicht Datenredundanz durch Verwendung von Daten-Striping in Kombination mit Paritätsinformationen. Statt eine physische Festplatte für Parität zu reservieren, erfolgt Striping für die Paritätsinformationen auf allen physischen Festplatten in der Festplattengruppe.

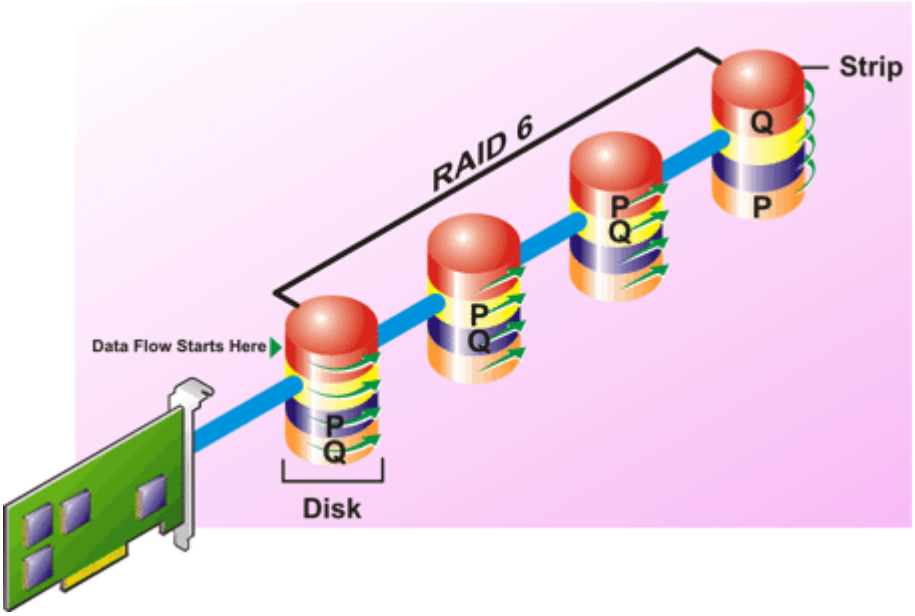


RAID 5-Eigenschaften:

- Gruppiert *n* Festplatten als eine große virtuelle Festplatte mit einer Kapazität von (*n*-1) Festplatten.
- Redundante Informationen (Parität) werden abwechselnd auf allen Festplatten gespeichert.
- Wenn eine Festplatte ausfällt, funktioniert die virtuelle Festplatte weiterhin, aber sie wird in einem herabgesetzten Zustand betrieben. Die Daten werden von den verbleibenden Festplatten rekonstruiert.
- Bessere Leseleistung, aber langsamere Schreibleistung.
- Redundanz zum Schutz der Daten.

RAID-Stufe 6 (Striping mit zusätzlicher verteilter Parität)

RAID 6 ermöglicht Datenredundanz durch Verwendung von Daten-Striping in Kombination mit Paritätsinformationen. Wie bei RAID 5 wird die Parität innerhalb jedes Stripe verteilt. RAID 6 verwendet jedoch eine zusätzliche physische Festplatte für Parität, sodass jeder Stripe in der Festplattengruppe zwei Festplattenblöcke mit Paritätsinformationen verwaltet. Durch diese zusätzliche Parität sind die Daten auch dann geschützt, wenn zwei Festplatten ausfallen. In der folgenden Abbildung sind die beiden Sätze von Paritätsinformationen **P** und **Q**.



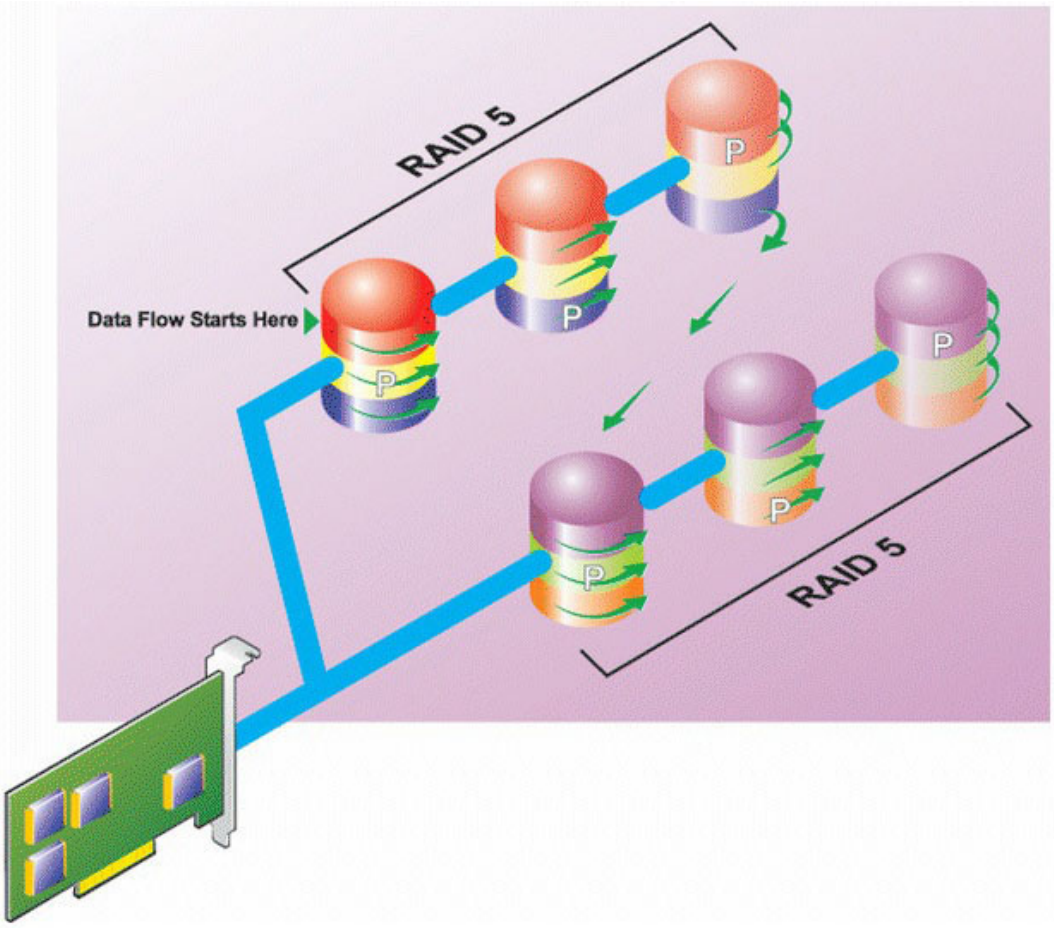
RAID 6-Eigenschaften:

- Gruppiert *n* Festplatten als eine große virtuelle Festplatte mit einer Kapazität von (*n*-2) Festplatten.
- Redundante Informationen (Parität) werden abwechselnd auf allen Festplatten gespeichert.
- Die virtuelle Festplatte bleibt bei bis zu zwei ausgefallenen Festplatten funktional. Die Daten werden von den verbleibenden Festplatten rekonstruiert.
- Bessere Leseleistung, aber langsamere Schreibleistung.
- Erhöhte Redundanz zum Schutz der Daten.
- Für Parität sind zwei Festplatten pro Bereich erforderlich. RAID 6 ist teurer in Bezug auf Festplatten-Speicherplatz.

RAID-Stufe 50 (Striping über RAID 5-Sets)

Bei RAID 50 erstreckt sich Striping über mehr als einen Bereich physischer Festplatten. Eine RAID 5-Festplattengruppe, die mit drei physischen Festplatten implementiert ist und dann mit einer Festplattengruppe von drei weiteren physischen Festplatten fortfährt, wäre beispielsweise ein RAID 50.

RAID 50 kann auch implementiert werden, wenn die Hardware es nicht direkt unterstützt. In diesem Fall können Sie mehr als eine virtuelle RAID 5-Festplatte implementieren und dann die RAID 5-Festplatten in dynamische Festplatten umwandeln. Sie können dann einen dynamischen Datenträger erstellen, der sich über alle virtuellen RAID 5-Festplatten erstreckt.

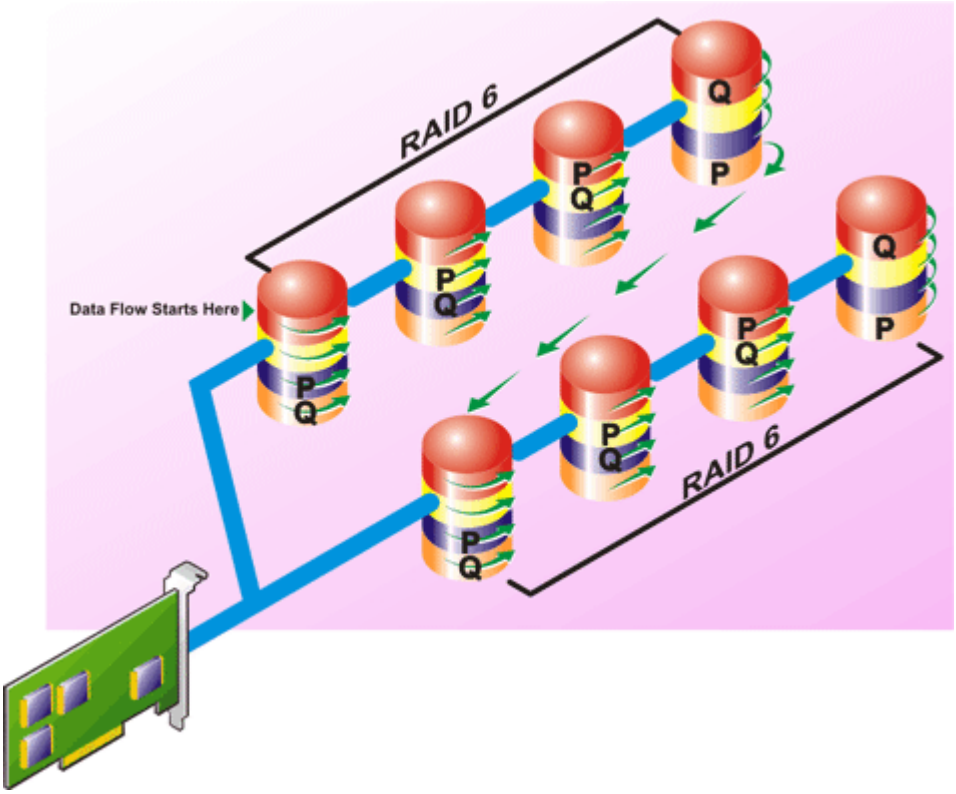


RAID 50-Eigenschaften:

- Gruppiert *n***s* Festplatten als eine große virtuelle Festplatte mit einer Kapazität von *s**(*n*-1) Festplatten, wobei *s* die Anzahl von Bereichen und *n* die Anzahl von Festplatten innerhalb jeden Bereiches darstellt.
- Redundante Informationen (Parität) werden abwechselnd auf allen Festplatten jedes RAID 5-Bereiches gespeichert.
- Bessere Leseleistung, aber langsamere Schreibleistung.
- Erfordert die gleiche Menge an Paritätsinformationen wie RAID 5.
- Die Daten werden über alle Bereiche gestriped. RAID 50 ist in Bezug auf Festplattenspeicherplatz teurer.

RAID-Stufe 60 (Striping über RAID 6-Sets)

Bei RAID 60 erstreckt sich Striping über mehr als einen Bereich physischer Festplatten, die als RAID 6 konfiguriert sind. Beispiel: Eine RAID 6-Festplattengruppe, die mit vier physischen Festplatten implementiert ist und dann mit einer Festplattengruppe von vier weiteren physischen Festplatten fortfährt, wäre beispielsweise ein RAID 60.

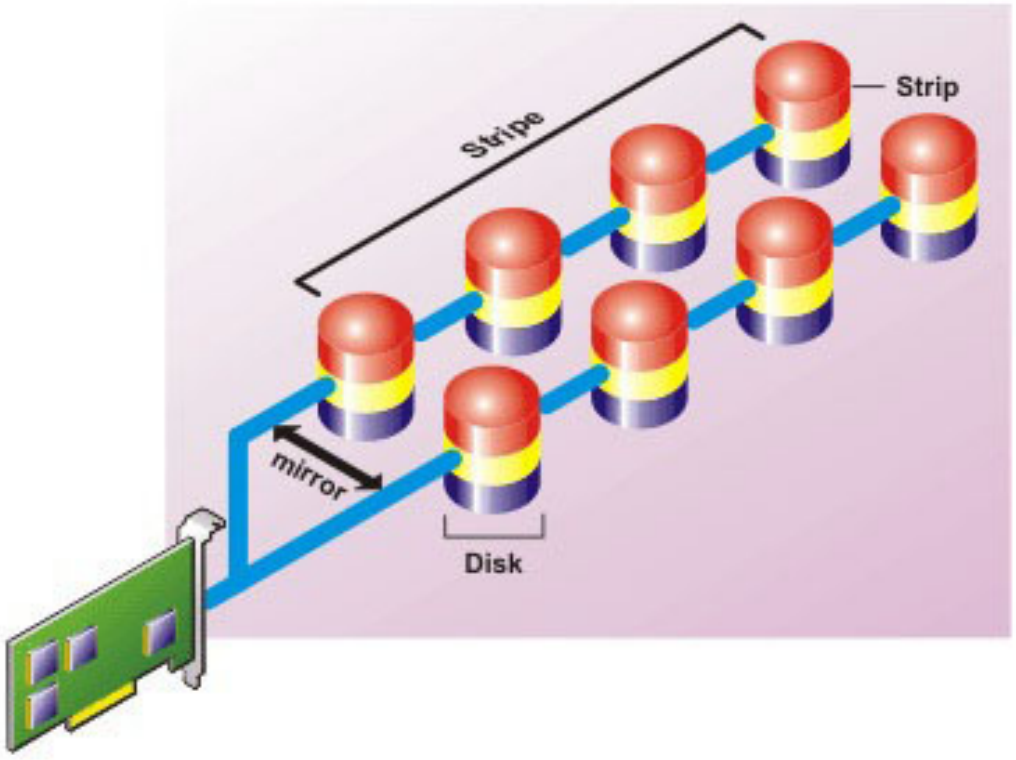


RAID 60-Eigenschaften:

- Gruppiert *n***s* Festplatten als eine große virtuelle Festplatte mit einer Kapazität von *s**(*n*-2) Festplatten, wobei *s* die Anzahl von Bereichen und *n* die Anzahl von Festplatten innerhalb jeden Bereiches darstellt.
- Redundante Informationen (Parität) werden abwechselnd auf allen Festplatten jedes RAID 6-Bereiches gespeichert.
- Bessere Leseleistung, aber langsamere Schreibleistung.
- Erhöhte Redundanz bietet höhere Datensicherung als ein RAID 50.
- Erfordert verhältnismäßig die gleiche Menge an Paritätsinformationen wie RAID 6.
- Für Parität sind zwei Festplatten pro Bereich erforderlich. RAID 60 ist in Bezug auf Festplattenspeicherplatz teurer.

RAID-Stufe 10 (Striping mit Spiegelung)

Für das RAB gilt RAID-Stufe 10 als eine Implementierung von RAID-Stufe 1. RAID 10 kombiniert gespiegelte physische Festplatten (RAID 1) und Daten-Striping (RAID 0). Mit RAID 10 erfolgt Daten-Striping über mehrere physische Festplatten. Die Festplattengruppe, für die Striping erfolgt ist, wird dann auf einen anderen Satz physischer Festplatten gespiegelt. RAID 10 kann als eine *Spiegelung von Stripes* betrachtet werden.



RAID 10-Eigenschaften:

- Gruppiert *n* Festplatten als eine große virtuelle Festplatte mit einer Kapazität von (*n*/2) Festplatten, wobei *n* für eine gerade Ganzzahl steht.
- Das Striping gespiegelter Daten erfolgt über Sätze physischer Festplatten. Diese Stufe bietet Redundanz durch Spiegelung.
- Wenn eine Festplatte ausfällt, funktioniert die virtuelle Festplatte weiterhin. Die Daten werden von der verbleibenden gespiegelten Festplatte gelesen.
- Verbesserte Lese- und Schreibleistung.
- Redundanz zum Schutz der Daten.

RAID-Level-Leistung vergleichen

In der folgenden Tabelle werden die Leistungseigenschaften der am häufigsten verwendeten RAID-Klassen verglichen. Diese Tabelle bietet allgemeine Richtlinien zur Auswahl einer RAID-Klasse. Schätzen Sie Ihre spezifischen Umgebungsanforderungen ab, bevor Sie eine RAID-Klasse wählen.

Tabelle 50. RAID-Level-Leistungsvergleich

RAID-Stufe	Datenredundanz	Leseleistung	Schreibleistung	Neuerstellungsleistung	Mindestanzahl von erforderlichen Festplatten	Vorschläge zur Verwendung
RAID 0	Keine	Sehr gut	Sehr gut	k. A.	N	Nicht-kritische Daten
RAID 1	Ausgezeichnet	Sehr gut	Gut	Gut	(N = 1)	Kleine Datenbanken, Datenbank-Protokolle und kritische Informationen
RAID-5	Gut	Sequenzielles Lesen: Gut.	Mittelmäßig, es sei denn Rückschreiben in	Mittelmäßig	N + 1 (N = wenigstens zwei Festplatten)	Datenbanken und andere lese-

Tabelle 50. RAID-Level-Leistungsvergleich (fortgesetzt)

RAID-Stufe	Datenredundanz	Leseleistung	Schreibleistung	Neuerstellungsleistung	Mindestanzahl von erforderlichen Festplatten	Vorschläge zur Verwendung
		Direktes Lesen: Sehr gut	Cache wird verwendet			intensive direkte Verwendungen
RAID-10	Ausgezeichnet	Sehr gut	Mittelmäßig	Gut	2N x X	Daten-intensive Umgebungen (große Datensätze)
RAID 50	Gut	Sehr gut	Mittelmäßig	Mittelmäßig	N + 2 (N = wenigstens 4)	Mittelgroße direkte oder Daten-intensive Verwendungen
RAID-6	Ausgezeichnet	Sequenzielles Lesen: Gut. Direktes Lesen: Sehr gut	Mittelmäßig, es sei denn Rückschreiben in Cache wird verwendet	Schlecht	N + 2 (N = wenigstens zwei Festplatten)	Kritische Informationen. Datenbanken und andere lese-intensive direkte Verwendungen
RAID 60	Ausgezeichnet	Sehr gut	Mittelmäßig	Schlecht	N + 2 (N = wenigstens 2)	Kritische Informationen. Mittelgroße direkte oder Daten-intensive Verwendungen
N = Anzahl physischer Festplatten X = Anzahl von RAID-Sets						

Unterstützte Controller

Unterstützte RAID-Controller

Die iDRAC-Schnittstellen unterstützen die folgenden BOSS-Controller:

- BOSS-S1 Adapter
- BOSS-S1 Modular (für Blade-Server)
- BOSS-S2 Adapter

Die iDRAC-Schnittstellen unterstützen die folgenden PERC11-Controller:

- PERC H755 Adapter
- PERC H755 Front
- PERC H755N Front

Die iDRAC-Schnittstellen unterstützen die folgenden PERC10-Controller:

- PERC H740P Mini
- PERC H740P-Adapter
- PERC H840-Adapter
- PERC H745P MX

Die iDRAC-Schnittstellen unterstützen die folgenden PERC9-Controller:

- PERC H330 Mini
- PERC H330-Adapter
- PERC H730P Mini
- PERC H730P-Adapter
- PERC H730P MX

Unterstützte Nicht-RAID-Controller

Die iDRAC-Schnittstelle unterstützt externe 12-Gbit/s-SAS-HBA-Controller und HBA330 Mini- oder Adapter-Controller.

iDRAC unterstützt HBA330 MMZ, HBA330 MX Adapter.

Unterstützte Gehäuse

iDRAC unterstützt MD1400- und MD1420-Gehäuse.

ANMERKUNG: Redundant Array of Inexpensive Disks (RBODs), die mit HBA-Controllern verbunden sind, werden nicht unterstützt.

ANMERKUNG: Bei PERC H480 mit Version 10.1 oder höher unterstützt die Firmware bis zu vier Gehäuse je Anschluss.

Übersicht über die unterstützten Funktionen für Speichergeräte

Die folgenden Tabellen enthalten die Funktionen, die über iDRAC durch die Speichergeräte unterstützt werden.

Tabelle 51. Unterstützte Funktionen für Speichercontroller

Funktion	PERC 11			PERC 10			PERC 9				
	H755 Front	H755N Front	H755 Adapter	H740P Mini	H740P Adapter	H840 Adapter	H330 Mini	H330 Adapter	H730P Mini	H730P Adapter	FD33xS
Physisches Laufwerk als einen globalen Hot Spare zuweisen oder die Zuweisung rückgängig machen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
In RAID konvertieren	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar
Zu RAID/Nicht-RAID konvertieren,	Echtzeit (wandelt das Laufwerk in ein nicht-RAID-ePD-PT-Volume um)	Echtzeit (wandelt das Laufwerk in ein nicht-RAID-ePD-PT-Volume um)	Echtzeit (wandelt das Laufwerk in ein nicht-RAID-ePD-PT-Volume um)	Echtzeit (wird nur im eHBA-Controller-Modus unterstützt, wandelt das Laufwerk in ein nicht-RAID-ePD-PT-Volume um)	Echtzeit (wird nur im eHBA-Controller-Modus unterstützt, wandelt das Laufwerk in ein nicht-RAID-ePD-PT-Volume um)	Echtzeit (wird nur im eHBA-Controller-Modus unterstützt, wandelt das Laufwerk in ein nicht-RAID-ePD-PT-Volume um)	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit

Tabelle 51. Unterstützte Funktionen für Speichercontroller (fortgesetzt)

Funktion	PERC 11			PERC 10			PERC 9				
	H755 Front	H755N Front	H755 Adapter	H740P Mini	H740P Adapter	H840 Adapter	H330 Mini	H330 Adapter	H730P Mini	H730P Adapter	FD33xS
Neu erstellen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Neuerstellung abbrechen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Virtuelle Laufwerke erstellen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Virtuelle Laufwerke umbenennen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Cache-Richtlinien für virtuelle Laufwerke bearbeiten	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Konsistenz der virtuellen Laufwerke überprüfen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Konsistenzüberprüfung abbrechen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Virtuelle Laufwerke initialisieren	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Initialisierung abbrechen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Virtuelle Laufwerke verschlüsseln	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Nicht anwendbar	Nicht anwendbar	Echtzeit	Echtzeit	Echtzeit
Dedizierten Hot Spare	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit

Tabelle 51. Unterstützte Funktionen für Speichercontroller (fortgesetzt)

Funktion	PERC 11			PERC 10			PERC 9				
	H755 Front	H755N Front	H755 Adapter	H740P Mini	H740P Adapter	H840 Adapter	H330 Mini	H330 Adapter	H730P Mini	H730P Adapter	FD33xS
zuweisen und Zuweisung rückgängig machen											
Virtuelle Laufwerke löschen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Hintergrundinitialisierung abbrechen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Online-Kapazitätserweiterung	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
RAID-Level-Migration	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Verwerfen des beibehaltenen Cache	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Nicht anwendbar	Nicht anwendbar	Echtzeit	Echtzeit	Echtzeit
Patrol Read-Modus einstellen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Manueller Patrol Read-Modus	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Patrol Read – Nicht konfigurierte Bereiche	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit (nur in Web-Schnittstelle)	Echtzeit (nur in Web-Schnittstelle)	Echtzeit (nur in Web-Schnittstelle)	Echtzeit (nur in Web-Schnittstelle)	Echtzeit (nur in Web-Schnittstelle)
Konsistenzprüfungsmodus	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Copyback-Betriebsart	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Lastausgleichsmodus	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit

Tabelle 51. Unterstützte Funktionen für Speichercontroller (fortgesetzt)

Funktion	PERC 11			PERC 10			PERC 9				
	H755 Front	H755N Front	H755 Adapter	H740P Mini	H740P Adapter	H840 Adapter	H330 Mini	H330 Adapter	H730P Mini	H730P Adapter	FD33xS
Konsistenzüberprüfungsrate	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Neuerstellungsrate	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Hintergrundinitialisierungsrate	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Rekonstruktionsrate	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Fremdkonfiguration importieren	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Fremdkonfiguration automatisch importieren	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Fremdkonfiguration löschen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Controller-Konfiguration zurücksetzen	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Sicherheitsschlüssel erstellen oder ändern	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Nicht anwendbar	Nicht anwendbar	Echtzeit	Echtzeit	Echtzeit
Secure Enterprise Key Manager	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar
Bestandsaufnahme und die Remote-Überwachung des Status von PCIe	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar

Tabelle 51. Unterstützte Funktionen für Speichercontroller (fortgesetzt)

Funktion	PERC 11			PERC 10			PERC 9				
	H755 Front	H755N Front	H755 Adapter	H740P Mini	H740P Adapter	H840 Adapter	H330 Mini	H330 Adapter	H730P Mini	H730P Adapter	FD33xS
SSD-Geräte											
Entfernen der PCIe SSD vorbereiten	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar
Daten von PCIe-SSD sicher löschen	Nicht anwendbar	Echtzeit	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar
Rückwandplatinen-Modus konfigurieren (geteilt/vereint)	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Komponenten-LEDs blinken oder Blinken beenden	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit	Echtzeit
Controller-Modus ändern	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt	Bereitgestellt
T10PI-Unterstützung für virtuelle Laufwerke	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar

ANMERKUNG: Zusätzliche Unterstützung für

- eHBA-Modus für PERC 10.2-Firmware (oder höher), die die Umwandlung in Nicht-RAID-Festplatten unterstützt
- Umwandlung des Controllers in HBA-Modus
- Uneven Span für RAID 10

Tabelle 52. Unterstützte Funktionen von Speicher-Controllern für MX-Plattformen

Funktionen	PERC 11	PERC 10	PERC 9
	H755 MX	H745P MX	H730P MX
Virtuelle Laufwerke initialisieren	Echtzeit	Echtzeit	Echtzeit
Initialisierung abbrechen	Echtzeit	Echtzeit	Echtzeit
Virtuelle Laufwerke verschlüsseln	Echtzeit	Echtzeit	Echtzeit

Tabelle 52. Unterstützte Funktionen von Speicher-Controllern für MX-Plattformen (fortgesetzt)

Funktionen	PERC 11	PERC 10	PERC 9
	H755 MX	H745P MX	H730P MX
Dedizierten Hot Spare zuweisen und Zuweisung rückgängig machen	Echtzeit	Echtzeit	Echtzeit
Virtuelle Laufwerke löschen	Echtzeit	Echtzeit	Echtzeit
Hintergrundinitialisierung abbrechen	Echtzeit	Echtzeit	Echtzeit
Online-Kapazitätserweiterung	Echtzeit	Echtzeit	Echtzeit
RAID-Level-Migration	Echtzeit	Echtzeit	Echtzeit
Verwerfen des beibehaltenen Cache	Echtzeit	Echtzeit	Echtzeit
Patrol Read-Modus einstellen	Echtzeit	Echtzeit	Echtzeit
Manueller Patrol Read-Modus	Echtzeit	Echtzeit	Echtzeit
Patrol Read – Nicht konfigurierte Bereiche	Echtzeit	Echtzeit	Echtzeit (nur in Web-Schnittstelle)
Konsistenzprüfungsmodus	Echtzeit	Echtzeit	Echtzeit
Copyback-Betriebsart	Echtzeit	Echtzeit	Echtzeit
Lastausgleichsmodus	Echtzeit	Echtzeit	Echtzeit
Konsistenzüberprüfungsrate	Echtzeit	Echtzeit	Echtzeit
Neuerstellungsrate	Echtzeit	Echtzeit	Echtzeit
Hintergrundinitialisierungsrate	Echtzeit	Echtzeit	Echtzeit
Rekonstruktionsrate	Echtzeit	Echtzeit	Echtzeit
Fremdkonfiguration importieren	Echtzeit	Echtzeit	Echtzeit
Fremdkonfiguration automatisch importieren	Echtzeit	Echtzeit	Echtzeit
Fremdkonfiguration löschen	Echtzeit	Echtzeit	Echtzeit
Controller-Konfiguration zurücksetzen	Echtzeit	Echtzeit	Echtzeit
Sicherheitsschlüssel erstellen oder ändern	Echtzeit	Echtzeit	Echtzeit
Bestandsaufnahme und die Remote-Überwachung des Status von PCIe SSD-Geräte	Echtzeit	Nicht anwendbar	Nicht anwendbar
Entfernen der PCIe SSD vorbereiten	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar
Daten von PCIe-SSD sicher löschen	Echtzeit	Nicht anwendbar	Nicht anwendbar
Rückwandplatinen-Modus konfigurieren (geteilt/vereint)	Echtzeit	Nicht anwendbar	Nicht anwendbar
Komponenten-LEDs blinken oder Blinken beenden	Echtzeit	Echtzeit	Echtzeit
Controller-Modus ändern	Nicht anwendbar	Nicht anwendbar	Bereitgestellt

Tabelle 52. Unterstützte Funktionen von Speicher-Controllern für MX-Plattformen (fortgesetzt)

Funktionen	PERC 11	PERC 10	PERC 9
	H755 MX	H745P MX	H730P MX
T10PI-Unterstützung für virtuelle Laufwerke	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar

ANMERKUNG: H745P MX unterstützt den eHBA-Modus mit PERC 10.2 und höher.

Tabelle 53. Unterstützte Funktionen für Speichergeräte

Funktion	PCIe-SSD-Festplatten	BOSS S1	BOSS S2
Virtuelle Laufwerke erstellen	Nicht anwendbar	Bereitgestellt	Bereitgestellt
Controller-Konfiguration zurücksetzen	Nicht anwendbar	Bereitgestellt	Bereitgestellt
Schnellinitialisierung	Nicht anwendbar	Bereitgestellt	Bereitgestellt
Virtuelle Laufwerke löschen	Nicht anwendbar	Bereitgestellt	Bereitgestellt
Vollinitialisierung	Nicht anwendbar	Nicht anwendbar	Nicht anwendbar
Bestandsaufnahme und die Remote-Überwachung des Status von PCIe SSD-Geräte	Echtzeit	Nicht anwendbar	Nicht anwendbar
Entfernen der PCIe SSD vorbereiten	Echtzeit	Nicht anwendbar	Nicht anwendbar
Daten von PCIe-SSD sicher löschen	Bereitgestellt	Nicht anwendbar	Nicht anwendbar
Komponenten-LEDs blinken oder Blinken beenden	Echtzeit	Nicht anwendbar	Echtzeit
Hotplugging von Laufwerken	Echtzeit	Nicht anwendbar	Echtzeit

Bestandsaufnahme für Speichergeräte erstellen und Speichergeräte überwachen

Sie können den Zustand remote überwachen und die Bestandsliste für die folgenden Comprehensive Embedded Management (CEM)-aktivierten Speichergeräte im Managed System über die iDRAC-Webschnittstelle anzeigen:

- RAID-Controller, Nicht-RAID-Controller, BOSS-Controller und PCIe-Extender
- Gehäuse mit Gehäuseverwaltungsmodulen (EMMs), Netzteile, Lüftersonde und Temperatursonde
- Physische Laufwerke
- Virtuelle Laufwerke
- Batterien

Es werden auch Informationen zu kürzlich aufgetretenen Speicherereignissen und zur Topologie der Speichergeräte angezeigt.

Für Speicherereignisse werden Warnungen und SNMP-Traps angezeigt. Die Ereignisse werden im Lifecycle-Protokoll aufgezeichnet.

ANMERKUNG:

- Wenn Sie den WSMan-Befehl der Gehäuseansicht auf einem System aufzählen, während ein Netzteilkabel entfernt wird, wird der primäre Status des Gehäuses als **Funktionsfähig** und nicht als **Warnung** angezeigt.
- Stellen Sie für eine genaue Bestandsaufnahme der BOSS-Controller sicher, dass der Vorgang zum Erfassen des Systeminventars beim Neustart (CSIOR) abgeschlossen ist. CSIOR ist standardmäßig aktiviert.
- Das Speicherintegritäts-Rollup folgt denselben Konventionen des Dell EMC OpenManage-Produkts. Weitere Informationen finden Sie unter *OpenManage Server Administrator – Benutzerhandbuch* verfügbar unter https://www.dell.com/openmanagemanuals.

- Physische Festplatten in einem System mit mehreren Rückwandplatinen werden möglicherweise unter einer anderen Rückwandplatine aufgelistet. Verwenden Sie die Blinkfunktion, um die Festplatten zu identifizieren.
- FQDD bestimmter Rückwandplatinen ist möglicherweise nicht identisch mit der Software- und Hardware-Bestandsaufnahme.
- Lifecycle-Protokoll für PERC-Controller ist nicht verfügbar, wenn die letzten Ereignisse des PERC-Controllers verarbeitet werden, dies beeinträchtigt die Funktionalität nicht. Die Verarbeitung vergangener Ereignisse kann je nach Konfiguration variieren

Netzwerkgeräte über die Weboberfläche überwachen

So zeigen Sie die Speichergeräteinformationen über die Weboberfläche an:

- Gehen Sie zu **Speicherung** > **Übersicht** > **Zusammenfassung**, um die Zusammenfassung der Speicherkomponenten und die kürzlich protokollierten Ereignisse anzuzeigen. Diese Seite wird automatisch alle 30 Sekunden aktualisiert.
- Gehen Sie zu **Speicherung** > **Übersicht** > **Controller,** um Informationen zu den RAID-Controllern anzuzeigen. Die Seite **Controller** wird angezeigt.
- Gehen Sie zu **Speicherung** > **Übersicht** > **Physische Laufwerke,** um Informationen zu den physischen Laufwerken anzuzeigen. Daraufhin wird die Seite **Physische Laufwerke** angezeigt.
- Gehen Sie zu **Speicherung** > **Übersicht** > **Virtuelle Laufwerke,** um Informationen zu den virtuellen Laufwerken anzuzeigen. Die Seite **Virtuelle Laufwerke** wird angezeigt.
- Gehen Sie zu **Speicherung** > **Übersicht** > **Gehäuse,** um Informationen zu Gehäusen anzuzeigen. Die Seite **Gehäuse** wird angezeigt.

Sie können Filter verwenden, um spezifische Geräteinformationen anzuzeigen.

ANMERKUNG:

- Die Speicherhardwareliste wird nicht angezeigt, wenn das System nicht über Speichergeräte mit CEM-Unterstützung verfügt.
- Das Verhalten von nicht von Dell zertifizierten oder NVMe-Geräten von Drittanbietern ist in iDRAC möglicherweise nicht konsistent.
- Wenn die NVMe SSDs in den Backplane-Slots NVMe-MI-Befehle unterstützen und die I2C-Verbindung zu den Backplane-Slots in Ordnung ist, entdeckt der iDRAC diese NVMe SSDs und meldet sie in den Schnittstellen unabhängig von den PCI-Verbindungen zu den jeweiligen Backplane-Slots.

ANMERKUNG:

Typ	Web-GUI-Unterstützung	Unterstützung für andere Schnittstellen
SATA	Nicht verfügbar	Bestandsaufnahme und RAID-Konfiguration
NVMe	Nur Bestandsaufnahme der physischen Festplatten	Bestandsaufnahme und RAID-Konfiguration

Weitere Informationen zu den angezeigten Eigenschaften und zur Verwendung der Filteroptionen finden Sie in der iDRAC-Online-Hilfe.

Speichergerät über RACADM überwachen

Um die Speichergeräteinformationen anzuzeigen, verwenden Sie den Befehl `storage`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Überwachen der Verwendung der Rückwandplatine über das Dienstprogramm für iDRAC-Einstellungen

Navigieren Sie im Dienstprogramm für die iDRAC-Einstellungen zu **System Summary** (Systemzusammenfassung). Daraufhin wird die Seite **iDRAC Settings.System Summary** (iDRAC-Einstellungen.Systemzusammenfassung) angezeigt. Im Abschnitt **Backplane Inventory** (Bestand der Rückwandplatinen) werden Informationen zu den Rückwandplatinen angezeigt. Weitere Informationen zu den verfügbaren Feldern finden Sie in der *iDRAC Settings Utility Online Help* (Online-Hilfe des Dienstprogramms für iDRAC-Einstellungen).

Anzeigen der Speichergerätetopologie

Diese Seite dient der Ansicht der hierarchischen physischen Aufbewahrung der wichtigsten Speicherkomponenten. Auf dieser Seite werden die Controller, die an diesen angeschlossenen Gehäuse sowie ein Link zu der physischen Festplatte in jedem Gehäuse aufgelistet. Zudem werden die physischen Festplatten angezeigt, die direkt mit dem Controller verbunden sind.

Zum Anzeigen der Speichergerätetopologie navigieren Sie zu **Storage (Speicher)** > **Overview (Übersicht)**. Auf der Seite **Overview** (Übersicht) werden die Speicherkomponenten im System hierarchisch dargestellt. Folgende Optionen stehen zur Verfügung:

- Controller
- Physische Festplatten
- Virtuelle Festplatten
- schrank

Klicken Sie für die Ansicht der jeweiligen Komponentendetails auf die zugehörigen Links.

Verwalten von physischen Festplatten

Sie können die folgenden Aktionen für die physischen Festplatten ausführen:

- Eigenschaften physischer Laufwerke anzeigen.
- Physische Festplatte als einen globalen Hotspare zuweisen oder die Zuweisung rückgängig machen.
- In RAID-fähige Festplatte konvertieren.
- In nicht-RAID-fähige Festplatte konvertieren.
- Blinken der LED oder Beenden des Blinkens.
- Physische Festplatte neu erstellen
- Neuerstellung der physischen Festplatte abbrechen
- Kryptografischer Löschvorgang

Zuweisen oder Aufheben der Zuweisung der physischen Festplatte als globales Hotspare

Ein globaler Hotspare ist eine nicht verwendete Backup-Festplatte, die Teil der Festplattengruppe ist. Hotspares verbleiben im Standby-Modus. Wenn eine in einer virtuellen Festplatte verwendete physische Festplatte fehlerhaft ist, wird der zugewiesene Hotspare aktiviert, um die fehlerhafte physische Festplatte ohne Unterbrechung des Systems und ohne Benutzereingriff zu ersetzen. Wenn ein Hotspare aktiviert wird, werden die Daten aller redundanten virtuellen Festplatten neu erstellt, die die fehlerhafte physische Festplatte verwendet haben.

ANMERKUNG: Ab der iDRAC-Version 3.00.00.00 können Sie globale Hotspares hinzufügen, wenn keine virtuellen Festplatten erstellt werden.

Sie können die Hotspare-Zuweisung ändern, indem Sie eine Festplattenzuweisung rückgängig machen und eine andere Festplatte je nach Bedarf wählen. Sie können auch mehr als eine physische Festplatte als einen globalen Hotspare zuweisen.

Globale Hotspares müssen manuell zugewiesen werden und die Zuweisung muss manuell rückgängig gemacht werden. Sie werden nicht spezifischen virtuellen Festplatten zugewiesen. Wenn Sie einer virtuellen Festplatte ein Hotspare (als Ersatz für eine physische Festplatte, die in der virtuellen Festplatte ausfällt) zuweisen möchten, lesen Sie die Angaben unter Dedizierten Hotspare zuweisen und Zuweisung rückgängig machen nach.

Wenn virtuelle Festplatten gelöscht werden, ist es möglich, dass die Zuweisung für alle zugewiesenen globalen Hotspares rückgängig gemacht wird, wenn die letzte virtuelle Festplatte, die mit dem Controller verknüpft ist, gelöscht wird.

Wenn Sie die Konfiguration zurücksetzen, wird die Zuweisung für alle virtuellen Festplatten gelöscht, und die Zuweisung für alle Hotspares wird aufgehoben.

Sie sollten sich mit den Größenanforderungen und anderen Überlegungen, die bei Hotspares zu beachten sind, vertraut machen.

Führen Sie vor dem Zuweisen einer physischen Festplatte als globaler Hotspare die folgenden Schritte aus:

- Stellen Sie sicher, dass der Lifecycle Controller aktiviert ist.
- Wenn sich keine Laufwerke im Zustand „Bereit“ befinden, dann fügen Sie zusätzliche Festplatten hinzu, und stellen Sie sicher, dass sich die Festplatten im betriebsbereiten Status befinden.

- Wenn sich physische Laufwerke im Nicht-RAID-Modus befinden, dann konvertieren Sie sie unter Verwendung von iDRAC-Schnittstellen wie z. B. die iDRAC-Webschnittstelle, RACADM, WSMan oder <STRG+R> in den RAID-Modus.

  ANMERKUNG: Drücken Sie während des POST F2, um das System-Setup oder die Device-Konfiguration aufzurufen. Die Option STRG+R wird für PERC 10 nicht mehr unterstützt. STRG+R funktioniert nur mit PERC 9, wenn der Bootmodus auf BIOS eingestellt ist.

Wenn Sie die Zuweisung einer physischen Festplatte als globales Hotspare im Modus „Zu ausstehenden Vorgängen hinzufügen“ aufgehoben haben, wird der ausstehende Vorgang, jedoch kein Job erstellt. Wenn Sie dann versuchen, die gleiche Festplatte als globales Hotspare zuzuweisen, wird der Vorgang „Aufhebung der Zuweisung für globales Hotspare anstehend“ deaktiviert.

Wenn Sie die Zuweisung einer physischen Festplatte als globales Hotspare im Modus „Zu ausstehenden Vorgängen hinzufügen“ aufgehoben haben, wird der ausstehende Vorgang, jedoch kein Job erstellt. Wenn Sie dann versuchen, die gleiche Festplatte als globales Hotspare zuzuweisen, wird der Vorgang „Aufhebung der Zuweisung für globales Hotspare anstehend“ deaktiviert.

Wenn das letzte VD gelöscht wird, kehren auch die globalen Hotspares in den Bereitschaftszustand zurück.

Wenn ein PD bereits ein globaler Hotspare ist, kann der Benutzer es dennoch wieder als globalen Hotspare zuweisen.

Zuweisen oder Aufheben der Zuweisung von globalen Hotspares über die Webschnittstelle

So weisen Sie ein globalen Hotspares einer physischen Festplatte zu oder heben die Zuweisung auf:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Speicherkonfiguration**.
   Die Seite **Speicherkonfiguration** wird angezeigt.
2. Wählen Sie im Drop-Down-Menü **Controller** den Controller aus, um die zugehörigen physikalischen Laufwerke anzuzeigen.
3. Klicken Sie auf **Konfiguration physischer Laufwerke**.
   Alle physischen Festplatten, die dem Controller zugeordnet sind, werden angezeigt.
4. Um die Zuweisung als globales Hot Spare zu erreichen, wählen Sie aus dem Drop-down-Menü in der Spalte **Aktion** die Option **Globales Hot Spare zuweisen** für eine oder mehrere physische Festplatten aus.
5. Um die Zuweisung als globales Hot Spare zurückzunehmen, wählen Sie aus dem Drop-down-Menü in der Spalte **Aktion** die Option **Zuweisung für globales Hot Spare zurücknehmen** für eine oder mehrere physische Festplatten aus.
6. Klicken Sie auf **Apply Now** (Jetzt übernehmen).
   Je nach Ihren Anforderungen können Sie auch **Bei nächstem Neustart** oder **Zu einer geplanten Zeit** anwenden. Basierend auf dem ausgewählten Betriebsmodus werden die Einstellungen angewendet.

Zuweisen oder Aufheben der Zuweisung für globale Hotspares über RACADM

Verwenden Sie den Befehl `storage` und legen Sie den Typ als globalen Hotspare fest.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Konvertieren einer physischen Festplatte in den RAID- und Nicht-RAID-Modus

Durch die Konvertierung einer physischen Festplatte in den RAID-Modus können Sie die Festplatte für alle RAID-Vorgänge verwenden. Wenn sich eine Festplatte im Nicht-RAID-Modus befindet, wird die Festplatte im Gegensatz zu nicht konfigurierten Festplatten im Status „Gut“ für das Betriebssystem freigegeben und in einem direkten Passthrough-Modus verwendet.

PERC 10 wird zur Konvertierung von Laufwerken in Nicht-RAID nicht unterstützt. Es wird jedoch in PERC 10.2 und höheren Versionen unterstützt.

Sie können die physischen Festplatten folgendermaßen in den RAID- und Nicht-RAID-Modus konvertieren:

- Beginnen Sie mit der Verwendung der iDRAC-Netzwerkschnittstellen, wie z. B. der Webschnittstelle, RACADM, Redfish oder WSMan.
- Durch Drücken von <Strg+R> während des Server-Neustarts und Auswahl des erforderlichen Controllers.

ANMERKUNG: Wenn sich die mit einem PERC-Controller verbundenen physischen Laufwerke im Nicht-RAID-Modus befinden, wird die in den iDRAC-Schnittstellen, wie z. B. der iDRAC GUI, RACADM, Redfish und WSMan angezeigte Datenträgergröße möglicherweise als ein wenig kleiner als die tatsächliche Größe des Datenträgers angezeigt. Sie können Betriebssysteme jedoch mit der vollen Kapazität des Datenträgers bereitstellen.

ANMERKUNG:

- Hot-Plug-Laufwerke im PERC H330 befinden sich immer im Nicht-RAID-Modus. Bei anderen RAID-Controllern befinden sie sich immer im RAID-Modus.
- Hot-Plug-Festplatten in PERC 11 sind entweder bereit oder EPD-PT, abhängig von der aktuellen Einstellung des automatischen Konfigurationsverhaltens.

Konvertierung von physischen Laufwerken in den RAID-fähigen oder nicht-RAID-Modus mithilfe der iDRAC-Weboberfläche

Führen Sie zum Konvertieren der physischen Laufwerke in den RAID-Modus oder den Nicht-RAID-Modus die folgenden Schritte aus:

1. Klicken Sie in der iDRAC-Weboberfläche auf **Storage** > **Übersicht** > **Physische Laufwerke**.
2. Klicken Sie auf **Filteroptionen**. Zwei Optionen werden angezeigt: **Alle Filter löschen** und **Erweiterter Filter**. Klicken Sie auf die Option **Erweiterter Filter**.
   Eine ausführliche Liste wird angezeigt, mit der Sie verschiedene Parameter konfigurieren können.
3. Wählen Sie aus dem Drop-down-Menü **Gruppieren nach** ein Gehäuse oder virtuelle Laufwerke aus.
   Die mit dem Gehäuse oder dem virtuellen Laufwerk verknüpften Parameter werden angezeigt.
4. Klicken Sie auf **Anwenden**, nachdem Sie alle gewünschten Parameter ausgewählt haben. Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.
   Die Einstellungen werden basierend auf der im Betriebsmodus ausgewählten Option angewendet.

Konvertierung von physikalischen Festplatten in den RAID-fähigen oder nicht-RAID-Modus mithilfe von RACADM

Verwenden Sie je nachdem, ob Sie in den RAID- oder Nicht-RAID-Modus konvertieren möchten die folgenden RACADM-Befehle

- Verwenden Sie den Befehl `racadm storage converttoraid`, um in den RAID-Modus zu konvertieren.
- Verwenden Sie den Befehl `racadm storage converttononraid`, um in den Nicht-RAID-Modus zu konvertieren.

ANMERKUNG: Auf dem S140-Controller können Sie nur die RACADM-Schnittstelle verwenden, um die Laufwerke vom Nicht-RAID-Modus in den RAID-Modus zu konvertieren. Die unterstützten Software-RAID-Modi sind der Windows- oder Linux-Modus.

Weitere Informationen zu den Befehlen finden Sie unter *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals

Löschen physischer Laufwerke

Mit der Systemlöschfunktion können Sie den Inhalt der physischen Laufwerke löschen. Diese Funktion ist über RACADM oder die LC-GUI zugänglich. Physische Laufwerke auf dem Server werden in zwei Kategorien unterteilt.

- Sicheres Löschen von Laufwerken – Enthält Laufwerke, die kryptografisches Löschen ermöglichen, wie ISE- und SED-SAS- und -SATA-Laufwerke sowie PCIe-SSDs.
- Laufwerke durch Überschreiben löschen – Umfasst alle Laufwerke, die das kryptografische Löschen nicht unterstützen.

ANMERKUNG: Vor dem Löschen von vFlash müssen Sie zunächst alle Partitionen über die iDRAC-Schnittstellen trennen, bevor Sie den Vorgang ausführen.

ANMERKUNG: Die Systemlöschfunktion gilt nur für Laufwerke im Server. iDRAC kann keine Laufwerke in einem externen Gehäuse, wie z. B. einem JBOD, löschen.

Der RACADM-Unterbefehl „SystemErase“ enthält Optionen für die folgenden Kategorien:

- Mit der Option **SecureErasePD** werden alle Laufwerke zum sicheren Löschen kryptografisch gelöscht.
- Die Option **OverwritePD** überschreibt Daten auf allen Laufwerken.

ANMERKUNG: Das kryptografische Löschen des physischen BOSS-Laufwerks kann mit der `SystemErase`-Methode durchgeführt werden und wird von LC-UI, WSMAN und RACADM unterstützt.

Verwenden Sie vor dem Ausführen von SystemErase den folgenden Befehl, um die Löschfunktion aller physischen Laufwerke für einen Server zu überprüfen:

```
# racadm storage get pdisks -o -p SystemEraseCapability
```

ANMERKUNG: Wenn SEKM auf dem Server aktiviert ist, deaktivieren Sie SEKM mithilfe des Befehls `racadm sekm disable`, bevor Sie diesen Befehl verwenden. Somit kann verhindert werden, dass Storage-Geräte gesperrt werden, die durch iDRAC gesichert sind, wenn SEKM-Einstellungen aus iDRAC gelöscht werden, indem Sie den Befehl ausführen.

Verwenden Sie diesen Befehl, um ISE- und SED-Laufwerke zu löschen:

```
# racadm systemerase -secureerasepd
```

Verwenden Sie den folgenden Befehl, um Laufwerke durch Überschreiben zu löschen:

```
# racadm systemerase -overwritepd
```

ANMERKUNG: RACADM SystemErase entfernt alle virtuellen Laufwerke von den physischen Laufwerken, die mit den obigen Befehlen gelöscht werden.

ANMERKUNG: RACADM SystemErase bewirkt, dass der Server neu gestartet wird, um die Löschvorgänge auszuführen.

ANMERKUNG: Einzelne PCIe-SSD- oder SED-Geräte können über die iDRAC-GUI oder RACADM gelöscht werden. Weitere Informationen finden Sie im Abschnitt *Löschen von PCIe-SSD-Gerätedaten* und im Abschnitt *Löschen von SED-Gerätedaten*.

Informationen zur Systemlöschfunktion innerhalb der Lifecycle Controller-Nutzeroberfläche finden Sie unter *Benutzerhandbuch für den Lifecycle Controller* verfügbar unter https://www.dell.com/idracmanuals.

Löschen von SED/ISE-Gerätedaten

ANMERKUNG: Dieser Vorgang wird nicht unterstützt, wenn das unterstützte Gerät Teil eines virtuellen Laufwerks ist. Das vom Ziel unterstützte Gerät muss vor der Durchführung der Gerätelöschung vom virtuellen Laufwerk entfernt werden.

Die kryptografische Löschung löscht alle auf der Festplatte vorhandenen Daten dauerhaft. Das Ausführen eines kryptografischen Löschvorgangs auf einem SED/ISE überschreibt alle Blöcke und führt zu permanentem Datenverlust auf dem unterstützten Gerät. Beim kryptografischen Löschvorgang kann der Host nicht auf das unterstützte Gerät zugreifen. Die SED/ISE-Gerätelöschung kann entweder in Echtzeit oder nach einem Neustart des Systems durchgeführt werden.

Falls das System neu gestartet wird oder wenn während einer kryptografischen Löschung der Strom ausfällt, wird der Vorgang abgebrochen. Sie müssen das System neu starten und den Vorgang erneut ausführen.

Stellen Sie vor dem Löschen von SED/ISE-Gerätedaten Folgendes sicher:

- Lifecycle Controller ist aktiviert.
- Sie haben die Berechtigungen zur Serversteuerung sowie zur Anmeldung.
- Das ausgewählte unterstützte Laufwerk ist nicht Teil eines virtuellen Laufwerks.

ANMERKUNG:

- Das Löschen von SED/ISE kann entweder in Echtzeit oder als mehrstufiger Vorgang durchgeführt werden.
- Nach dem Löschen des Laufwerks kann es aufgrund von Daten-Caching weiterhin als aktiv im Betriebssystem angezeigt werden. Starten Sie in diesem Fall das Betriebssystem neu und das gelöschte Laufwerk wird nicht mehr angezeigt oder meldet keine Daten.
- Der kryptografische Löschvorgang wird für Hot-Plug-fähige NVMe-Festplatten nicht unterstützt. Starten Sie den Server neu, bevor Sie den Vorgang starten. Wenn der Vorgang weiterhin fehlschlägt, stellen Sie sicher, dass CSIOR aktiviert ist und die NVMe-Festplatten durch Dell Technologies qualifiziert sind.

Löschen von SED/ISE-Gerätedaten über die Webschnittstelle

So löschen Sie die Daten auf dem unterstützten Gerät:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Storage** > **Übersicht** > **Physische Festplatten**.
   Daraufhin wird die Seite **Physische Festplatten** angezeigt.

2. Wählen Sie im Drop-Down-Menü **Controller** den Controller aus, um die zugehörigen Geräte anzuzeigen.
3. Wählen Sie in den Drop-Down-Menüs die Option **Kryptografisches Löschen** für eine oder mehrere SED/ISEs aus.

   Wenn Sie **Kryptografisches Löschen** ausgewählt haben und Sie die anderen Optionen im Dropdown-Menü anzeigen möchten, wählen Sie **Maßnahme** aus und klicken Sie dann auf das Drop-Down-Menü, um die anderen Optionen anzuzeigen.
4. Wählen Sie im Dropdown-Menü **Betriebsmodus wählen** eine der folgenden Optionen aus:
   - **Jetzt ausführen** – Wählen Sie diese Option aus, um die Maßnahmen sofort anzuwenden, ohne dass ein Systemneustart erforderlich ist.
   - **Beim nächsten Neustart** – Wählen Sie diese Option aus, um die Aktionen beim nächsten Systemneustart anzuwenden.
   - **Zu einer geplanten Zeit** – Wählen Sie diese Option aus, um die Maßnahmen zu einem geplanten Datum und Uhrzeit anzuwenden:
     - **Startzeit** und **Endzeit** – Klicken Sie auf die Kalender-Symbole und wählen Sie die Tage aus. Wählen Sie aus dem Drop-Down-Menü das Zeitintervall. Die Maßnahme wird zwischen der Startzeit und Endzeit angewandt.
     - Wählen Sie aus dem Drop-Down-Menü den Typ des Neustarts aus:
       - Kein Neustart (manueller System-Neustart)
       - Ordentliches Herunterfahren
       - Erzwungenes Herunterfahren
       - System aus- und wieder einschalten (Hardwareneustart)
5. Klicken Sie auf **Anwenden**.

   Wenn der Job nicht erfolgreich erstellt wurde, wird eine Meldung angezeigt, die besagt, dass der Job nicht angezeigt wurde. Die Meldungs-ID und die empfohlene Reaktion werden ebenfalls angezeigt.

   Wurde der Job erfolgreich erstellt, wird eine Meldung angezeigt, die besagt, dass die Job-ID für den ausgewählten Controller erstellt wurde. Klicken Sie auf **Job-Warteschlange**, um den Fortschritt des Auftrags auf der Seite Job-Warteschlange anzuzeigen.

   Wenn ein ausstehender Vorgang nicht erstellt wurde, erscheint eine Fehlermeldung. Wenn der ausstehende Vorgang erfolgreich war und die Job-Erstellung nicht erfolgreich war, wird eine Fehlermeldung angezeigt.

Löschen eines SED-Geräts unter Verwendung von RACADM

Zum sicheren Löschen eines SED-Geräts:

```
racadm storage cryptographicerase:<SED FQDD>
```

So erstellen Sie den Ziel-Job nach dem Ausführen des Befehls `cryptographicerase`:

```
racadm jobqueue create <SED FQDD> -s TIME_NOW -realtime
```

So erstellen Sie den stufenweisen Ziel-Job nach dem Ausführen des Befehls „cryptographicerase“:

```
racadm jobqueue create <SED FQDD> -s TIME_NOW -e <start_time>
```

So fragen Sie die ausgegebene Job-ID ab:

```
racadm jobqueue view -i <job ID>
```

Weitere Informationen finden Sie unter *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Physische Festplatte neu erstellen

Das Neuerstellen einer physischen Festplatte ist die Fähigkeit, die Inhalte einer ausgefallenen Festplatte zu rekonstruieren. Dies gilt nur, wenn die Option zum automatischen Neuerstellen auf „false“ (falsch) eingestellt ist. Wenn eine redundante virtuelle Festplatte vorhanden ist, werden beim Neuerstellungsvorgang die Inhalte einer fehlerhaften physischen Festplatte neu erstellt. Eine Neuerstellung kann während des Normalbetriebs stattfinden, wobei sich jedoch die Systemleistung verschlechtert.

Mit der Option zum Abbrechen der Neuerstellung können Sie eine laufende Neuerstellung abbrechen. Wenn Sie eine Neuerstellung abbrechen, bleibt die virtuelle Festplatte in einem herabgesetzten Zustand. Wenn eine zusätzliche physische Festplatte ausfällt, kann die virtuelle Festplatte ausfallen. Dies führt eventuell zu Datenverlust. Es wird empfohlen, so früh wie möglich eine Neuerstellung auf der ausgefallenen physischen Festplatte durchzuführen.

Wenn Sie die Neuerstellung einer physischen Festplatte abbrechen, die als Hotspare zugewiesen ist, reinitiieren Sie die Neuerstellung auf derselben physischen Festplatte, um die Daten wiederherzustellen. Das Abbrechen der Neuerstellung einer physischen Festplatte und das Zuweisen einer anderen physischen Festplatte als Hotspare hat nicht zur Folge, dass der neu zugewiesene Hotspare die Daten neu erstellt.

Verwalten von virtuellen Festplatten

Sie können die folgenden Vorgänge für die virtuellen Festplatten ausführen:

- Erstellen
- Löschen
- Richtlinien bearbeiten
- Initialisieren
- Übereinstimmungsüberprüfung
- Übereinstimmungsüberprüfung abbrechen
- Virtuelle Festplatten verschlüsseln
- Dedizierte Ersatzlaufwerke zuweisen oder die Zuweisung rückgängig machen
- Blinken von virtuellen Festplatten und Blinken beenden
- Hintergrundinitialisierung abbrechen
- Online-Kapazitätserweiterung
- RAID-Level-Migration

ANMERKUNG: Sie können 240 virtuelle Festplatten über iDRAC-Schnittstellen verwalten und überwachen. Um VDs zu erstellen, verwenden Sie entweder die Device-Konfiguration (F2), das PERCCLI-Befehlszeilen-Tool oder Dell OpenManage Server Administrator (OMSA).

ANMERKUNG: Die Anzahl ist für PERC 10 geringer, da es keine verketteten Anordnungen unterstützt.

Erstellen von virtuellen Laufwerken

Um RAID-Funktionen zu implementieren, müssen Sie ein virtuelles Laufwerk erstellen. Ein virtuelles Laufwerk bezieht sich auf den Datenspeicher, den ein RAID-Controller mit einem oder mehreren physischen Laufwerken erstellt hat. Obwohl ein virtuelles Laufwerk aus mehreren physischen Laufwerken bestehen kann, wird es vom Betriebssystem als ein einzelnes Laufwerk behandelt.

Bevor Sie eine virtuelle Festplatte erstellen, sollten Sie sich mit den Informationen unter Erwägungen vor der Erstellung von virtuellen Festplatten vertraut machen.

Sie können ein virtuelles Laufwerk mithilfe der die mit dem PERC-Controller verbundenen physischen Laufwerke erstellen. Um ein virtuelles Laufwerk zu erstellen, müssen Sie über die Benutzerberechtigung für die Serversteuerung verfügen. Sie können maximal 64 virtuelle Laufwerke und maximal 16 virtuelle Laufwerke in derselben Laufwerkgruppe erstellen.

In den folgenden Fällen können Sie keine virtuelles Laufwerk erstellen:

- Physische Laufwerke sind nicht für die Erstellung virtueller Laufwerke verfügbar. Installieren Sie zusätzliche physische Laufwerke.
- Die maximale Anzahl virtueller Laufwerke, die auf dem Controller erstellt werden können, wurde erreicht. Sie müssen mindestens ein virtuelles Laufwerk löschen und dann ein neues virtuelles Laufwerk erstellen.
- Die maximale Anzahl der von einer Laufwerkgruppe unterstützten virtuellen Laufwerke wurde erreicht. Sie müssen ein virtuelles Laufwerk aus der ausgewählten Gruppe löschen und dann ein neues virtuelles Laufwerk erstellen.
- Auf dem ausgewählten Controller wird derzeit eine Aufgabe ausgeführt oder ist geplant. Sie müssen warten, bis die Aufgabe abgeschlossen ist, oder die Aufgabe löschen, bevor Sie einen neuen Vorgang beginnen. Sie können den Status der geplanten Aufgabe auf der Seite „Job-Warteschlange“ anzeigen und verwalten.
- Das physische Laufwerk befindet sich im Nicht-RAID-Modus. Es muss unter Verwendung der iDRAC-Schnittstellen wie beispielsweise der iDRAC-Webschnittstelle, RACADM, Redfish, WSMan oder <STRG+R> in den RAID-Modus konvertiert werden.

ANMERKUNG: Wenn Sie eine virtuelle Festplatte im Modus „Zu ausstehenden Vorgängen hinzufügen“ erstellen und ein Job nicht erstellt wird und Sie dann die virtuelle Festplatte löschen, wird der ausstehende Erstellungsvorgang für die virtuelle Festplatte gelöscht.

ANMERKUNG: RAID 6 und RAID 60 werden in PERC H330 nicht unterstützt.

ANMERKUNG: Mit dem BOSS Controller können Sie nur virtuelle Laufwerke erstellen, deren Größe der Größe des physischen Speichermediums M.2 entspricht. Stellen Sie sicher, dass Sie die Größe der virtuellen Festplatte auf Null setzen, wenn Sie das

Serverkonfigurationsprofil verwenden, um eine virtuelle Festplatte von BOSS zu erstellen. Für andere Schnittstellen wie RACADM, WSMan und Redfish sollte die Größe des virtuellen Laufwerks nicht angegeben werden.

Erwägungen vor der Erstellung von virtuellen Laufwerken

Vor dem Erstellen von virtuellen Laufwerken sollten Sie Folgendes beachten:

- Namen für virtuelle Laufwerke nicht auf Controller gespeichert – Die Namen der virtuellen Laufwerke, die Sie erstellen, werden nicht im Controller gespeichert. Das bedeutet, wenn Sie einen Neustart mit einem anderen Betriebssystem ausführen, benennt das neue Betriebssystem das virtuelle Laufwerk eventuell mit seiner eigenen Namenkonvention um.
- Die Laufwerkgruppierung ist eine logische Gruppierung von Laufwerken, die mit einem RAID-Controller verbunden sind, auf dem ein oder mehrere virtuelle Laufwerke erstellt werden, sodass alle virtuellen Laufwerke in der Laufwerkgruppe alle physischen Laufwerke in der Laufwerkgruppe verwenden. Die aktuelle Implementierung unterstützt das Sperren von gemischten Laufwerkgruppen während der Erstellung von logischen Geräten.
- Physische Laufwerke sind an Laufwerkgruppen gebunden. Aus diesem Grund gibt es keine Vermischung von RAID-Stufen auf einer Laufwerkgruppe.
- Die Anzahl an physischen Laufwerken, die in einem virtuellen Laufwerk enthalten sein können, unterliegt Einschränkungen. Diese Einschränkungen hängen vom Controller ab. Beim Erstellen eines virtuellen Laufwerks unterstützen Controller eine bestimmte Anzahl an Stripes und Bereichen (Methoden zur Zusammenführung des Speichers auf physischen Laufwerken). Da die Gesamtanzahl der Stripes und Bereiche begrenzt ist, ist die Anzahl der physischen Laufwerke, die verwendet werden können, ebenfalls begrenzt. Die Einschränkungen für Stripes und Bereiche wirken sich wie folgt auf die RAID-Stufen aus:
  - Die maximale Anzahl von Bereichen wirkt sich auf Verkettung, RAID 10, RAID 50 und RAID 60 aus.
  - Die maximale Anzahl von Stripes wirkt sich auf RAID 0, RAID 5, RAID 50, RAID 6 und RAID 60 aus.
  - Die Anzahl der physischen Laufwerke in einer Spiegelung ist immer 2. Dies wirkt sich auf RAID 1 und RAID 10 aus.

  ANMERKUNG:
  - RAID 1 wird nur für BOSS-Controller unterstützt.
  - SWRAID-Controller unterstützt RAID 0, 1, 5 und 10.
- Virtuelle Laufwerke können auf PCIe-SSDs nicht erstellt werden. PERC 11 und höhere Controller unterstützen jedoch die Erstellung virtueller Laufwerke mit PCIe-SSDs.

Erstellen von virtuellen Festplatten über die Webschnittstelle

So erstellen Sie eine virtuelle Festplatte:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Speicher** > **Übersicht** > **Virtuelle LaufwerkeErweiterter Filter**.
2. Gehen Sie im Abschnitt **Virtuelles Laufwerk** wie folgt vor:
   a. Wählen Sie aus dem Drop-Down-Menü **Controller** den Controller aus, für den Sie die virtuelle Festplatte erstellen möchten.
   b. Wählen Sie die RAID-Stufe für die virtuelle Festplatte aus dem Drop-Down-Menü **Layout** aus.

      Nur jene RAID-Stufen, die vom Controller unterstützt werden, werden im Drop-Down-Menü angezeigt, und zwar auf Basis der Gesamtzahl der verfügbaren physikalischen Festplatten.
   c. Wählen Sie den **Medientyp**, die **Blockgröße**, die **Leserichtlinie**, die **Schreibrichtlinie**, die **Festplatten-Cache-Regeln**.

      Es werden nur die Werte, die vom Controller unterstützt werden, in den Drop-Down-Menüs für diese Eigenschaften angezeigt.
   d. Geben Sie im Feld **Kapazität** die Größe des virtuellen Laufwerks ein.

      Es wird die maximale Größe angezeigt, die dann auf Basis der ausgewählten Festplatten aktualisiert wird.
   e. Das Feld für die **Span-Anzahl** wird basierend auf den ausgewählten physischen Festplatten angezeigt (Schritt 3). Sie können diesen Wert nicht festlegen. Er wird automatisch berechnet, nachdem Sie Festplatten für Multi-RAID-Stufe ausgewählt haben. Das Feld **Span-Anzahl** gilt nur für RAID 10, RAID 50 und RAID 60. Wenn Sie RAID 10 gewählt haben und der Controller ungleichmäßiges RAID 10 unterstützt, wird der Wert für die Spannenanzahl nicht angezeigt. Der Controller stellt automatisch den entsprechenden Wert ein. Bei RAID 50 und RAID 60 wird dieses Feld nicht angezeigt, wenn die minimale Anzahl von Festplatten für die Erstellung von RAID verwendet wird. Es kann geändert werden, wenn mehr Festplatten verwendet werden.
3. Wählen Sie im Abschnitt **Physische Festplatten auswählen** die Anzahl der physischen Festplatten aus.

   Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.
4. Wählen Sie im Dropdown-Menü die Option **Betriebsmodus anwenden**, wenn Sie die Einstellungen übernehmen möchten.
5. Klicken **Sie auf**.

   Basierend auf der Option **Betriebsmodus wählen** werden die Einstellungen angewendet.

   ANMERKUNG: Sie dürfen alphanumerische Zeichen, Leerzeichen, Bindestriche und Unterstriche im Festplattennamen verwenden.

Alle anderen von Ihnen eingegebenen Sonderzeichen werden beim Erstellen der virtuellen Festplatte entfernt und durch Leerzeichen ersetzt.

Erstellen von virtuellen Festplatten über RACADM

Verwenden Sie den Befehl `racadm storage createvd`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

ANMERKUNG: Das Aufteilen von Festplatten oder das Konfigurieren von Teil-VDs wird auf den von S140-Controller verwalteten Laufwerken nicht mit RACADM unterstützt.

Bearbeiten von Cache-Richtlinien für virtuelle Laufwerke

Sie können die Lese-, Schreib- oder Festplatten-Cache-Regeln einer virtuellen Festplatte ändern.

ANMERKUNG: Einige der Controller unterstützen nicht alle Lese- oder Schreibrichtlinien. Aus diesem Grund wird beim Anwenden einer Richtlinie eine Fehlermeldung angezeigt.

Die Leseregeln bestimmen, ob der Controller beim Suchen von Daten sequenzielle Sektoren auf der virtuellen Festplatte lesen soll.

- **Adaptives Vorauslesen**: Der Controller leitet das Vorauslesen nur dann ein, wenn durch die letzten beiden Leseanforderungen ein Zugriff auf sequenzielle Sektoren der Festplatte erfolgte. Wenn nachfolgende Leseanforderungen auf wahlfreie Sektoren der Festplatte zugreifen, kehrt der der Controller zur Kein Vorauslesen-Richtlinie zurück. Der Controller prüft weiterhin, ob Leseanforderungen auf sequenzielle Sektoren der Festplatte zugreifen, und initiiert Vorauslesen (falls erforderlich).
- **Vorauslesen**: Beim Suchen von Daten liest der Controller sequenzielle Sektoren auf dem virtuellen Laufwerk. Anhand der Vorauslesen-Richtlinie kann eventuell die Systemleistung verbessert werden, wenn die Daten auf sequenzielle Sektoren des virtuellen Laufwerks geschrieben werden.
- **Kein Vorauslesen** – Das Auswählen der Regel „Kein Vorauslesen“ gibt an, dass der Controller die Regel „Vorauslesen“ nicht verwenden sollte.

Die Schreibregeln bestimmen, ob der Controller ein Schreibanfrage-Beendungssignal sendet, wenn sich die Daten im Cache befinden oder nachdem sie auf die Festplatte geschrieben wurden.

- **Durchschreiben**: Der Controller sendet erst dann ein Signal für den Abschluss der Schreibanforderung, nachdem die Daten auf das Laufwerk geschrieben wurden. Durchschreiben-Caching bietet eine bessere Datensicherheit als die Rückschreiben-Caching, da das System annimmt, dass die Daten erst verfügbar sind, nachdem sie sicher auf die Festplatte geschrieben wurden.
- **Rückschreiben**: Der Controller sendet ein Signal zum Abschluss der Schreibanforderung, sobald sich die Daten im Controller-Cache befinden, jedoch noch nicht auf die Festplatte geschrieben wurden. Das Rückschreiben-Caching kann zu einer verbesserten Leistung führen, da nachfolgende Leseanforderungen Daten schnell vom Cache und dann von der Festplatte abrufen können. Es kann jedoch im Falle eines Festplattenausfalls zu Datenverlust kommen, der verhindert, dass Daten auf eine Festplatte geschrieben werden. Für andere Anwendungen können auch Probleme auftreten, wenn Aktionen davon ausgehen, dass die Daten auf der Festplatte verfügbar sind.
- **Rückschreiben erzwingen** – Der Schreib-Cache wird unabhängig davon aktiviert, ob sich im Controller ein Akku befindet. Wenn der Controller keine Batterie hat und Rückschreiben in Cache erzwingen verwendet wird, kann bei einem Stromausfall ein Datenverlust auftreten.

Die Festplatten-Cache-Richtlinie gilt für Lesevorgänge auf einer bestimmten virtuellen Festplatte. Diese Einstellungen wirken sich nicht auf die Vorauslesen-Richtlinie aus.

ANMERKUNG:

- Der nicht-flüchtige Controller-Cache und die Akkusicherung des Controllers wirken sich auf die Leseregel oder die Schreibregel aus, die ein Controller unterstützen kann. Nicht alle PERCs sind mit Akkus oder Cache ausgerüstet.
- Für das Vorauslesen und das Zurückschreiben ist ein Cache erforderlich. Wenn der Controller also nicht über Cache verfügt, können Sie den Richtlinienwert nicht festlegen.

  Wenn der PERC mit Cache ausgerüstet ist, jedoch ohne Akku, und die Richtlinie so festgelegt wurde, dass der Zugriff auf den Cache erforderlich ist, kann es bei einem Stromausfall zu Datenverlusten kommen. Daher wird diese Richtlinie bei einigen PERCs nicht unterstützt.

  Daher wird je nach PERC der Richtlinienwert festgelegt.

Löschen von virtuellen Festplatten

Das Löschen einer virtuellen Festplatte löscht alle Informationen, einschließlich der Dateisysteme und Volumes, die sich auf der virtuellen Festplatte befinden, und entfernt die virtuelle Festplatte aus der Konfiguration des Controllers. Wenn virtuelle Festplatten gelöscht werden, ist es möglich, dass die Zuweisung für alle zugewiesenen globalen Hotspares rückgängig gemacht wird, wenn die letzte virtuelle Festplatte, die mit dem Controller verknüpft ist, gelöscht wird. Wenn die letzte virtuelle Festplatte einer Festplattengruppe gelöscht wird, werden alle zugewiesenen dedizierten Hotspares automatisch globale Hotspares.

Wenn Sie Sie alle VDs für einen globalen Hotspare löschen, wird das globale Hotspare automatisch gelöscht.

Sie müssen über die Berechtigung zur Anmeldung und zur Server-Steuerung verfügen, um die virtuellen Festplatten zu löschen.

Wenn dieser Vorgang erlaubt ist, können Sie ein virtuelles Startlaufwerk löschen. Dieser Vorgang erfolgt über das Seitenband und ist unabhängig vom Betriebssystem. Deshalb wird eine Warnmeldung angezeigt, bevor Sie das virtuelle Laufwerk löschen.

Wenn Sie eine virtuelle Festplatte löschen und eine neue virtuelle Festplatte mit denselben Eigenschaften wie die der gelöschten virtuellen Festplatte erstellen, erkennt der Controller die Daten, als ob die erste virtuelle Festplatte nie gelöscht worden wäre. Wenn Sie die alten Daten nach der Neuerstellung einer neuen virtuellen Festplatte nicht behalten möchten, initialisieren Sie die virtuelle Festplatte erneut.

Überprüfen der Übereinstimmung der virtuellen Festplatte

Dieser Vorgang überprüft die Richtigkeit der redundanten (Paritäts-)Informationen. Diese Aufgabe gilt nur für redundante virtuelle Laufwerke. Bei Bedarf können über die Übereinstimmungsüberprüfung redundante Daten neu erstellt werden. Falls das virtuelle Laufwerk einen beeinträchtigten Status aufweist, kann dieser möglicherweise durch das Durchführen einer Konsistenzprüfung in den betriebsbereiten Status überführt werden. Sie können den Task Übereinstimmungsüberprüfung mithilfe der Web-Schnittstelle oder RACADM durchführen.

Sie können den Vorgang der Übereinstimmungsüberprüfung auch abbrechen. Das Abbrechen der Übereinstimmungsüberprüfung ist ein Echtzeit-Vorgang.

Sie müssen über die Berechtigung zur Anmeldung und zur Server-Steuerung verfügen, um die Übereinstimmung von virtuellen Festplatten zu prüfen.

ANMERKUNG: Konsistenzprüfung wird nicht unterstützt, wenn die Laufwerke im RAID0-Modus eingerichtet sind.

ANMERKUNG: Wenn Sie den Vorgang zum Abbrechen der Übereinstimmungsüberprüfung durchführen, wenn keine Übereinstimmungsüberprüfung durchgeführt wird, wird der ausstehende Vorgang in der GUI als BGI-Abbruch statt als Abbruch der Übereinstimmungsüberprüfung angezeigt.

Initialisieren von virtuellen Festplatten

Durch das Initialisieren virtueller Festplatten werden alle Daten auf der Festplatte gelöscht, es ändert sich jedoch nicht die Konfiguration der virtuellen Festplatte. Sie müssen eine virtuelle Festplatte initialisieren, die vor der Verwendung konfiguriert wurde.

ANMERKUNG: Initialisieren Sie keine virtuellen Laufwerke, wenn Sie versuchen, eine vorhandene Konfiguration neu zu erstellen.

Sie können eine Schnellinitialisierung oder eine vollständige Initialisierung durchführen oder die Initialisierung abbrechen.

ANMERKUNG: Das Abbrechen der der Initialisierung ist ein Echtzeitvorgang. Sie können die Initialisierung nur über die iDRAC-Web-Schnittstelle, nicht aber über RACADM abbrechen.

Schnellinitialisierung

Die Schnellinitialisierung initialisiert alle in der virtuellen Festplatte enthaltenen physischen Festplatten. Sie aktualisiert die Metadaten auf den physischen Festplatten, sodass der gesamte Festplatten-Speicherplatz für künftige Schreibvorgänge verfügbar ist. Die Initialisierung kann schnell abgeschlossen werden, da vorhandene Informationen auf den physischen Festplatten nicht gelöscht werden, obwohl künftige Schreibvorgänge die auf den physischen Festplatten verbleibenden Informationen überschreiben.

Die Schnellinitialisierung löscht nur die Startsektor- und Stripe-Daten. Führen Sie nur dann eine Schnellinitialisierung durch, wenn Sie zeitlich eingeschränkt sind oder die Festplatten neu sind oder noch nicht verwendet wurden. Die Schnellinitialisierung nimmt in der Regel weniger Zeit in Anspruch (etwa 30 bis 60 Sekunden).

VORSICHT: Das Ausführen einer schnellen Initialisierung bewirkt, dass auf vorhandene Daten nicht mehr zugegriffen werden kann.

Die Schnellinitialisierung schreibt keine Nullen in die Festplattenblöcke auf den physischen Festplatten. Dies liegt daran, dass die Schnellinitialisierung keinen Schreibvorgang durchführt und die Auswirkung auf die Festplatte geringer ist.

Eine Schnellinitialisierung auf einer virtuellen Festplatte überschreibt die ersten und die letzten 8 MB der virtuellen Festplatte und löscht alle Startdaten oder Partitionsinformationen. Dieser Vorgang dauert nur 2-3 Sekunden und wird beim Neuerstellen von virtuellen Festplatten empfohlen.

Eine Hintergrundinitialisierung beginnt fünf Minuten nach Abschluss der Schnellinitialisierung.

Vollständige oder langsame Initialisierung

Die vollständige Initialisierung (auch als langsame Initialisierung bezeichnet) initialisiert alle in der virtuellen Festplatte enthaltenen physischen Festplatten. Sie aktualisiert die Metadaten auf den physischen Festplatten und löscht alle vorhandenen Daten und Dateisysteme. Sie können eine vollständige Initialisierung nach der Erstellung der virtuellen Festplatte durchführen. Im Vergleich zur Schnellinitialisierung möchten Sie ggf. die vollständige Initialisierung verwenden, wenn Sie Probleme mit einer physischen Festplatte haben oder vermuten, dass sie beschädigte Festplattenblöcke aufweist. Die vollständige Initialisierung weist beschädigte Blöcke neu zu und schreibt Nullen in alle Festplattenblöcke.

Bei der vollständigen Initialisierung einer virtuellen Festplatte ist keine Hintergrundinitialisierung erforderlich. Bei der vollständigen Initialisierung kann der Host nicht auf die virtuelle Festplatte zugreifen. Wenn das System während der vollständigen Initialisierung neu gestartet wird, wird der Vorgang abgebrochen und eine Hintergrundinitialisierung auf der virtuellen Festplatte gestartet.

Es wird empfohlen, stets eine vollständige Initialisierung auf Laufwerken durchzuführen, die zuvor Daten enthalten haben. Eine vollständige Initialisierung kann bis zu 1-2 Minuten pro GB dauern. Die Geschwindigkeit der Initialisierung richtet sich nach dem Controller-Modell, der Geschwindigkeit der Festplatten und der Firmware-Version.

Die vollständige Initialisierung initialisiert eine physische Festplatte nach der anderen.

ANMERKUNG: Die vollständige Initialisierung wird nur in Echtzeit unterstützt. Nur wenige Controller unterstützen die vollständige Initialisierung.

Verschlüsseln der virtuellen Laufwerke

Wenn Verschlüsselung auf einem Controller deaktiviert ist (das heißt, der Sicherheitsschlüssel wurde gelöscht), aktivieren Sie manuell die Verschlüsselung für virtuelle Festplatten, die mit SED-Laufwerken erstellt werden. Falls die virtuelle Festplatte nach der Aktivierung der Verschlüsselung auf einem Controller erstellt wird, wird sie automatisch verschlüsselt. Sie wird automatisch als verschlüsselte virtuelle Festplatte konfiguriert, es sei denn, die aktivierte Verschlüsselungsoption wird während der Erstellung der virtuellen Festplatte deaktiviert.

Sie müssen über die Berechtigung zur Anmeldung und zur Server-Steuerung zur Verwaltung der Schlüssel für die Verschlüsselung verfügen.

ANMERKUNG: Obwohl Verschlüsselung auf den Controllern aktiviert ist, muss der Benutzer manuell die Verschlüsselung auf der VD aktivieren, wenn die VD vom iDRAC erstellt wird. Nur wenn die VD vom OMSA erstellt wird, wird sie automatisch verschlüsselt.

Zuweisen oder Aufheben der Zuweisung von dezidierten Hotspares

Ein dedizierter Hotspare ist eine nicht verwendete Backup-Festplatte, die einer virtuellen Festplatte zugewiesen ist. Wenn eine physische Festplatte in der virtuellen Festplatte versagt, wird der Hotspare aktiviert, um die fehlerhafte physische Festplatte ohne Unterbrechung des Systems oder erforderlichen Benutzereingriff zu ersetzen.

Sie müssen über Berechtigungen zum Anmelden und für die Server-Steuerung verfügen, um diesen Vorgang auszuführen.

Sie können nur Festplatten mit 4 KB als Hotspare zu virtuellen 4-KB-Festplatten zuweisen.

Wenn Sie eine physische Festplatte als dedizierten Hotspare im Modus „Zu ausstehenden Vorgängen hinzufügen“ zugewiesen haben, wird der ausstehende Vorgang erstellt, jedoch kein Job erstellt. Wenn Sie versuchen, die Zuweisung des dedizierten Hotspares aufzuheben, wird der ausstehende Vorgang für das Zuweisen eines dedizierten Hotspares gelöscht.

Wenn Sie die Zuweisung einer physischen Festplatte als dedizierten Hotspare im Modus „Zu ausstehenden Vorgängen hinzufügen“ aufgehoben haben, wird der ausstehende Vorgang erstellt, jedoch kein Job erstellt. Wenn Sie dann versuchen, den dedizierten Hotspares zuzuweisen, wird der ausstehende Vorgang für das Aufheben der Zuweisung eines dedizierten Hotspares gelöscht.

ANMERKUNG: Während des Exportvorgangs des Protokolls können Sie keine Informationen über dedizierte Hotspares auf der Seite **Manage Virtual Disks** (Virtuelle Laufwerke verwalten) anzeigen. Im Anschluss an den Exportvorgang des Protokolls laden Sie die Seite **Manage Virtual Disks** (Virtuelle Laufwerke verwalten) erneut oder aktualisieren Sie sie, damit die Informationen angezeigt werden.

Umbenennen von virtuellen Festplatten

Zum Ändern des Namens einer virtuellen Festplatte muss der Benutzer über die Systemsteuerungsberechtigung verfügen. Der Name der virtuellen Festplatte darf nur alphanumerische Zeichen, Leerzeichen, Gedankenstriche und Unterstriche enthalten. Die maximale Länge des Namens hängt vom jeweiligen Controller an. In den meisten Fällen beträgt die maximale Länge 15 Zeichen. Der Name darf nicht mit einem Leerzeichen beginnen oder enden und das Feld darf nicht leer sein. Bei jeder Umbenennung einer virtuellen Festplatte wird ein LC-Protokoll erstellt.

Bearbeiten der Festplattenkapazität

Online Capacity Expansion (OCE) ermöglicht es Ihnen, die Speicherkapazität der ausgewählten RAID-Stufen zu erhöhen, während das System online bleibt. Der Controller verteilt die Daten auf dem Array neu (Neukonfiguration) und platziert neuen Speicherplatz am Ende jedes RAID-Array.

Online Capacity Expansion (OCE) kann auf zwei Arten erreicht werden:

- Wenn freier Speicherplatz auf dem kleinsten physischen Laufwerk in der virtuellen Festplattengruppe nach dem Starten der LBA virtueller Festplatten verfügbar ist, kann die Kapazität der virtuellen Festplatte in diesem freien Speicherplatz erweitert werden. Diese Option ermöglicht Ihnen die Eingabe der neuen erhöhten Größe der virtuellen Festplatte. Wenn in einer Festplattengruppe auf einer virtuellen Festplatte nur Speicherplatz vor dem Starten der LBA verfügbar ist, ist das Bearbeiten der Festplattenkapazität in derselben Festplattengruppe nicht zulässig, selbst wenn verfügbarer Speicherplatz auf einem physischen Laufwerk vorhanden ist.
- Die Kapazität eines virtuellen Laufwerks kann ebenfalls erweitert werden, indem Sie zusätzliche kompatible physische Laufwerke zur bestehenden virtuellen Festplattengruppe hinzufügen. Diese Option erlaubt Ihnen nicht die Eingabe der neuen erhöhten Größe der virtuellen Festplatte. Die neue erhöhte Größe der virtuellen Festplatte wird basierend auf dem verwendeten Festplatten-Speicherplatz der bestehenden physischen Festplattengruppe auf einer bestimmten virtuellen Festplatte, der RAID-Stufe der virtuellen Festplatte und der Anzahl der neuen Laufwerke (zur virtuellen Festplatte hinzugefügt) berechnet und dem Benutzer angezeigt.

Die Kapazitätserweiterung erlaubt dem Benutzer die Angabe der endgültigen Größe der virtuellen Festplatte. Die interne finale Größe der virtuellen Festplatte wird an PERC in Prozent übertragen. (Dieser Prozentsatz ist der leere Speicherplatz im Array, den der Benutzer für die Erweiterung der lokalen Festplatte verwenden möchte.) Aufgrund dieser Prozentsatzlogik kann sich die finale Größe der virtuellen Festplatte nach der Neukonfiguration von dem unterscheiden, was der Benutzer für folgendes Szenario angegeben hat: Der Benutzer verwendet nicht die maximal mögliche Größe der virtuellen Festplatte als finale Größe der virtuellen Festplatte (Prozentsatz kleiner als 100 %). Der Benutzer sieht keinen Unterschied zwischen dieser eingegebenen Größe der virtuellen Festplatte und der finalen Größe der Festplatte nach der Neukonfiguration, wenn die maximal mögliche Größe der virtuellen Festplatte vom Benutzer eingegeben wird.

RAID-Level-Migration

RAID-Level-Migration (RLM) bezieht sich auf die Änderung des RAID-Levels eines virtuellen Laufwerks. iDRAC9 bietet eine Option zum Erhöhen der Größe eines virtuellen Laufwerks unter Verwendung von RLM. RLM erlaubt gewissermaßen die Migration des RAID-Levels eines virtuellen Laufwerks, was wiederum die Größe des virtuellen Laufwerks senken kann.

Die RAID-Level-Migration ist die Konvertierung eines virtuellen Laufwerks von einem RAID-Level zum anderen. Wenn Sie ein virtuelles Laufwerk in ein anderes RAID-Level migrieren, werden die Benutzerdaten neu verteilt und erhalten das Format der neuen Konfiguration.

Diese Konfiguration wird unterstützt wird von der Bereitstellung- und Echtzeitoption unterstützt.

Die folgende Tabelle beschreibt die möglichen neu konfigurierbaren Layouts des virtuellen Laufwerks während der Neukonfiguration (RLM) eines virtuellen Laufwerks mit und ohne Hinzufügen von Festplatten.

Tabelle 54. Mögliches Layout des virtuellen Laufwerks

Layout des virtuellen Quelllaufwerks	Mögliches Layout des virtuellen Ziellaufwerks mit hinzugefügtem Laufwerk	Mögliches Layout des virtuellen Ziellaufwerks ohne hinzugefügtes Laufwerk
R0 (einzelne Festplatte)	R1	-
R0	R5/R6	-
R1	R0/R5/R6	R0

Tabelle 54. Mögliches Layout des virtuellen Laufwerks (fortgesetzt)

Layout des virtuellen Quelllaufwerks	Mögliches Layout des virtuellen Ziellaufwerks mit hinzugefügtem Laufwerk	Mögliches Layout des virtuellen Ziellaufwerks ohne hinzugefügtes Laufwerk
R5	R0/R6	R0
R6	R0/R5	R0/R5

Zulässige Operationen während OCE oder RLM

Die folgenden Vorgänge sind während OCE/RLM zulässig:

Tabelle 55. Zulässige Operationen

Ab Controller-Ende, hinter dem ein Laufwerk OCE/RLM durchläuft	Ab Laufwerkende (das OCE/RLM durchläuft)	Ab eines beliebigen bereiten physischen Laufwerks im selben Controller	Ab einem beliebigen Laufwerkende (das nicht OCE/RLM durchläuft) im selben Controller
Konfigurations-Reset	Löschen	Blinken	Löschen
Exportieren des Protokolls	Blinken	Blinken beenden	Blinken
Patrol Read-Modus einstellen	Blinken beenden	Globalen Hotspare zuweisen	Blinken beenden
Patrol Read starten		In eine Nicht-RAID-Festplatte konvertieren	Umbenennen
Controller-Eigenschaften ändern			Regel ändern
Strom der physischen Festplatte verwalten			Langsam initialisieren
In RAID-fähige Festplatten konvertieren			Schnell initialisieren
In Nicht-RAID-Festplatten konvertieren			Mitgliedfestplatte ersetzen
Controller-Modus ändern			

OCE- und RLM-Beschränkungen oder -Einschränkungen

Nachstehend sind die allgemeinen Einschränkungen für OCE und RLM aufgeführt:

- OCE/RLM beschränkt sich auf das Szenario, bei dem die Laufwerksgruppe nur ein VD enthält.
- OCE wird auf Systemen mit RAID50 und RAID60 nicht unterstützt. RLM wird nicht auf Systemen mit RAID10, RAID50 und RAID60 unterstützt.
- Wenn der Controller bereits die maximal zulässige Anzahl virtueller Laufwerke enthält, können Sie auf RAID-Level weder eine Migration noch eine Kapazitätserweiterung eines virtuellen Laufwerks durchführen.
- Der Controller ändert die Cache-Schreibrichtlinie aller virtuellen Laufwerke, für die ein RLM-/OCE-Vorgang durchgeführt wird, zu „Write-Through“, bis der Vorgang abgeschlossen ist.
- Die Neukonfiguration virtueller Laufwerke beeinträchtigt normalerweise die Laufwerkleistung bis zum Abschluss des Vorgangs.
- Eine Laufwerksgruppe darf nicht mehr als 32 physische Laufwerke insgesamt enthalten.
- Wenn auf dem entsprechenden VD/PD bereits ein Vorgang im Hintergrund (wie BGI/Rebuild/Copyback/Patrol Read) ausgeführt wird, dann ist die Neukonfiguration (OCE/RLM) zu dem Zeitpunkt nicht zulässig.
- Während der Neukonfiguration (OCE/RLM) auf Laufwerken, die mit dem VD verknüpft sind, bewirkt jegliche Art der Laufwerksmigration, dass die Neukonfiguration fehlschlägt.
- Jedes für OCE/RLM neu hinzugefügte Laufwerk wird nach Abschluss der Neukonfiguration Bestandteil des VD. Doch der Status für diese neuen Laufwerke ändert sich direkt nach Beginn der Neukonfiguration in „Online“.

Initialisierung abbrechen

Diese Funktion bietet die Möglichkeit, die Hintergrundinitialisierung auf einer virtuellen Festplatte abzubrechen. Auf PERC-Controllern beginnt die Hintergrundinitialisierung redundanter virtueller Festplatten automatisch nach der Erstellung einer virtuellen Festplatte. Die Hintergrundinitialisierung redundanter virtueller Festplatten bereitet die virtuelle Festplatte auf Paritätsinformationen vor und verbessert die Schreibleistung. Einige Prozesse wie das Erstellen einer virtuellen Festplatte können jedoch nicht ausgeführt werden, während die Hintergrundinitialisierung läuft. Das Abbrechen der Initialisierung bietet die Möglichkeit, die Hintergrundinitialisierung manuell abzubrechen. Nach dem Abbrechen wird die Hintergrundinitialisierung automatisch innerhalb von 0 bis 5 Minuten neu gestartet.

ANMERKUNG: Die Hintergrundinitialisierung ist nicht auf virtuelle Festplatten mit RAID 0 anwendbar.

Verwalten von virtuellen Festplatten über die Webschnittstelle

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Speicherkonfiguration** > **Virtuelle Laufwerkkonfiguration**.
2. Wählen Sie aus dem Drop-Down-Menü **Virtuelles Laufwerk** den Controller aus, für den Sie die virtuellen Laufwerke verwalten möchten.
3. Wählen Sie aus dem Drop-Down-Menü **Aktion** eine Aktion aus.

   Wenn Sie eine Aktion auswählen, wird das zusätzliche Fenster **Aktion** angezeigt. Wählen bzw. geben Sie den gewünschten Wert ein.
   - **Umbenennen**
   - **Löschen**
   - **Cache-Regel bearbeiten** – Sie können die Cache-Richtlinie für die folgenden Optionen ändern:
     - **Leserichtlinie** – Folgende Werte können ausgewählt werden:
       - **Adaptives Vorauslesen** – Gibt an, dass die Steuerung für den angegebenen Datenträger die Vorauslese-Cache-Richtlinie verwendet, falls die zwei letzten Zugriffe auf die Festplatte in sequenziellen Sektoren vorgenommen wurden. Falls die Leseanforderungen zufällig sind, kehrt der Controller zum Modus 'Kein Vorauslesen' zurück.
       - **Kein Vorauslesen** – Zeigt an, dass für den gewählten Datenträger die Kein Vorauslesen-Regel verwendet wird.
       - **Vorauslesen** – Gibt an, dass der Controller für den angegebenen Datenträger die angeforderten Daten sequenziell voraus liest und zusätzliche Daten im Cache-Speicher speichert, um auf eine künftige Datenanforderung vorbereitet zu sein. Dies beschleunigt das sequenzielle Lesen von Daten, ergibt aber kaum bessere Ergebnisse, wenn auf zufällige Daten zugegriffen wird.
     - **Schreibregel** – Ändern der Schreib-Cache-Regel auf eine der folgenden Optionen:
       - **Durchschreiben** – Zeigt an, dass der Controller für den gewählten Datenträger ein Datenübertragungsabschluss-Signal an den Host sendet, wenn das Festplatten-Subsystem alle Daten einer Transaktion empfangen hat.
       - **Rückschreiben** — Gibt an, dass der Controller für den angegebenen Datenträger ein Datenübertragungsabschluss-Signal an das Hostsystem sendet, wenn der Controller-Cachespeicher alle Daten in einer Transaktion erhalten hat. Der Controller schreibt dann die zwischengespeicherten Daten auf das Speichergerät im Hintergrund.
       - **Rückschreiben erzwingen** — Wenn durch Rückschreiben erzwingen Daten im Cache-Speicher abgelegt werden, wird Schreib-Cache aktiviert, egal ob der Controller eine Batterie hat oder nicht. Wenn der Controller keine Batterie hat und Rückschreiben in Cache erzwingen verwendet wird, kann bei einem Stromausfall ein Datenverlust auftreten.
     - **Festplatten-Cache-Regel** – Ändern der Festplatten-Cache-Regel auf eine der folgenden Optionen:
       - **Standardeinstellung** – Zeigt an, dass die Festplatte ihren Standardmodus für den Schreib-Cache verwendet. Für SATA-Festplatten lautete dieser „aktiviert“ und für SAS- Festplatten „deaktiviert“.
       - **Aktiviert** – Zeigt an, dass der Schreib-Cache der Festplatte aktiviert ist. Dies erhöht die Leistung und die Wahrscheinlichkeit eines Datenverlusts bei einem Stromausfall.
       - **Deaktiviert** – Zeigt an, dass der Schreib-Cache der Festplatte deaktiviert ist. Dies verringert die Leistung und die Wahrscheinlichkeit eines Datenverlusts.
   - **Kapazität der Festplatte bearbeiten** – Sie können in diesem Fenster die physikalischen Laufwerke zum ausgewählten virtuellen Laufwerk hinzufügen. In diesem Fenster werden außerdem die aktuelle Kapazität und die neue Kapazität des virtuellen Laufwerks nach dem Hinzufügen der physischen Laufwerke angezeigt.
   - **RAID-Level-Migration** – Zeigt den Laufwerknamen, das aktuelle RAID-Level und die Größe des virtuellen Laufwerks an. Ermöglicht Ihnen die Auswahl eines neuen RAID-Levels. Der Benutzer muss möglicherweise den vorhandenen virtuellen Laufwerken zusätzliche Laufwerke hinzufügen, um zu einem neuen RAID-Level zu migrieren. Diese Funktion gilt nicht für RAID 10, 50 und 60.
   - **Initialisieren: Schnell** – Aktualisiert die Metadaten auf den physischen Laufwerken, sodass der gesamte Laufwerkpeicherplatz für künftige Schreibvorgänge verfügbar ist. Die Initialisierungsoption kann schnell abgeschlossen werden, da vorhandene Informationen auf den physischen Laufwerken nicht gelöscht werden, obwohl künftige Schreibvorgänge alle Informationen überschreiben, die auf den physischen Laufwerken verbleiben.
   - **Initialisieren: Vollständig**: Alle vorhandenen Daten und Dateisysteme werden gelöscht.

     ANMERKUNG: Die Option **Initialisieren: Vollständig** gilt nicht für PERC H330-Controller.

- **Übereinstimmungsüberprüfung** - Zum Überprüfen der Übereinstimmung eines virtuellen Laufwerks wählen Sie **Übereinstimmungsüberprüfung** im entsprechenden Dropdown-Menü.

  ANMERKUNG: Übereinstimmungsprüfung wird nicht unterstützt auf Laufwerken, die im RAID0-Modus eingerichtet sind.

Weitere Informationen zu diesen Optionen finden Sie in der *CMC-Online-Hilfe*.

4. Klicken Sie auf **Jetzt anwenden**, um die Änderungen sofort durchzuführen. Klicken Sie auf **Nächster Neustart**, um die Änderungen nach dem nächsten Neustart anzuwenden. Klicken Sie auf **Zu einer geplanten Zeit**, um die Änderungen zu einem bestimmten Zeitpunkt anzuwenden und **Alle Ausstehenden verwerfen**, um die Änderungen zu verwerfen.

   Basierend auf dem ausgewählten Betriebsmodus werden die Einstellungen angewendet.

Verwalten von virtuellen Festplatten über RACADM

Verwenden Sie die folgenden RACADM-Befehle, um virtuelle Festplatten zu verwalten:

- So löschen Sie eine virtuelle Festplatte:

```
racadm storage deletevd:<VD FQDD>
```

- So initialisieren Sie eine virtuelle Festplatte:

```
racadm storage init:<VD FQDD> -speed {fast|full}
```

- So überprüfen Sie die Übereinstimmung von virtuellen Festplatten (nicht unterstützt auf RAID0):

```
racadm storage ccheck:<vdisk fqdd>
```

  So brechen Sie die Konsistenzprüfung ab:

```
racadm storage cancelcheck: <vdisks fqdd>
```

- So verschlüsseln Sie virtuelle Festplatten:

```
racadm storage encryptvd:<VD FQDD>
```

- So weisen Sie dedizierte Hotspares zu oder machen die Zuweisung rückgängig:

```
racadm storage hotspare:<Physical Disk FQDD> -assign <option> -type dhs -vdkey: <FQDD of VD>
```

<option>=Ja

Hotspare zuweisen

<Option>=Nein

Zuweisung von Hotspare aufheben

RAID-Konfigurationsfunktionen

Die folgende Tabelle zeigt einige der RAID-Konfigurationsfunktionen, die in RACADM und WSMan verfügbar sind:

VORSICHT: Wenn ein physisches Laufwerk dazu gezwungen wird, online oder offline zu gehen, kann dies zu Datenverlusten führen.

Tabelle 56. RAID-Konfigurationsfunktionen

Funktion	RACADM-Befehl	Beschreibung
Online erzwingen	`racadm storage forceonline:<PD FQDD>`	Ein Stromausfall, beschädigte Daten oder andere Gründe können dazu führen, dass ein physisches Laufwerk offline gesetzt wird. Mit dieser Funktion können Sie erzwingen, dass eine physische Festplatte wieder in einen Online-Zustand gesetzt wird, wenn alle anderen Optionen erschöpft sind. Sobald der Befehl ausgeführt wird,

Tabelle 56. RAID-Konfigurationsfunktionen (fortgesetzt)

Funktion	RACADM-Befehl	Beschreibung
		versetzt der Controller das Laufwerk wieder in den Online-Zustand und stellt die Mitgliedschaft innerhalb der virtuellen Festplatte wieder her. Dies geschieht nur, wenn der Controller das Laufwerk lesen und in die entsprechenden Metadaten schreiben kann.
ANMERKUNG: Die Datenwiederherstellung ist nur dann möglich, wenn ein begrenzter Teil der Festplatte beschädigt ist. Die Funktion „Online erzwingen“ kann eine bereits fehlerhafte Festplatte nicht reparieren.		
Offline erzwingen	`racadm storage forceoffline:<PD FQDD>`	Diese Funktion entfernt ein Laufwerk aus einer virtuellen Laufwerkkonfiguration, so dass es offline geht, was zu einer herabgestuften Konfiguration des virtuellen Laufwerks führt. Die Funktion ist hilfreich, wenn ein Laufwerk wahrscheinlich bald ausfallen wird oder einen SMART-Ausfall meldet, aber noch immer online ist. Sie kann auch verwendet wird, wenn Sie ein Laufwerk nutzen möchten, das Teil einer bestehenden RAID-Konfiguration ist.
Physisches Laufwerk ersetzen	`racadm storage replacephysicaldisk:<Source PD FQDD > -dstpd <Destination PD FQDD>`	Mit dieser Funktion können Sie Daten von einem physischen Laufwerk, das ein Mitglied eines virtuellen Laufwerks ist, auf ein anderes physisches Laufwerk kopieren. Das Quelllaufwerk sollte sich im Online-Zustand befinden, während sich die Zielfestplatte im Zustand „Bereit“ befinden und eine ähnlichen Größe und einen ähnlichen Typ zum Ersetzen der Quelle aufweisen sollte.
Virtuelles Laufwerk als Startgerät	`racadm storage setbootvd:<controller FQDD> -vd <VirtualDisk FQDD>`	Ein virtuelles Laufwerk kann mit dieser Funktion als Startgerät konfiguriert werden. Dies ermöglicht eine Fehlertoleranz, wenn ein virtuelles Laufwerk mit Redundanz als Startgerät ausgewählt wurde und außerdem das Betriebssystem darauf installiert ist.
Fremdkonfigurationen entsperren	`racadm storage unlock:<Controller FQDD> -key <Key id> -passwd <passphrase>`	Diese Funktion wird verwendet, um gesperrte Laufwerke zu authentifizieren, die eine andere Quellcontrollerverschlüsselung aufweisen als das Ziel. Sobald die Konfiguration entsperrt ist, kann das Laufwerk erfolgreich von einem Controller zu einem anderen migriert werden.

Verwalten von Controllern

Sie können die folgenden Schritte für Controller ausführen:

- Controller-Eigenschaften konfigurieren
- Fremdkonfigurationen importieren oder automatisch importieren
- Fremdkonfiguration löschen
- Controller-Konfiguration zurücksetzen
- Sicherheitsschlüsseln erstellen, ändern oder löschen
- Beibehaltenen Cache verwerfen

Konfigurieren der Controller-Eigenschaften

Sie können die folgenden Eigenschaften für den Controller konfigurieren:

- Patrol Read-Modus (automatisch oder manuell)
- Patrol Read starten oder stoppen, wenn der Patrol Read-Modus manuell bedient wird
- Patrol Read – Nicht konfigurierte Bereiche
- Übereinstimmungsüberprüfungsmodus
- Copyback-Modus
- Lastausgleichsmodus
- Übereinstimmungsüberprüfungsrate
- Neuerstellungsrate
- Hintergrund-Initialisierungsrate
- Rekonstruktionsrate
- Erweiterter automatischer Fremdkonfigurationsimport
- Sicherheitsschlüssel erstellen oder ändern
- Verschlüsselungsmodus (Verwaltung von lokalen Schlüsseln und Secure Enterprise Key Manager)

Sie müssen über die Berechtigung zur Anmeldung und Server-Steuerung verfügen, um die Controller-Eigenschaften konfigurieren zu können.

Überlegungen zum Patrol Read-Modus

Patrol Read identifiziert Festplattenfehler, um Festplattenausfälle und Datenverlust oder -beschädigung zu vermeiden. Es läuft automatisch einmal pro Woche auf SAS- und SATA-Festplatten.

Patrol Read wird unter den folgenden Umständen nicht auf einem physischen Laufwerk ausgeführt:

- Das physische Laufwerk ist eine SSD.
- Das physische Laufwerk ist nicht in einem virtuellen Laufwerk eingeschlossen oder als Hot Spare zugewiesen.
- Das physische Laufwerk ist in einem virtuellen Laufwerk enthalten, das zurzeit in eines der folgenden Verfahren eingebunden ist:
  - Eine Neuerstellung
  - Eine Neukonfiguration oder ein Neuaufbau
  - Eine Hintergrundinitialisierung
  - Eine Übereinstimmungsüberprüfung

Zusätzlich wird der Patrol Read-Vorgang bei hoher E/A-Aktivität unterbrochen und wieder aufgenommen, wenn die E/A-Aktivitäten abgeschlossen sind.

ANMERKUNG: Weitere Informationen dazu, wie oft der Patrol Read-Vorgang ausgeführt wird, wenn er sich im automatischen Modus befindet, stehen in der entsprechenden Controller-Dokumentation zur Verfügung.

ANMERKUNG: Vorgänge im Patrol Read-Modus wie **Starten** und **Stoppen** werden nicht unterstützt, wenn keine virtuellen Laufwerke auf dem Controller verfügbar sind. Sie können jedoch die Vorgänge erfolgreich mit den iDRAC-Schnittstellen aufrufen. Die Vorgänge schlagen fehl, wenn der verknüpfte Job gestartet wird.

Load-Balance

Die Eigenschaft „Load-Balance“ ermöglicht die automatische Nutzung beider Controller-Schnittstellen oder den Anschluss der Konnektoren am selben Gehäuse, um E/A-Aufforderungen weiterzuleiten. Diese Eigenschaft ist nur für SAS-Controller verfügbar.

Hintergrund-Initialisierungsrate

ANMERKUNG: Sowohl H330 als auch H345 müssen den Treiber geladen haben, damit die Hintergrund-Initialisierungsvorgänge ausgeführt werden können.

Auf PERC-Controllern beginnt die Hintergrundinitialisierung redundanter virtueller Laufwerke automatisch innerhalb von 0 bis 5 Minuten nach der Erstellung eines virtuellen Laufwerks. Die Hintergrundinitialisierung redundanter virtueller Laufwerke bereitet das virtuelle Laufwerk auf die Verwaltung redundanter Daten vor und verbessert die Schreibleistung. Nachdem die Hintergrundinitialisierung einer virtuellen RAID 5-Festplatte abgeschlossen wurde, wurden beispielsweise die Paritätsinformationen initialisiert. Nachdem die Hintergrundinitialisierung einer virtuellen RAID 1-Festplatte abgeschlossen wurde, werden die physischen Laufwerke gespiegelt.

Die Hintergrundinitialisierung hilft dem Controller, Probleme zu identifizieren und zu beheben, die später durch die redundanten Daten auftreten können. In dieser Hinsicht ähnelt die Hintergrundinitialisierung einer Übereinstimmungsüberprüfung. Die Hintergrundinitialisierung sollte ausgeführt werden können, bis sie abgeschlossen ist. Im Falle einer Unterbrechung startet die Hintergrundinitialisierung automatisch innerhalb von 0 bis 5 Minuten erneut. Einige Prozesse, wie Lese- und Schreibvorgänge, sind möglich, während die Hintergrundinitialisierung ausgeführt wird. Andere Prozesse, wie das Erstellen eines virtuellen Laufwerks, können jedoch nicht ausgeführt werden, während die Hintergrundinitialisierung läuft. Diese Prozesse führen dazu, dass die Hintergrundinitialisierung abgebrochen wird.

Die Hintergrundinitialisierungsrate, konfigurierbar zwischen 0 und 100 %, ist der Prozentsatz der Systemressourcen für die Ausführung der Hintergrundinitialisierung. Bei 0 % hat die Hintergrundinitialisierung die niedrigste Priorität für den Controller, dauert am längsten und hat die geringste Auswirkung auf die Systemleistung. Eine Hintergrundinitialisierung von 0 % bedeutet nicht, dass der Ablauf angehalten oder unterbrochen wird. Bei 100 % hat die Hintergrundinitialisierung die höchste Priorität für den Controller. Die Hintergrundinitialisierungszeit wird minimiert und diese Einstellung hat die größte Auswirkung auf die Systemleistung.

Übereinstimmungsüberprüfung

Die Übereinstimmungsüberprüfung überprüft die Richtigkeit der redundanten Informationen (Paritätsinformationen). Diese Aufgabe gilt nur für redundante virtuelle Laufwerke. Bei Bedarf können über die Übereinstimmungsüberprüfung redundante Daten neu erstellt werden. Falls das virtuelle Laufwerk den Zustand „Fehlerhafte Redundanz“ aufweist, kann dieser Zustand möglicherweise durch das Durchführen einer Übereinstimmungsüberprüfung in den Zustand „Bereit“ geändert werden.

Die Übereinstimmungsüberprüfungsrate, konfigurierbar zwischen 0 und 100 %, ist der Prozentsatz der Systemressourcen für die Übereinstimmungsüberprüfung. Bei 0 % hat die Übereinstimmungsüberprüfung die niedrigste Priorität für den Controller, dauert am längsten und hat die geringste Auswirkung auf die Systemleistung. Eine Übereinstimmungsüberprüfungsrate von 0 % bedeutet nicht, dass die Übereinstimmungsüberprüfung angehalten oder unterbrochen wird. Bei 100 % hat die Übereinstimmungsüberprüfung die höchste Priorität für den Controller. Die Übereinstimmungsüberprüfungszeit wird minimiert und diese Einstellung hat die größte Auswirkung auf die Systemleistung.

Sicherheitsschlüssel erstellen oder ändern

Bei der Konfiguration der Controller-Eigenschaften können Sie Sicherheitsschlüssel erstellen oder ändern. Der Controller verwendet den Verschlüsselungsschlüssel, um den Zugriff auf SED freizugeben oder zu sperren. Sie können nur einen Verschlüsselungsschlüssel für jeden verschlüsselungsfähigen Controller erstellen. Der Sicherheitsschlüssel verwaltet die folgenden Funktionen:

1. **Local Key Management (LKM) System** - LKM wird zur Generierung der Schlüssel-ID sowie des Kennworts oder Schlüssels verwendet, die erforderlich sind, um das virtuelle Laufwerk zu sichern. Wenn Sie LKM (Local Key Management) verwenden, müssen Sie den Verschlüsselungsschlüssel erstellen, indem Sie die Sicherheitsschlüssel-Kennung und die Passphrase angeben.
2. **Secure Enterprise Key Manager (SEKM)** - Diese Funktion generiert den Schlüssel mithilfe des Key Management Servers (KMS). Wenn Sie SEKM verwenden, müssen Sie iDRAC mit den KMS-Daten und der SSL-bezogenen Konfiguration konfigurieren.

ANMERKUNG:

- Dieser Task wird auf den PERC-Hardware-Controllern, die im eHBA-Modus ausgeführt werden, nicht unterstützt.
- Wenn Sie den Sicherheitsschlüssel im Betriebsmodus „Zu ausstehenden Vorgängen hinzufügen“ erstellen und kein Job erstellt wurde und Sie dann den Sicherheitsschlüssel löschen, wird der Job „Ausstehende Sicherheitsschlüsselerstellung“ gelöscht.

ANMERKUNG:

- Für die Aktivierung von SEKM müssen Sie sicherstellen, dass die unterstützte PERC-Firmware installiert ist.
- Sie können die PERC-Firmware nicht auf die vorhergehende Version herabstufen, wenn SEKM aktiviert ist. Eine Herabstufung anderer PERC-Controller-Firmware im selben System schlägt eventuell ebenfalls fehl, wenn sich der Controller nicht im SEKM-Modus befindet. Zum Herabstufen der Firmware für die PERC-Controller, die sich nicht im SEKM-Modus befinden, können Sie die OS DUP-Aktualisierungsmethode verwenden oder SEKM auf den Controllern deaktivieren und das Herabstufen des iDRAC wiederholen.

ANMERKUNG: Beim Import eines gesperrten Hot-Plug-Volumes von einem Server auf einen anderen werden Ihnen die CTL-Einträge für die Controller-Attribute angezeigt, die im LC-Protokoll angewendet werden.

Konfigurieren der Controller-Eigenschaften über die Webschnittstelle

1. Gehen Sie in der iDRAC-Web-Schnittstelle zu **Storage (Speicher)** > **Overview (Übersicht)** > **Controllers (Controller)**. Daraufhin wird die Seite **Controller-Setup** angezeigt.
2. Wählen Sie im Bereich **Controller** den Controller aus, den Sie konfigurieren möchten.
3. Geben Sie die erforderlichen Informationen für die verschiedenen Eigenschaften an.

   Die Spalte **Current Value (Aktueller Wert)** zeigt die vorhandenen Werte für jede Eigenschaft an. Sie können diesen Wert ändern, indem Sie die Option aus dem Drop-Down-Menü **Action (Aktion)** für jede Eigenschaft auswählen.

   Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.
4. Wählen Sie bei **Apply Operation Mode (Betriebsmodus anwenden)**, wann Sie die Einstellungen anwenden möchten.
5. Klicken Sie auf **Anwenden**.

   Basierend auf dem ausgewählten Betriebsmodus werden die Einstellungen angewendet.

Konfigurieren von VR-Controller-Eigenschaften über RACADM

- So legen Sie den Patrol Read-Modus fest:

  ```
  racadm set storage.controller.<index>.PatrolReadMode  {Automatic | Manual | Disabled}
  ```

- Wenn der Patrol Read-Modus auf „Manuell“ eingestellt ist, verwenden Sie die folgenden Befehle zum Starten und Beenden des Patrol Read-Modus:

  ```
  racadm storage patrolread:<Controller FQDD> -state {start|stop}
  ```

  ANMERKUNG: Vorgänge im Patrol Read-Modus wie Starten und Stoppen werden nicht unterstützt, wenn keine virtuellen Festplatten auf dem Controller verfügbar sind. Sie können jedoch die Vorgänge erfolgreich mit den iDRAC-Schnittstellen aufrufen. Die Vorgänge schlagen fehl, wenn der verknüpfte Auftrag gestartet wird.
- Um den Übereinstimmungsüberprüfungsmodus festzulegen, verwenden Sie das Objekt **Storage.Controller.CheckConsistencyMode**.
- Um den Copyback-Modus zu aktivieren oder zu deaktivieren, verwenden Sie das Objekt **Storage.Controller.CopybackMode**.
- Um den Lastausgleichsmodus zu aktivieren oder zu deaktivieren, verwenden Sie das Objekt **Storage.Controller.PossibleloadBalancedMode**.
- Um den Prozentsatz der Systemressourcen festzulegen, der für die Ausführung der Übereinstimmungsüberprüfung auf einer redundanten virtuellen Festplatte abgestellt sind, verwenden das Objekt **Storage.Controller.CheckConsistencyRate**.
- Um den Prozentsatz der Controller-Ressourcen festzulegen, der für die Neuerstellung einer fehlerhaften Festplatte abgestellt wurden, verwenden Sie das Objekt **Storage.Controller.RebuildRate**.
- Um den Prozentsatz der Controller-Ressourcen festzulegen, der für die Hintergrundinitialisierung einer virtuellen Festplatte nach deren Erstellung abgestellt wurden, verwenden Sie das Objekt **Storage.Controller.BackgroundInitializationRate**
- Um den Prozentsatz der Controller-Ressourcen festzulegen, der für die Neuerstellung einer Festplattengruppe nach dem Hinzufügen einer physischen Festplatte oder der Änderungen der RAID-Ebene einer virtuellen Festplatte in einer Festplattengruppe abgestellt wurde, verwenden Sie das Objekt **Storage.Controller.ReconstructRate**.
- Um den erweiterten automatischen Import einer Fremdkonfigurationen für den Controller zu (de-)aktivieren, verwenden Sie das Objekt **Storage.Controller.EnhancedAutoImportForeignConfig**.
- Verwenden Sie zum Erstellen, Ändern oder Löschen des Sicherheitsschlüssels zum Verschlüsseln von virtuellen Festplatten die folgenden Befehle:

  ```
  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>
  ```

Importieren oder automatisches Importieren von Fremdkonfigurationen

Bei einer Fremdkonfiguration handelt es sich um Daten auf physischen Festplatten, die von einem Controller zu einem anderen verschoben wurden. Virtuelle Festplatten, die sich auf verschobenen physischen Festplatten befinden, werden als Fremdkonfiguration betrachtet.

Sie können Fremdkonfigurationen importieren, sodass die virtuellen Festplatten nach dem Verschieben der physischen Festplatten nicht verloren gehen. Eine Fremdkonfiguration kann nur importiert werden, wenn sie eine virtuelle Festplatte enthält, die entweder den Zustand „Ready“ (Bereit) oder „Degraded“ (Herabgesetzt) hat, oder ein Hotspare, das für ein virtuelles Laufwerk bestimmt ist, das importiert werden kann oder bereits vorhanden ist.

Alle Daten der virtuellen Festplatten müssen vorhanden sein, doch wenn die virtuelle Festplatte eine redundante RAID-Stufe verwendet, dann sind die zusätzlichen redundanten Daten nicht erforderlich.

Wenn beispielsweise die Fremdkonfiguration nur eine Seite einer Spiegelung in einer virtuellen RAID 1-Festplatte enthält, befindet sich die virtuelle Festplatte im Zustand „Degraded“ (Herabgesetzt) und kann importiert werden. Wenn die Fremdkonfiguration nur eine physische Festplatte enthält, die ursprünglich als RAID 5 mit drei physischen Festplatten konfiguriert wurde, befindet sich die virtuelle RAID 5-Festplatte im Zustand „Failed“ (Fehlerhaft) und kann nicht importiert werden.

Eine Fremdkonfiguration kann neben virtuellen Festplatten auch eine physische Festplatte enthalten, die auf einem Controller als Hotspare zugewiesen und dann auf einen anderen Controller verschoben wurde. Die Aufgabe „Import Foreign Configuration“ (Fremdkonfiguration importieren) importiert die neue physische Festplatte als Hotspare. Wenn die physische Festplatte auf dem vorhergehenden Controller ein dedizierter Hotspare war, aber die virtuelle Festplatte, zu der der Hotspare zugewiesen war, nicht mehr in der Fremdkonfiguration enthalten ist, wird die physische Festplatte als globaler Hotspare importiert.

Wenn mit Local Key Manager (LKM) gesperrte Fremdkonfigurationen ermittelt werden, ist der Import von Fremdkonfigurationen in dieser Version im iDRAC nicht möglich. Sie müssen die Laufwerke über die Tastenkombination STRG+R entsperren und dann den Import von Fremdkonfigurationen aus dem iDRAC fortsetzen.

Die Aufgabe „Import Foreign Configuration“ (Fremdkonfiguration importieren) wird nur angezeigt, wenn der Controller eine Fremdkonfiguration erkannt hat. Durch Überprüfung des Zustands der physischen Festplatte können Sie auch feststellen, ob eine physische Festplatte eine Fremdkonfiguration (virtuelle Festplatte oder Hotspare) enthält. Wenn der Zustand der physischen Festplatte „Foreign“ (Fremd) lautet, enthält die physische Festplatte die gesamte virtuelle Festplatte oder einen Teil davon oder weist eine Hotspare-Zuweisung auf.

ANMERKUNG: Die Aufgabe „Import Foreign Configuration“ (Fremdkonfiguration importieren) importiert alle virtuellen Festplatten auf physischen Festplatten, die zum Controller hinzugefügt wurden. Wenn mehr als eine fremde virtuelle Festplatte vorhanden ist, werden alle Konfigurationen importiert.

Der PERC9-Controller bietet Unterstützung für den automatischen Import der Fremdkonfiguration ohne weitere Benutzerinteraktionen. Der automatische Import kann aktiviert oder deaktiviert werden. Wenn diese Option aktiviert ist, kann der PERC-Controller automatisch die ermittelten Fremdkonfigurationen ohne manuellen Eingriff importieren. Wenn diese Option deaktiviert ist, wird der Import einer Fremdkonfiguration vom PERC nicht automatisch ausgeführt.

Sie müssen über die Berechtigung zur Anmeldung und Serversteuerung für den Import von Fremdkonfigurationen verfügen.

Dieser Task wird auf den PERC-Hardware-Controllern, die im HBA-Modus ausgeführt werden, nicht unterstützt.

ANMERKUNG: Es wird nicht empfohlen, ein externes Gehäusekabel zu entfernen, während das Betriebssystem auf dem System ausgeführt wird. Das Entfernen eines Kabels könnte zu einer Fremdkonfiguration führen, wenn die Verbindung wiederhergestellt ist.

Sie können Fremdkonfigurationen in den folgenden Fällen verwalten:

- Alle physischen Laufwerke in einer Konfiguration werden entfernt und wieder eingesetzt.
- Einige der physischen Laufwerke in einer Konfiguration werden entfernt und wieder eingesetzt.
- Alle physischen Laufwerke eines virtuellen Laufwerks werden entfernt, aber zu unterschiedlichen Zeitpunkten, und dann wieder eingesetzt.
- Die physischen Laufwerke eines nicht redundanten virtuellen Laufwerks werden entfernt.

Die folgenden Beschränkungen gelten für die physischen Laufwerke, die für den Import in Frage kommen:

- Der Laufwerkzustand einer physischen Festplatte kann sich im Zeitraum zwischen dem Scannen der Fremdkonfiguration und dem tatsächlichen Import ändern. Der Import einer Fremdkonfiguration erfolgt nur für Laufwerke, die den Zustand „Unconfigured Good“ (Nicht konfiguriert, gut) aufweisen.
- Festplatten, die fehlerhaft oder offline sind, können nicht importiert werden.
- Die Firmware unterbindet den Import von mehr als acht Fremdkonfigurationen.

Importieren von Fremdkonfigurationen über die Webschnittstelle

ANMERKUNG: Wenn eine unvollständige Fremdfestplattenkonfiguration im System vorhanden ist, wird der Zustand einer oder mehrerer vorhandener virtueller Online-Festplatten ebenfalls als fremd angezeigt.

ANMERKUNG: Das Importieren von Fremdkonfigurationen für BOSS-Controller wird nicht unterstützt.

So importieren Sie die Fremdkonfiguration:

1. Navigieren Sie in der iDRAC9-Webschnittstelle zu **Konfiguration** > **Speicherkonfiguration**.
2. Wählen Sie aus dem Drop-Down-Menü **Controller** den Controller aus, in den Sie die Fremdkonfiguration importieren möchten.
3. Klicken Sie unter **Fremdkonfiguration** auf **Import** und anschließend auf **Übernehmen**.

Importieren von Fremdkonfigurationen über RACADM

So importieren Sie die Fremdkonfiguration:

```
racadm storage importconfig:<Controller FQDD>
```

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Fremdkonfiguration löschen

Nach der Verlegung einer physischen Festplatte von einem Controller zu einem anderen kann es vorkommen, dass die physische Festplatte die gesamte virtuelle Festplatte oder einen Teil davon enthält (Fremdkonfiguration). Durch Überprüfung des Zustands der physischen Festplatte können Sie feststellen, ob eine vorher verwendete physische Festplatte eine Fremdkonfiguration (virtuelle Festplatte) enthält. Wenn der Status der physischen Festplatte „Foreign“ (Fremd) lautet, enthält die physische Festplatte die gesamte virtuelle Festplatte oder einen Teil davon. Sie können die Informationen zur virtuellen Festplatte von den zuvor verbundenen physischen Festplatten löschen.

Mit dem Vorgang zum Löschen der Fremdkonfiguration werden alle Daten auf den physischen Festplatten, die dem Controller hinzugefügt wurden, dauerhaft gelöscht. Sind mehrere fremde virtuelle Festplatten vorhanden, werden alle Konfigurationen gelöscht. Es ist daher vielleicht besser, die virtuelle Festplatte zu importieren als die Daten zu vernichten. Zum Entfernen der Fremddaten muss eine Initialisierung vorgenommen werden. Wenn Sie über eine unvollständige Fremdkonfiguration verfügen, die nicht importiert werden kann, können Sie die Option Fremde Konfiguration löschen verwenden, um die Fremddaten auf den physischen Festplatten zu löschen.

Löschen von Fremdkonfigurationen über die Webschnittstelle

So löschen Sie eine Fremdkonfiguration:

1. Navigieren Sie in der iDRAC9-Webschnittstelle zu **Konfiguration** > **Speicherkonfiguration** > **Controller-Konfiguration**.
   Die Seite **Controller-Konfiguration** wird angezeigt.
2. Wählen Sie aus dem Drop-Down-Menü **Controller** den Controller aus, für den Sie die Fremdkonfiguration: löschen möchten.

   ANMERKUNG: Um eine Fremdkonfiguration auf BOSS-Controllern zu löschen, klicken Sie auf „Konfiguration zurücksetzen“.
3. Klicken Sie auf **Konfiguration löschen**.
4. Klicken Sie auf **Anwenden**.
   Basierend auf dem ausgewählten Betriebsmodus werden die virtuellen Festplatten, die sich auf der physischen Festplatte befinden, gelöscht.

Löschen von Fremdkonfigurationen über RACADM

So löschen Sie eine Fremdkonfiguration:

```
racadm storage clearconfig:<Controller FQDD>
```

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Zurücksetzen der Controller-Konfiguration

Sie können die Konfiguration für einen Controller zurücksetzen. Dieser Vorgang löscht virtuelle Festplatten und macht die Zuweisung aller Hotspares auf dem Controller rückgängig. Es werden keine Daten gelöscht, sondern es werden nur die Festplatten aus der Konfiguration entfernt. Durch das Zurücksetzen der Konfiguration werden ferner keine Fremdkonfigurationen entfernt. Die Echtzeit-Unterstützung dieser Funktion steht nur auf der PERC 9.1-Firmware zur Verfügung. Durch das Zurücksetzen der Konfiguration werden keine Daten gelöscht. Sie können genau dieselbe Konfiguration ohne einen Initialisierungsvorgang neu erstellen, was dazu führen kann, dass die Daten wiederhergestellt werden. Sie müssen über die Berechtigung zur Serversteuerung verfügen.

ANMERKUNG: Durch das Zurücksetzen der Controller-Konfiguration wird keine Fremdkonfiguration entfernt. Zum Entfernen einer Fremdkonfiguration müssen Sie sie löschen.

Zurücksetzen der Controller-Konfiguration über die Webschnittstelle

Um einen Konfigurations-Reset durchzuführen:

1. Gehen Sie in der iDRAC-Web-Schnittstelle zu **Storage (Speicher)** > **Overview (Übersicht)** > **Controllers (Controller)**.
2. Wählen Sie bei **Actions (Aktionen)** die Aktion **Reset Configuration (Konfigurations-Reset)** für einen oder mehrere Controller aus.
3. Wählen Sie für jeden Controller aus dem Drop-Down-Menü **Betriebsmodus anwenden** den Zeitpunkt für die Anwendung der Einstellungen aus.
4. Klicken Sie auf **Anwenden**.

   Basierend auf dem ausgewählten Betriebsmodus werden die Einstellungen angewendet.

Zurücksetzen der Controller-Konfiguration über RACADM

Um einen Konfigurations-Reset durchzuführen:

```
racadm storage resetconfig:<Controller FQDD>
```

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Wechseln des Controller-Modus

Bei PERC 9.1-Controllern können Sie die Persönlichkeit des Controllers ändern, indem Sie den Modus von RAID auf HBA umschalten. Der Controller funktioniert ähnlich wie ein HBA-Controller, in dem die Treiber durch das Betriebssystem übergeben werden. Der Wechsel des Controller-Modus ist ein gestufter Vorgang und erfolgt nicht in Echtzeit.

PERC 10 und höher Controller unterstützen den erweiterten HBA-Modus, wobei Sie HBA in den aktuellen Controller-Modus-Optionen ersetzen. PERC 9 unterstützt jedoch weiterhin den HBA-Modus.

ANMERKUNG:

- Der erweiterte HBA-Modus unterstützt Nicht-RAID-PDs VDs aller RAID-Level.
- Er unterstützt nur die Erstellung von VDs mit RAID0, RAID1 und RAID10.
- Der erweiterte HBA-Modus wird auf PERC 11 nicht unterstützt.

Der erweiterte HBA-Modus bietet die folgenden Funktionen:

- Virtuelle Laufwerke mit RAID-Klasse 0, 1 oder 10 erstellen.
- Nicht-RAID-Laufwerke dem Host präsentieren.
- Eine standardmäßige Cache-Regel für virtuelle Laufwerke als Rückschreiben mit Vorauslesen konfigurieren.
- Virtuelle Laufwerke und Nicht-RAID-Laufwerke als gültige Startgeräte konfigurieren.
- Alle unkonfigurierten Laufwerke automatisch zu Nicht-RAID konvertieren:
  - Beim Systemstart
  - Bei Controllerrücksetzung

- Wenn nicht konfigurierten Laufwerke als Ersatz eingesetzt werden

ANMERKUNG: Das Erstellen oder Importieren von virtuellen RAID 5-, 6-, 50- oder 60-Laufwerken wird nicht unterstützt. Außerdem werden im erweiterten HBA-Modus Nicht-RAID-Laufwerke zuerst in aufsteigender Reihenfolge nummeriert, während RAID-Volumes in absteigender Reihenfolge nummeriert werden.

Stellen Sie vor dem Ändern des Controller-Modus von RAID auf HBA Folgendes sicher:

- Der RAID-Controller unterstützt die Änderung des Controller-Modus. Die Option zum Ändern des Controller-Modus ist auf Controllern nicht verfügbar, auf denen die RAID-Persönlichkeit eine Lizenz erfordert.
- Alle virtuellen Laufwerke müssen gelöscht oder entfernt werden.
- Hot Spares (Ersatzlaufwerke) müssen gelöscht oder entfernt werden.
- Fremde Konfigurationen müssen gelöscht oder deaktiviert werden.
- Alle physischen Festplatten in einem fehlerhaften Zustand müssen entfernt werden.
- Alle lokalen Sicherheitsschlüssel für SEDs müssen gelöscht werden.
- Auf dem Controller darf kein Cache beibehalten werden.
- Sie haben Berechtigungen zur Serversteuerung, um den Controller-Modus zu ändern.

ANMERKUNG: Stellen Sie sicher, dass Sie vor dem Ändern des Modus die Fremdkonfiguration, den Sicherheitsschlüssel, die virtuellen Festplatten und Hot Spares sichern, da die Daten gelöscht werden.

ANMERKUNG: Stellen Sie sicher, dass eine CMC-Lizenz (nicht für MX-Plattformen) für Speicherschlitten PERC FD33xS und FD33xD vorhanden ist, bevor Sie den Controller-Modus ändern. Weitere Informationen zur CMC-Lizenz für die Speicherschlitten finden Sie im *Benutzerhandbuch für Dell Chassis Management Controller 1.2 für PowerEdge FX2/FX2s* unter dell.com/cmcmanuals.

Ausnahmen beim Wechseln des Controller-Modus

Die folgende Liste enthält die Ausnahmen beim Festlegen des Controller-Modus mithilfe der iDRAC-Schnittstellen, wie z.B. Web-Schnittstelle, RACADM oder WSMan:

- Wenn sich der PERC-Controller im RAID-Modus befindet, müssen Sie alle virtuellen Festplatten, Ersatzgeräte, fremde Konfigurationen, Schlüssel oder beibehaltenen Cache löschen, bevor Sie ihn in den HBA-Modus umschalten.
- Während Sie den Controller-Modus einstellen, können Sie keine anderen RAID-Vorgänge konfigurieren. Beispiel: Wenn sich der PERC im RAID-Modus befindet und Sie den ausstehenden Wert des PERCs auf den HBA-Modus einstellen und versuchen, das BGI-Attribut festzulegen, wird der ausstehende Wert nicht initialisiert.
- Wenn Sie den PERC-Controller vom HBA- auf den RAID-Modus umschalten, bleiben die Festplatten im Nicht-RAID-Zustand und werden nicht automatisch in den Status „Ready“ (Bereit) gesetzt. Darüber hinaus wird das Attribut **RAIDEnhancedAutoImportForeignConfig** automatisch auf **Enabled (Aktiviert)** gesetzt.

Die folgende Liste enthält die Ausnahmen beim Festlegen des Controller-Modus mithilfe der Serverkonfigurationsprofil-Funktion bei Verwendung der WSMan- oder RACADM-Schnittstelle:

- Die Serverkonfigurationsprofil-Funktion ermöglicht Ihnen das Konfigurieren mehrerer RAID-Vorgänge zusammen mit dem Festlegen des Controller-Modus. Wenn sich zum Beispiel der PERC-Controller im HBA-Modus befindet, können Sie das Serverkonfigurationsprofil (SCP) für den Export bearbeiten und den Controller-Modus in RAID ändern, Laufwerke in den "Ready" -Zustand konvertieren und virtuelle Festplatten erstellen.
- Beim Ändern des Modus von RAID in HBA wird das Attribut **RAIDaction pseudo** auf „update“ festgelegt (Standardverhalten). Das Attribut wird ausgeführt und erstellt eine virtuelle Festplatte, die ausfällt. Der Controller-Modus wird geändert, der Auftrag wird jedoch mit Fehlern abgeschlossen. Um dieses Problem zu vermeiden, müssen Sie einen Kommentar für das RAI Daction-Attribut in der SCP-Datei hinzufügen.
- Wenn sich der PERC-Controller im HBA-Modus befindet, schlägt die Erstellung der virtuellen Festplatte fehl, wenn Sie die Import-Vorschau auf die zur Änderung des Controller-Modus auf RAID bearbeitete Export-SCP-Datei anwenden, und versuchen eine virtuelle Festplatte zu erstellen. Die Importvorschau unterstützt bei einer Änderung des Controller-Modus keine Prüfung von RAID-Stacking-Vorgängen.

Umschalten des Controller-Modus unter Verwendung der iDRAC-Weboberfläche

Führen Sie zum Umschalten des Controller-Modus die folgenden Schritte aus:

1. Klicken Sie in der iDRAC-Weboberfläche auf **Speicher** > **Übersicht** > **Controller**.
2. Klicken Sie auf der Seite **Controller** auf **Aktion** > **Bearbeiten**.
   Die Spalte **Aktueller Wert** zeigt die aktuelle Einstellung des Controllers an.

3. Wählen Sie im Drop-Down-Menü den Controller-Modus aus, in den Sie wechseln möchten, und klicken Sie auf **Beim nächsten Neustart**.
   Starten Sie das System neu, um die Änderung in Kraft zu setzen.

Wechseln des Controller-Modus unter Verwendung von RACADM

Führen Sie die folgenden Befehle aus, um den Controller-Modus unter Verwendung von RACADM zu wechseln:

- So zeigen Sie den aktuellen Modus des Controllers an:

  ```
  $ racadm get Storage.Controller.1.RequestedControllerMode[key=<Controller_FQDD>]
  ```

  Die folgende Ausgabe wird angezeigt:

  ```
  RequestedControllerMode = NONE
  ```

- So legen Sie den Controller-Modus als HBA fest:

  ```
  $ racadm set Storage.Controller.1.RequestedControllerMode  HBA [Key=<Controller_FQDD>]
  ```

- So erstellen Sie einen Job und wenden Änderungen an:

  ```
  $ racadm jobqueue create <Controller Instance ID> -s TIME_NOW -r pwrcycle
  ```

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

12-GB/s-SAS-HBA-Adapter-Vorgänge

Bei Dell PowerEdge-Servern muss ein Betriebssystem installiert sein und der entsprechende Gerätetreiber geladen werden, damit Dell HBAs betrieben werden können. Nach dem POST werden die HBA-Ports deaktiviert. Der HBA-Gerätetreiber ist für das Zurücksetzen des HBA und das Aktivieren der mit Speichergeräten verbundenen Ports verantwortlich. Ohne Betriebssystem wird der Treiber nicht geladen und es wird nicht garantiert, dass iDRAC mit Dell HBAs verbundene Speichergeräte anzeigen kann.

Die Nicht-RAID-Controller sind die HBAs, die nicht alle RAID-Funktionen aufweisen. Diese unterstützen keine virtuellen Festplatten.

Die 14G iDRAC-Schnittstelle unterstützt 12-Gbit/s-SAS-HBA-Controller, HBA330-Controller (integriert und Adapter), HBA330 MMZ- und HBA330 MX-Adapter.

AMD Plattformen unterstützen HBA355i-Front- und HBA355i-Adapter-Controller.

Sie können die folgenden Schritte für Nicht-RAID-Controller ausführen:

- Anzeigen von Controllern, physischen Festplatten und Gehäuseeigenschaften für Nicht-RAID-Controller. Außerdem können Sie die Eigenschaften von EMM, Lüfter, Stromversorgungseinheit und Temperatursonde anzeigen, die mit dem Gehäuse verknüpft sind. Die Eigenschaften werden basierend auf dem Controller-Typ angezeigt.
- Anzeigen von Informationen zum Bestand von Software und Hardware.
- Aktualisieren der Firmware für Gehäuse hinter dem 12 GB/s-SAS-HBA-Controller (in mehreren Stufen)
- Überwachen der Abfrage bzw. der Abfragehäufigkeit für den SMART-Trip-Status für physische Festplatten, wenn eine Änderung erkannt wurde
- Überwachen der Hotplugs für physische Festplatten oder des Entfernungsstatus für den Hotplug
- Blinken der LEDs oder Beenden des Blinkens

ANMERKUNG:

- Bandlaufwerke werden nur eingeschränkt unterstützt, wenn Sie hinter 12-Gbit/s-SAS oder HBA355e angeschlossen sind.
- Obwohl die LED für das Bandlaufwerk nicht verfügbar ist, kann die Option Blinken/Blinken beenden erfolgreich sein.

ANMERKUNG:

- Aktivieren Sie den Vorgang „System-Bestandsaufnahme beim Neustart erstellen“ (CSIOR), bevor die Inventarisierung oder Überwachung der Nicht-RAID-Controller erfolgt.
- Die Echtzeit-Überwachung auf SMART-fähigen Festplatten und SES-Gehäusesensoren erfolgt nur für SAS-HBA-Controller mit 12 GBit/s und interne HBA-330-Controller.

ANMERKUNG: Die Erkennung von ausgefallenen Laufwerken hinter SAS-HBA-Controllern wird nicht unterstützt.

Überwachen der voraussagenden Fehleranalyse auf Festplatten

Storage Management unterstützt die Selbstüberwachungsanalyse- und Berichttechnologie (SMART) auf physischen Festplatten, die SMART-aktiviert sind.

SMART führt eine voraussagende Fehleranalyse auf jeder Festplatte durch und sendet Warnungen, wenn ein Festplattenversagen vorhergesehen wird. Die Controller überprüfen physische Festplatten auf Fehlervoraussagen und leiten, falls Fehlervoraussagen gefunden wurden, entsprechende Informationen an iDRAC weiter. iDRAC gibt sofort eine Warnung aus.

Controller-Vorgänge im Nicht-RAID-Modus oder HBA-Modus

Wenn sich der Controller im Nicht-RAID-Modus (HBA-Modus) befindet, gilt Folgendes:

- Virtuelle Festplatten oder Hotspares sind nicht verfügbar.
- Der Sicherheitsstatus des Controllers ist deaktiviert.
- Alle physikalischen Festplatten befinden sich im Nicht-RAID-Modus.

Sie können die folgenden Vorgänge ausführen, wenn sich der Controller im Nicht-RAID-Modus befindet:

- Physische Festplatte blinken/Blinken deaktivieren.
- Konfigurieren Sie alle Eigenschaften einschließlich der folgenden:
  - Lastausgleichsmodus
  - Übereinstimmungsüberprüfungsmodus
  - Patrol Read-Modus
  - Copyback-Modus
  - Controller-Startmodus
  - Erweiterter automatischer Fremdkonfigurationsimport
  - Neuerstellungsrate
  - Übereinstimmungsüberprüfungsrate
  - Rekonstruktionsrate
  - Hintergrund-Initialisierungsrate
  - Gehäuse- oder Rückwandplatinen-Modus
  - Patrol Read – Nicht konfigurierte Bereiche
- Zeigen Sie alle Eigenschaften an, die auf einen RAID-Controller zutreffen, mit Ausnahme von virtuellen Festplatten.
- Fremdkonfiguration löschen

ANMERKUNG: Wenn ein Vorgang im Nicht-RAID-Modus nicht unterstützt wird, wird eine Fehlermeldung angezeigt.

Sie können die Gehäusetemperatursonden, Lüfter und Netzteile nicht überwachen, wenn sich der Controller im Nicht-RAID-Modus befindet.

Ausführen der RAID-Konfigurations-Jobs auf mehreren Speicher-Controllern

Während der Ausführung von Vorgängen auf mehr als zwei Speicher-Controllern über eine beliebige unterstützte Schnittstelle müssen Sie Folgendes sicherstellen:

- Führen Sie die Jobs auf jedem Controller einzeln aus. Warten Sie jedoch, bis jeder Job abgeschlossen wurde, bevor Sie mit der Konfiguration und der Erstellung des nächsten Controllers beginnen.
- Planen Sie mithilfe der Zeitplanoptionen mehrere Jobs zur Ausführung zu einem späteren Zeitpunkt.

Manage Preserved Cache (Beibehaltenen Cache verwalten)

Die Funktion „Manage Preserved Cache“ (Beibehaltenen Cache verwalten) ist ein Controller-Option, mit der der Benutzer die Daten des Controller-Cache verwerfen kann. Gemäß der Write-Back-Regel werden Daten erst in den Cache und dann auf die physische Festplatte geschrieben. Wenn die virtuelle Festplatte offline geht oder aus irgendeinem Grund gelöscht wird, werden die Daten im Cache gelöscht.

Die PREC Controller behält die Daten, die in den gesicherten bzw. geänderten Cache geschrieben wurden, bei einem bei Stromausfall oder bei Trennung der Kabel bei, bis Sie die virtuelle Festplatte wiederherstellen oder den Cache löschen.

Der Status des Controllers wird vom beibehaltenen Cache beeinflusst. Der Controllerstatus wird als „Degraded“ (Herabgesetzt) angezeigt, wenn der Controller einen beibehaltenen Cache hat. Das Verwerfen des beibehaltenen Cache ist nur dann möglich, wenn alle folgenden Bedingungen erfüllt sind:

- Der Controller verfügt über keine Fremdkonfiguration.
- Der Controller weist keine virtuellen Festplatten auf, die offline sind oder fehlen.
- Kabelverbindungen zu einer virtuellen Festplatte sind nicht unterbrochen.

Managing PCIe SSDs

Peripheral Component Interconnect Express (PCIe) solid-state device (SSD) is a high-performance storage device designed for solutions requiring low latency, high Input Output Operations per Second (IOPS), and enterprise class storage reliability and serviceability. The PCIe SSD is designed based on Single Level Cell (SLC) and Multi-Level Cell (MLC) NAND flash technology with a high-speed PCIe 2.0, PCIe 3.0, or PCIe 4.0 compliant interface. In 14th generation of PowerEdge servers, we have three different ways to connect SSDs. You can use an extender to connect the SSDs via backplane, directly connect the SSDs from backplane to mother board using slimline cable without extender, and use HHHL (Add-In) card which sits on the motherboard.

NOTE:

- 14th generation of PowerEdge servers are supporting Industry standard NVMe-MI specification based NVMe SSDs
- PERC 11 supports PCIe SSD/NVMe devices behind PERC inventory monitoring and configuration.

Using iDRAC interfaces, you can view and configure NVMe PCIe SSDs.

The key features of PCIe SSD are:

- Hot plug capability
- High-performance device

In few of the 14th generation of PowerEdge servers, up to 32 NVMe SSDs are supported.

You can perform the following operations for PCIe SSDs:

- Inventory and remotely monitor the health of PCIe SSDs in the server
- Prepare to remove the PCIe SSD
- Securely erase the data
- Blink or unblink the device LED (Identify the device)

You can perform the following operations for HHHL SSDs:

- Inventory and real-time monitoring of the HHHL SSD in the server
- Failed card reporting and logging in iDRAC and OMSS
- Securely erasing the data and removing the card
- TTY logs reporting

You can perform the following operations for SSDs:

- Drive status reporting such as Online, Failed, and Offline

NOTE: Hot plug capability, prepare to remove, and blink or unblink the device LED is not applicable for HHHL PCIe SSD devices.

NOTE: When NVMe devices are controlled behind SW RAID, prepare to remove and cryptographic erase operations are not supported, blink and unblink are supported.

Erstellen einer Bestandsaufnahme für und Überwachen von PCIe-SSDs

Die folgenden Bestandsaufnahme- und Überwachungsinformationen sind für PCIe-SSDs verfügbar:

- Hardware-Informationen:
  - PCIe-SSD-Extender-Karte
  - PCIe-SSD-Rückwandplatine

    Wenn das System über eine dedizierte PCIe-Rückwandplatine verfügt, werden zwei FQDDs angezeigt. Ein FQDD ist für reguläre Laufwerke und das andere für SSDs vorgesehen. Wenn die Rückwandplatine geteilt (universal) wird, wird nur ein FQDD angezeigt. Falls die SSDs direkt angeschlossen sind, meldet sich der Controller-FQDD als CPU.1 und zeigt damit an, dass die SSD direkt mit der CPU verbunden ist.
- Die Software umfasst nur die Firmware-Version für die PCIe-SSD.

Erstellen einer Bestandsaufnahme für und Überwachen von PCIe-SSDs über die Webschnittstelle

Wenn Sie den Bestand der PCIe-SSD-Geräte erfassen und diese überwachen möchten, gehen Sie in der iDRAC-Webschnittstelle zu **Speicher** > **Übersicht** > **Physische Festplatten**. Die Seite **Eigenschaften** wird angezeigt. Bei PCIe-SSDs wird in der Spalte **Name** der Wert **PCIe SSD** angezeigt. Erweitern Sie die Spalte, um die Eigenschaften anzuzeigen.

Bestandsaufnahme und Überwachung von PCIe-SSDs mithilfe von RACADM

Verwenden Sie den Befehl `racadm storage get controllers:<PcieSSD controller FQDD>`, um eine Bestandsaufnahme zu erstellen und PCIe-SSDs zu überwachen.

Anzeigen aller PCIe-SSD-Festplatten:

```
racadm storage get pdisks
```

Anzeigen von PCIe-Extender-Karten:

```
racadm storage get controllers
```

Anzeigen von Informationen zur PCIe-SSD

```
racadm storage get enclosures
```

ANMERKUNG: Für alle genannten Befehle werden auch die PERC-Geräte angezeigt.

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Vorbereiten auf das Entfernen von PCIe-SSDs

ANMERKUNG: Dieser Vorgang wird nicht unterstützt, wenn:

- Die PCIe-SSD mit dem S140-Controller konfiguriert wird.
- Das NVMe-Gerät sich hinter PERC 11 befindet.

PCIe-SSDs unterstützen den ordnungsgemäßen Hot Swap, was Ihnen das Hinzufügen oder Entfernen eines Geräts ermöglicht, ohne das System, auf dem die Geräte installiert sind, anzuhalten oder neu zu starten. Um Datenverlust zu vermeiden, müssen Sie den Vorgang „Zum Entfernen vorbereiten“ durchführen, bevor Sie ein Gerät physisch entfernen.

Ein kontrollierter Hot-Swap-Vorgang wird nur unterstützt, wenn die PCIe-SSDs auf einem unterstützten System installiert sind, auf dem ein unterstütztes Betriebssystem ausgeführt wird. Um sicherzustellen, dass Sie über die richtige Konfiguration für Ihre PCIe-SSD verfügen, lesen Sie das systemspezifische Benutzerhandbuch.

Der Vorgang „Zum Entfernen vorbereiten“ wird für PCIe SSDs auf den VMware vSphere (ESXi)-Systemen und HHHL PCIe SSD-Geräten nicht unterstützt.

ANMERKUNG: Der Vorgang „Zum Entfernen vorbereiten“ wird auf Systemen mit ESXi 6.0 mit iDRAC-Service-Modul-Version 2.1 oder höher unterstützt.

Der Vorgang „Zum Entfernen vorbereiten“ kann unter Verwendung des iDRAC-Service-Moduls in Echtzeit durchgeführt werden.

Dieser Vorgang stoppt alle im Hintergrund laufenden Aktivitäten und sämtliche I/O-Aktivitäten, damit das Gerät sicher entfernt werden kann. Der Vorgang führt dazu, dass die Status-LEDs am Gerät blinken. Sie können nach Ausführen des Vorgangs „Zum Entfernen vorbereiten“ das Gerät sicher aus dem System entfernen, wenn Folgendes zutrifft:

- Die PCIe-SSD blinkt im LED-Muster „kann sicher entfernt werden“ (blinkt gelb).
- Das System kann nicht mehr auf das PCIe SSD zugreifen.

Bevor Sie das PCIe-SSD auf die Entfernung vorbereiten, müssen folgende Voraussetzungen erfüllt sein:

- iDRAC-Servicemodul ist installiert.
- Lifecycle Controller ist aktiviert.
- Sie haben die Berechtigungen zur Serversteuerung sowie zur Anmeldung.

Vorbereiten zum Entfernen von PCIe-SSDs über die Webschnittstelle

So bereiten Sie die PCIe-SSD auf das Entfernen vor:

1. Gehen Sie in der iDRAC-Web-Webschnittstelle zu **Storage (Speicher)** > **Overview (Übersicht)** > **Physical Disks (Physische Festplatten)**.
   Daraufhin wird die Seite **Setup von physischen Festplatten** angezeigt.
2. Wählen Sie aus dem Drop-Down-Menü **Controller** den Extender aus, um die zugehörigen PCIe-SSDs anzuzeigen.
3. Wählen Sie in den Drop-Down-Menüs die Option **Zum Entfernen vorbereiten** für eine oder mehrere PCIe-SSDs aus.

   Wenn Sie die Option **Zum Entfernen vorbereiten** ausgewählt haben und Sie die anderen Optionen in dem Drop-Down-Menü anzeigen möchten, wählen Sie **Maßnahme** aus, und klicken Sie dann auf das Drop-Down-Menü, um die anderen Optionen anzuzeigen.

   ANMERKUNG: Stellen Sie sicher, dass iSM installiert ist und ausgeführt wird, um den Vorgang `preparetoremove`auszuführen.

4. Wählen Sie aus dem Drop-Down-Menü **Betriebsmodus anwenden** die Option **Jetzt anwenden** aus, um die Maßnahmen sofort anzuwenden.

   Wenn Jobs zum Fertigstellen bereitstehen, ist diese Option grau unterlegt.

   ANMERKUNG: Für PCIe-SSD-Geräte ist nur die Option **Jetzt anwenden (Apply Now)** verfügbar. Dieser Vorgang wird im stufenweisen Modus nicht unterstützt.

5. Klicken Sie auf **Anwenden**.

   Wenn der Auftrag nicht erstellt wird, wird eine entsprechende Meldung angezeigt. Die Meldungs-ID und die empfohlene Antwortmaßnahme werden ebenfalls angezeigt.

   Wenn der Auftrag erfolgreich erstellt wurde, wird eine Meldung angezeigt, dass die Auftrags-ID für den ausgewählten Controller erstellt wurde. Klicken Sie auf **Job Queue (Auftragswarteschlange)**, um den Fortschritt des Auftrags auf der Seite **Job Queue (Auftragswarteschlange)** anzuzeigen.

   Wenn der ausstehende Vorgang nicht erstellt wird, wird eine Fehlermeldung angezeigt. Wenn der ausstehende Vorgang erfolgreich war, die Auftragserstellung jedoch nicht, wird eine Fehlermeldung angezeigt.

Vorbereiten auf das Entfernen einer PCIe-SSD über RACADM

So bereiten Sie das PCIeSSD-Laufwerk auf das Entfernen vor:

```
racadm storage preparetoremove:<PCIeSSD FQDD>
```

So erstellen Sie den Zielauftrag nach der Ausführung des Befehls `preparetoremove`:

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW --realtime
```

So fragen Sie die ausgegebene Job-ID ab:

```
racadm jobqueue view -i <job ID>
```

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Löschen von Daten auf PCIe-SSD-Geräten

ANMERKUNG: Dieser Vorgang wird nicht unterstützt, wenn die PCIe-SSD mithilfe des SWRAID-Controllers konfiguriert wurde.

Die kryptografische Löschung löscht alle auf der Festplatte vorhandenen Daten dauerhaft. Das Ausführen eines kryptografischen Löschvorgangs auf einer PCIe-SSD überschreibt alle Blöcke und führt zu permanentem Datenverlust auf der PCIe-SSD. Beim kryptografischen Löschvorgang kann der Host nicht auf die PCIe-SSD zugreifen. Die Änderungen werden nach dem Neustart des Systems angewendet.

Falls das System neu gestartet wird oder wenn während einer kryptografischen Löschung der Strom ausfällt, wird der Vorgang abgebrochen. Sie müssen das System neu starten und den Vorgang erneut ausführen.

Stellen Sie vor dem Löschen von Daten auf PCIe-SSD-Geräten Folgendes sicher:

- Lifecycle Controller ist aktiviert.

- Sie haben die Berechtigungen zur Serversteuerung sowie zur Anmeldung.

ANMERKUNG:
- Das Löschen von PCIe-SSDs kann nur als ein gestufter Vorgang ausgeführt werden.
- Nachdem das Laufwerk gelöscht wurde, wird es im Betriebssystem als online angezeigt, es wird jedoch nicht initialisiert. Sie müssen das Laufwerk initialisieren und formatieren, bevor Sie es erneut verwenden.
- Nachdem Sie eine PCIe-SSD per Hot-Plug verbunden haben, kann es einige Sekunden dauern, bis sie auf der Weboberfläche angezeigt wird.

Löschen von PCIe-SSD-Gerätedaten über die Webschnittstelle

So löschen Sie die Daten auf dem PCIe-SSD-Gerät:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Speicher** > **Überblick** > **Physische Festplatten**.
   Daraufhin wird die Seite **Physical Disk (Physische Festplatte)** angezeigt.
2. Wählen Sie im Drop-Down-Menü **Controller** den Controller aus, für den Sie die zugehörigen PCIe-SSDs auswählen möchten.
3. Wählen Sie in den Drop-Down-Menüs die Option **Kryptografisches Löschen** für eine oder mehrere PCIe-SSDs aus.

   Wenn Sie **Kryptografisches Löschen** ausgewählt haben und Sie die anderen Optionen im Dropdown-Menü anzeigen möchten, wählen Sie **Maßnahme** aus, und klicken Sie dann auf das Drop-Down-Menü, um die anderen Optionen anzuzeigen.
4. Wählen Sie im Dropdown-Menü **Betriebsmodus wählen** eine der folgenden Optionen aus:
   - **At Next Reboot (Beim nächsten Neustart)** – Wählen Sie diese Option aus, um die Aktionen während des nächsten Systemneustarts anzuwenden.
   - **Zu einer geplanten Zeit** – Wählen Sie diese Option aus, um die Maßnahmen zu einem geplanten Datum und Uhrzeit anzuwenden:
     - **Start Time (Startzeit)** und **End Time (Endzeit)** – Klicken Sie auf die Kalendersymbole und wählen Sie das Datum aus. Wählen Sie aus dem Drop-Down-Menü das Zeitintervall. Die Maßnahme wird zwischen der Startzeit und Endzeit angewandt.
     - Wählen Sie aus dem Drop-Down-Menü den Typ des Neustarts aus:
       - Kein Neustart (manueller System-Neustart)
       - Ordentliches Herunterfahren
       - Erzwungenes Herunterfahren
       - System aus- und wieder einschalten (Hardwareneustart)
5. Klicken Sie auf **Anwenden**.

   Wenn der Auftrag nicht erstellt wird, wird eine entsprechende Meldung angezeigt. Die Meldungs-ID und die empfohlene Antwortmaßnahme werden ebenfalls angezeigt.

   Wenn der Auftrag erfolgreich erstellt wurde, wird eine Meldung angezeigt, dass die Auftrags-ID für den ausgewählten Controller erstellt wurde. Klicken Sie auf **Job Queue (Auftragswarteschlange)**, um den Fortschritt des Auftrags auf der Seite „Job Queue“ (Auftragswarteschlange) anzuzeigen.

   Wenn der ausstehende Vorgang nicht erstellt wird, wird eine Fehlermeldung angezeigt. Wenn der ausstehende Vorgang erfolgreich war, die Auftragserstellung jedoch nicht, wird eine Fehlermeldung angezeigt.

Löschen eines PCIe-SSD-Geräts unter Verwendung von RACADM

Zum sicheren Löschen eines PCIe-SSD-Geräts:

```
racadm storage secureerase:<PCIeSSD FQDD>
```

So erstellen Sie den Ziel-Job nach dem Ausführen des Befehls `secureerase`:

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW -e <start_time>
```

So fragen Sie die ausgegebene Job-ID ab:

```
racadm jobqueue view -i <job ID>
```

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Verwalten von Gehäusen oder Rückwandplatinen

Sie können die folgenden Schritte für Gehäuse oder Rückwandplatinen ausführen:

- Eigenschaften anzeigen
- Universellen oder Split-Modus konfigurieren
- Steckplatzinformationen anzeigen (universell oder freigegeben)
- SGPIO-Modus festlegen
- Set Asset Tag
- Bestandsname

Konfigurieren des Rückwandplatinen-Modus

Die Dell PowerEdge-Server der 14. Generation unterstützen eine neue interne Speichertopologie, bei der zwei Storage-Controller (PERCs) mit einem Satz von internen Laufwerken über einen einzigen Expander verbunden werden können. Diese Konfiguration wird für einen hohen Leistungsmodus ohne Failover- oder High Availability (HA)-Funktionalität verwendet. Der Expander teilt das interne Laufwerks-Array zwischen den zwei Speicher-Controllern auf. In diesem Modus zeigt die Erstellung der virtuellen Festplatte nur die Laufwerke, die mit einem bestimmten Controller verbunden sind. Es gibt keine Lizenzierungsanforderungen für diese Funktion. Diese Funktion wird nur auf wenigen Systemen unterstützt.

Die Rückwandplatine unterstützt die folgenden Modi:

- Unified-Modus – Dies ist der Standardmodus. Der primäre PERC-Controller hat Zugriff auf alle Laufwerke, die an die Rückwandplatine angeschlossen sind, selbst wenn ein zweiter PERC-Controller installiert ist.
- Split-Modus – Ein Controller hat Zugriff auf die ersten zwölf Laufwerke und der zweite Controller hat Zugriff auf die letzten zwölf Laufwerke. Die Laufwerke, die an den ersten Controller angeschlossen sind, sind mit 0-11 nummeriert, während die Laufwerke, die an den zweiten Controller angeschlossen sind, mit 12-23 nummeriert sind.
- Split-Modus 4:20 – Ein Controller hat Zugriff auf die ersten vier Laufwerke und der zweite Controller hat Zugriff auf die letzten 20 Laufwerke. Die Laufwerke, die an den ersten Controller angeschlossen sind, sind mit 0-3 nummeriert, während die Laufwerke, die an den zweiten Controller angeschlossen sind, mit 4-23 nummeriert sind.
- Split-Modus 8:16 – Ein Controller hat Zugriff auf die ersten acht Laufwerke und der zweite Controller hat Zugriff auf die letzten 16 Laufwerke. Die Laufwerke, die an den ersten Controller angeschlossen sind, sind mit 0-7 nummeriert, während die Laufwerke, die an den zweiten Controller angeschlossen sind, mit 8-23 nummeriert sind.
- Split-Modus 16:8 – Ein Controller hat Zugriff auf die ersten 16 Laufwerke und der zweite Controller hat Zugriff auf die letzten acht Laufwerke. Die Laufwerke, die an den ersten Controller angeschlossen sind, sind mit 0-15 nummeriert, während die Laufwerke, die an den zweiten Controller angeschlossen sind, mit 16-23 nummeriert sind.
- Split-Modus 20:4 – Ein Controller hat Zugriff auf die ersten 20 Laufwerke und der zweite Controller hat Zugriff auf die letzten vier Laufwerke. Die Laufwerke, die an den ersten Controller angeschlossen sind, sind mit 0-19 nummeriert, während die Laufwerke, die an den zweiten Controller angeschlossen sind, mit 20-23 nummeriert sind.
- Split-Modus 6:6:6:6 – In einem Gehäuse sind vier Blades installiert und jedem Blade sind sechs Laufwerke zugewiesen. Dieser Modus wird nur auf PowerEdge-Blades der C-Serie unterstützt.
- Informationen nicht verfügbar – Es sind keine Informationen zum Controller verfügbar.

iDRAC erlaubt die Einstellung des Split-Modus, wenn der Expander in der Lage ist, die Konfiguration zu unterstützen. Stellen Sie sicher, dass Sie diesen Modus aktiviert haben, bevor Sie den zweiten Controller installieren. iDRAC führt eine Überprüfung auf die Expander-Funktion durch, bevor dieser Modus konfiguriert werden kann, und überprüft nicht, ob der zweite PERC-Controller vorhanden ist.

ANMERKUNG: Kabelfehler (oder andere Fehler) können angezeigt werden, wenn Sie die Rückwandplatine in den Split-Modus versetzen, wenn nur ein PERC angeschlossen ist, oder wenn Sie die Rückwandplatine in den Unified-Modus versetzen und zwei PERCs angeschlossen sind.

Um die Einstellung zu ändern, müssen Sie über eine Berechtigung zur Serversteuerung verfügen.

Wenn sich andere RAID-Vorgänge im Status „Ausstehend“ befinden oder ein RAID-Job geplant ist, können Sie den Rückwandplatinen-Modus nicht mehr ändern. Ebenso können Sie, wenn diese Einstellung ausstehend ist, keine anderen RAID-Jobs planen.

ANMERKUNG:

- Warnungen werden angezeigt, wenn die Einstellung geändert wird, da die Wahrscheinlichkeit von Datenverlusten besteht.
- LC-Lösch- oder iDRAC-Reset-Vorgänge wirken sich nicht auf die Expander-Einstellung für diesen Modus aus.

- Dieser Vorgang wird nur in Echtzeit unterstützt und wird nicht bereitgestellt.
- Sie können die Konfiguration der Rückwandplatine mehrmals ändern.
- Der Splitting-Vorgang der Rückwandplatine kann zu Datenverlust oder Fremdkonfiguration führen, wenn sich die Zugehörigkeit eines Laufwerks zwischen den Controllern ändert.
- Je nach Laufwerkzugehörigkeit kann sich der Splitting-Vorgang der Rückwandplatine auf die RAID-Konfiguration auswirken.

Änderungen an dieser Einstellung werden erst nach einem System-Reset wirksam. Wenn Sie vom Split- zum Unified-Modus wechseln, wird beim nächsten Systemstart eine Fehlermeldung angezeigt, da der zweite Controller keine Laufwerke erkennen kann. Außerdem sieht der erste Controller eine Fremdkonfiguration. Wenn Sie den Fehler ignorieren, gehen die vorhandenen virtuellen Festplatten verloren.

Konfigurieren des Rückwandplatinen-Modus über die Webschnittstelle

So konfigurieren Sie den Rückwandplatinen-Modus über die iDRAC-Webschnittstelle:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Speicherkonfiguration** > **Gehäusekonfiguration**.
2. Wählen Sie aus dem Menü **Controller** den Controller aus, um die zugehörigen Gehäuse zu konfigurieren.
3. Wählen Sie aus dem Dropdown-Menü **Aktion** die Option **Gehäusemodus bearbeiten** aus.
   Die Seite **Gehäusemodus bearbeiten** wird angezeigt.
4. Wählen Sie in der Spalte **Aktueller Wert** den erforderlichen Gehäusemodus für die Rückwandplatine oder das Gehäuse aus: Dies sind die Optionen:
   - Unified-Betrieb
   - Split-Betrieb
   - Split-Betrieb 4:20
   - Split-Betrieb 8:16
   - Split-Betrieb 16:8
   - Split-Betrieb 20:4

   ANMERKUNG: Die verfügbaren Modi für C6420 sind: Split-Betrieb und Split-Betrieb-6:6:6:6. Einige Werte werden möglicherweise nur auf bestimmten Plattformen unterstützt.

   Für R740xd und R940 ist ein Power-Cycle des Servers erforderlich, damit die neue Rückwandplatinenzone angewendet wird. Für C6420 ist ein Aus- und Einschalten (des Blade-Gehäuses) erforderlich, damit die neue Rückwandplatinenzone angewendet wird.
5. Klicken Sie auf **Zu ausstehenden Vorgängen hinzufügen**.
   Eine Auftragskennung wird erstellt.
6. Klicken Sie auf **Jetzt übernehmen**.
7. Wechseln Sie zur Seite **Job-Warteschlange**, und stellen Sie sicher, dass der Job-Status als „Abgeschlossen“ angezeigt wird.
8. Schalten Sie das System aus und wieder ein, damit die Einstellung wirksam wird.

Gehäuse über RACADM konfigurieren

Um das Gehäuse oder die Rückwandplatine zu konfigurieren, verwenden Sie den Befehl `set` bei den Objekten im **BackplaneMode**.

Gehen Sie wie folgt vor, um beispielsweise das Attribut „BackplaneMode“ in den Split-Betrieb zu setzen:

1. Führen Sie den folgenden Befehl zur Anzeige des aktuellen Rückwandplatinenmodus aus:

   ```
   racadm get storage.enclosure.1.backplanecurrentmode
   ```

   Das Ergebnis ist Folgendes:

   ```
   BackplaneCurrentMode=UnifiedMode
   ```
2. Führen Sie den folgenden Befehl zur Anzeige des angeforderten Modus aus:

   ```
   racadm get storage.enclosure.1.backplanerequestedmode
   ```

   Das Ergebnis ist Folgendes:

   ```
   BackplaneRequestedMode=None
   ```

3. Geben Sie den folgenden Befehl ein, um den angeforderten Rückwandplatinen-Betrieb in den Split-Betrieb umzustellen:

```
racadm set storage.enclosure.1.backplanerequestedmode "splitmode"
```

Die Meldung wird angezeigt und besagt, dass der Befehl erfolgreich ist.

4. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob das Attribut **backplanerequestedmode** in den Split-Modus gesetzt wurde:

```
racadm get storage.enclosure.1.backplanerequestedmode
```

Das Ergebnis ist Folgendes:

```
BackplaneRequestedMode=None (Pending=SplitMode)
```

5. Führen Sie den Befehl `storage get controllers` aus und notieren Sie die Controller-Instanz-ID.
6. Führen Sie den folgenden Befehl aus, um einen Job zu erstellen:

```
racadm jobqueue create <controller instance ID> -s TIME_NOW --realtime
```

Daraufhin wird eine Job-ID ausgegeben.

7. Führen Sie den folgenden Befehl aus, um den Job-Status abzufragen:

```
racadm jobqueue view -i JID_xxxxxxxx
```

wobei `JID_xxxxxxxx` für die in Schritt 6 erstellte Job-ID steht.

Der Status wird als „Ausstehend“ angezeigt.

Setzen Sie die Abfrage der Job-ID fort, bis der Status „Fertig“ angezeigt wird (dieser Vorgang kann bis zu drei Minuten dauern).

8. Führen Sie den folgenden Befehl zur Anzeige des `backplanerequestedmode`-Attributwerts aus:

```
racadm get storage.enclosure.1.backplanerequestedmode
```

Das Ergebnis ist Folgendes:

```
BackplaneRequestedMode=SplitMode
```

9. Führen Sie den folgenden Befehl aus, um einen Kaltstart des Servers auszuführen:

```
racadm serveraction powercycle
```

10. Nachdem das System die Vorgänge für den Einschalt-Selbsttest (POST) und CSIOR abgeschlossen hat, geben Sie den folgenden Befehl ein, um `backplanerequestedmode` zu überprüfen:

```
racadm get storage.enclosure.1.backplanerequestedmode
```

Das Ergebnis ist Folgendes:

```
BackplaneRequestedMode=None
```

11. Führen Sie die folgenden Schritte aus, um zu überprüfen, ob der Rückwandplatinenmodus auf Split-Modus gesetzt ist:

```
racadm get storage.enclosure.1.backplanecurrentmode
```

Das Ergebnis ist Folgendes:

```
BackplaneCurrentMode=SplitMode
```

12. Führen Sie den folgenden Befehl aus, und überprüfen Sie, dass nur 0–11-Laufwerke angezeigt werden:

```
racadm storage get pdisks
```

Weitere Informationen zu den RACADM-Befehlen finden Sie im *iDRAC RACADM Command Line Interface Reference Guide* (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC), das unter **dell.com/idracmanuals** verfügbar ist.

Anzeigen von Universalsteckplätzen

Einige Rückwandplatinen von PowerEdge-Servern der 14. Generation unterstützen SAS/SATA- und PCIe-SSD-Festplatten im gleichen Steckplatz. Diese Steckplätze werden als Universalsteckplätze bezeichnet und sind mit dem primären Storage-Controller (PERC) und entweder einer PCIe-Extender-Karte oder Direct Connect Manager über CPU-Rückwandplatinen verdrahtet und unterstützen sowohl SAS/SATA- als auch PCIe-SSD-Festplatten im gleichen Steckplatz. Die Rückwandplatinen-Firmware enthält Informationen über die Steckplätze, die diese Funktion unterstützen. Die Rückwandplatine unterstützt SAS/SATA-Festplatten oder PCIe-SSDs. In der Regel handelt es sich bei den vier Steckplätzen mit höherer Nummerierung um Universalsteckplätze. Beispiel: Bei einer universellen Rückwandplatine mit 24 Steckplätzen unterstützen Steckplätze 0-19 nur SAS/SATA-Festplatten, während die Steckplätze 20-23 sowohl SAS/SATA als auch PCIe-SSD unterstützen.

Der Rollup-Funktionszustand für das Gehäuse stellt den kombinierten Status für alle Laufwerke im Gehäuse bereit. Der Gehäuse-Link auf der Seite **Topologie** zeigt die gesamten Gehäuseinformationen an, unabhängig vom zugewiesenen Controller. Beide Storage-Controller (PERC und PCIe-Extender) können an die gleiche Rückwandplatine angeschlossen werden, aber nur die Rückwandplatine, die dem PERC-Controller zugewiesen ist, wird auf der Seite **Systembestand** angezeigt.

Auf der Seite **Speicher** > **Gehäuse** > **Eigenschaften** zeigt der Abschnitt **Übersicht über die physischen Laufwerke** Folgendes:

- **Slot unbelegt** – Wenn ein Steckplatz leer ist.
- **PCIe-fähig** – Wenn keine PCIe-fähigen Steckplätzen vorhanden sind, wird diese Spalte nicht angezeigt.
- **Bus-Protokoll** – handelt es sich um eine universelle Rückwandplatine mit PCIe-SSD in einem der Steckplätze installiert, zeigt diese Spalte **PCIe** an.
- **Hot Spare** – Diese Spalte ist bei PCIe-SSDs nicht verfügbar.

ANMERKUNG: Bei Universalsteckplätzen wird Hot-Swapping unterstützt. Wenn Sie ein PCIe-SSD-Laufwerk entfernen und gegen ein SAS/SATA-Laufwerk austauschen möchten, stellen Sie sicher, dass Sie zuerst den Task „PrepareToRemove“ für das PCIe-SSD-Laufwerk ausführen. Wenn Sie diesen Task nicht ausführen, treten auf dem Hostbetriebssystem möglicherweise Probleme auf, z. B. ein blauer Bildschirm, Kernel-Panik usw.

Einrichten des SGPIO-Modus

Der Speicher-Controller kann mit der Rückwandplatine im I2C-Modus (Standardeinstellung für Dell Rückwandplatinen) oder mit dem seriellen SGPIO-Modus (General Purpose Input/Output) verbunden werden. Diese Verbindung wird für blinkende LEDs auf den Festplatten benötigt. Die Dell PERC-Controller und Rückwandplatinen unterstützen diese beiden Modi. Um bestimmte Channel-Adapter zu unterstützen, muss der Rückwandplatinen-Modus in den SGPIO-Modus geändert werden.

Der SGPIO-Modus wird nur für passive Rückwandplatinen unterstützt. Er wird nicht für Expander-Rückwandplatinen oder passive Rückwandplatinen im Downstream-Modus unterstützt. Die Rückwandplatinen-Firmware enthält Informationen über die Funktionen, den aktuellen Status und den angeforderten Status.

Nach dem LC-Wipe-Vorgang oder dem iDRAC-Reset auf die Standardeinstellungen wird der SGPIO-Modus in den Status „Deaktiviert“ zurückgesetzt. Sie vergleicht die iDRAC-Einstellung mit der Rückwandplatineneinstellung. Wenn die Rückwandplatine in den SGPIO-Modus gesetzt wurde, passt iDRAC seine Einstellung an die Einstellung der Rückwandplatine an.

Das Aus- und Einschalten des Servers ist erforderlich, damit die Änderungen der Einstellung wirksam werden.

Sie müssen über Berechtigungen zur Server-Steuerung verfügen, um diese Einstellung ändern zu können.

ANMERKUNG: Sie können den SGPIO-Modus nicht über die iDRAC-Web-Schnittstelle festlegen.

Festlegen des SGPIO-Modus über RACADM

Um den SGPIO-Modus zu konfigurieren, verwenden Sie den Befehl `set` mit den Objekten in der Gruppe `SGPIOMode`.

Wenn diese Option auf „Disabled“ (Deaktiviert) gesetzt ist, lautet der Modus „I2C“. Wenn diese Option aktiviert ist, wird sie auf den SGPIO-Modus gesetzt.

Weitere Informationen erhalten Sie im *iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)* unter **dell.com/idracmanuals**.

Gehäusesystemkennnummer festlegen

Durch das Festlegen der Gehäusesystemkennnummer können Sie die Systemkennnummer eines Speichergehäuses konfigurieren.

Benutzer können die Systemkennnummer-Eigenschaft des Gehäuses ändern, um Gehäuse zu identifizieren. Diese Felder werden auf ungültige Werte geprüft und bei Eingabe eines ungültigen Werts wird ein Fehler angezeigt. Diese Felder sind Teil der Gehäuse-Firmware; die zunächst angezeigten Daten sind die in der Firmware gespeicherten Werte.

ANMERKUNG: Die Systemkennnummer hat eine Zeichenbegrenzung von 10, wobei das Nullzeichen enthalten ist.

ANMERKUNG: Diese Vorgänge werden für interne Gehäuse nicht unterstützt.

Festlegen von Gehäusebestandsnamen

Durch das Festlegen von Gehäusebestandsnamen kann der Benutzer den Bestandsnamen eines Speichergehäuses konfigurieren.

Der Benutzer kann die Bestandsnameneigenschaft des Gehäuses so ändern, dass es leicht identifiziert werden kann. Diese Felder werden auf ungültige Werte geprüft und bei Eingabe eines ungültigen Werts wird ein Fehler angezeigt. Diese Felder sind Teil der Gehäuse-Firmware; die zunächst angezeigten Daten sind die in der Firmware gespeicherten Werte.

ANMERKUNG: Für den Bestandsnamen gilt eine Zeichenbegrenzung von 32, einschließlich der Null.

ANMERKUNG: Diese Vorgänge werden für interne Gehäuse nicht unterstützt.

Auswählen des Betriebsmodus zum Anwenden von Einstellungen

Beim Erstellen und Verwalten von virtuellen Festplatten, beim Einrichten von physischen Festplatten, Controllern und Gehäusen oder beim Zurücksetzen von Controllern und bevor Sie die verschiedenen Einstellungen anwenden, müssen Sie den Betriebsmodus auswählen. Das heißt, geben Sie an, wann Sie die Einstellungen anwenden möchten:

- Sofort
- Während des nächsten Systemneustarts
- Zu einem festgelegten Zeitpunkt
- Als eine ausstehende Operation, die als Stapel im Rahmen eines einzelnen Jobs angewendet werden sollen.

Auswählen des Betriebsmodus über die Webschnittstelle

So wählen Sie den Betriebsmodus aus, um die Einstellungen zu übernehmen:

1. Sie können den Betriebsmodus auswählen, wenn Sie sich auf einer der folgenden Seiten befinden:
   - **Storage (Speicher)** > **Physical Disks (Physische Festplatten)**.
   - **Storage (Speicher)** > **Virtual Disks (Virtuelle Festplatten)**
   - **Storage (Speicher)** > **Controllers (Controller)**
   - **Storage (Speicher)** > **Enclosures (Gehäuse)**
2. Wählen Sie eine der folgenden Optionen aus dem Drop-Down-Menü **Betriebsmodus anwenden** aus:
   - **Apply Now (Jetzt anwenden)** – Wählen Sie diese Option aus, um die Einstellungen sofort anzuwenden. Diese Option ist nur für PERC 9-Controller verfügbar. Wenn Jobs zum Fertigstellen bereitstehen, ist diese Option grau unterlegt. Dieser Job dauert mindestens 2 Minuten.
   - **At Next Reboot (Beim nächsten Neustart)** – Wählen Sie diese Option aus, um die Einstellungen während des nächsten Systemneustarts anzuwenden.
   - **Zu einer geplanten Zeit** – Wählen Sie diese Option aus, um die Einstellungen zu einem geplanten Datum und Uhrzeit anzuwenden:
     - **Start Time (Startzeit)** und **End Time (Endzeit)** – Klicken Sie auf die Kalendersymbole und wählen Sie die Tage aus. Wählen Sie aus dem Drop-Down-Menü das Zeitintervall. Die Einstellungen werden zwischen der Startzeit und Endzeit angewendet.
     - Wählen Sie aus dem Drop-Down-Menü den Typ des Neustarts aus:
       - Kein Neustart (manueller System-Neustart)

- Ordentliches Herunterfahren
- Erzwungenes Herunterfahren
- System aus- und wieder einschalten (Hardwareneustart)

- **Add to Pending Operations (Zu ausstehenden Vorgängen hinzufügen)** – Wählen Sie diese Option aus, um einen ausstehenden Vorgang zu erstellen, um die Einstellungen anzuwenden. Sie können alle ausstehenden Vorgänge für einen Controller auf der Seite **Storage (Speicher)** > **Overview (Übersicht)** > **Pending Operations (Ausstehende Vorgänge)** anzeigen.

ANMERKUNG:

- Die Option **Add to Pending Operations (Zu ausstehenden Vorgängen hinzufügen)** ist für die Seite **Pending Operations (Ausstehende Vorgänge)** und für PCIe-SSDs auf der Seite **Physical Disks (Physische Festplatten)** > **Setup** nicht verfügbar.
- Nur die Option **Jetzt anwenden** ist auf der Seite **Gehäuse-Setup** verfügbar.

3. Klicken Sie auf **Anwenden**.
   Basierend auf dem ausgewählten Betriebsmodus werden die Einstellungen angewendet.

Auswählen des Betriebsmodus über RACADM

Um den Betriebsmodus auszuwählen, verwenden Sie den Befehl `jobqueue`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Anzeigen und Anwenden von ausstehenden Vorgängen

Sie können alle ausstehenden Vorgänge für den Speicher-Controller anzeigen und bestätigen. Alle Einstellungen werden gleichzeitig, mit dem nächsten Neustart oder zu einem geplanten Zeitpunkt, basierend auf den ausgewählten Optionen, angewendet. Sie können alle ausstehenden Vorgänge für einen Controller löschen. Einzelne ausstehende Vorgänge können nicht gelöscht werden.

Ausstehende Vorgänge werden auf die ausgewählten Komponenten (Controller, Gehäuse, physische Laufwerke und virtuelle Laufwerke) erstellt.

Konfigurationsjobs werden nur auf einem Controller erstellt. Bei PCIe-SSDs wird der Job auf der PCIe-SSD-Festplatte und nicht auf dem PCIe-Extender erstellt.

Anzeigen, Anwenden oder Löschen von ausstehenden Vorgängen über die Webschnittstelle

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Storage (Speicher)** > **Overview (Übersicht)** > **Pending Operations (Ausstehende Vorgänge)**.
   Die Seite **Ausstehende Vorgänge** wird angezeigt.
2. Wählen Sie in der Dropdown-Liste **Komponente** den Controller aus, für den Sie die ausstehenden Vorgänge anzeigen, festschreiben oder löschen möchten.
   Die Liste der ausstehenden Vorgänge wird für den ausgewählten Controller angezeigt.

ANMERKUNG:

- Ausstehende Vorgänge werden für das Importieren von Fremdkonfigurationen, Löschen von Fremdkonfigurationen, Vorgänge von Sicherheitsschlüsseln und das Verschlüsseln virtueller Laufwerke erzeugt. Auf der Seite **Pending Operations** (Ausstehenden Vorgänge) und in der entsprechenden Popup-Nachricht werden sie jedoch nicht angezeigt.
- Aufträge für PCIe SSDs können nicht über die Seite **Ausstehende Vorgänge** erstellt werden.

3. Klicken Sie zum Löschen der ausstehenden Vorgänge für den ausgewählten Controller auf **Alle ausstehenden Vorgänge löschen**.
4. Wählen Sie aus dem Drop-Down-Menü eine der folgenden Optionen und klicken Sie auf **Anwenden**, um die ausstehenden Vorgänge anzuwenden:
   - **Apply Now** (Jetzt anwenden) – Wählen Sie diese Option aus, um alle Vorgänge sofort anzuwenden. Diese Option ist für PERC 9-Controller mit der aktuellsten Firmware-Version verfügbar.
   - **At Next Reboot** (Beim nächsten Neustart) – Wählen Sie diese Option aus, um alle Vorgänge während des nächsten Systemneustarts anzuwenden.
   - **At Scheduled Time** (Zu einer geplanten Zeit) – Wählen Sie diese Option aus, um die Vorgänge zu einem geplanten Datum und einer bestimmten Uhrzeit anzuwenden.

- **Start Time** (Startzeit) und **End Time** (Endzeit) – Klicken Sie auf das Kalender-Symbol und wählen Sie das Datum aus. Wählen Sie aus dem Drop-Down-Menü das Zeitintervall. Die Maßnahme wird zwischen der Startzeit und Endzeit angewandt.
- Wählen Sie aus dem Drop-Down-Menü den Typ des Neustarts aus:
  - Kein Neustart (manueller System-Neustart)
  - Ordentliches Herunterfahren
  - Erzwungenes Herunterfahren
  - System aus- und wieder einschalten (Hardwareneustart)

5. Wenn der Anwendungsauftrag nicht erstellt wird, wird in einer Meldung darauf hingewiesen, dass die Auftragserstellung nicht erfolgreich war. Außerdem werden die Meldungs-ID und die empfohlene Maßnahme angezeigt.
6. Wenn der Anwendungsauftrag erfolgreich erstellt wurde, wird in einer Meldung angezeigt, dass die Auftrags-ID für den ausgewählten Controller erstellt wurde. Klicken Sie auf **Job Queue** (Auftragswarteschlange), um den Fortschritt des Auftrags auf der Seite **Job Queue** anzuzeigen.

   Wenn die Vorgänge zum Löschen oder Importieren von Fremdkonfigurationen, Vorgänge für Sicherheitsschlüssel oder das Verschlüsseln von virtuellen Festplatten den Status „Ausstehend“ aufweisen und diese die einzigen noch ausstehenden Vorgänge sind, können Sie auf der Seite **Pending Operations** (Ausstehenden Vorgänge) keinen Auftrag erstellen. Sie müssen einen anderen Speicherkonfigurationsvorgang ausführen oder RACADM oder WSMan verwenden, um den erforderlichen Konfigurationsauftrag auf dem entsprechenden Controller zu erstellen.

   Das Anzeigen oder Löschen von ausstehenden Vorgänge für PCIe-SSD-Laufwerke auf der Seite **Pending Operations** (Ausstehende Vorgänge) ist nicht möglich. Verwenden Sie den racadm-Befehl, um die ausstehenden Vorgänge für PCIe-SSD-Laufwerke zu löschen.

Anzeigen und Anwenden von ausstehenden Vorgänge über RACADM

Um ausstehende Vorgänge anzuwenden, verwenden Sie den Befehl **jobqueue**.

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Speicher-Geräte – Szenarien des Anwenden-Vorgangs

Fall 1: Der Anwenden-Vorgang (Jetzt anwenden, Bei nächstem Neustart oder Zu geplantem Zeitpunkt) wurde ausgewählt und es sind keine ausstehenden Vorgänge vorhanden.

Wenn Sie die Option **Jetzt anwenden**, **Bei nächstem Neustart** oder **Zu geplantem Zeitpunkt** ausgewählt und dann auf **Anwenden** geklickt haben, wird zunächst der ausstehende Vorgang für den ausgewählten Speicher-Konfigurationsvorgang erstellt.

- Wenn der ausstehende Vorgang erfolgreich abgeschlossen wurde und keine ausstehenden Vorgänge vorhanden sind, wird der Auftrag erstellt. Wenn der Auftrag erfolgreich erstellt wurde, wird eine Meldung angezeigt, dass die Auftrags-ID für den ausgewählten Controller erstellt wurde. Klicken Sie auf **Job Queue (Auftragswarteschlange)**, um den Fortschritt des Auftrags auf der Seite **Job Queue (Auftragswarteschlange)** anzuzeigen. Wenn der Auftrag nicht erstellt wird, wird eine entsprechende Meldung angezeigt. Außerdem werden die Meldungs-ID und die empfohlene Maßnahme angezeigt.
- Wenn der ausstehende Vorgang nicht erfolgreich erstellt wird und keine früheren ausstehenden Vorgänge vorhanden sind, wird eine Fehlermeldung mit einer ID und der empfohlenen Maßnahme als Antwort angezeigt.

Fall 2: Das Anwenden eines Vorgangs (Jetzt anwenden, Bei nächstem Neustart oder Zu geplantem Zeitpunkt) wurde ausgewählt und es sind ausstehende Vorgänge vorhanden.

Wenn Sie die Option **Jetzt anwenden**, **Bei nächstem Neustart** oder **Zu geplantem Zeitpunkt** ausgewählt und dann auf **Anwenden** geklickt haben, wird zunächst der ausstehende Vorgang für den ausgewählten Speicher-Konfigurationsvorgang erstellt.

- Wenn der ausstehende Vorgang erfolgreich erstellt wurde und ausstehende Vorgänge vorhanden sind, wird eine Meldung angezeigt.
  - Klicken Sie auf den Link **Ausstehende Vorgänge anzeigen**, um die ausstehenden Vorgänge für das Gerät anzuzeigen.
  - Klicken Sie auf **Create Job (Auftrag erstellen)**, um einen Auftrag für das ausgewählte Gerät zu erstellen. Wenn der Auftrag erfolgreich erstellt wurde, wird eine Meldung angezeigt, dass die Auftrags-ID für den ausgewählten Controller erstellt wurde. Klicken Sie auf **Job Queue (Auftragswarteschlange)**, um den Fortschritt des Auftrags auf der Seite **Job Queue (Auftragswarteschlange)** anzuzeigen. Wenn der Auftrag nicht erstellt wird, wird eine entsprechende Meldung angezeigt. Die Meldungs-ID und die empfohlene Antwortmaßnahme werden ebenfalls angezeigt.
  - Klicken Sie auf **Abbrechen**, um den Job nicht zu erstellen und auf der Seite zu bleiben und weitere Speicher-Konfigurationsvorgänge auszuführen.

- Wenn der ausstehende Vorgang nicht erfolgreich erstellt wurde und ausstehende Vorgänge vorhanden sind, wird eine Fehlermeldung angezeigt.
  - Klicken Sie auf **Ausstehende Vorgänge**, um die ausstehenden Vorgänge für das Gerät anzuzeigen.
  - Klicken Sie auf **Create Job For Successful Operations (Auftrag für erfolgreiche Vorgänge erstellen)**, um den Auftrag für die vorhandenen ausstehenden Vorgänge zu erstellen. Wenn der Auftrag erfolgreich erstellt wurde, wird eine Meldung angezeigt, dass die Auftrags-ID für den ausgewählten Controller erstellt wurde. Klicken Sie auf **Job Queue (Auftragswarteschlange)**, um den Fortschritt des Auftrags auf der Seite **Job Queue (Auftragswarteschlange)** anzuzeigen. Wenn der Auftrag nicht erstellt wird, wird eine entsprechende Meldung angezeigt. Außerdem werden die Meldungs-ID und die empfohlene Maßnahme angezeigt.
  - Klicken Sie auf **Abbrechen**, um den Job nicht zu erstellen und auf der Seite zu bleiben und weitere Speicher-Konfigurationsvorgänge auszuführen.

Fall 3: „Zu ausstehenden Vorgängen hinzufügen“ wurde ausgewählt und es sind keine ausstehenden Vorgänge vorhanden.

Wenn Sie **Zu ausstehenden Vorgängen hinzufügen** ausgewählt und dann auf die Schaltfläche **Anwenden** geklickt haben, wird zuerst der ausstehende Vorgang für den ausgewählten Speicher-Konfigurationsvorgang erstellt.

- Wenn der ausstehende Vorgang erfolgreich erstellt wurde und keine ausstehende Vorgänge vorhanden sind, wird eine Informationsmeldung angezeigt:
  - Klicken Sie auf **OK**, um auf der Seite zu verbleiben und weitere Speicher-Konfigurationsvorgänge auszuführen.
  - Klicken Sie auf **Ausstehende Vorgänge**, um die ausstehenden Vorgänge für das Gerät anzuzeigen. Bis der Job auf dem ausgewählten Controller erstellt wird, werden diese ausstehenden Vorgänge nicht angewendet.
- Wenn der ausstehende Vorgang nicht erfolgreich erstellt wurde und keine ausstehende Vorgänge vorhanden sind, wird eine Fehlermeldung angezeigt.

Fall 4: „Zu ausstehenden Vorgängen hinzufügen“ wurde ausgewählt und es sind frühere ausstehende Vorgänge vorhanden.

Wenn Sie **Zu ausstehenden Vorgängen hinzufügen** ausgewählt und dann auf die Schaltfläche **Anwenden** geklickt haben, wird zuerst der ausstehende Vorgang für den ausgewählten Speicher-Konfigurationsvorgang erstellt.

- Wenn der ausstehende Vorgang erfolgreich erstellt wurde und ausstehende Vorgänge vorhanden sind, wird eine Informationsmeldung angezeigt:
  - Klicken Sie auf **OK**, um auf der Seite zu verbleiben und weitere Speicher-Konfigurationsvorgänge auszuführen.
  - Klicken Sie auf **Ausstehende Vorgänge**, um die ausstehenden Vorgänge für das Gerät anzuzeigen.
- Wenn der ausstehende Vorgang nicht erfolgreich erstellt wurde und ausstehende Vorgänge vorhanden sind, wird eine Fehlermeldung angezeigt.
  - Klicken Sie auf **OK**, um auf der Seite zu verbleiben und weitere Speicher-Konfigurationsvorgänge auszuführen.
  - Klicken Sie auf **Ausstehende Vorgänge**, um die ausstehenden Vorgänge für das Gerät anzuzeigen.

ANMERKUNG:

- Wird die Option zum Erstellen eines Jobs auf der Speicher-Konfigurationsseite zu irgendeinem Zeitpunkt nicht angezeigt, gehen Sie zu der Seite **Speicher-Überblick** > **Ausstehende Vorgänge**, um die vorhandenen ausstehenden Vorgänge anzuzeigen und erstellen Sie den Job auf dem entsprechenden Controller.
- Nur die Fälle 1 und 2 gelten für PCIe-SSDs. Sie können die ausstehenden Vorgänge für PCIe-SSDs nicht anzeigen und daher ist die Option **Add to Pending Operations** (Zu ausstehenden Vorgängen hinzufügen) nicht verfügbar. Verwenden Sie den Befehl „racadm“, um die ausstehenden Vorgänge für PCIe-SSDs zu löschen.

Blinken oder Beenden des Blinkens der Komponenten-LEDs

Sie können eine physische Festplatte, eine virtuelle Festplatte und PCIe-SSDs innerhalb eines Gehäuses durch das Blinken einer der Leuchtdioden (LEDs) auf der Festplatte finden.

Sie müssen Anmeldeberechtigungen haben, um eine LED zu blinken oder das Blinken zu beenden.

Der Controller muss in der Lage sein, die Konfiguration in Echtzeit auszuführen. Die Echtzeit-Unterstützung dieser Funktion steht nur in der PERC 9.1-Firmware und einer höheren Version zur Verfügung.

ANMERKUNG: Blinken oder das Beenden des Blinkens wird für Server ohne Rückwandplatine nicht unterstützt.

Blinken oder Beenden des Blinkens der Komponenten-LEDs über die Webschnittstelle

So blinken Sie eine Komponenten-LED oder beenden Sie das Blinken:

1. Gehen Sie in der iDRAC-Webschnittstelle gemäß Ihren Anforderungen zu einer der folgenden Seiten:
   - **Storage (Speicher)** > **Overview (Übersicht)** > **Physical Disks (Physische Festplatten)** > **Status** – Zeigt die Seite mit identifizierten physischen Festplatten an, auf der Sie die LEDs der physischen Festplatten und PCIe-SSDs aktivieren und deaktivieren können.
   - **Storage (Speicher)** > **Overview (Übersicht)** > **Virtual Disks (Virtuelle Festplatten)** > **Status** – Zeigt die Seite mit identifizierten virtuellen Festplatten an, auf der Sie die LEDs der virtuellen Festplatten aktivieren und deaktivieren können.
2. Wenn Sie das physische Laufwerk auswählen:
   - Aus- oder Abwählen aller Komponenten-LEDs – Wählen Sie die Option **Select/Deselect All (Alle auswählen/abwählen)** aus und klicken Sie auf **Blink (Blinken)**, um das Blinken der Komponenten-LEDs zu starten. Klicken Sie gleichermaßen auf **Unblink (Blinken beenden)**, um das Blinken der Komponenten-LEDs zu stoppen.
   - Aus- oder Abwählen individueller Komponenten-LEDs – Wählen Sie eine oder mehrere Komponenten aus und klicken Sie auf **Blink (Blinken)**, um das Blinken der ausgewählten Komponenten-LEDs zu starten. Klicken Sie gleichermaßen auf **Unblink (Blinken beenden)**, um das Blinken der Komponenten-LEDs zu stoppen.
3. Wenn Sie Sie das virtuelle Laufwerk auswählen:
   - Aus- oder Abwählen aller physischen Festplattenlaufwerke oder PCIe-SSDs – Wählen Sie die Option **Select/Deselect All (Alle auswählen/abwählen)** aus und klicken Sie auf **Blink (Blinken)**, um das Blinken aller physischen Festplattenlaufwerke und PCIe-SSDs zu starten. Klicken Sie gleichermaßen auf **Unblink (Blinken beenden)**, um das Blinken der LEDs zu stoppen.
   - Aus- oder Abwählen individueller physischer Festplattenlaufwerke oder PCIe-SSDs – Wählen Sie ein oder mehrere physische Festplattenlaufwerke aus und klicken Sie auf **Blink (Blinken)**, um das Blinken der LEDs für die physischen Festplattenlaufwerke oder die PCIe-SSDs zu starten. Klicken Sie gleichermaßen auf **Unblink (Blinken beenden)**, um das Blinken der LEDs zu stoppen.
4. Wenn Sie sich auf der Seite **Virtuelle Festplatte identifizieren** befinden:
   - Aus- oder Abwählen aller virtuellen Festplatten – Wählen Sie die Option **Select/Deselect All (Alle auswählen/abwählen)** aus und klicken Sie auf **Blink (Blinken)**, um das Blinken der LEDs für alle virtuellen Festplatten zu starten. Klicken Sie gleichermaßen auf **Unblink (Blinken beenden)**, um das Blinken der LEDs zu stoppen.
   - Aus- oder Abwählen individueller virtueller Festplatten – Wählen Sie eine oder mehrere virtuelle Festplatten aus und klicken Sie auf **Blink (Blinken)**, um das Blinken der LEDs für die virtuellen Festplatten zu starten. Klicken Sie gleichermaßen auf **Unblink (Blinken beenden)**, um das Blinken der LEDs zu stoppen.

   Wenn die Vorgänge „Blinken“ oder „Blinken beenden“ nicht erfolgreich sind, wird eine Fehlermeldung angezeigt.

Aktivieren oder Deaktivieren der Komponenten-LEDs über RACADM

Verwenden Sie zum Aktivieren und Deaktivieren der Komponenten-LEDs die folgenden Befehle:

```
racadm storage blink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

```
racadm storage unblink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

Weitere Informationen finden Sie im *iDRAC RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC)* unter **dell.com/idracmanuals**.

Softwareneustart

Wenn ein Softwareneustart durchgeführt wird, werden die folgenden Verhaltensweisen beobachtet:

- PERC-Controller in der iDRAC-Benutzeroberfläche sind direkt nach dem Neustart ausgegraut. Sie werden verfügbar, sobald die erneute Bestandsaufnahme nach dem Neustart erfolgreich abgeschlossen wurde. Dies gilt nur für PERC-Controller und nicht für NVME/HBA/BOSS.
- Storage-Dateien in SupportAssist sind leer, wenn PERC-Controller in der Benutzeroberfläche ausgegraut sind.
- Die LC-Protokollierung für vergangene und kritische Ereignisse erfolgt für PERC während der `perc reinventory`. REST ist für alle LCL von PERC-Komponenten unterdrückt. LCL wird wieder aufgenommen, nachdem die erneute Bestandsaufnahme für PERC abgeschlossen ist.

- Sie können keinen Echtzeitjob starten, bis die erneute Bestandsaufnahme für PERC abgeschlossen ist.
- Telemetrie-Daten werden erst erfasst, wenn die erneute Bestandsaufnahme für PERC abgeschlossen ist.
- Nachdem die PERC-Bestandsaufnahme abgeschlossen ist, wird der Normalbetrieb aufgenommen.

19

BIOS-Einstellungen

Unter den BIOS-Einstellungen können Sie mehrere Attribute anzeigen, die für einen bestimmten Server verwendet werden. Sie können verschiedene Parameter für jedes Attribut in dieser BIOS-Konfigurationseinstellung ändern. Wenn Sie ein Attribut ausgewählt haben, werden verschiedene Parameter angezeigt, die sich auf dieses bestimmte Attribut beziehen. Sie können mehrere Parameter eines Attributs ändern und Änderungen anwenden, bevor Sie ein anderes Attribut ändern. Wenn ein Benutzer eine Konfigurationsgruppe erweitert, werden die Attribute in alphabetischer Reihenfolge angezeigt.

ANMERKUNG:

- Hilfeinhalte auf Merkmalsebene werden dynamisch generiert.
- Der direkte iDRAC-USB-Port steht ohne Neustart des Hosts zur Verfügung, auch wenn alle USB-Anschlüsse deaktiviert sind.

Übernehmen

Die Schaltfläche **Anwenden** bleibt so lange ausgegraut, bis eines der Attribute geändert wird. Wenn Sie an einem Attribut Änderungen vorgenommen und auf **Anwenden** geklickt haben, können Sie das Attribut mit den erforderlichen Änderungen ändern. Falls die Anforderung das BIOS-Attribut nicht festlegen kann, gibt sie einen Fehler mit dem entsprechenden HTTP-Antwortstatuscode aus, der dem SMIL-API-Fehler oder dem Job-Erstellungsfehler zugeordnet ist. An dieser Stelle wird eine Meldung generiert und angezeigt. Weitere Informationen finden Sie unter *Referenzhandbuch zu Ereignis- und Fehlermeldungen für Dell EMC PowerEdge-Server der 14. Generation* verfügbar unter https://www.dell.com/idracmanuals.

Änderungen verwerfen

Die Schaltfläche **Änderungen verwerfen** ist grau unterlegt, bis eines der Attribute modifiziert wird. Wenn Sie auf die Schaltfläche **Änderungen verwerfen** klicken, werden alle letzten Änderungen verworfen und mit den vorherigen oder ursprünglichen Werten wiederhergestellt.

Anwenden und neu starten

Wenn ein Benutzer den Wert eines Attributs oder einer Startreihenfolge ändert, werden dem Benutzer zwei Optionen angezeigt, um die Konfiguration anzuwenden. **Anwenden und neu starten** oder beim **nächsten Neustart anwenden**. In beiden Anwendungsoptionen wird der Benutzer auf die Seite der Jobwarteschlange umgeleitet, um den Fortschritt dieses bestimmten Jobs zu überwachen.

Ein Benutzer kann in den LC-Protokollen Überwachungsinformationen zur BIOS-Konfiguration anzeigen.

Wenn Sie auf **Anwenden und neu starten** klicken, wird der Server sofort neu gestartet, um alle erforderlichen Änderungen zu konfigurieren. Falls die Anforderung die BIOS-Attribute nicht festlegen kann, wird ein Fehler mit dem entsprechenden HTTP-Antwortstatuscode ausgegeben, der dem SMIL-API-Fehler oder dem Job-Erstellungsfehler zugeordnet ist. An diesem Punkt wird eine EEMI-Meldung generiert und angezeigt.

Beim nächsten Neustart anwenden

Wenn ein Benutzer den Wert eines Attributs oder einer Startreihenfolge ändert, werden dem Benutzer zwei Optionen angezeigt, um die Konfiguration anzuwenden. **Anwenden und neu starten** oder beim **nächsten Neustart anwenden**. In beiden Anwendungsoptionen wird der Benutzer auf die Seite der Jobwarteschlange umgeleitet, um den Fortschritt dieses bestimmten Jobs zu überwachen.

Ein Benutzer kann in den LC-Protokollen Überwachungsinformationen zur BIOS-Konfiguration anzeigen.

Wenn Sie auf **Beim nächsten Neustart anwenden** klicken, werden alle erforderlichen Änderungen beim nächsten Neustart des Servers konfiguriert. Es werden keine sofortigen Änderungen aufgrund der letzten Konfigurationsänderungen vorgenommen, bis der nächste Sitzungsneustart erfolgreich durchgeführt wird. Falls die Anforderung die BIOS-Attribute nicht festlegen kann, wird ein Fehler mit dem entsprechenden HTTP-Antwortstatuscode ausgegeben, der dem SMIL-API-Fehler oder dem Job-Erstellungsfehler zugeordnet ist. An diesem Punkt wird eine EEMI-Meldung generiert und angezeigt.

Alle ausstehenden Werte löschen

Die Schaltfläche **Alle ausstehenden Werte löschen** ist nur aktiviert, wenn auf der Grundlage der letzten Konfigurationsänderungen ausstehende Werte vorhanden sind. Falls der Benutzer die Konfigurationsänderungen nicht übernehmen möchte, kann er auf die Schaltfläche **Alle ausstehenden Werte löschen** klicken, um alle Änderungen zu verwerfen. Falls die Anforderung die BIOS-Attribute nicht entfernt, wird ein Fehler mit dem entsprechenden HTTP-Antwortstatuscode ausgegeben, der dem SMIL-API-Fehler oder dem Job-Erstellungsfehler zugeordnet ist. An diesem Punkt wird eine EEMI-Meldung generiert und angezeigt.

Ausstehender Wert

Die Konfiguration eines BIOS-Attributs über iDRAC wird nicht sofort auf das BIOS angewendet. Es erfordert einen Neustart des Servers, damit die Änderungen wirksam werden. Wenn Sie ein BIOS-Attribut ändern, wird der **ausstehende Wert** aktualisiert. Wenn ein Attribut bereits einen ausstehenden Wert hat (und der konfiguriert wurde), wird das in der GUI angezeigt.

Ändern der BIOS-Konfiguration

Durch das Ändern der BIOS-Konfiguration werden Überwachungsprotokolleinträge erstellt, die in LC-Protokollen eingetragen werden.

BIOS Live Scan

BIOS Live Scan verifiziert die Integrität und Authentizität des BIOS-Images im primären BIOS-ROM, wenn der Host eingeschaltet ist, sich aber nicht in POST befindet.

ANMERKUNG:
- Für diese Funktion wird eine iDRAC Datacenter-Lizenz benötigt.
- Sie müssen über Debug-Berechtigungen verfügen, um diese Funktion verwenden zu können.

iDRAC führt die Verifizierung unveränderlicher Abschnitte des BIOS-Image automatisch in den folgenden Szenarien durch:
- Beim Aus- und Einschalten/Kaltstart
- Nach einem vom Benutzer festgelegten Zeitplan
- Nach Bedarf (von Benutzer initiiert)

Erfolgreiche Ergebnisse des Live Scans werden im LC-Protokoll protokolliert. Fehlerhafte Ergebnisse werden sowohl im LCL als auch im SEL protokolliert.

Themen:

- BIOS Live Scan
- BIOS-Wiederherstellung und Hardware-RoT (Root of Trust)

BIOS Live Scan

BIOS Live Scan verifiziert die Integrität und Authentizität des BIOS-Images im primären BIOS-ROM, wenn der Host eingeschaltet ist, sich aber nicht in POST befindet.

ANMERKUNG:
- Für diese Funktion wird eine iDRAC Datacenter-Lizenz benötigt.
- Sie müssen über Debug-Berechtigungen verfügen, um diese Funktion verwenden zu können.

iDRAC führt die Verifizierung unveränderlicher Abschnitte des BIOS-Image automatisch in den folgenden Szenarien durch:
- Beim Aus- und Einschalten/Kaltstart
- Nach einem vom Benutzer festgelegten Zeitplan
- Nach Bedarf (von Benutzer initiiert)

Erfolgreiche Ergebnise des Live Scans werden im LC-Protokoll protokolliert. Fehlerhafte Ergebnisse werden sowohl im LCL als auch im SEL protokolliert.

BIOS-Wiederherstellung und Hardware-RoT (Root of Trust)

Für PowerEdge-Server ist es zwingend erforderlich, eine fehlerhafte oder beschädigte BIOS-Image-Datei aufgrund von böswilligen Angriffen, Spannungsspitzen oder anderen unvorhersehbaren Ereignissen wiederherzustellen. Eine alternative Reserve des BIOS-Images wäre notwendig, um das BIOS wiederherzustellen, damit der PowerEdge-Server aus dem nicht startfähigen Modus zurück in den Betriebsmodus versetzt werden kann. Dieses alternative/Recovery-BIOS wird in einem zweiten SPI (multipliziert mit primärem BIOS SPI) gespeichert.

Die Wiederherstellungssequenz kann über einen der folgenden Ansätze mit iDRAC als Hauptorchestrator der BIOS-Wiederherstellungsaufgabe initiiert werden:

1. **Automatische Wiederherstellung des primären BIOS-Image/Wiederherstellungs-Image**: Das BIOS-Image wird automatisch während des Host-Startvorgangs wiederhergestellt, nachdem die BIOS-Beschädigung durch das BIOS selbst erkannt wurde.
2. **Erzwungene Wiederherstellung des primären BIOS/Wiederherstellungs-Images** – Der Nutzer initiiert eine OOB-Anfrage zum Aktualisieren des BIOS, entweder weil es sich um ein neues aktualisiertes BIOS handelt oder das BIOS gerade durch einen Fehler beim Starten abgestürzt ist.
3. **Primäre BIOS ROM-Aktualisierung** – Das einzelne primäre ROM wird in Daten-ROM und Code-ROM aufgeteilt. iDRAC hat vollen Zugriff auf den Code-ROM. MUX wird eingeschaltet, um bei Bedarf auf den Code-ROM zuzugreifen.
4. **BIOS Hardware-RoT (Root of Trust)** – Diese Funktion ist in Servern mit den Modellnummern RX5X, CX5XX und TX5X verfügbar. Während der Host-Startvorgänge (nur Kaltstart oder Aus- und Einschalten; nicht während eines Neustarts) sorgt iDRAC dafür, dass ein RoT durchgeführt wird. RoT wird automatisch ausgeführt und der Benutzer kann es nicht über eine Schnittstelle initiieren. Mit der iDRAC Boot First Richtlinie werden die Host-BIOS-ROM-Inhalte bei jedem Aus- und wieder Einschalten sowie bei jedem Kaltstart geprüft. Dieser Prozess sorgt dafür, dass das BIOS sicher gestartet und der Host-Startvorgang weiter gesichert wird.

ANMERKUNG: Weitere Informationen zum Hardware-RoT finden Sie unter diesem Link: https://downloads.dell.com/Manuals/Common/dell-emc-idrac9-security-root-of-trust-bios-live-scanning.pdf

20

Virtuelle Konsole konfigurieren und verwenden

iDRAC hat eine Enhanced HTML5-Option in der virtuellen Konsole hinzugefügt, die vKVM (virtuelle Tastatur, Video und Maus) über einen standardmäßigen VNC-Client ermöglicht. Sie können die virtuelle Konsole dazu verwenden, das Remote-System zu verwalten, indem Sie Tastatur, Video und Maus auf der Management-Station verwenden, um die entsprechenden Geräte auf einem verwalteten Remote-Server zu steuern. Hierbei handelt es sich um eine Lizenzfunktion für Rack- und Tower-Server. Sie ist auf Blade-Servern standardmäßig verfügbar. Sie benötigen die Berechtigung zur iDRAC-Konfiguration, um auf alle Konfigurationen der virtuellen Konsole zuzugreifen.

Nachfolgend finden Sie eine Liste der konfigurierbaren Attribute in der virtuellen Konsole:

- Virtuelle Konsole aktiviert – aktiviert/deaktiviert
- Max. Sitzungen – 1-6
- Aktive Sitzungen – 0-6
- Remote-Präsenz-Schnittstelle
- Videoverschlüsselung – aktiviert/deaktiviert
- Lokales Servervideo – aktiviert/deaktiviert
- Plug-in-Typ – eHTML5 (standardmäßig), ActiveX, Java, HTML5
- Dynamische Maßnahme bei Timeout einer Freigabeanforderung – uneingeschränkter Zugriff, nur Lesezugriff und Verweigerung des Zugriffs
- Automatische Systemsperre – aktiviert/deaktiviert
- Tastatur/Maus-Verbindungszustand – automatisch verbinden, verbunden und getrennt

Zentrale Funktionen:

- Es werden maximal sechs virtuelle Konsole-Sitzungen gleichzeitig unterstützt. Alle Sitzungen zeigen jeweils dieselbe verwaltete Serverkonsole an.
- Sie können die virtuelle Konsole in einem unterstützten Webbrowser starten, indem Sie das Java-, ActiveX-, HTML5- oder eHTML5-Plug-in verwenden.

  ANMERKUNG:
  - Jede Änderung in der Web-Serverkonfiguration führt zum Beenden der vorhandenen Sitzung der virtuellen Konsole.
  - Der Typ der virtuellen Konsole ist standardmäßig auf eHTML5 gesetzt.
  - Selbst wenn die Videoverschlüsselungsoption in der GUI deaktiviert ist, können Sie die Funktion weiterhin über andere Schnittstellen konfigurieren, wenn der Plug-in-Typ eHTML5 ist. Für den eHTML5-Plug-in-Typ ist die Medienverschlüsselung standardmäßig aktiviert.
- Wenn Sie die Sitzung einer virtuellen Konsole öffnen, zeigt der verwaltete Server nicht an, dass die Konsole umgeleitet wurde.
- Sie können mehrere Sitzungen für virtuelle Konsolen von einer einzelnen Management Station aus auf einem oder mehreren Managed Systems gleichzeitig öffnen.
- Es ist nicht möglich, zwei Sitzungen für virtuelle Konsolen von der Management Station aus zum verwalteten Server über dasselbe HTML5-Plug-in zu öffnen.
- Wenn ein zweiter Benutzer eine Virtuelle Konsole-Sitzung anfordert, wird der erste Benutzer benachrichtigt und erhält die Option, den Zugriff abzulehnen, den schreibgeschützten Zugriff zu erlauben oder vollständig freigegebenen Zugriff zu erlauben. Der zweite Benutzer wird benachrichtigt, dass ein anderer Benutzer die Steuerung übernommen hat. Wenn der erste Benutzer nicht innerhalb von 30 Sekunden antwortet, wird dem zweiten Benutzer je nach Standardeinstellung ein Zugriff gewährt. Wenn weder der erste noch der zweite Benutzer über Administratorberechtigungen verfügt, wird die Sitzung des zweiten Benutzers automatisch beendet, wenn der erste Benutzer seine aktive Sitzung beendet.
- Start- und Absturzprotokolle werden als Videoprotokolle im MPEG1-Format erfasst.
- Der Absturzbildschirm wird als JPEG-Datei erfasst.
- Tastaturmakros werden auf allen Plug-ins unterstützt.
- Tastaturmakros werden auf allen Plug-ins unterstützt. Die folgende Liste enthält Makros, die vom ActiveX- und Java-Plug-in unterstützt werden:

Tabelle 57. Tastaturmakros, die vom ActiveX- und Java-Plug-in unterstützt werden

MAC-Client	Win-Client	Linux-Client
Strg-Alt-Entf	Strg-Alt-Entf	Strg-Alt-Entf
Alt-SysRq-B	Alt-SysRq-B	Alt-SysRq-B
-	Win-P	-
-	-	Strg-Alt-F<1–12>
Alt-SysRq	-	-
SysRq	-	-
Druck	-	-
Alt-Druck	-	-
Anhalten	-	-

ANMERKUNG: Informationen zu Tastaturmakros, die im HTML-Plug-in unterstützt werden, finden Sie im Abschnitt HTML5-basierte virtuelle Konsole.

ANMERKUNG: Die Anzahl der aktiven Sitzungen für die virtuelle Konsole wird in der Weboberfläche nur für aktive Weboberflächensitzungen angezeigt. Diese Zahl beinhaltet keine Sitzungen von anderen Schnittstellen wie z. B. SSH und RACADM.

ANMERKUNG: Informationen zum Konfigurieren Ihres Browsers, um auf die virtuelle Konsole zuzugreifen, finden Sie unter Web-Browser für die Verwendung der virtuellen Konsole konfigurieren auf Seite 74.

ANMERKUNG: Um den KVM-Zugriff zu deaktivieren, verwenden Sie die Option **Deaktivieren** unter den Einstellungen für das Gehäuse in der OME-Modular-Weboberfläche.

Themen:

- Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen
- Virtuelle Konsole konfigurieren
- Vorschau der virtuellen Konsole
- Virtuelle Konsole starten
- Viewer für virtuelle Konsole verwenden

Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen

Die folgende Tabelle listet die unterstützten Bildschirmauflösungen und entsprechenden Bildwiederholfrequenzen für die Sitzung einer virtuellen Konsole auf, die auf dem verwalteten Server ausgeführt wird.

Tabelle 58. Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen

Bildschirmauflösung	Bildwiederholfrequenz (Hz)
720x400	70
640x480	60, 72, 75, 85
800x600	60, 70, 72, 75, 85
1024x768	60, 70, 72, 75, 85
1280x1024	60
1.920 x 1.200	60

Es wird empfohlen, die Bildschirmauflösung auf 1920x1200 Pixel oder höher einzustellen.

Die virtuelle Konsole unterstützt eine maximale Videoauflösung von 1920x1200 bei einer Bildwiederholfrequenz von 60 Hz. Um diese Auflösung zu erreichen, müssen folgende Bedingungen erfüllt sein:

- KVM/Monitor an VGA angeschlossen, der eine Auflösung von 1920 x 1200 unterstützt
- Aktueller Matrox-Videotreiber (für Windows)

Wenn ein lokaler KVM/Monitor mit maximaler Auflösung von weniger als 1920x1200 mit einem der VGA-Stecker verbunden ist, wird die in der virtuellen Konsole unterstützte maximale Auflösung reduziert.

Die virtuelle Konsole des iDRAC nutzt den integrierten Matrox G200-Grafikcontroller, um die maximale Auflösung des angeschlossenen Monitors zu bestimmen, wenn ein physischer Bildschirm vorhanden ist. Wenn der Monitor eine Auflösung von 1920x1200 oder mehr unterstützt, unterstützt die virtuelle Konsole eine Auflösung von 1920x1200. Wenn der angeschlossene Monitor eine geringere max. Auflösung (wie viele KVMs) unterstützt, ist die maximale Auflösung der virtuellen Konsole begrenzt.

Maximale Auflösung der virtuellen Konsole basierend auf dem Anzeigeverhältnis des Monitors:

- 16:10-Monitor: 1920x1200 ist die maximale Auflösung
- 16:9-Monitor: 1920x1080 ist die maximale Auflösung

Wenn ein physischer Monitor nicht an einen VGA-Port am Server angeschlossen ist, diktiert das installierte Betriebssystem die verfügbaren Auflösungen für die virtuelle Konsole.

Maximale Auflösung der virtuellen Konsole basierend auf Host-BS ohne physischen Monitor:

- Windows: 1600x1200 (1600x1200, 1280x1024, 1152x864, 1024x768, 800x600)
- Linux: 1024x768 (1024x768, 800x600, 848x480, 640x480)

ANMERKUNG: Wenn eine höhere Auflösung über die virtuelle Konsole erforderlich ist und ein physischer KVM oder Monitor vorhanden ist, kann ein VGA-Display-Emulator-Dongle genutzt werden, um eine externe Monitorverbindung mit einer Auflösung von bis zu 1920x1080 zu simulieren.

ANMERKUNG: Wenn eine Sitzung für die virtuelle Konsole aktiv ist und ein Monitor mit niedrigerer Auflösung mit der virtuellen Konsole verbunden ist, wird die Serverkonsolen-Auflösung möglicherweise zurückgesetzt, wenn der Server auf der lokalen Konsole ausgewählt ist. Wenn auf dem System ein Linux-Betriebssystem ausgeführt wird, kann eine X11-Konsole auf dem lokalen Monitor eventuell nicht angezeigt werden. Drücken Sie < Strg > < Alt > < F1 > in der virtuellen iDRAC-Konsole, um Linux zu einer Textkonsole zu wechseln.

Virtuelle Konsole konfigurieren

Vor der Konfigurierung der virtuellen Konsole müssen Sie sicherstellen, dass die Management Station konfiguriert ist.

Sie können die virtuelle Konsole über die iDRAC-Webschnittstelle oder die RACADM-Befehlszeilenschnittstelle konfigurieren.

Virtuelle Konsole über die Weboberfläche konfigurieren

So konfigurieren Sie die virtuelle Konsole über die iDRAC-Weboberfläche:

1. Gehen Sie zu **Konfiguration** > **Virtuelle Konsole**. Klicken Sie auf den Link **Virtuelle Konsole starten**, dann wird die Seite der virtuellen Konsole angezeigt.
2. Aktivieren Sie die virtuelle Konsole und geben Sie die erforderlichen Werte ein. Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

   ANMERKUNG: Wenn Sie ein Nano-Betriebssystem verwenden, deaktivieren Sie die Funktion **Automatische Systemsperrung** auf der Seite **Virtuelle Konsole**.

3. Klicken Sie auf **Anwenden**. Die virtuelle Konsole ist konfiguriert.

Virtuelle Konsole über RACADM konfigurieren

Verwenden Sie zum Konfigurieren der virtuellen Konsole den Befehl `set` mit den Objekten in der Gruppe **iDRAC.VirtualConsole**.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Vorschau der virtuellen Konsole

Vor dem Starten der virtuellen Konsole können Sie den Zustand der virtuellen Konsole auf der Seite **System** > **Properties (Eigenschaften)** > **System Summary (Systemzusammenfassung)** in der Vorschau anzeigen. Der Bereich **Virtual Console Preview (Vorschau für virtuelle Konsole)** zeigt ein Bild mit dem Zustand der virtuellen Konsole an. Das Bild wird alle 30 Sekunden aktualisiert. Hierbei handelt es sich um eine lizenzierte Funktion.

ANMERKUNG: Das Virtuelle Konsole-Bild ist nur verfügbar, wenn Sie Virtuelle Konsole aktiviert haben.

Virtuelle Konsole starten

Sie können die virtuelle Konsole über die iDRAC-Weboberfläche oder eine URL starten.

ANMERKUNG: Starten Sie die Sitzung für eine virtuelle Konsole nicht über einen Webbrowser auf dem Managed System.

Stellen Sie vor dem Starten der virtuellen Konsole Folgendes sicher:

- Sie verfügen über Administratorrechte.
- Der Webbrowser ist für die Verwendung der Plug-ins HTML5, eHTML5, Java oder ActiveX konfiguriert.
- Die Mindestnetzwerkbandbreite von 1 MB/s ist verfügbar.

ANMERKUNG: Wenn der integrierte Videocontroller im BIOS deakiviert ist und Sie die virtuelle Konsole starten, ist der Viewer der virtuellen Konsole leer.

Während des Starts der virtuellen Konsole über einen 32-Bit- oder 64-Bit-IE-Browser verwenden Sie HTML5/eHTML5 oder das erforderliche Plug-in (Java oder ActiveX), das im entsprechenden Browser zur Verfügung steht. Die Einstellungen in den Internetoptionen sind für alle Browser gleich.

Beim Starten der virtuellen Konsole über das Java-Plug-in wird gelegentlich ein Java-Kompilierungsfehler angezeigt. Um dieses Problem zu lösen, gehen Sie zu **Java-Systemsteuerung** > **Allgemein** > **Netzwerkeinstellungen** und wählen Sie **Direkte Verbindung** aus.

Wenn die virtuelle Konsole für die Verwendung des ActiveX-Plug-ins konfiguriert wurde, scheitert der erste Startversuch möglicherweise. Der Grund dafür liegt in einer langsamen Netzwerkverbindung und einem Timeout nach zwei Minuten bei den temporären Anmeldeinformationen (die von der virtuellen Konsole für den Verbindungsaufbau verwendet werden). Beim Herunterladen des ActiveX-Client-Plug-ins wird diese Zeit möglicherweise überschritten. Nachdem Sie das Plug-in erfolgreich heruntergeladen haben, können Sie die virtuelle Konsole wie gewohnt starten.

Um die virtuelle Konsole unter Verwendung des HTML5/eHTML5-Plug-ins zu starten, müssen Sie den Pop-up-Blocker deaktivieren.

Die virtuelle Konsole bietet folgende Konsolensteuerelemente:

1. **Allgemein**: Sie können Tastaturmakros, Seitenverhältnis und Touch-Modus festlegen.
2. **KVM**: zeigt die Werte für Bildfrequenz, Bandbreite, Komprimierung und Paketrate an.
3. **Performance**: Mit dieser Option können Sie die Videoqualität und die Videogeschwindigkeit ändern.
4. **Nutzerliste**: Sie können die Liste der Nutzer anzeigen, die mit der Konsole verbunden sind.

Sie können auf virtuelle Datenträger zugreifen, indem Sie auf die Option **Mit virtuellem Datenträger verbinden** klicken, die in der virtuellen Konsole verfügbar ist.

Virtuelle Konsole über die Weboberfläche starten

Sie können die virtuelle Konsole wie folgt starten:

- Gehen Sie zu **Konfiguration** > **Virtuelle Konsole**. Klicken Sie auf den Link **Virtuelle Konsole starten**. Daraufhin wird die Seite der virtuellen Konsole angezeigt.

Der **Viewer für die virtuelle Konsole** zeigt den Desktop des Remote-Systems an. Mit dem Viewer können Sie die Maus- und Tastaturfunktionen des Remote-Systems von Ihrer lokalen Managementstation aus steuern.

Mehrere Meldungskästchen erscheinen, nachdem Sie die Anwendung starten. Um den unbefugten Zugriff auf die Anwendung zu verhindern, müssen Sie diese Dialogfelder innerhalb von drei Minuten durchlaufen. Ansonsten werden Sie aufgefordert, die Anwendung erneut zu starten.

Wenn während des Starts des Viewers ein oder mehrere Fenster mit Sicherheitshinweisen angezeigt werden, klicken Sie zum Fortsetzen des Vorgangs auf „Ja“.

Im Viewer-Fenster werden eventuell zwei Mauszeiger angezeigt: einer für den verwalteten Server und ein anderer für Ihre Managementstation.

Virtuelle Konsole über URL starten

So starten Sie die virtuelle Konsole über die URL:

1. Öffnen Sie einen unterstützten Web-Browser, und geben Sie in das Adressfeld die folgende URL in Kleinbuchstaben ein: **https://iDRAC_ip/console**
2. Je nach Anmeldekonfiguration wird die entsprechende **Anmeldeseite** angezeigt:
   - Wenn die Einmalanmeldung deaktiviert und die lokale, Active Directory-, LDAP- oder Smart-Anmeldung aktiviert ist, wird die entsprechende **Anmeldeseite** angezeigt.
   - Wenn die Einmalanmeldung aktiviert ist, wird der **Viewer für die virtuelle Konsole** gestartet, und die **virtuelle Konsole** wird im Hintergrund angezeigt.

   ANMERKUNG: Internet Explorer unterstützt folgende Anmeldungen: lokal, Active Directory, LDAP, Smart Card (SC) und Single Sign-On (SSO). Firefox unterstützt lokale, AD- und SSO-Anmeldungen auf Windows-basierten Betriebssystemen und lokale, Active Directory- und LDAP-Anmeldungen auf Linux-basierten Betriebssystemen.

   ANMERKUNG: Wenn Sie keine Zugriffsberechtigung auf die virtuelle Konsole haben, aber berechtigt sind, auf den virtuellen Datenträger zuzugreifen, wird durch die Verwendung dieser URL anstatt der virtuellen Konsole der virtuelle Datenträger verwendet.

Deaktivieren von Warnmeldungen beim Starten der Virtuellen Konsole oder Virtueller Datenträger mit dem Java- oder ActiveX-Plug-In

Sie können die Warnmeldungen, die beim Starten der Virtuellen Konsole oder des Virtuellen Datenträgers mit dem Java-Plug-In generiert werden, deaktivieren.

ANMERKUNG: Sie benötigen Java 8 oder höher, um diese Funktion zu verwenden und die virtuelle iDRAC-Konsole über ein IPv6-Netzwerk zu starten.

1. Anfänglich wird beim Start der virtuellen Konsole oder des virtuellen Datenträgers mit dem Java-Plug-In die Eingabeaufforderung zur Prüfung des Herausgebers angezeigt. Klicken Sie auf **Yes** (Ja).

   Eine Zertifikat-Warnmeldung weist darauf hin, dass kein vertrauenswürdiges Zertifikat gefunden wurde.

   ANMERKUNG: Wenn das Zertifikat im Zertifikatspeicher des Betriebssystem oder an einem zuvor vom Benutzer festgelegten Speicherort gefunden wird, wird diese Warnmeldung nicht angezeigt.

2. Klicken Sie auf **Continue** (Weiter).
   Der Viewer der Virtuellen Konsole oder des Virtuellen Datenträgers wird gestartet.

   ANMERKUNG: Der Viewer des Virtuellen Datenträgers wird gestartet, wenn die Virtuelle Konsole deaktiviert ist.
3. Klicken Sie im Menü **Extras** auf **Sitzungsoptionen** und anschließend auf die Registerkarte **Zertifikat**.
4. Klicken Sie auf **Pfad durchsuchen** und geben Sie einen Speicherort für das Benutzerzertifikat an, klicken Sie dann auf **Anwenden** und auf **OK**, und schließen Sie den Viewer.
5. Starten Sie die Virtuelle Konsole erneut.
6. Wählen Sie in der Zertifikat-Warnmeldung die Option **Diesem Zertifikat immer vertrauen** aus, und klicken Sie dann auf **Weiter**.
7. Beenden Sie den Viewer.
8. Wenn Sie die Virtuelle Konsole neu starten, wird die Warnmeldung nicht mehr angezeigt.

Viewer für virtuelle Konsole verwenden

Der Viewer für die virtuelle Konsole verfügt über verschiedene Steuerungen wie Maussynchronisierung, virtuelle Konsolenskalierung, Chatoptionen, Tastaturmakros, Stromversorgungsmaßnahmen, weitere Bootgeräte und Zugriff auf virtuelle Datenträger. Weitere Informationen zu diesen Funktionen finden Sie in der *iDRAC Online-Hilfe*.

ANMERKUNG: Wenn der Remote-Server ausgeschaltet wird, wird die Meldung „Kein Signal“ angezeigt.

Die Titelleiste des Viewers für die virtuelle Konsole zeigt den DNS-Namen oder die IP-Adresse des iDRAC an, mit dem Sie über die Management Station verbunden sind. Wenn der iDRAC keinen DNS-Namen aufweist, wird die IP-Adresse angezeigt. Das Format lautet:

- Für Rack- und Tower-Server:

```
<DNS name / IPv6 address / IPv4 address>, <Model>, User: <username>, <fps>
```

- Für Blade-Server:

```
<DNS name / IPv6 address / IPv4 address>, <Model>, <Slot number>, User: <username>, <fps>
```

Gelegentlich zeigt der Viewer für die virtuelle Konsole möglicherweise Videos in geringer Qualität an. Der Grund dafür kann eine langsame Netzwerkverbindung sein, die dazu führt, dass ein oder zwei Video-Frames verloren gehen, wenn Sie die Sitzung für die virtuelle Konsole starten. Für die Übertragung aller Video-Frames und zur Verbesserung der nachfolgenden Videoqualität müssen Sie eine der folgenden Maßnahmen ausführen:

- Klicken Sie auf der Seite **Systemzusammenfassung** unter **Vorschau für virtuelle Konsole** auf **Aktualisieren**.
- Schieben Sie im **Viewer für die virtuelle Konsole** auf der Registerkarte **Leistung** den Regler auf **Maximale Video-Qualität**.

eHTML5 based virtual console

NOTE: While using eHTML5 to access virtual console, the language must be consistent across client and target keyboard layout, OS, and browser. For example, all must be in English (US) or any of the supported languages.

To launch the eHTML5 virtual console, you must enable the virtual console feature from the iDRAC Virtual Console page and set the **Plug-in Type** option to eHTML5.

NOTE: By default the virtual console type is set to eHTML5.

You can launch virtual console as a pop-up window by using one of the following methods:

- From iDRAC Home page, click the **Start the Virtual Console** link available in the Console Preview session
- From iDRAC Virtual Console page, click **Start the Virtual Console** link.
- From iDRAC login page, type **https//<iDRAC IP>/console**. This method is called as Direct Launch.

In the eHTML5 virtual console, the following menu options are available:

- Power
- Boot
- Chat
- Keyboard
- Screen Capture
- Refresh
- Full Screen
- Disconnect Viewer
- Console Controls
- Virtual Media

The **Pass all keystrokes to server** option is not supported on eHTML5 virtual console. Use keyboard and keyboard macros for all the functional keys.

- **General** —
  - **Console control** — This has the following configuration options:
    - Keyboard Macros — This is supported in eHTML5 virtual console and are listed as the following drop-down options. Click **Apply** to apply the selected key combination on the server.
      - 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
- Pause
- Tab
- Ctrl+Enter
- SysRq
- Alt+SysRq
- Win-P

▪ Aspect Ratio — The eHTML5 virtual console video image automatically adjusts the size to make the image visible. The following configuration options are displayed as a drop-down list:
- Maintain
- Don't Maintain

Click **Apply** to apply the selected settings on the server.

▪ Touch Mode — The eHTML5 virtual console supports the Touch Mode feature. The following configuration options are displayed as a drop-down list:
- Direct
- Relative

Click **Apply** to apply the selected settings on the server.

- **Virtual Clipboard** - Virtual clipboard enables you to cut / copy / paste text buffer from virtual console to iDRAC host server. Host server could be BIOS, UEFI or in OS prompt. This is a one-way action from client computer to iDRAC's host server only. Follow these steps to use the Virtual clipboard:
  - Place the mouse cursor or keyboard focus on the desired window in the host server desktop.
  - Select the **Console Controls** menu from vConsole.
  - Copy the OS clipboard buffer using keyboard hotkeys, mouse, or touch pad controls depending on the Client OS. Or, you can type the text manually in the text box.
  - Click **Send Clipboard to Host**.
  - Then, the text appears on the host server's active window.

  NOTE:
  - This feature is only available in Datacenter license.
  - This feature only supports ASCII text.
  - Control characters are not supported.
  - Characters such as **New line** and **Tab** are allowed.
  - Text buffer size is limited to 4000 characters.
  - If more than maximum buffer is pasted, then the edit box in iDRAC GUI will truncate it to maximum buffer size.
- **KVM** - This menu has list of the following read only components:
  - Frame Rate
  - Bandwidth

- Compression
- Packet Rate

- **Performance** - You can use the slider button to adjust **Maximum Video Quality** and **Maximum Video Speed**.
- **User List** - You can see the list of users that are logged in to the Virtual console.
- **Keyboard** — The difference between physical and virtual keyboard is that virtual keyboard changes its layout according to the browser language.
- **Virtual Media** — Click **Connect Virtual Media** option to start the virtual media session.
  - **Connect Virtual Media** - This menu contains the options for Map CD/DVD, Map Removable Disk, Map External Device, and Reset USB.
  - **Virtual Media Statistics** - This menu shows the Transfer Rate (Read-only). Also, it shows the details of CD/DVD and Removable Disks details such as Mapping details, status (read-only or not), duration, and Read/Write Bytes.
  - **Create Image** - This menu allows you to select a local folder and generate FolderName.img file with local folder contents.

NOTE: For security reasons read/write access is disabled while accessing virtual console in eHTML5. With Java or ActiveX plug-ins, you can accept security messaging before the plug-in is given the read/write authority.

Supported Browsers

The eHTML5 virtual console is supported on the following browsers:

- Internet Explorer 11
- Google Chrome 83/84
- Mozilla Firefox 80/81
- Safari 13.1.1

NOTE: It is recommended to have Mac OS version 10.10.2 (or onward) installed in the system.

For more details on supported browsers and versions, see the *iDRAC-Versionshinweise* verfügbar unter https://www.dell.com/idracmanuals.

HTML5 based virtual console

NOTE: While using HTML5 to access virtual console, the language must be consistent across client and target keyboard layout, OS, and browser. For example, all must be in English (US) or any of the supported languages.

To launch the HTML5 virtual console, you must enable the virtual console feature from the iDRAC Virtual Console page and set the **Plug-in Type** option to HTML5.

You can launch virtual console as a pop-up window by using one of the following methods:

- From iDRAC Home page, click the **Start the Virtual Console** link available in the Console Preview session
- From iDRAC Virtual Console page, click **Start the Virtual Console** link.
- From iDRAC login page, type **https//<iDRAC IP>/console**. This method is called as Direct Launch.

In the HTML5 virtual console, the following menu options are available:

- Power
- Boot
- Chat
- Keyboard
- Screen Capture
- Refresh
- Full Screen
- Disconnect Viewer
- Console Controls
- Virtual Media

The **Pass all keystrokes to server** option is not supported on HTML5 virtual console. Use keyboard and keyboard macros for all the functional keys.

- **Console control** — This has the following configuration options:
  - Keyboard Macros — This is supported in HTML5 virtual console and are listed as the following drop-down options. Click **Apply** to apply the selected key combination on the server.
    - 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
        - Pause
        - Tab
        - Ctrl+Enter
        - SysRq
        - Alt+SysRq
        - Win-P
    - Aspect Ratio — The HTML5 virtual console video image automatically adjusts the size to make the image visible. The following configuration options are displayed as a drop-down list:
        - Maintain
        - Don't Maintain

      Click **Apply** to apply the selected settings on the server.
    - Touch Mode — The HTML5 virtual console supports the Touch Mode feature. The following configuration options are displayed as a drop-down list:
        - Direct
        - Relative

      Click **Apply** to apply the selected settings on the server.

- **Virtual Clipboard** - Virtual clipboard enables you to cut / copy / paste text buffer from virtual console to iDRAC host server. Host server could be BIOS, UEFI or in OS prompt. This is a one-way action from client computer to iDRAC's host server only. Follow these steps to use the Virtual clipboard:
    - Place the mouse cursor or keyboard focus on the desired window in the host server desktop.
    - Select the **Console Controls** menu from vConsole.
    - Copy the OS clipboard buffer using keyboard hotkeys, mouse, or touch pad controls depending on the Client OS. Or, you can type the text manually in the text box.

- Click **Send Clipboard to Host**.
- Then, the text appears on the host server's active window.

NOTE:
- This feature is only available in Datacenter license.
- This feature only supports ASCII text.
- Control characters are not supported.
- Characters such as **New line** and **Tab** are allowed.
- Text buffer size is limited to 4000 characters.
- If more than maximum buffer is pasted, then the edit box in iDRAC GUI will truncate it to maximum buffer size.

- **Keyboard** — The difference between physical and virtual keyboard is that virtual keyboard changes its layout according to the browser language.
- Touch Mode — The HTML5 virtual console supports the Touch Mode feature. The following configuration options are displayed as a drop-down list:
  - Direct
  - Relative

  Click **Apply** to apply the selected settings on the server.
- Mouse Acceleration — Select the mouse acceleration based on the operating system. The following configuration options are displayed as a drop-down list:
  - Absolute (Windows, latest versions of Linux, Mac OS-X)
  - Relative, no acceleration
  - Relative (RHEL, earlier versions of Linux)
  - Linux RHEL 6.x and SUSE Linux Enterprise Server 11 or later

  Click **Apply** to apply the selected settings on the server.
- **Virtual Media** — Click **Connect Virtual Media** option to start the virtual media session. when the virtual media is connected, you can see the options like Map CD/DVD, Map Removable Disk, and Reset USB.

NOTE: For security reasons read/write access is disabled while accessing virtual console in HTML5. With Java or ActiveX plug-ins, you can accept security messaging before the plug-in is given the read/write authority.

Supported Browsers

The HTML5 virtual console is supported on the following browsers:
- Internet Explorer 11
- Google Chrome 83/84
- Mozilla Firefox 80/81
- Safari 13.1.1

NOTE: It is recommended to have Mac OS version 10.10.2 (or onward) installed in the system.

For more details on supported browsers and versions, see the *iDRAC-Versionshinweise* verfügbar unter https://www.dell.com/idracmanuals.

Mauszeiger synchronisieren

ANMERKUNG: Diese Funktion gilt nicht für den Plug-in-Typ eHTML5.

Wenn Sie über die virtuelle Konsole eine Verbindung zu einem Managed System herstellen, wird die Mausbeschleunigungsgeschwindigkeit auf dem Managed System möglicherweise nicht mit dem Mauszeiger auf der Management Station synchronisiert, so dass möglicherweise zwei Mauszeiger im Fenster „Viewer“ angezeigt werden.

Wenn Sie Red Hat Enterprise Linux oder Novell SUSE Linux verwenden, konfigurieren Sie den Mausmodus für Linux, bevor Sie den Viewer für die virtuelle Konsole starten. Die Standardmauseinstellungen des Betriebssystems dienen dazu, den Mauszeiger im Viewer der virtuellen Konsole zu steuern.

Wenn auf der Client-Anzeige der virtuellen Konsole zwei Mauszeiger angezeigt werden, weist dies darauf hin, dass das Betriebssystem des Servers die Relativposition unterstützt. Dies ist in der Regel bei Linux-Betriebssystemen oder dem Lifecycle Controller von Dell der Fall. Dabei werden zwei Mauszeiger angezeigt, wenn die Mausbeschleunigungseinstellungen des Servers von denen des Virtuelle

Konsole-Clients abweichen. Um dieses Problem zu beheben, wechseln Sie zu Einzel-Cursor oder passen Sie die Mausbeschleunigung auf dem verwalteten System und der Management Station an:

- Um auf einen einzigen Cursor zu wechseln, wählen Sie im Menü **Hilfsprogramme Ein Cursor** aus.
- Um die Mausbeschleunigung festzulegen, gehen Sie zu **Extras** > **Sitzungsoptionen** > **Maus**. Wählen Sie auf der Registerkarte **Mausbeschleunigung** basierend auf dem Betriebssystem **Windows** oder **Linux** aus.

Um den Modus mit nur einem Cursor zu beenden, drücken Sie <F9> oder die konfigurierte Beendigungstaste.

ANMERKUNG: Dies gilt nicht für verwaltete Systeme, die auf Windows-Betriebssystemen ausgeführt werden, da diese die Absolutposition unterstützen.

Wenn Sie mithilfe der virtuellen Konsole eine Verbindung zu einem verwalteten System herstellen möchten, auf dem ein Betriebssystem einer aktuellen Linux-Distribution installiert ist, können Probleme mit der Maussynchronisierung auftreten. Mögliche Ursache hierfür ist die Funktion zur vorhersehbaren Zeigerbeschleunigung des GNOME-Desktops. Um eine fehlerfreie Maussynchronisierung in der virtuellen iDRAC-Konsole sicherzustellen, muss diese Funktion deaktiviert sein. Führen Sie im Mausabschnitt der Datei **etc/X11/xorg.conf** Folgendes hinzu, um die vorhersehbare Zeigerbeschleunigung zu deaktivieren:

```
Option "AccelerationScheme" "lightweight".
```

Treten die Synchronisierungsprobleme weiterhin auf, nehmen Sie zusätzlich in der Datei **<user_home>/.gconf/desktop/gnome/peripherals/mouse/%gconf.xml** folgende Änderung vor:

Ändern Sie die Werte für `motion_threshold` und `motion_acceleration` in `-1`.

Wenn Sie die Mausbeschleunigung auf dem GNOME-Desktop ausschalten, gehen Sie im Viewer für die virtuelle Konsole zu **Extras** > **Sitzungsvorgänge** > **Maus**. Wählen Sie unter **Mausbeschleunigung** die Option **Keine** aus.

Für den exklusiven Zugriff auf die Konsole des verwalteten Servers müssen Sie die lokale Konsole deaktivieren und die Anzahl der **Max. Sitzungen** auf der Seite **Virtuelle Konsole** auf `1` setzen.

Weitergeben aller Tastenanschläge über die virtuelle Konsole für Java- oder ActiveX-Plugin

Sie können die Option **Pass all keystrokes to server** (Alle Tastenanschläge an den Server senden) aktivieren und alle Tastenanschläge und Tastenkombinationen von der Management Station an das verwaltete System über den Viewer für die virtuelle Konsole senden. Wenn diese Funktion deaktiviert ist, werden alle Tastenkombinationen an die Management Station gesendet, auf der die Sitzung für die virtuelle Konsole ausgeführt wird. Um alle Tastenanschläge an den Server zu senden, gehen Sie im Viewer für die virtuelle Konsole zu **Tools** > **Session Options (Sitzungsoptionen)** > **General (Allgemein)** und wählen Sie die Option **Pass all keystrokes to server** (Alle Tastenanschläge an den Server senden), um die Tastenanschläge der Management Station an das verwaltete System zu übergeben.

Das Verhalten der Funktion „Alle Tastenanschläge an den Server senden“ hängt von den folgenden Aspekten ab:

- Plugin-Typ (Java oder ActiveX), auf Basis dessen die Sitzung für die virtuelle Konsole gestartet wird.

  Für den Java-Client muss die native Bibliothek laden sein, damit das Durchreichen aller Tastatenanschläge an den Server und der Modus mit nur einem Cursor funktioniert. Wenn die nativen Bibliotheken nicht geladen sind, werden die Optionen **Pass all keystrokes to server** (Alle Tastenanschläge an den Server senden) und **Single Cursor** (Einzel-Cursor) deaktiviert. Wenn Sie eine dieser Optionen dennoch auswählen, wird eine Fehlermeldung angezeigt, in der darauf hingewiesen wird, dass die ausgewählten Optionen nicht unterstützt werden.

  Für den ActiveX-Client muss native Bibliothek geladen sein, damit die Option „Pass all keystrokes to server“ (Alle Tastenanschläge an den Server senden) funktioniert. Wenn die nativen Bibliotheken nicht geladen sind, wird die Option **Pass all keystrokes to server** (Alle Tastenanschläge an den Server senden) deaktiviert. Wenn Sie diese Option dennoch auswählen, wird eine Fehlermeldung angezeigt, in der darauf hingewiesen wird, dass die ausgewählte Option nicht unterstützt werden.

  Aktivieren Sie für Mac OS die Option **Zugriff für Hilfsgeräte aktivieren** im Fenster **Universeller Zugriff**, damit die Funktion „Alle Tastenanschläge an den Server senden“ aktiviert ist.

- Betriebssystem, das auf der Management Station und dem verwalteten System ausgeführt wird. Die Tastenkombinationen, die für das Betriebssystem der Management Station von Bedeutung sind, werden nicht an das verwaltete System übergeben.
- Modus für den Viewer für die virtuelle Konsole – Fensteransicht oder Vollbildschirm.

  Im Vollbildschirmmodus ist die Funktion **Alle Tastenanschläge an den Server senden** standardmäßig aktiviert.

  Im Fenstermodus werden die Tastenanschläge nur weitergeleitet, wenn der Viewer für die virtuelle Konsole sichtbar und aktiv ist.

  Wenn Sie vom Fenster- in den Vollbildschirmmodus wechseln, wird der vorherige Status der Funktion „Alle Tastenanschläge an den Server senden“ wieder aufgenommen.

Java-basierte Sitzung für die virtuelle Konsole, die auf dem Windows-Betriebssystem ausgeführt wird

- Die Tastenkombination „Strg+Alt+Entf“ wird nicht an das Managed System gesendet, sie wird jedoch immer durch Management Station interpretiert.
- Wenn die Option „Alle Tastenanschläge an den Server senden“ aktiviert ist, werden die folgenden Tastenkombinationen nicht an das verwaltete System gesendet:
  - Zurück (Browser) - Taste
  - Vor (Browser) – Taste
  - Aktualisierung (Browser) – Taste
  - Stopp (Browser) – Taste
  - Suchen (Browser) – (Taste)
  - Favoriten (Browser) – Taste
  - Start- und Startseite (Browser) – Taste
  - Stumm – Taste
  - Leiser – Taste
  - Lauter – Taste
  - Nächster Titel – Taste
  - Vorheriger Titel – Taste
  - Datenträger anhalten – Taste
  - Datenträger abspielen/anhalten – Taste
  - E-Mail starten – Taste
  - Datenträger starten – Taste
  - Anwendung 1 starten – Taste
  - Anwendung 2 starten – Taste
- Alle individuellen Tasten (keine Kombination verschiedener Tasten) werden immer an das verwaltete System gesendet. Dazu gehören auch alle Funktionstasten sowie die Umschalt-, Alt-, Strg- und Menütasten. Einige dieser Tasten wirken sich sowohl auf die Management Station als auch auf das verwaltete System aus.

  Wenn beispielsweise die Management Station und das verwaltete System auf einem Windows-Betriebssystem ausgeführt werden und „Pass All Keys“ (Alle Tastenanschläge an den Server senden) deaktiviert ist, wird beim Drücken der Windows-Taste zum Öffnen des Menüs **Start** das Menü **Start** auf der Management Station und dem verwalteten System geöffnet. Wenn jedoch „Pass All Keys“ (Alle Tastenanschläge an den Server senden) aktiviert ist, wird das Menü **Start** nur auf dem verwalteten System und nicht auf der Management Station geöffnet.

- Wenn die Option „Alle Tastenanschläge weiterreichen“ deaktiviert ist, hängt das Verhalten von den gedrückten Tastenkombinationen und den speziellen Tastenkombinationen ab, die durch das Betriebssystem auf der Management Station interpretiert werden.

Java-basierte Sitzung für virtuelle Konsole, die auf dem Linux-Betriebssystem ausgeführt wird

Das für das Windows-Betriebssystem dargestellte Verhalten gilt auch für das Linux-Betriebssystem, jedoch mit den folgenden Ausnahmen:

- Wenn die Option „Alle Tastenanschläge an den Server senden“ aktiviert ist, wird die Tastenkombination „<Strg+Alt+Entf>“ an das Betriebssystem auf dem Managed System weitergeleitet.
- Die magischen S-Abf-Tasten sind Tastenkombinationen, die durch den Linux-Kernel interpretiert werden. Diese sind nützlich, wenn das Betriebssystem auf der Management Station oder dem verwalteten System nicht mehr reagiert und Sie das System wiederherstellen müssen. Sie können die magischen S-Abf-Tasten auf dem Linux-Betriebssystem über eines der folgenden Verfahren aktivieren:
  - Fügen Sie einen Eintrag zu „**/etc/sysctl.conf**“ hinzu.
  - echo "1" > /proc/sys/kernel/sysrq
- Wenn die Option „Pass all keystrokes to server (Alle Tastenanschläge an den Server senden)“ aktiviert ist, werden die magischen S-Abf-Tasten an das Betriebssystem auf dem verwalteten System weitergeleitet. Das Tastensequenzverhalten in Bezug auf das Zurücksetzen des Betriebssystems, also ein Neustart ohne Aufheben der Bereitstellung oder Synchronisieren, hängt davon ab, ob die magische S-Abf-Taste auf der Management Station aktiviert oder deaktiviert ist:
  - Ist die magische S-Abf-Taste auf der Management Station aktiviert, wird die Management Station über die Tastenkombinationen „<Strg+Alt+S-Abf+b>“ oder „<Alt+S-Abf+b>“, ungeachtet vom Status des Systems, zurückgesetzt.
  - Ist die magische S-Abf-Taste auf der Management Station deaktiviert, wird das Betriebssystem auf dem Managed System über die Tastenkombinationen „<Strg+Alt+S-Abf+b>“ oder „<Alt+S-Abf+b>“ zurückgesetzt.

- Weitere S-Abf-Tastenkombinationen (z. B. „<Alt+S-Abf+k>“, „<Strg+Alt+S-Abf+m>“, usw.) werden unabhängig davon, ob die S-Abf-Tasten auf der Management Station aktiviert sind, an das Managed System weitergeleitet.

Verwenden der magischen S-Abf-Tasten über die Remote-Konsole

Sie können die magischen S-Abf-Tasten über die Remote-Konsole über eine der folgenden Optionen aktivieren:

- Opensoure-IPMI-Tool
- Verwenden von SSH oder External Serial Connector

Verwenden des Opensource-IPMI-Hilfsprogramms

Stellen Sie sicher, dass die BIOS/iDRAC-Einstellungen die Konsolenumleitung über SOL unterstützen.

1. Führen Sie an der Eingabeaufforderung den folgenden Befehl zum Aktivieren von SOL aus:

   ```
   Ipmitool –I lanplus –H <ipaddr> -U <username> -P <passwd> sol activate
   ```

   Die SOL-Sitzung wird aktiviert.
2. Nachdem der Server auf dem Betriebssystem gestartet wurde, wird die Anmeldeaufforderung `localhost.localdomain` angezeigt. Melden Sie sich unter Verwendung des Betriebssystembenutzernamens und -kennworts an.
3. Sollte S-Abf nicht aktiviert sein, aktivieren Sie es mit `echo 1 >/proc/sys/kernel/sysrq`.
4. Führen Sie die Break-Sequenz `~B` aus.
5. Verwenden Sie die magische S-Abf-Taste, um die S-Abf-Funktion zu aktivieren. Beispiel: Der folgende Befehl zeigt die Arbeitsspeicherinformationen auf der Konsole an:

   ```
   echo m > /proc/sysrq-trigger displays
   ```

Verwenden von SSH oder des externen seriellen Anschlusses mit direkter Verbindung über serielles Kabel

1. Führen Sie für SSH-Sitzungen, nachdem Sie sich mit dem iDRAC-Nutzernamen und -Kennwort angemeldet haben, bei der `/admin>`-Aufforderung den Befehl `console com2` aus. Es wird die Aufforderung `localhost.localdomain` angezeigt.
2. Bei der Konsolenumleitung über den externen seriellen Anschluss mit direkter Verbindung zum System über ein serielles Kabel wird die Anmeldeaufforderung `localhost.localdomain` angezeigt, nachdem der Server auf dem Betriebssystem gestartet wird.
3. Melden Sie sich unter Verwendung des Betriebssystembenutzernamens und -kennworts an.
4. Wenn SysRq nicht aktiviert ist, aktivieren Sie es über `echo 1 >/proc/sys/kernel/sysrq`.
5. Verwenden Sie die magische Taste, um die SysRq-Funktion zu aktivieren. Mit dem folgenden Befehl wird beispielsweise der Server neu gestartet:

   ```
   echo b > /proc/sysrq-trigger
   ```

   ANMERKUNG: Sie müssen die Break-Sequenz erst nach der Verwendung der magischen S-Abf-Tasten ausführen.

ActiveX-basierte Sitzung für virtuelle Konsole, die auf dem Windows-Betriebssystem ausgeführt wird

Das Verhalten der Funktion „Alle Tastenanschläge an den Server senden“ in einer ActiveX-basierten Sitzung für die virtuelle Konsole, die unter dem Windows-Betriebssystem ausgeführt wird, ähnelt dem Verhalten, das in Bezug auf die Java-basierte Sitzung für die virtuelle Konsole erläutert wurde, die auf der Windows-Management Station ausgeführt wird. Es gelten allerdings die folgenden Ausnahmen:

- Wenn die Funktion „Alle Tastenanschläge senden“ deaktiviert ist, wird durch Drücken der Taste F1 die Hilfe-Anwendung auf der Management Station und auf dem Managed System gestartet, und es wird die folgende Meldung angezeigt:

  ```
  Click Help on the Virtual Console page to view the online Help
  ```

- Die Datenträger-Tasten sind möglicherweise nicht ausdrücklich blockiert.
- Die Tastenkombinationen <Alt + Leer>, <Strg + Alt + +> und <Strg + Alt + -> werden nicht an das Managed System gesendet und werden durch das Betriebssystem auf der Management Station interpretiert.

21

Verwenden des iDRAC Service Module

Das iDRAC-Service-Modul ist eine Softwareanwendung, die auf dem Server installiert werden sollte (Sie ist nicht standardmäßig installiert). Sie ergänzt den iDRAC mit Überwachungsinformationen vom Betriebssystem. Sie ergänzt den iDRAC durch die Bereitstellung zusätzlicher Daten für die Arbeit mit iDRAC-Schnittstellen, wie z. B. der Web-Schnittstelle, der RACADM und WSMAN. Sie können die vom iDRAC-Service-Modul überwachten Funktionen konfigurieren, um den CPU- und Speicherverbrauch im Serverbetriebssystem zu steuern. Die Host-BS-Befehlszeilenschnittstelle wurde eingeführt, um den Status des vollständigen Ein- und Ausschaltvorgangs für alle Systemkomponenten mit Ausnahme des Netzteils zu aktivieren oder zu deaktivieren.

ANMERKUNG: iDRAC9 verwendet die ISM-Version 3.01 und höher.

ANMERKUNG: Sie können das iDRAC Service Module nur dann verwenden, wenn Sie die iDRAC Express oder iDRAC Enterprise/ Datacenter Lizenz installiert haben.

Stellen Sie vor der Verwendung des iDRAC-Service-Moduls Folgendes sicher:

- Sie verfügen über die Berechtigung zum Anmelden, Konfigurieren und zur Serversteuerung in iDRAC, sodass Sie die Funktionen des iDRAC-Servicemoduls aktivieren und deaktivieren können.
- Deaktivieren Sie nicht die Option **iDRAC-Konfiguration über lokale RACADM-Schnittstelle**.
- Der Betriebssystem-zu-iDRAC-Passthrough-Kanal wurde über den internen USB-Bus in iDRAC aktiviert.

ANMERKUNG: Wenn Sie einen LC-Wipe-Vorgang durchführen, werden möglicherweise nach wie vor die alten `idrac.Servicemodule` Werte angezeigt.

ANMERKUNG:

- Wenn das iDRAC-Service-Modul zum ersten Mal ausgeführt wird, wird standardmäßig das Betriebssystem zum iDRAC-Passthrough-Kanal im iDRAC aktiviert. Wenn Sie diese Funktion deaktivieren, nachdem Sie das iDRAC-Service-Modul installiert haben, müssen Sie sie manuell im iDRAC aktivieren.
- Wenn der Passthrough-Kanal zwischen Betriebssystem und iDRAC über LOM in iDRAC aktiviert wird, können Sie das iDRAC Service Module nicht verwenden.

Themen:

- Installieren des iDRAC Service Module
- Unterstützte Betriebssysteme für das iDRAC Service Module
- Überwachungsfunktionen des iDRAC-Servicemoduls
- Verwendung des iDRAC Servicemoduls über die iDRAC-Weboberfläche
- Verwenden des iDRAC Servicemodul von RACADM

Installieren des iDRAC Service Module

Sie können das iDRAC-Servicemodul von **dell.com/support** herunterladen. Sie müssen über die Administratorberechtigung für das Betriebssystem des Servers verfügen, um das iDRAC-Servicemodul zu installieren. Weitere Informationen zur Installation finden Sie im Benutzerhandbuch zu iDRAC-Servicemodul unter www.dell.com/idracservicemodule.

ANMERKUNG: Diese Funktion gilt nicht für Dell Precision PR7910-Systeme.

Installieren des iDRAC-Servicemoduls in iDRAC Express und Basic

Klicken Sie auf der Seite **iDRAC Service Module Setup** (iDRAC-Servicemodul-Setup) auf **Install Service Module** (Servicemodul installieren).

1. Das Installationsprogramm für das Servicemodul ist für das Host-Betriebssystem verfügbar und es wird eine Aufgabe in iDRAC erstellt. Melden Sie sich für Microsoft Windows- oder Linux-Betriebssysteme remote oder lokal auf dem Server an.

2. Suchen Sie nach dem bereitgestellten Volume mit der Bezeichnung **SMINST** in Ihrer Geräteliste und führen Sie das entsprechende Skript aus:
   - Öffnen Sie unter Windows die Eingabeaufforderung und führen Sie die Stapeldatei **ISM-Win.bat** aus.
   - Öffnen Sie unter Linux die Shell-Eingabeaufforderung und führen Sie die Stapeldatei **ISM-LX.sh** aus.
3. Nachdem die Installation abgeschlossen ist, wird das Servicemodul in iDRAC als **installiert** zusammen mit dem Installationsdatum angezeigt.

   ANMERKUNG: Das Installationsprogramm ist für 30 Minuten für das Host-Betriebssystem verfügbar. Wenn Sie die Installation nicht innerhalb von 30 Minuten starten, müssen Sie die Installation des Servicemoduls neu starten.

Installieren von iDRAC Service Module in iDRAC Enterprise

1. Klicken Sie im Assistenten **SupportAssist Registration (Registrierung von SupportAssist)** auf **Next (Weiter)**.
2. Klicken Sie auf der Seite **iDRAC Service Module Setup (iDRAC Service Module-Setup)** auf **Install Service Module (Service Module installieren)**.
3. Klicken Sie auf **Launch Virtual Console (Virtuelle Konsole starten)** und auf **Continue (Weiter)** im Dialogfeld der Sicherheitswarnung.
4. Um die iSM-Installationsprogrammdatei zu lokalisieren, melden Sie sich remote oder lokal beim Server an.

   ANMERKUNG: Das Installationsprogramm ist für das Host-Betriebssystem 30 Minuten verfügbar. Wenn Sie die Installation nicht innerhalb von 30 Minuten starten, müssen Sie sie neu starten.

5. Suchen Sie das bereitgestellte Volume **SMINST** in der Geräteliste und führen Sie das entsprechende Skript aus:
   - Öffnen Sie unter Windows die Eingabeaufforderung und führen Sie die Batch-Datei **ISM-Win.bat** aus.
   - Öffnen Sie unter Linux die Shell-Eingabeaufforderung und führen Sie die Skriptdatei **ISM-Lx.sh** aus.
6. Folgen Sie den Anweisungen auf dem Bildschirm, um die Installation abzuschließen.
   Auf der Seite **iDRAC Service Module Setup (iDRAC Service Module-Setup)** wird die Schaltfläche **Install Service Module (Service Module installieren)**deaktiviert, wenn die Installation abgeschlossen und der Service Module-Status **Running (Ausgeführt)** ist.

Unterstützte Betriebssysteme für das iDRAC Service Module

Eine Liste der Betriebssysteme, die vom iDRAC-Servicemodul unterstützt werden, finden Sie im Benutzerhandbuch zum iDRAC-Servicemodul, das unter www.dell.com/idracservicemodule verfügbar ist.

Überwachungsfunktionen des iDRAC-Servicemoduls

Das iDRAC Service Module (iSM) bietet die folgenden Überwachungsfunktionen:

- Unterstützung des Redfish-Profils für Netzwerkattribute
- Remote-iDRAC-Hardware-Reset
- iDRAC-Zugriff über Host-BS (experimentelle Funktion)
- Bandinterne iDRAC-SNMP-Warnungen
- Anzeigen von Informationen zum Betriebssystem (BS)
- Replizieren von Lifecycle Controller-Protokollen zu den Betriebssystemprotokollen
- Automatische Systemwiederherstellung ausführen
- WMI (Windows Management Instrumentation) -Management-Provider bestücken
- Integration mit SupportAssist-Sammlung. Dies gilt nur, wenn das iDRAC Service-Modul Version 2.0 oder höher installiert ist.
- Bereiten Sie das Entfernen der NVMe-PCIe-SSD vor. Für weitere Informationen https://www.dell.com/support/article/sln310557.
- Aus- und Einschalten des Servers (Remote)

Unterstützung des Redfish-Profils für Netzwerkattribute

Das iDRAC Service Module v2.3 bietet zusätzliche Netzwerkattribute für iDRAC, die über mithilfe der REST-Clients über iDRAC abgerufen werden können. Weitere Informationen finden Sie unter „Unterstützung für das iDRAC-Redfish-Profil“.

Betriebssystem-Informationen

OpenManage Server Administrator gibt derzeit Betriebssysteminformationen und Hostnamen an iDRAC weiter. Das iDRAC Service Module stellt iDRAC ähnliche Informationen, wie beispielsweise BS-Name, BS-Version und FQDN (Fully Qualified Domain Name), bereit. Standardmäßig ist diese Überwachungsfunktion deaktiviert. Diese Option ist nicht deaktiviert, wenn OpenManage Server Administrator auf dem Hostbetriebssystem installiert ist.

Mit iSM Version 2.0 oder höher wird die Betriebssystem-Informationsfunktion um die Überwachung der Betriebssystem-Netzwerkschnittstelle erweitert. Wenn Version 2.0 oder höher des iDRAC Service Module mit iDRAC 2.00.00.00 verwendet wird, startet es die Überwachung der Betriebssystem-Netzwerkschnittstellen. Sie können diese Informationen über die iDRAC-Weboberfläche, RACADM oder WSMan abrufen.

Replizieren von Lifecycle-Protokollen zum BS-Protokoll

Sie können eine Replikation der Lifecycle Controller-Protokolle in die Protokolle des Betriebssystems durchführen, sobald die Funktion in iDRAC aktiviert wird. Dies ist ähnlich wie bei der System Event Log (SEL)-Replikation von OpenManage Server Administrator. Alle Ereignisse, bei der die Option **OS Log** (**BS-Protokoll)** als das Ziel ausgewählt ist (auf der Seite Alerts (Warnungen) oder in den entsprechenden RACADM- oder WSMan-Schnittstellen), werden unter Verwendung des iDRAC Service Module in das BS-Protokoll repliziert. Der Standardsatz von Protokollen, die in die Betriebssystemprotokolle aufgenommen werden sollten, ist derselbe, der auch für SNMP-Warnungen oder -Traps konfiguriert wird.

Das iDRAC Service Module protokolliert auch die Ereignisse, die während der Ausfallzeiten des Betriebssystems aufgetreten sind. Die BS-Protokollierung des iDRAC Service Module erfolgt gemäß den IETF-Syslog-Standards für Linux-basierte Betriebssysteme.

ANMERKUNG: Ab iDRAC Service Module Version 2.1 kann der Replikationsspeicherort für die Lifecycle Controller-Protokolle im Windows-BS unter Verwendung des iDRAC Service Module-Installationsprogramms konfiguriert werden. Sie können während der Installation des iDRAC Service Module oder der Bearbeitung des iDRAC Service Module-Installationsprogramms den Speicherort festlegen.

Wenn OpenManage Server Administrator installiert ist, ist diese Überwachungsfunktion zur Vermeidung doppelter SEL-Einträge in der BS-Protokolldatei deaktiviert.

ANMERKUNG: Unter Microsoft Windows starten Sie den Windows Ereignisprotokolldienst neu oder starten das Host-BS neu, wenn iSM-Ereignisse unter Systemprotokollen anstelle der Anwendungsprotokolle protokolliert wird.

Optionen zur automatischen Systemwiederherstellung

Die automatische Systemwiederherstellungsfunktion ist ein Hardware-basierter Zeitgeber. Wenn ein Hardwarefehler auftritt, wird unter Umständen keine Benachrichtigung ausgegeben, der Server wird jedoch genauso zurückgesetzt, als wenn der Netzschalter betätigt worden wäre. Die Implementierung von ASR erfolgt über einen Timer, der kontinuierlich abwärts zählt. Der Health Monitor lädt den Zähler in regelmäßigen Abständen neu, um zu verhindern, dass er auf Null herunterzählt. Wenn der ASR bis auf Null herunterzählt, wird davon ausgegangen, dass das Betriebssystem gesperrt wurde. In diesem Fall versucht das System automatisch, einen Neustart durchzuführen.

Sie können Optionen zur automatischen Systemwiederherstellung wie z. B. Neustart, Aus-/Einschalten oder Ausschalten des Servers nach einem festgelegten Zeitintervall ausführen. Diese Funktion ist nur dann aktiviert, wenn der Watchdog-Zeitgeber des Betriebssystems deaktiviert ist. Wenn OpenManage Server Administrator installiert ist, ist diese Überwachungsfunktion zur Vermeidung doppelter Watchdog-Zeitgeber deaktiviert.

Windows Management Instrumentation-Provider

Bei WMI handelt es sich um eine Gruppe von Erweiterungen des Windows-Treibermodells, die eine Betriebssystemschnittstelle bereitstellt, über die instrumentierte Komponenten Informationen und Benachrichtigungen zur Verfügung stellen. WMI ist die Microsoft-Implementierung des Web-Based Enterprise Management (WBEM) und Common Information Model (CIM) der Distributed Management Task Force (DMTF) für die Verwaltung von Serverhardware, Betriebssystemen und Anwendungen. WMI-Anbieter helfen bei der

Integration mit Systemverwaltungskonsolen wie Microsoft System Center und ermöglichen die Erstellung von Skripten zur Verwaltung von Microsoft Windows Server-Lösungen.

Sie können die WMI-Option in iDRAC aktivieren oder deaktivieren. iDRAC gibt die WMI-Klassen über das iDRAC Service Module weiter und stellt so Informationen zum Serverstatus bereit. Standardmäßig ist die WMI-Informationsfunktion aktiviert. Das iDRAC Service Module stellt die von WSMan überwachten Klassen in iDRAC über WMI zur Verfügung. Die Klassen werden im Namespace `root/cimv2/dcim` verfügbar gemacht.

Auf die Klassen können Sie mithilfe einer beliebigen Standard-WMI-Client-Schnittstelle zugreifen. Weitere Informationen finden Sie in den Profildokumenten.

Diese Beispiele verwenden die Klassen **DCIM_iDRACCardString** und **DCIM_iDRACCardInteger**, um die Möglichkeiten zu illustrieren, die die WMI-Informationsfunktion im iDRAC-Servicemodul bietet. Weitere Informationen zu den unterstützten Klassen und Profilen finden Sie in der WSMan-Profildokumentation unter https://www.dell.com/support.

Die aufgeführten Attribute werden verwendet, um **Nutzerkonten** zusammen mit den erforderlichen Berechtigungen zu konfigurieren:

Attributname	WSMAN-Klasse	Berechtigung	Lizenz	Beschreibung	Unterstützter Vorgang
Nutzername	DCIM_IDRACCardString	**Schreibberechtigungen:** Nutzerkonfiguration, Anmeldung **Leseberechtigungen:** Anmeldung	Basic-Support	16users: Users.1#UserName to Users.16#UserName	Enum, Get, Invoke
Kennwort	DCIM_IDRACCardString	**Schreibberechtigungen:** Nutzerkonfiguration, Anmeldung **Leseberechtigungen:** Anmeldung	Basic-Support	Users.1#Password to Users.16#Password	Enum, Get, Invoke
Berechtigung	DCIM_iDRACCardInteger	**Schreibberechtigungen:** Nutzerkonfiguration, Anmeldung **Leseberechtigungen:** Anmeldung	Basic-Support	Users.1#Password to Users.16#Password	Enum, Get, Invoke

- `Enumerate` oder `Get`-Vorgang stellt für die genannten Klassen die attributbezogenen Daten bereit.
- Sie können das Attribut festlegen, indem Sie den Befehl `ApplyAttribute` oder `SetAttribute` aus der Klasse **DCIM_iDRACCardService** aufrufen.

ANMERKUNG: Die **DCIM_Account**-Klasse wurde aus WSMAN entfernt und die Funktion wird über das Attributmodell bereitgestellt. Die Klassen **DCIM_iDRACCardString** und **DCIM_iDRACCardInteger** bieten ähnliche Unterstützung bei der Konfiguration von iDRAC-Nutzerkonten.

Remote-iDRAC-Hardware-Reset

Durch die Verwendung von iDRAC können Sie die unterstützten Server auf kritische Probleme mit der Systemhardware, -firmware oder -software überwachen. Manchmal reagiert iDRAC ggf. aus verschiedenen Gründen nicht mehr. Während solcher Szenarien müssen Sie den Server ausschalten und iDRAC zurücksetzen. Um die iDRAC-CPU zurückzusetzen, müssen Sie den Server bzw. das System aus- und wieder einschalten.

Durch die Verwendung der iDRAC-Funktion für einen Remote-Hard-Reset, wenn iDRAC nicht mehr reagiert, können Sie iDRAC remote zurücksetzen, ohne das System aus- und wieder einzuschalten. Um iDRAC remote zurückzusetzen, stellen Sie sicher, dass Sie über Administratorrechte auf dem Hostbetriebssystem verfügen. Standardmäßig ist die iDRAC-Funktion für den Remote-Hard-Reset aktiviert. Ermöglicht Ihnen die Durchführung eines Remote-iDRAC-Hardware-Reset über die iDRAC-Weboberfläche, RACADM und WSMan.

Befehlsverwendung

Dieser Abschnitt enthält Informationen zur Befehlsverwendung auf Windows-, Linux- und ESXi-Betriebssystemen zur Durchführung eines iDRAC-Hardware-Resets.

- **Windows**
  - Unter Verwendung der lokalen Windows Management Instrumentation (WMI):
  - `winrm i iDRACHardReset wmi/root/cimv2/dcim/DCIM_iSMService? InstanceID="iSMExportedFunctions"`
  - Unter Verwendung der Remote-WMI-Schnittstelle:

    ```
    winrm i iDRACHardReset wmi/root/cimv2/dcim/dcim_ismservice?
    InstanceID="iSMExportedFunctions" -u:<admin-username> -p:<admin-password> -r:http://
    <remote-hostname OR IP>/wsman -a:Basic -encoding:utf-8 -skipCACheck -skipCNCheck
    ```

  - Unter Verwendung des Windows PowerShell-Skripts mit und ohne force-Option:

    ```
    Invoke-iDRACHardReset –force
    ```

    ```
    Invoke-iDRACHardReset
    ```

  - Unter Verwendung der Verknüpfung **Programmmenü**:

    Zur Vereinfachung bietet iSM eine Verknüpfung im **Programm-Menü** des Windows-Betriebssystems. Wenn Sie die Option **Remote-Hard-Reset für iDRAC** auswählen, werden Sie dazu aufgefordert, das Zurücksetzen von iDRAC zu bestätigen. Nach der Bestätigung wird iDRAC zurückgesetzt und das Ergebnis des Vorgangs wird angezeigt.

  ANMERKUNG: Die folgende Warnmeldung wird im **Ereignisanzeige** unter der Kategorie **Anwendungsprotokolle** angezeigt. Bei dieser Warnung sind keine weiteren Maßnahmen erforderlich.

  ANMERKUNG: `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 stellt einen ausführbaren Befehl auf allen iSM-unterstützten Linux-Betriebssystemen bereit. Sie können diesen Befehl durch die Anmeldung beim Betriebssystem mithilfe von SSH (oder gleichwertig) ausführen.

  ```
  Invoke-iDRACHardReset
  ```

  ```
  Invoke-iDRACHardReset –f
  ```

- **ESXi**

  Auf allen von iSM unterstützten ESXi-Betriebssystemen unterstützt iSM Version 2.3 einen CMPI-Methodenanbieter (Common Management Programming Interface), um den iDRAC-Reset remote unter Verwendung der WinRM-Remote-Befehle durchzuführen.

  ```
  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
  ```

  ANMERKUNG: Das VMware ESXi-Betriebssystem fordert den Benutzer nicht auf, den Reset des iDRAC vor dem Durchführen zu bestätigen.

  ANMERKUNG: Aufgrund von Einschränkungen des VMware ESXi-Betriebssystems wird die iDRAC-Konnektivität nach dem Zurücksetzen nicht vollständig wiederhergestellt. Stellen Sie sicher, dass Sie iDRAC manuell zurücksetzen.

Tabelle 59. Fehlerbehandlung

Ergebnis	Beschreibung
0	Erfolgreich
1	Nicht unterstützte BIOS-Version für iDRAC-Reset
2	Nicht unterstützte Plattform
3	Zugriff verweigert
4	iDRAC-Reset fehlgeschlagen

Bandinterne Unterstützung für iDRAC-SNMP-Warnungen

Bei Verwendung des iDRAC-Servicemoduls in Version 2.3 können Sie SNMP-Benachrichtigungen vom Hostbetriebssystem empfangen, die den vom iDRAC generierten Benachrichtigungen ähneln.

Sie können die iDRAC-SNMP-Warnungen auch ohne Konfiguration von iDRAC überwachen und den Server remote durch Konfigurieren der SNMP-Traps und -Ziele auf dem Hostbetriebssystem verwalten. In iDRAC Service Module v2.3 oder höher konvertiert diese Funktion alle in die Betriebssystemprotokolle replizierten Lifecycle-Protokolle in SNMP-Traps.

ANMERKUNG: Diese Funktion ist nur dann aktiv, wenn die Replikationsfunktion der Lifecycle-Protokolle aktiviert ist.

ANMERKUNG: Auf Linux-Betriebssystemen erfordert diese Funktion ein aktiviertes Master- oder BS-SNMP mit SNMP-Multiplexing-Protokoll (SMUX).

Standardmäßig ist diese Funktion deaktiviert. Obwohl der In-Band-SNMP-Warnmechanismus mit dem iDRAC-SNMP-Warnmechanismus koexistieren kann, verfügen die aufgezeichneten Protokolle möglicherweise über redundante SNMP-Warnungen von beiden Quellen. Es wird empfohlen, entweder die In-Band- oder Out-of-Band-Option anstelle von beiden zu verwenden.

Befehlsverwendung

Dieser Abschnitt enthält Informationen zur Befehlsverwendung auf Windows-, Linux- und ESXi-Betriebssystemen.

- **Windows-Betriebssystem**
  - Unter Verwendung der lokalen Windows Management Instrumentation (WMI):

    ```
    winrm i EnableInBandSNMPTraps wmi/root/cimv2/dcim/DCIM_iSMService?
    InstanceID="iSMExportedFunctions" @{state="[0/1]"}
    ```

  - Unter Verwendung der Remote-WMI-Schnittstelle:

    ```
    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-Betriebssystem**

  Auf allen iSM-unterstützten Linux-Betriebssystemen stellt iSM einen ausführbaren Befehl bereit. Sie können diesen Befehl durch die Anmeldung beim Betriebssystem mithilfe von SSH (oder gleichwertig) ausführen.

  Beginnend mit iSM 2.4.0 können Sie Agent-x als das Standardprotokoll für die bandinternen iDRAC-SNMP-Alarme unter Verwendung des folgenden Befehls konfigurieren:

  ```
  ./Enable-iDRACSNMPTrap.sh 1/agentx –force
  ```

  Wenn –force nicht angegeben ist, stellen Sie sicher, dass die net-SNMP konfiguriert ist und starten den snmpd-Dienst neu.

  - Gehen Sie wie folgt vor, um diese Funktion zu aktivieren:

    ```
    Enable-iDRACSNMPTrap.sh 1
    ```

    ```
    Enable-iDRACSNMPTrap.sh enable
    ```

  - Gehen Sie wie folgt vor, um diese Funktion zu deaktivieren:

    ```
    Enable-iDRACSNMPTrap.sh 0
    ```

    ```
    Enable-iDRACSNMPTrap.sh disable
    ```

  ANMERKUNG: Die Option **--force** konfiguriert Net-SNMP für die Weiterleitung der Traps. Sie müssen jedoch das Trap-Ziel konfigurieren.

- **VMware ESXi-Betriebssystem**

  Auf allen von iSM unterstützten ESXi-Betriebssystemen unterstützt iSM Version 2.3 einen CMPI-Methodenanbieter (Common Management Programming Interface), um diese Funktion remote unter Verwendung der WinRM-Remote-Befehle zu aktivieren.

```
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]"}
```

ANMERKUNG: Sie müssen die systemweiten VMware ESXi-SNMP-Einstellungen für Traps überprüfen und konfigurieren.

ANMERKUNG: Weitere Einzelheiten finden Sie im technischen Whitepaper zu bandinternen SNMP-Benachrichtigungen **In-Band SNMP Alerts**, das unter https://www.dell.com/support verfügbar ist.

iDRAC-Zugriff über Host-BS

Mit dieser Funktion können Sie die Hardwareparameter über die iDRAC-Weboberfläche, WSMan und RedFish-Schnittstellen mit der Host-IP-Adresse konfigurieren und überwachen, ohne die iDRAC-IP-Adresse zu konfigurieren. Sie können die iDRAC-Anmeldeinformationen verwenden, wenn der iDRAC-Server nicht konfiguriert ist, oder weiterhin dieselben iDRAC-Anmeldeinformationen nutzen, wenn der iDRAC-Server zuvor schon konfiguriert wurde.

iDRAC-Zugriff über Windows-Betriebssysteme

Sie können diese Aufgabe mithilfe der folgenden Methoden durchführen:

- Installieren Sie die iDRAC-Zugriffsfunktion unter Verwendung des Webpack.
- Konfiguration unter Verwendung des iSM-PowerShell-Skripts

Installation unter Verwendung von MSI

Sie können diese Funktion unter Verwendung des web-pack installieren. Diese Funktion ist bei einer typischen iSM-Installation deaktiviert. Falls diese Funktion aktiviert ist, lautet die standardmäßige Überwachungsportnummer 1266. Sie können diese Portnummer innerhalb des Bereichs von 1024 und 65535 ändern. iSM leitet die Verbindung zu iDRAC weiter. iSM erstellt dann einen eingehende Firewall-Regel, OS2iDRAC. Die Überwachungsportnummer wird zur OS2iDRAC-Firewall-Regel im Hostbetriebssystem hinzugefügt, wodurch eingehende Verbindungen ermöglicht werden. Die Firewall-Regel wird automatisch aktiviert, wenn diese Funktion aktiviert ist.

Beginnend mit iSM 2.4.0 können Sie den aktuellen Status und die Listening-Portkonfiguration durch Verwendung der folgenden PowerShell-cmdlet abrufen:

```
Enable-iDRACAccessHostRoute -status get
```

Die Ausgabe dieses Befehls gibt an, ob diese Funktion aktiviert oder deaktiviert ist. Wenn diese Funktion aktiviert ist, wird die Überwachungsportnummer angezeigt.

ANMERKUNG: Die Microsoft IP-Hilfsdienste müssen auf Ihrem System ausgeführt werden, damit diese Funktion funktioniert.

Verwenden Sie für den Zugriff auf die iDRAC-Weboberfläche das Format `https://<host-name>` oder `OS-IP>:443/login.html` im Browser, wobei Folgendes gilt:

- `<host-name>`: vollständiger Hostname des Servers, auf dem iSM für den iDRAC-Zugriff über die Betriebssystemfunktion installiert und konfiguriert ist. Sie können die BS-IP-Adresse verwenden, wenn der Hostname nicht vorhanden ist.
- `443`: die standardmäßige iDRAC-Portnummer. Diese wird als Verbindungsportnummer bezeichnet, an die alle eingehenden Verbindungen auf der Überwachungsportnummer umgeleitet werden. Sie können die Portnummer über die iDRAC-Weboberfläche, WSMan und RACADM-Schnittstellen ändern.

Konfiguration unter Verwendung von iSM-PowerShell-cmdlet

Falls diese Funktion während der Installation von iSM deaktiviert ist, können Sie sie unter Verwendung des folgenden, von iSM bereitgestellten Windows PowerShell-Befehls aktivieren:

```
Enable-iDRACAccessHostRoute
```

Falls die Funktion bereits konfiguriert wurde, können Sie sie deaktivieren oder modifizieren, indem Sie den PowerShell-Befehl mit den entsprechenden Optionen verwenden. Folgende Optionen sind verfügbar:

- **Status**: Dieser Parameter ist obligatorisch. Bei den Werten wird nicht zwischen Groß- und Kleinschreibung unterschieden. Mögliche Werte sind **true**, **false** oder **get**.
- **Port**: Dies ist die Überwachungsportnummer. Wenn Sie keine Portnummer angeben, wird die standardmäßige Portnummer 1266 verwendet. Wenn der Parameterwert für **Status** FALSE ist, können Sie die restlichen Parameter ignorieren. Sie müssen eine neue Portnummer eingeben, die nicht bereits für diese Funktion konfiguriert ist. Die neuen Portnummereinstellungen überschreiben die vorhandene, eingehende OS2iDRAC-Firewall-Regel und Sie können die neue Portnummer für die Verbindung mit iDRAC verwenden. Der Wertebereich liegt zwischen 1024 und 65535.

- **IPRange**: Dieser Parameter ist optional und liefert einen Bereich von IP-Adressen, die eine Verbindung zu iDRAC über das Hostbetriebssystem herstellen dürfen. Der IP-Adressbereich liegt im Classless Inter-Domain Routing (CIDR)-Format vor – einer Kombination aus IP-Adresse und Subnetzmaske. Beispiel: 10.94.111.21/24. Der Zugriff auf iDRAC ist für IP-Adressen, die nicht innerhalb dieses Bereichs liegen, beschränkt.

ANMERKUNG: Diese Funktion unterstützt nur IPv4-Adressen.

iDRAC-Zugriff über Linux-Betriebssysteme

Sie können diese Funktion mithilfe der Datei `setup.sh` installieren, die im Umfang des Webpakets verfügbar ist. Diese Funktion ist bei einer standardmäßigen oder typischen iSM-Installation deaktiviert. Verwenden Sie zum Abrufen des Status dieser Funktion den folgenden Befehl:

```
Enable-iDRACAccessHostRoute get-status
```

Um diese Funktion zu installieren, aktivieren und konfigurieren, verwenden Sie den folgenden Befehl:

```
./Enable-iDRACAccessHostRoute <Enable-Flag> [ <source-port> <source-IP-range/source-ip-range-mask>]
```

<Enable-Flag>=0

Deaktivieren

<source-port> und <source-IP-range/source-ip-range-mask> sind nicht erforderlich.

<Enable-Flag>=1

Aktivieren

<source-port> ist erforderlich und <source-ip-range-mask> ist optional.

<source-IP-range>

IP-Bereich im Format *<IP-Adresse/Subnetzmaske>*. Beispiel: 10.95.146.98/24

Koexistenz von OpenManage Server Administrator mit dem iDRAC Service Module

In einem System können OpenManage Server Administrator und das iDRAC Service Module gleichzeitig und unabhängig voneinander funktionieren.

Wenn Sie die Überwachungsfunktionen während der Installation des iDRAC Service Module aktiviert haben, deaktiviert das iDRAC Service Module nach Abschluss der Installation und Erkennung von OpenManage Server Administrator jene Überwachungsfunktionen, die sich überschneiden. Wenn OpenManage Server Administrator ausgeführt wird, deaktiviert das iDRAC Service Module die sich überschneidenden Überwachungsfunktionen nach Anmeldung beim Betriebssystem und bei iDRAC.

Wenn Sie diese Überwachungsfunktionen zu einem späteren Zeitpunkt mithilfe der iDRAC-Schnittstellen erneut aktivieren, werden die gleichen Prüfungen durchgeführt, und die Funktionen werden abhängig davon aktiviert, ob OpenManage Server Administrator ausgeführt wird oder nicht.

Verwendung des iDRAC Servicemoduls über die iDRAC-Weboberfläche

So verwenden Sie das iDRAC Servicemodul über die iDRAC-Weboberfläche:

1. Gehen Sie zu **iDRAC-Einstellungen** > **Übersicht** > **iDRAC-Service-Modul** > **Service-Modul konfigurieren**.
   Die Seite **iDRAC Service Module-Setup** wird geöffnet.
2. Sie können Folgendes anzeigen:
   - Die auf dem Hostbetriebssystem installierte Version des iDRAC-Servicemoduls.
   - Den Verbindungsstatus des iDRAC Service Module mit iDRAC.

   ANMERKUNG: Wenn ein Server über mehrere Betriebssysteme verfügt und das iDRAC-Service-Modul in allen Betriebssystemen installiert ist, dann stellt der iDRAC nur eine Verbindung mit der neuesten Instanz von iSM unter allen Betriebssystemen her. Ein Fehler wird für alle älteren iSM-Instanzen auf anderen Betriebssystemen angezeigt. Zum Verbinden von iSM und iDRAC auf einem

anderen Betriebssystem, auf dem iSM bereits installiert ist, deinstallieren Sie iSM auf diesem bestimmten Betriebssystem und installieren Sie es neu.

3. Wählen Sie zum Ausführen bandexterner Überwachungsfunktionen eine oder mehrere der folgenden Optionen aus:
   - **BS-Information** – Informationen zum Betriebssystem anzeigen.
   - **Lifecycle-Protokoll im BS-Protokoll replizieren**– Lifecycle Controller Protokolle in die Betriebssystemprotokolle einfügen. Diese Option ist deaktiviert, wenn OpenManage Server Administrator auf dem System installiert ist.
   - **WMI-Informationen** – Schließt WMI-Informationen ein.
   - **Automatische Systemwiederherstellung** – Ausführen der automatischen Systemwiederherstellung nach einer festgelegten Zeit (in Sekunden):
     - **Neustarten**
     - **System ausschalten**
     - **System aus- und einschalten**

     Diese Option ist deaktiviert, wenn OpenManage Server Administrator auf dem System installiert ist.

Verwenden des iDRAC Servicemodul von RACADM

Zur Verwendung des iDRAC-Servicemoduls über RACADM verwenden Sie die Objekte in der Gruppe `ServiceModule`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

22

Verwendung der USB-Schnittstelle für das Server-Management

Auf den Servern der 14. Generation steht ein dedizierter Micro-USB-Port zur Konfiguration des iDRAC zur Verfügung. Sie können die folgenden Funktionen über den Micro-USB-Port ausführen:

- eine Verbindung über die USB-Netzwerkschnittstelle mit dem System herstellen, um auf Systemmanagementtools wie die iDRAC-Weboberfläche und RACADM zuzugreifen.
- einen Server mithilfe von SCP-Dateien konfigurieren, die auf einem USB-Laufwerk gespeichert sind.

ANMERKUNG: Um einen USB-Anschluss zu verwalten oder einen Server zu konfigurieren, indem Sie (SCP-)Profildateien für die Serverkonfiguration auf ein USB-Laufwerk importieren, müssen Sie die Berechtigung Systemsteuerung haben.

ANMERKUNG: Wenn ein USB-Gerät abgeschlossen wird, wird eine Warnmeldung/ein Bericht generiert. Diese Funktion ist nur auf Intel-basierten Servern verfügbar.

Um die Management-USB-Einstellungen zu konfigurieren, navigieren Sie zu **iDRAC-Einstellungen** > **Einstellungen** > **Verwaltungs-USB-Einstellungen**. Die folgenden Optionen sind verfügbar:

- **USB-Verwaltungsschnittstelle**: Wählen Sie **Aktiviert**, damit der Port entweder die SCP-Datei importieren kann, wenn ein USB-Laufwerk angeschlossen ist, oder über den Micro-USB-Anschluss auf den iDRAC zugreifen kann.

  ANMERKUNG: Stellen Sie sicher, dass das USB-Laufwerk eine gültige SCP-Datei enthält.

  ANMERKUNG: Verwenden Sie einen OTG-Adapter für das Konvertieren von USB-Typ-A auf USB-Micro-B. Verbindungen von USB-Hubs werden nicht unterstützt.
- **Über iDRAC verwaltet: USB-SCP**: Wählen Sie aus den folgenden Optionen, um das System mit einem von einem USB-Laufwerk importierten SCP zu konfigurieren:
  - **Deaktiviert**: Deaktiviert den SCP-Import.
  - **Nur aktiviert, wenn der Server standardmäßige Anmeldeinformationseinstellungen hat**: Wenn diese Option ausgewählt ist, kann das SCP nur importiert werden, wenn das Standardkennwort für die folgenden Optionen nicht geändert wird:
    - BIOS
    - iDRAC-Weboberfläche
  - **Nur für komprimierte Konfigurationsdateien aktiviert**: Wählen Sie diese Option, um den Import von SCP-Dateien nur dann zu erlauben, wenn die Dateien im komprimierten Format vorliegen.

    ANMERKUNG: Wenn Sie diese Option auswählen, können Sie die komprimierte Datei mit einem Kennwort schützen. Sie können ein Kennwort eingeben, um die Datei zu schützen, indem Sie die Option **Kennwort für Zip-Datei** verwenden.
  - **Aktiviert**: Wählen Sie diese Option, um das Importieren von SCP-Dateien zu ermöglichen, ohne eine Überprüfung während der Laufzeit durchzuführen.

Themen:

- Zugriff auf die iDRAC-Schnittstelle über eine direkte USB-Verbindung
- Konfigurieren von iDRAC über das Server-Konfigurationsprofil auf dem USB-Gerät

Zugriff auf die iDRAC-Schnittstelle über eine direkte USB-Verbindung

Die iDRAC Direct-Funktion ermöglicht die direkte Verbindung Ihres Laptops mit dem iDRAC USB-Anschluss. Diese Funktion erlaubt die direkte Interaktion mit den iDRAC-Schnittstellen wie Webschnittstelle, RACADM und WSMan zur erweiterten Serververwaltung und -wartung.

Eine Liste der unterstützten Browser und Betriebssysteme finden Sie unter *iDRAC-Versionshinweise* verfügbar unter https://www.dell.com/idracmanuals.

ANMERKUNG: Wenn Sie ein Windows-Betriebssystem verwenden, müssen Sie möglicherweise einen RNDIS-Treiber installieren, um diese Funktion nutzen zu können.

Zum Zugriff auf die iDRAC-Schnittstelle über den USB-Anschluss:

1. Schalten Sie alle Wireless-Netzwerke ab, und trennen Sie die Verbindung zu allen anderen kabelgebundenen Netzwerken.
2. Stellen Sie sicher, dass der USB-Port aktiviert ist. Weitere Informationen finden Sie unter Konfigurieren der USB-Verwaltungsschnittstelle auf Seite 314.
3. Warten Sie, bis der Laptop die IP-Adresse 169.254.0.4 bezieht. Es kann einige Sekunden dauern, bis die IP-Adressen bezogen werden. iDRAC bezieht die IP-Adresse 169.254.0.3.
4. Beginnen Sie mit der Verwendung von iDRAC-Netzwerkschnittstellen, wie z. B. Webschnittstelle, RACADM oder WSMan. Um beispielsweise auf die iDRAC-Webschnittstelle zuzugreifen, öffnen Sie einen unterstützten Browser, geben Sie die Adresse *169.254.0.3* ein und drücken Sie die Eingabetaste.
5. Wenn iDRAC den USB-Anschluss verwendet, zeigt die LED durch Blinken Aktivität an. Dabei leuchtet die LED viermal pro Sekunde auf.
6. Trennen Sie das USB-Kabel nach Abschluss der gewünschten Aktionen vom System. Danach schaltet sich die LED aus.

Konfigurieren von iDRAC über das Server-Konfigurationsprofil auf dem USB-Gerät

Mit dem iDRAC USB-Verwaltungsport können Sie den iDRAC am Server konfigurieren. Konfigurieren Sie die USB-Verwaltungsport-Einstellungen in iDRAC, setzen Sie dann das USB-Gerät mit dem Server-Konfigurationsprofil ein, und importieren Sie dann das Server-Konfigurationsprofil vom USB-Gerät auf iDRAC.

ANMERKUNG: Sie können die USB-Verwaltungsschnittstelle unter Verwendung der iDRAC-Schnittstellen nur dann festlegen, wenn kein USB-Gerät mit dem Server verbunden ist.

Konfigurieren der USB-Verwaltungsschnittstelle

Sie können den iDRAC Direct-USB-Port über das System-BIOS aktivieren oder deaktivieren. Navigieren Sie zu **System-BIOS** > **Integrierte Geräte**. Wählen Sie **Ein** zum Aktivieren und **Aus** zum Deaktivieren des iDRAC Direct-USB-Ports.

Sie müssen im iDRAC zum Konfigurieren der USB-Verwaltungsschnittstelle über die Berechtigung zur Server-Steuerung verfügen. Wenn ein USB-Gerät angeschlossen ist, zeigt die Seite **System-Bestandsaufnahme** die USB-Geräteinformationen unter dem Abschnitt Hardware-Bestandsaufnahme an.

Ein Ereignis wird im Lifecycle Controller-Protokoll protokolliert, wenn:

- das Gerät sich im automatischen oder iDRAC-Modus befindet und das USB-Gerät angeschlossen oder entfernt wird
- der USB-Verwaltungsanschlussmodus geändert wird
- das Gerät automatisch von iDRAC auf BS schaltet
- das Gerät von iDRAC oder dem Betriebssystem ausgeworfen wird.

Wenn ein Gerät seine Leistungsanforderungen an die Stromversorgung übersteigt, wie von USB-Spezifikation erlaubt, wird das Gerät getrennt, und ein Überstromereignis wird mit den folgenden Eigenschaften generiert:

- Kategorie: „Systemfunktionszustand“
- Typ: USB-Gerät
- Schweregrad: Warnung
- Zulässige Benachrichtigungen: E-Mail, SNMP-Trap, Remote Syslog- und WS-Ereignisse
- Maßnahmen: Keine

Eine Fehlermeldung wird angezeigt, und im Lifecycle Controller-Protokoll protokolliert wenn:

- Sie versuchen, den USB-Verwaltungsanschluss ohne Benutzerberechtigung für die Serversteuerung zu konfigurieren.
- Ein USB-Gerät wird von iDRAC verwendet und Sie versuchen, den USB-Verwaltungsanschlussmodus zu ändern.
- Ein USB-Gerät wird von iDRAC verwendet und Sie entfernen das Gerät.

Konfigurieren der USB-Verwaltungsschnittstelle über die Webschnittstelle

So konfigurieren Sie die USB-Schnittstelle:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **iDRAC-Einstellungen** > **Einstellungen** > **Verwaltungs-USB-Einstellungen**.
2. Die **USB-Verwaltungsschnittstelle** wird aktiviert.
3. Wählen Sie im Drop-down-Menü **Über iDRAC verwaltet: USB-SCP-Konfiguration** Optionen zur Konfiguration eines Servers, indem Sie auf einem USB-Laufwerk gespeicherte Serverkonfigurationsprofil-Dateien importieren:
   - **Deaktiviert**
   - **Nur aktiviert, wenn der Server standardmäßige Anmeldeinformationseinstellungen hat**
   - **Nur für komprimierte Konfigurationsdateien aktiviert**
   - **Aktiviert**

   Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

   ANMERKUNG: iDRAC9 ermöglicht Ihnen, die komprimierte Datei mit einem Kennwort zu schützen, nachdem Sie „Nur für komprimierte Konfigurationsdateien aktiviert“ ausgewählt haben, um die Datei vor dem Import zu komprimieren. Sie können ein Kennwort eingeben, um die Datei zu schützen, indem Sie die Option „Kennwort für Zip-Datei“ verwenden.
4. Klicken Sie auf **Anwenden**, um die Einstellungen zu übernehmen.

Konfigurieren der USB-Verwaltungsschnittstelle über RACADM

Zum Konfigurieren der USB-Verwaltungsschnittstelle verwenden Sie die folgenden RACADM-Unterbefehle und -Objekte:

- So zeigen Sie den Status der USB-Schnittstelle an:

```
racadm get iDRAC.USB.PortStatus
```

- So zeigen Sie die Konfiguration der USB-Schnittstelle an:

```
racadm get iDRAC.USB.ManagementPortMode
```

- So zeigen Sie die USB-Gerätebestandsaufnahme an:

```
racadm hwinventory
```

- So richten Sie die Konfiguration von Überstromalarm ein:

```
racadm eventfilters
```

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Konfigurieren der USB-Verwaltungsschnittstelle über das Dienstprogramm für iDRAC-Einstellungen

So konfigurieren Sie die USB-Schnittstelle:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Medien und USB-Schnittstelleneinstellungen**.
   Die Seite **iDRAC-Einstellungen für Media und USB-Schnittstelleneinstellungen** wird angezeigt.
2. Wählen Sie vom Drop-Down-Menü **iDRAC-Direct: USB-Konfigurations-XML** die Optionen zur Konfiguration eines Servers, indem Sie das Server-Konfigurationsprofil auf einem USB-Laufwerk speichern:
   - **Deaktiviert**
   - **Aktiviert, wenn der Server nur standardmäßige Anmeldeinformationseinstellungen besitzt**
   - **Nur für komprimierte Konfigurationsdateien aktiviert**
   - **Aktiviert**

   Weitere Informationen zu den verfügbaren Feldern finden Sie in der *iDRAC Settings Utility Online Help* (Online-Hilfe des Dienstprogramms für iDRAC-Einstellungen).
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**. Die Einstellungen sind damit gespeichert.

Importieren des Serverkonfigurationsprofils vom USB-Gerät

Stellen Sie sicher, dass Sie im Stammverzeichnis des USB-Geräts mit dem Namen `System_Configuration_XML` ein Verzeichnis erstellen, in dem sowohl die Konfigurations- als auch die Steuerungsdateien enthalten sind:

- Das Serverkonfigurationsprofil (SCP) befindet sich im `System_Configuration_XML`-Unterverzeichnis unter dem Stammverzeichnis des USB-Geräts. Diese Datei enthält alle Attributwert-Paare des Servers. Dazu gehören Attribute von iDRAC, PERC, RAID und BIOS. Sie können diese Datei bearbeiten, um Attribute auf dem Server zu konfigurieren. Der Dateiname kann `<servicetag>-config.xml`, `<servicetag>-config.json`, `<modelnumber>-config.xml`, `<modelnumber>-config.json`,`config.xml` oder `config.json` sein.
- Steuerungsdatei – Schließt die Parameter zur Steuerung des Importvorgangs ein und verfügt nicht über die Attribute des iDRAC oder einer anderen Komponente im System. Diese Steuerungsdatei enthält die folgenden drei Parameter:
  - ShutdownType – Ordentliches Herunterfahren, erzwungen, Kein Neustart.
  - TimeToWait (in Sekunden) – mindestens 300 und höchstens 3600.
  - EndHostPowerState – aktiviert oder deaktiviert.

Beispiel für `control.xml`-Datei:

```
<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>
```

Sie müssen zum Ausführen dieses Vorgangs über die Berechtigung zur Serversteuerung verfügen.

ANMERKUNG: Während des Imports des SCP verursacht eine Änderung der USB-Managementeinstellungen in der SCP-Datei SCP einen fehlgeschlagenen Job oder einen Job, der mit Fehlern abgeschlossen wird. Sie können die Attribute im SCP auskommentieren, um Fehler zu vermeiden.

So importieren Sie das Server-Konfigurationsprofil vom USB-Gerät zu iDRAC:

1. Konfigurieren der USB-Verwaltungsschnittstelle
   - Stellen Sie den **USB-Verwaltungsanschlussmodus** auf **Automatisch** oder **iDRAC**.
   - Stellen Sie **iDRAC-Verwaltet: USB XML-Konfiguration** auf **Aktiviert mit Standard-Anmeldeinformationen** oder **Aktiviert** ein.
2. Stecken Sie den USB-Speicherstick (der die Dateien `configuration.xml` und `control.xml` enthält) in die iDRAC-USB-Schnittstelle ein.

   ANMERKUNG: Bei Dateiname und Dateityp wird bei XML-Dateien zwischen Groß- und Kleinschreibung unterschieden. Stellen Sie sicher, dass beide in Kleinbuchstaben geschrieben sind.
3. Das Serverkonfigurationsprofil wird auf dem USB-Gerät im Unterverzeichnis `System_Configuration_XML` im Stammverzeichnis des USB-Geräts ermittelt. Es wird in der folgenden Reihenfolge ermittelt:
   - `<servicetag>-config.xml/<servicetag>-config.json`
   - `<modelnum>-config.xml/<modelnum>-config.json`
   - `config.xml/config.json`
4. Ein Server-Import-Job wird gestartet.

   Wenn das Profil nicht ermittelt wird, wird der Vorgang beendet.

Wenn **iDRAC-Verwaltet: USB XML-Konfiguration** auf **Aktiviert mit Standard-Anmeldeinformationen** eingestellt wurde und das BIOS-Setup-Kennwort nicht Null ist, oder wenn eines der iDRAC-Benutzerkontos geändert wurde, wird eine Fehlermeldung angezeigt und der Vorgang wird beendet.

5. LCD-Bedienfeld und LED, falls vorhanden, zeigen den Status an, dass ein Import-Job gestartet wurde.
6. Wenn eine Konfiguration vorhanden ist, die bereitgestellt werden muss, und der **Herunterfahren-Typ** in der Steuerungsdatei auf **Kein Neustart** festgelegt ist, müssen Sie den Server neu starten, damit die Einstellungen konfiguriert werden. Andernfalls wird der Server neu gestartet wird und die Konfiguration wird angewendet. Nur wenn der Server bereits ausgeschaltet war, wird die bereitgestellte Konfiguration angewendet, und zwar auch dann, wenn die Option **Kein Neustart** festgelegt ist.
7. Nachdem der Import-Job abgeschlossen ist, zeigt die LCD/LED an, dass der Job abgeschlossen ist. Falls ein Neustart erforderlich ist, zeigt die LCD den Job-Status „Unterbrochen – Warten auf Neustart“ an.
8. Wenn das USB-Gerät weiterhin mit dem Server verbunden ist, wird das Ergebnis des Importvorgangs in der Datei `results.xml` des USB-Geräts aufgezeichnet.

LCD-Meldungen

Wenn das LCD-Bedienfeld verfügbar ist, werden die folgenden Meldungen in einer Reihenfolge angezeigt:

1. Importieren – Wenn Sie das Server-Konfigurationsprofil aus dem USB-Gerät kopiert wird.
2. Anwenden – Wenn der Job ausgeführt wird.
3. Abgeschlossen – Wenn der Job erfolgreich abgeschlossen wurde.
4. Mit Fehlern beendet – Wenn der Job mit Fehlern abgeschlossen wurde.
5. Fehlgeschlagen – Wenn der Job fehlgeschlagen ist.

Weitere Details finden Sie in der Ergebnis-Datei auf dem USB-Gerät.

Verhalten der LED-Blinkfunktion

Die USB-LED zeigt den Status einer Server-Konfigurationsprofiloperation an, die über den USB-Port ausgeführt wird. Diese LED ist möglicherweise nicht auf allen Systemen verfügbar.

- Dauerhaft grün – Das Server-Konfigurationsprofil wird von dem USB-Gerät kopiert.
- Grün blinkend – Der Job wird ausgeführt.
- Gelb blinkend – Der Auftrag ist fehlgeschlagen oder mit Fehlern abgeschlossen.
- Dauerhaft grün – Der Job wurde erfolgreich abgeschlossen.

ANMERKUNG: Bei PowerEdge R840 und R940xa blinkt die USB-LED nicht, wenn ein Importvorgang über den USB-Anschluss ausgeführt wird. Überprüfen Sie den Status des Vorgangs mit Hilfe der LCD-Anzeige.

Protokolle und Ergebnis-Datei

Die folgenden Informationen werden für den Importvorgang protokolliert:

- Das automatische Importieren aus USB wird in der Lifecycle Controller-Protokolldatei protokolliert.
- Wenn das USB-Gerät eingesetzt bleibt, werden die Job-Ergebnisse in der Ergebnis-Datei, die sich im USB-Stick befindet, aufgezeichnet.

Eine Ergebnis-Datei namens `Results.xml`, wird in dem Unterverzeichnis mit den folgenden Informationen aktualisiert oder erstellt:

- Service-Tag-Nummer – Die Daten werden aufgezeichnet , nachdem der Importvorgang entweder eine Job-ID oder einen Fehler zurückgegeben hat.
- Job-ID – Die Daten werden aufgezeichnet , nachdem der Importvorgang eine Job-ID zurückgegeben hat.
- Startdatum und Uhrzeit des Jobs – Die Daten werden aufgezeichnet , nachdem der Importvorgang eine Job-ID zurückgegeben hat.
- Status – Die Daten werden aufgezeichnet, wenn der Import-Vorgang einen Fehler zurückgibt oder wenn die Job-Ergebnisse verfügbar sind.

23

Verwenden von Quick Sync 2

Mit Dell OpenManage Mobile auf einem Android- oder iOS-Mobilgerät können Sie auf einfache Weise direkt oder über die OpenManage Essentials oder OpenManage Enterprise (OME)-Konsole auf den Server zugreifen. Sie können die Serverinformationen und den Bestand prüfen, LC- und Systemereignisprotokolle anzeigen, automatische Benachrichtigungen von der OME-Konsole auf dem Mobilgerät erhalten, eine IP-Adresse zuweisen und das iDRAC-Kennwort ändern, wichtige BIOS-Attribute konfigurieren und bei Bedarf Fehlerbehebungsschritte durchführen. Sie können auch den Server aus- und einschalten, auf die Systemkonsole oder die iDRAC-GUI zugreifen.

OMM kann kostenlos im Apple App Store oder im Google Play Store heruntergeladen werden.

Sie müssen die OpenManage Mobile-Anwendung auf dem Mobilgerät installieren (unterstützt Mobilgeräte mit Android 5.0 und höher und iOS 9.0 und höher), um den Server über die iDRAC Quick Sync 2-Schnittstelle zu verwalten.

ANMERKUNG: Dieser Abschnitt wird nur auf Servern angezeigt, die über das Quick Sync 2-Modul im linken Rack-Winkel verfügen.

ANMERKUNG: Diese Funktion wird derzeit auf Mobilgeräten mit Android-Betriebssystemen und Apple iOS unterstützt.

In der aktuellen Version steht diese Funktion für alle PowerEdge-Server der 14. Generation zur Verfügung. Hierfür muss Quick Sync 2 im linken Bedienfeld (integriert im **linken Rack-Winkel**) und Bluetooth Low Energy (und optional Wi-Fi) auf Mobilgeräten aktiviert sein. Daher handelt es sich um ein Hardware-Up-Sell und die Funktionen sind nicht abhängig von der iDRAC-Softwarelizenzierung.

ANMERKUNG: Weitere Informationen zur Konfiguration von Quick Sync 2 in MX-Plattformsystemen finden Sie im Benutzerhandbuch für *OpenManage Enterprise Modular* und im Benutzerhandbuch für *OpenManage Mobile* unter **dell.com/support/manuals**.

Die Vorgehensweisen zur Konfiguration von iDRAC Quick Sync 2:

ANMERKUNG: Gilt nicht für MX-Plattformen.

Aktivieren Sie nach der Konfiguration von Quick Sync die Quick Sync 2-Taste im linken Bedienfeld. Stellen Sie sicher, dass die Quick Sync 2-LED leuchtet. Greifen Sie über ein Mobilgerät (Android 5.0 oder höher oder iOS 9.0 oder höher, OMM 2.0 oder höher) auf Quick Sync 2-Informationen zu.

Mit dem OpenManage Mobile können Sie:

- Bestandsinformationen anzeigen
- Überwachungsinformationen anzeigen
- Die grundlegende iDRAC-Netzwerkeinstellungen konfigurieren

Weitere Informationen über OpenManage Mobile finden Sie im *Dell EMC OpenManage Mobile – Benutzerhandbuch* verfügbar unter https://www.dell.com/openmanagemanuals

Themen:

- Konfigurieren von iDRAC Quick Sync 2
- Verwenden vom Mobile-Gerät zum Anzeigen von iDRAC-Informationen

Konfigurieren von iDRAC Quick Sync 2

Mithilfe der iDRAC-Webschnittstelle RACADM, WSMan und iDRAC HII können Sie die iDRAC Quick Sync 2-Funktion konfigurieren, um auf das mobile Gerät zugreifen zu können:

- **Zugang** – Konfigurieren auf „Lese-/Schreibzugriff“, „Schreibgeschützt“ und „Deaktiviert“. „Lese-/Schreibzugriff“ ist die Standardeinstellung.
- **Zeitüberschreitung** – Konfigurieren auf „Aktiviert“ oder „Deaktiviert“. „Aktiviert“ ist die Standardoption.
- **Zeitüberschreitungsbegrenzung** – Gibt an, nach welcher Zeit der Quick Sync 2-Modus deaktiviert wird. Standardmäßig ist Sekunden ausgewählt. Der Standardwert beträgt 120 Sekunden. Der Zeitbereich liegt zwischen 120 und 3600 Sekunden.
  1. Wenn diese Option aktiviert ist, können Sie eine Zeit angeben, nach der der Quick Sync 2-Modus abgeschaltet wird. Drücken Sie zum Einschalten die Taste erneut.

2. Deaktiviert – Der Zeitgeber lässt nicht zu, dass Sie eine Zeitüberschreitungsperiode eingeben.

- **Leseauthentifizierung** – Auf „Aktiviert“ eingestellt. Dies ist die Standardoption.
- **WLAN** – Auf „Aktiviert“ eingestellt. Dies ist die Standardoption.

Sie müssen die Berechtigung zur Serversteuerung besitzen, um diese Einstellungen konfigurieren zu können. Damit die Einstellungen wirksam werden, ist kein Serverneustart erforderlich. Aktivieren Sie nach der Konfiguration die Schaltfläche „Quick Sync 2“ in der linken Systemsteuerung. Stellen Sie sicher, dass die Quick Sync-Anzeigeleuchte leuchtet. Greifen Sie dann über ein mobiles Gerät auf die Quick Sync-Informationen zu.

Wenn die Konfiguration geändert wird, wird ein Eintrag im Lifecycle Controller-Protokoll eingetragen.

Konfigurieren von iDRAC Quick Sync 2-Einstellungen unter Verwendung der Webschnittstelle

So konfigurieren Sie iDRAC Quick Sync 2:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Hardware Settings (Hardwareeinstellungen)** > **iDRAC Quick Sync**.
2. Wählen Sie im Abschnitt **iDRAC Quick Sync** aus dem Drop-Down-Menü **Access** (Zugriff) eine der folgenden Optionen für die Bereitstellung des Zugriffs auf das mobile Android- oder iOS-Gerät aus:
   - Lesen-Schreiben
   - Nur-Lesen
   - Deaktiviert
3. Aktivieren Sie den Zeitgeber.
4. Geben Sie den Timeoutgrenzwert an.

   Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.
5. Klicken Sie auf **Anwenden**, um die Einstellungen zu übernehmen.

Konfigurieren von iDRAC Quick Sync 2-Einstellungen über RACADM

Zum Konfigurieren der iDRAC Quick Sync 2-Funktion verwenden Sie die racadm-Objekte in der **System.QuickSync**-Gruppe. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Konfigurieren von iDRAC Quick Sync 2-Einstellungen über das Dienstprogramm für iDRAC-Einstellungen

So konfigurieren Sie iDRAC Quick Sync 2:

1. Gehen Sie in der iDRAC-Web-Schnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Hardware Settings (Hardwareeinstellungen)** > **iDRAC Quick Sync**.
2. Im **iDRAC Quick Sync-**Abschnitt:
   - Geben Sie die Zugriffsebene an.
   - Aktivieren Sie Timeout.
   - Geben Sie die benutzerdefinierte Zeitüberschreitungsbegrenzung an (120 bis 3600 Sekunden).

   Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
   Die Einstellungen werden angewendet.

Verwenden vom Mobile-Gerät zum Anzeigen von iDRAC-Informationen

Eine Anleitung zum Anzeigen von iDRAC-Informationen auf dem mobilen Gerät finden Sie unter *Dell EMC OpenManage Mobile – Benutzerhandbuch* verfügbar unter https://www.dell.com/openmanagemanuals.

24

Virtuelle Datenträger verwalten

iDRAC bietet virtuelle Datenträger mit HTML5-basiertem Client mit lokaler ISO- und IMG-Datei und Unterstützung für Remote-ISO- und IMG-Dateien. Der virtuelle Datenträger ermöglicht dem verwalteten Server, auf Datenträgergeräte der Management Station oder auf ISO-CD/DVD-Images einer Netzwerkfreigabe zuzugreifen, als wären sie Geräte auf dem verwalteten Server. Sie benötigen die Berechtigung zur iDRAC-Konfiguration, um die Konfiguration zu ändern.

Nachfolgend sind die konfigurierbaren Attribute aufgeführt:

- Angeschlossene Datenträger aktiviert – aktiviert/deaktiviert
- Verbindungsmodus – automatisch verbinden, verbunden und getrennt
- Max. Sitzungen – 1
- Aktive Sitzungen – 1
- Virtuelle Datenträgerverschlüsselung – aktiviert (standardmäßig)
- Diskettenemulation — deaktiviert (standardmäßig)
- Einmaliges Starten – aktiviert/deaktiviert
- Verbindungsstatus – verbunden/getrennt

Über die Funktion für den virtuellen Datenträger können Sie die folgenden Schritte ausführen:

- Remote auf Datenträger zugreifen, die über das Netzwerk mit einem Remote-System verbunden sind
- Anwendungen installieren
- Treiber-Update
- Ein Betriebssystem auf dem Managed System installieren

Hierbei handelt es sich um eine Lizenzfunktion für Rack- und Tower-Server. Sie ist für Blade-Server standardmäßig verfügbar.

Zentrale Funktionen:

- Virtuelle Datenträger unterstützen virtuelle optische Laufwerke (CD/DVD) und USB-Flash-Festplatten.
- Sie können nur eine USB-Flash-Festplatte, ein Image oder einen Schlüssel und nur ein optisches Laufwerk auf der Managementstation mit einem verwalteten System verbinden. Unterstützte optische Laufwerke umfassen maximal ein verfügbares optisches Laufwerk oder eine einzige ISO-Imagedatei.

  Die folgende Abbildung zeigt ein typisches Setup für einen virtuellen Datenträger.

- Alle verbundenen virtuellen Datenträger emulieren ein physisches Laufwerk auf dem Managed System.
- Auf Windows-basierten, verwalteten Systemen werden die Laufwerke der virtuellen Datenträger automatisch geladen, wenn sie angeschlossen und mit einem Laufwerksbuchstaben konfiguriert sind.
- Auf Linux-basierten Managed Systems mit bestimmten Konfigurationen werden die virtuellen Datenträgerlaufwerke nicht automatisch gemountet. Verwenden Sie zum manuellen Mounten der Laufwerke den Mount-Befehl.
- Alle Zugriffsanforderungen werden auf den virtuellen Datenträger vom verwalteten System über das Netzwerk zur Management Station geleitet.
- Die virtuellen Geräte werden als zwei Laufwerke auf dem Managed System angezeigt, ohne dass der Datenträger auf den Laufwerken installiert ist.
- Sie können zwar das (schreibgeschützte) CD/DVD-Laufwerk zwischen zwei Managed Systems auf der Management Station freigeben, nicht aber den USB-Datenträger.
- Virtuelle Datenträger erfordern eine verfügbare Netzwerkbandbreite von mindestens 128 Kbit/s.
- Wenn LOM- oder NIC-Failovers auftreten, wird die Sitzung für den virtuellen Datenträger möglicherweise getrennt.

Nachdem Sie ein Virtual Media-Image über die virtuelle Konsole angehängt haben, wird das Laufwerk möglicherweise nicht im Windows-Hostbetriebssystem angezeigt. Überprüfen Sie den Windows-Geräte-Manager auf unbekannte Massenspeichergeräte. Klicken Sie mit der rechten Maustaste auf das unbekannte Gerät und aktualisieren Sie den Treiber oder wählen Sie Treiber deinstallieren. Das Gerät wird von Windows nach dem Trennen und Wiederverbinden von vMedia erkannt.

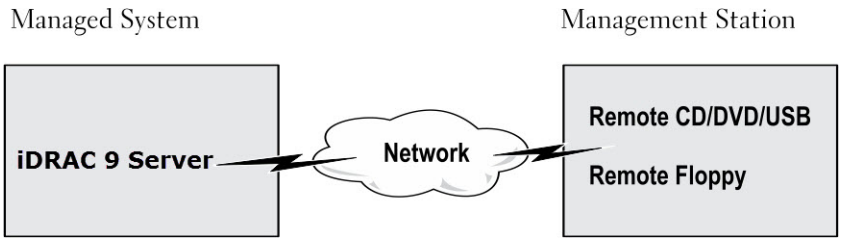


Abbildung 4. Setup für den virtuellen Datenträger

Themen:

- Unterstützte Laufwerke und Geräte
- Virtuellen Datenträger konfigurieren
- Auf virtuellen Datenträger zugreifen
- Startreihenfolge über das BIOS festlegen
- Einmalstart für virtuelle Datenträger aktivieren

Unterstützte Laufwerke und Geräte

Die folgende Tabelle listet die Laufwerke auf, die durch den virtuellen Datenträger unterstützt werden.

Tabelle 60. Unterstützte Laufwerke und Geräte

Laufwerk	Unterstützte Speichermedien
Virtuelle optische Laufwerke	• CD-ROM • DVDs • CD-RW • Kombinationslaufwerk mit dem CD-ROM-Datenträger
USB-Flash-Festplatten	• USB-CD-ROM-Laufwerk mit CD-ROM-Datenträger • USB-Schlüssel-Image im ISO9660-Format

Virtuellen Datenträger konfigurieren

Bevor Sie die Einstellungen für den virtuellen Datenträger konfigurieren, müssen Sie sicherstellen, dass Sie zuvor Ihren Web-Browser für die Verwendung des Java- oder ActiveX-Plugins konfigurieren.

Konfigurieren von virtuellen Datenträgern über die iDRAC-Webschnittstelle

So konfigurieren Sie die Einstellungen für den virtuellen Datenträger:

VORSICHT: Setzen Sie iDRAC nicht zurück, während eine virtuelle Datenträgersitzung ausgeführt wird. Andernfalls könnten unerwünschte Ergebnisse auftreten, beispielsweise der Verlust von Daten.

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Configuration (Konfiguration)** > **Virtual Media (Virtuelle Datenträger)** > **Attached Media (Verbundene Datenträger)**.
2. Nehmen Sie die erforderlichen Einstellungen vor. Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.
3. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Virtuelle Datenträger über RACADM konfigurieren

Verwenden Sie zum Konfigurieren des virtuellen Datenträgers den Befehl `set` bei den Objekten in der Gruppe **iDRAC.VirtualMedia**.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Virtuelle Datenträger über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren

Sie können virtuelle Datenträger über das Dienstprogramm für die iDRAC-Einstellungen verbinden, trennen und automatisch verbinden. Führen Sie dazu folgende Schritte durch:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Datenträger- und USB-Port-Einstellungen**.
   Die Seite **iDRAC-Einstellungen für Media und USB-Schnittstelleneinstellungen** wird angezeigt.
2. Wählen Sie im Bereich **Virtual Media (Virtueller Datenträger)** die Option **Detach (Trennen)**, **Attach (Verbinden)** oder **Auto attach (Automatisch verbinden)** basierend auf der Anforderung. Weitere Informationen zu den Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
   Die Einstellungen des virtuellen Datenträgers werden konfiguriert.

Status des verbundenen Datenträgers und Systemantwort

Die folgende Tabelle beschreibt die Systemantwort auf der Basis der Einstellungen des verbundenen Datenträgers.

Tabelle 61. Status des verbundenen Datenträgers und Systemantwort

Status des verbundenen Datenträgers	Systemreaktion
Trennen	Image konnte dem System nicht zugeordnet werden.
Verbinden	Der Datenträger wird verbunden, auch wenn die **Client-Ansicht** geschlossen wird.
Automatisch verbinden	Der Datenträger wird verbunden, wenn die **Client-Ansicht** geöffnet wird. Er wird getrennt, wenn die **Client-Ansicht** geschlossen wird.

Server-Einstellungen für das Anzeigen virtueller Geräte im virtuellen Datenträger

Sie müssen die folgenden Einstellungen in der Management Station konfigurieren, damit leere Laufwerke sichtbar werden. Klicken Sie dazu im Windows Explorer im Menü **Organisieren** auf **Ordner- und Suchoptionen**. Deaktivieren Sie auf der Registerkarte **Ansicht** die Option **Leere Laufwerke im Ordner „Computer“ ausblenden** und klicken Sie auf **OK**.

Auf virtuellen Datenträger zugreifen

Sie können auf den virtuellen Datenträger mit oder ohne Verwendung der virtuellen Konsole zugreifen. Bevor Sie auf den virtuellen Datenträger zugreifen, müssen Sie Ihre Web-Browser konfigurieren.

Virtueller Datenträger und RFS schließen sich gegenseitig aus. Wenn die RFS-Verbindung aktiv ist und Sie versuchen, den Client des virtuellen Datenträgers zu starten, wird folgende Fehlermeldung angezeigt: *Virtual Media is currently unavailable (Virtueller Datenträger ist aktuell nicht verfügbar). Eine Sitzung für einen virtuellen Datenträger oder eine Remote-Dateifreigabe ist in Verwendung.*

Falls die RFS-Verbindung nicht aktiv ist und Sie versuchen, den Client des virtuellen Datenträgers zu starten, wird der Client erfolgreich gestartet. Sie können dann den virtuellen Datenträger-Client dazu verwenden, Geräte und Dateien den virtuellen Datenträgern zuzuweisen.

Virtuellen Datenträger über die virtuelle Konsole starten

Bevor Sie den virtuellen Datenträger über die virtuelle Konsole starten können, müssen Sie Folgendes sicherstellen:

- Die virtuelle Konsole ist aktiviert.

- Das System ist so konfiguriert, dass leere Laufwerke eingeblendet werden. Gehen Sie im Windows Explorer zu **Ordneroptionen**, deaktivieren Sie das Kontrollkästchen **Leere Laufwerke im Ordner „Computer“ ausblenden**, und klicken Sie auf **OK**.

So greifen Sie über die virtuelle Konsole auf den virtuellen Datenträger zu:

1. Gehen Sie in der iDRAC-Web-Schnittstelle zu **Configuration (Konfiguration)** > **Virtual Console (Virtuelle Konsole)**. Daraufhin wird die Seite **Virtuelle Konsole** angezeigt.
2. Klicken Sie auf **Launch Virtual Console (Virtuelle Konsole starten)**. Der **Virtuelle Konsole-Viewer** wird gestartet.
   ANMERKUNG: Unter Linux ist Java der Standard-Plug-In-Typ für den Zugriff auf die virtuelle Konsole. Öffnen Sie unter Windows die `.jnlp`-Datei, um die virtuelle Konsole mit Java zu starten.
3. Klicken Sie auf **Virtual Media (Virtueller Datenträger)** > **Connect Virtual Media (Virtuellen Datenträger verbinden)**. Die Sitzung des virtuellen Datenträgers wird hergestellt, und das Menü **Virtueller Datenträger** zeigt die Liste der für die Zuordnung verfügbaren Geräte an.
   ANMERKUNG: Das Fenster **Virtuelle Konsole-Viewer** muss während des Zugriffs auf den virtuellen Datenträger aktiviert bleiben.

Virtuelle Datenträger ohne virtuelle Konsole starten

Bevor Sie den virtuellen Datenträger starten, wenn die **Virtuelle Konsole** deaktiviert ist, stellen Sie sicher, dass das System so konfiguriert ist, dass leere Laufwerke eingeblendet werden. Gehen Sie dazu im Windows Explorer zu **Ordneroptionen**, deaktivieren Sie die Option **Leere Laufwerke im Ordner „Computer“ ausblenden** und klicken Sie auf **OK**.

So greifen Sie auf den virtuellen Datenträger bei deaktivierter virtueller Konsole zu:

1. Navigieren Sie in der iDRAC-Weboberfläche zu **Konfiguration** > **Virtuelle Datenträger**.
2. Klicken Sie auf **Virtuelle Datenträger verbinden**.

Alternativ können Sie die virtuellen Datenträger auch anhand folgender Schritte starten:

1. Gehen Sie zu **Konfiguration** > **Virtuelle Konsole**.
2. Klicken Sie auf **Virtuelle Konsole starten**. Die folgende Meldung wird angezeigt:

```
Virtual Console has been disabled. Do you want to continue using Virtual Media redirection?
```

3. Klicken Sie auf **OK**. Daraufhin wird das Fenster **Virtuelle Datenträger** angezeigt.
4. Klicken Sie im Menü **Virtuelle Datenträger** auf **CD/DVD zuordnen** oder auf **Wechseldatenträger zuordnen**. Weitere Informationen finden Sie im Abschnitt Virtuelles Laufwerk zuordnen.
5. Die **Statistik für virtuelle Datenträger** zeigt die Liste der Ziellaufwerke, ihre Zuordnung, ihren Status (schreibgeschützt oder nicht), die Verbindungsdauer, die Lese/Schreib-Bytes und die Übertragungsrate an.

ANMERKUNG: Die Laufwerksbuchstaben der virtuellen Komponente auf dem verwalteten System entsprechen nicht den Buchstaben des physischen Laufwerks auf der Management Station.

ANMERKUNG: Der virtuelle Datenträger funktioniert u. U. nicht ordnungsgemäß auf Systemen mit Windows-Betriebssystem, die mit Internet Explorer Enhanced Security konfiguriert wurden. Um dieses Problem zu lösen, schlagen Sie in der Dokumentation zum Microsoft-Betriebssystem nach oder wenden Sie sich an den Systemadministrator.

Images von virtuellen Datenträgern hinzufügen

Sie können ein Datenträger-Image des Remote-Ordners erstellen und dieses als mittels USB angeschlossenes Gerät für das Server-Betriebssystem bereitstellen. So fügen Sie Images von virtuellen Datenträgern hinzu:

1. Klicken Sie auf **Virtual Media (Virtueller Datenträger)** > **Create Image... (Image erstellen ...)**.
2. Klicken Sie im Feld **Source Folder** (Quellordner) auf **Browse** (Durchsuchen) und navigieren Sie zu der Datei oder dem Verzeichnis, die bzw. das als Quelle für die Image-Datei verwendet werden soll. Die Image-Datei befindet sich auf der Management Station oder dem Laufwerk C: des verwalteten Systems.
3. Der Standardpfad zur Speicherung der erstellen Imagedateien (normalerweise das Desktop-Verzeichnis) wird im Feld **Imagedateiname** angezeigt. Zum Ändern dieses Speicherorts klicken Sie auf **Browse** (Durchsuchen) und geben Sie einen Speicherort an.
4. Klicken Sie auf **Abbild erstellen**.

   Die Abbilderstellung beginnt. Falls der Standort der Abbilddatei sich innerhalb des Quellordners befindet, wird eine Warnmeldung angezeigt, die besagt, dass die Abbilderstellung nicht fortgesetzt werden kann, weil der Standort der Abbilddatei im Quellordner

eine Endlosschleife verursacht. Falls sich der Standort der Abbilddatei nicht im Quellordner befindet, kann die Erstellung des Abbilds fortgesetzt werden.

Nach der Erstellung des Abbildes wird eine Erfolgsmeldung angezeigt.

5. Klicken Sie auf **Fertigstellen**.

   Das Abbild wird erstellt.

   Wenn ein Ordner als Image hinzugefügt wird, wird eine **.img**-Datei auf dem Desktop der Management Station erstellt, über die diese Funktion verwendet wird. Wenn diese **.img**-Datei verschoben oder gelöscht wird, funktioniert der entsprechende Eintrag für diesen Ordner im Menü **Virtual Media** (Virtueller Datenträger) nicht. Es wird daher empfohlen, die **.img**-Datei während der Verwendung des *Image* nicht zu verschieben oder zu löschen. Allerdings kann die **.img**-Datei entfernt werden, sobald die Auswahl des entsprechenden Eintrags zunächst aufgehoben und dann mithilfe von **Remove Image** (Image entfernen) entfernt wird.

Details zum virtuellen Gerät anzeigen

Klicken Sie zum Anzeigen der Details zum virtuellen Gerät im Viewer der virtuellen Konsole auf **Tools** > **Stats (Statistiken)**. Im Fenster **Stats (Statistiken)** zeigt der Bereich **Virtual Media (Virtueller Datenträger)** die zugeordneten virtuellen Geräte und die Lese-/Schreibaktivität für jedes Gerät an. Wenn ein virtueller Datenträger verbunden ist, werden diese Informationen angezeigt. Falls kein virtueller Datenträger verbunden ist, wird die Meldung „Virtual Media is not connected“ (Virtueller Datenträger ist nicht verbunden) angezeigt.

Wenn der virtuelle Datenträger ohne die virtuelle Konsole gestartet wird, dann wird der Bereich **Virtual Media (Virtueller Datenträger)** als Dialogfeld angezeigt. Er enthält Informationen über die zugeordneten Geräte.

Zugriff auf Treiber

Dell EMC Power Edge-Server verfügen im in den System integrierten Flash-Speicher über alle unterstützten Betriebssystemtreiber. Mit iDRAC können Sie Treiber leicht zur Bereitstellung des Betriebssystems auf Ihrem Server mounten oder entfernen.

So mounten Sie die Treiber:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Virtuelle Datenträger**.
2. Klicken Sie auf **Treiber mounten**.
3. Wählen Sie das Betriebssystem im Pop-up-Fenster aus und klicken Sie auf **Treiber mounten**.

   ANMERKUNG: Die Zurverfügungstellung dauert standardmäßig 18 Stunden.

So entfernen Sie die Treiber nach Fertigstellung des Mountvorgangs:

1. Gehen Sie zu **Konfiguration** > **Virtuelle Datenträger**.
2. Klicken Sie auf **Treiber entfernen**.
3. Klicken Sie im Pop-up-Fenster auf **OK**.

ANMERKUNG: Die Option **Treiber mounten** wird möglicherweise nicht angezeigt, wenn das Treiberpaket auf dem System nicht zur Verfügung steht. Stellen Sie sicher, dass Sie das neueste Treiberpaket über https://www.dell.com/support herunterladen und installieren.

USB-Gerät zurücksetzen

So setzen Sie das USB-Gerät zurück:

1. Klicken Sie im Viewer der virtuellen Konsole auf **Tools** > **Statistik**.
   Das Fenster **Statistik** wird angezeigt.
2. Klicken Sie unter **Virtueller Datenträger**auf **USB-Reset**.
   Es wird eine Meldung angezeigt, über die der Benutzer gewarnt wird, dass sich das Zurücksetzen der USB-Verbindung auf den gesamten Input für das Zielgerät auswirken kann, einschließlich des virtuellen Datenträgers und der Maus.
3. Klicken Sie auf **Yes** (Ja).

   Das USB-Gerät wird zurückgesetzt.

   ANMERKUNG: Der virtuelle iDRAC-Datenträger wird nicht beendet, auch wenn Sie sich von der Sitzung für die iDRAC-Webschnittstelle abgemeldet haben.

Virtuelles Laufwerk zuordnen

So ordnen Sie das virtuelle Laufwerk zu:

ANMERKUNG: Bei der Verwendung von ActiveX oder Java-basierten virtuellen Medien müssen Sie über Administratorrechte verfügen, um eine Betriebssystem-DVD oder eine USB-Flash-Festplatte (das mit der Verwaltungsstation verbunden ist) zuzuordnen. Um die Laufwerke zuzuordnen, starten Sie IE als Administrator oder fügen Sie die iDRAC-IP-Adresse zur Liste der vertrauenswürdigen Sites hinzu.

1. Um eine virtuelle Datenträgersitzung vom Menü **Virtueller Datenträger** aus zu starten, klicken Sie auf **Virtuellen Datenträger verbinden**.

   Für jedes Gerät, das für die Zuordnung vom Host-Server her bereit steht, wird ein Menüelement unter dem Menü **Virtueller Datenträger** angezeigt. Das Menüelement wird nach dem Gerätetyp benannt, wie z. B.:
   - CD/DVD zuordnen
   - Entfernbare Festplatte zuordnen

   Die Option **DVD/CD zuordnen** kann für ISO-Dateien verwendet werden und die Option **Wechseldatenträger zuordnen** kann für Abbilder verwendet werden.

   ANMERKUNG:
   - Sie können keine physischen Datenträger, wie USB-basierte Laufwerke, CDs oder DVSs, unter Verwendung der virtuellen HTML5-Konsole zuordnen.
   - Sie können USB-Schlüssel nicht als virtuelle Datenträger-Laufwerke unter Verwendung der virtuellen Konsole/des virtuellen Datenträgers über eine RDP-Sitzung zuordnen.
   - Sie können keine physischen Datenträger mit NTFS-Format in eHTML-Wechselmedien zuordnen, verwenden Sie FAT- oder exFAT-Geräte.

2. Klicken Sie auf den Gerätetyp, den Sie zuordnen möchten.

   ANMERKUNG: Die aktive Sitzung zeigt an, ob eine virtuelle Datenträger-Sitzung von der gegenwärtig aktiven Weboberflächensitzung oder einer anderen Weboberflächensitzung aus aktiv ist.

3. Wählen Sie im Feld **Laufwerk/Abbilddatei** das Gerät aus der Dropdown-Liste aus.

   Die Liste enthält alle verfügbaren (nicht zugeordneten) Geräte, die Sie zuordnen können (CD/DVD, Wechseldatenträger), und Image-Dateitypen, die Sie zuordnen können (ISO oder IMG). Die Abbilddateien befinden sich im Standardverzeichnis für Abbilddateien (normalerweise dem Desktop des Benutzers). Falls das Gerät nicht in der Dropdown-Liste verfügbar ist, klicken Sie auf **Durchsuchen**, um das Gerät anzugeben.

   Der richtige Dateityp für CD/DVD ist ISO und IMG für Wechseldatenträger.

   Wenn das Abbild im Standard-Dateipfad (Desktop) erstellt wird, wenn Sie die Option **Wechseldatenträger zuordnen** auswählen, so ist das erstellte Abbild zur Auswahl im Dropdown-Menü verfügbar.

   Wenn das Abbild an einem anderen Speicherort erstellt wird und Sie die Option **Entfernbare Festplatte zuordnen** auswählen, ist das erstellte Abbild nicht zur Auswahl im Dropdown-Menü verfügbar. Klicken Sie auf **Durchsuchen**, um das Abbild anzugeben.

   ANMERKUNG:
   - Die Option **Schreibgeschützt** wird in eHTML5-basierten JAVA-Wechselmedien ausgegraut.
   - Die Diskettenemulation wird im eHTML5-Plug-in nicht unterstützt.

4. Wählen Sie **Nur-Lesen**, um schreibbare Geräte als Nur-Lesen zuzuordnen.

   Für CD/DVD-Geräte ist diese Option standardmäßig aktiviert, und Sie können sie nicht deaktivieren.

   ANMERKUNG: Wenn Sie für die Zuordnung die virtuelle, HTML5-basierte Konsole verwenden, werden ISO- und IMG-Dateien als schreibgeschützte Dateien zugeordnet.

5. Klicken Sie auf **Gerät zuordnen,** um das Gerät dem Host-Server zuzuordnen.

   Nach der Zuordnung des Geräts/der Datei ändert sich der Name des zugehörigen Menüelements **Virtueller Datenträger**, um den Gerätenamen anzugeben. Falls das CD/DVD-Gerät beispielsweise einer Abbilddatei mit Namen `foo.iso` zugeordnet ist, dann wird das CD/DVD-Menüelement im Menü „Virtueller Datenträger“ **foo.iso auf CD/DVD zugeordnet** genannt. Ein Häkchen bei diesem Menüelement gibt an, dass es zugeordnet ist.

Korrekte virtuelle Laufwerke für die Zuordnung anzeigen

Auf einer Linux-basierten Managementstation zeigt das **Client**-Fenster des virtuellen Datenträgers möglicherweise Wechseldatenträger an, die nicht Teil der Managementstation sind. Um sicherzustellen, dass die richtigen virtuellen Laufwerke für die Zuordnung verfügbar sind, müssen Sie die Porteinstellung für die angeschlossene SATA-Festplatte aktivieren. Führen Sie dazu folgende Schritte durch:

1. Starten Sie das Betriebssystem auf der Managementstation neu. Drücken Sie während des POST <F2>, um das **System-Setup** aufzurufen.
2. Navigieren Sie zu **SATA-Einstellungen**. Die Portdetails werden angezeigt.
3. Aktivieren Sie die Schnittstellen, die derzeit tatsächlich vorhanden und mit der Festplatte verbunden sind.
4. Greifen Sie auf das **Client**-Fenster des virtuellen Datenträgers zu. Es zeigt die korrekten Laufwerke an, die zugeordnet werden können.

Zuordnung für virtuelles Laufwerk aufheben

So heben Sie die Zuordnung für ein virtuelles Laufwerk auf:

1. Wählen Sie im Menü **Virtuelle Datenträger** einen der folgenden Schritte aus:
   - Klicken Sie auf das Gerät, dessen Zuweisung aufgehoben werden soll.
   - Klicken Sie auf **Virtuelle Datenträger trennen**.

   Es wird eine Meldung angezeigt, die um Bestätigung bittet.
2. Klicken Sie auf **Yes** (Ja).
   Das Häkchen für das Menüelement wird nicht angezeigt, was bedeutet, dass es dem Host-Server nicht zugeordnet ist.

   ANMERKUNG: Nach Aufhebung der Zuordnung für ein USB-Gerät, das von einem Clientsystem mit dem Macintosh-Betriebssystem aus an vKM angeschlossen ist, steht das Gerät, für das die Zugordnung aufgehoben wurde, möglicherweise nicht auf dem Client zur Verfügung. Starten Sie das System neu oder stellen Sie das Gerät auf dem Clientsystem manuell bereit, damit das Gerät angezeigt wird.

ANMERKUNG: Um die Zuordnung eines virtuellen DVD-Laufwerks unter Linux OS aufzuheben, müssen Sie das Laufwerk unmounten und entfernen.

Startreihenfolge über das BIOS festlegen

Über das Dienstprogramm für die System-BIOS-Einstellungen können Sie das Managed System so konfigurieren, dass es von virtuellen optischen Laufwerken oder virtuellen Floppy-Laufwerken gestartet wird.

ANMERKUNG: Werden virtuelle Datenträger geändert, während sie verbunden sind, kann dies ggf. zum Anhalten der System-Startsequenz führen.

So aktivieren Sie das Managed System für den Startvorgang:

1. Starten Sie das verwaltete System.
2. Drücken Sie die Taste <F2>, um die Seite **System-Setup** aufzurufen.
3. Gehen Sie zu **System BIOS Settings (System-BIOS-Einstellungen)** > **Boot Settings (Starteinstellungen)** > **BIOS Boot Settings (BIOS-Starteinstellungen)** > **Boot Sequence (Startsequenz)**.
   Im Popup-Fenster werden die virtuellen optischen Laufwerke und virtuellen Diskettenlaufwerke mit den Standard-Startgeräten aufgeführt.
4. Stellen Sie sicher, dass das virtuelle Laufwerk aktiviert und als erstes Gerät mit startfähigem Datenträger aufgelistet ist. Falls erforderlich, folgen Sie zur Änderung der Startreihenfolge den Anweisungen auf dem Bildschirm.
5. Klicken Sie auf **OK**, navigieren Sie zurück zur Seite mit den **System-BIOS-Einstellungen**, und klicken Sie dann auf **Fertigstellen**.
6. Klicken Sie auf **Ja**, um die Änderungen zu speichern und die Seite zu schließen.

   Das verwaltete System wird neu gestartet.

   Das verwaltete System versucht, basierend auf der Startreihenfolge, von einem startfähigen Gerät zu starten. Wenn das virtuelle Gerät angeschlossen ist und ein startfähiger Datenträger vorhanden ist, startet das System zum virtuellen Gerät. Ansonsten ignoriert das System das Gerät – ähnlich wie ein physisches Gerät ohne startfähigen Datenträger.

Einmalstart für virtuelle Datenträger aktivieren

Sie können die Startreihenfolge für den Start nur einmal ändern, nachdem Sie das virtuelle Remote-Datenträgergerät verbunden haben.

Bevor Sie die Einmalstart-Option aktivieren, müssen Sie Folgendes sicherstellen:

- Sie verfügen über die Berechtigung *Benutzer konfigurieren*.
- Ordnen Sie die lokalen oder virtuellen Laufwerke (CD/DVD, Floppy oder das USB-Flash-Gerät) dem startfähigen Datenträger oder dem Image über die Optionen für den virtuellen Datenträger zu.
- Der virtuelle Datenträger befindet sich im Status *Verbunden*, damit die virtuellen Laufwerke in der Startsequenz angezeigt werden.

So aktivieren Sie die Einmalstartoption und starten das Managed System über den virtuellen Datenträger:

1. Gehen Sie in der iDRAC-Web-Schnittstelle zu **Übersicht** > **Server** > **Verbundener Datenträger**.
2. Wählen Sie unter **Virtueller Datenträger** die Option **Einmalstart aktivieren** aus, und klicken Sie dann auf **Anwenden**.
3. Schalten Sie das Managed System ein und drücken Sie **<F2>** während des Startens.
4. Ändern Sie die Startreihenfolge zum Starten vom virtuellen Datenträgergerät.
5. Starten Sie den Server neu.
   Das Managed System startet einmalig vom virtuellen Datenträger.

25

vFlash SD-Karte verwalten

ANMERKUNG: vFlash wird auf AMD Platform-Servern unterstützt.

Die vFlash SD-Karte ist eine SD-Karte (Secure Digital), die ab Werk bestellt und installiert werden kann. Sie können eine Karte mit maximal 16 GB Kapazität verwenden. Nachdem Sie die Karte eingesetzt haben, müssen Sie zum Erstellen und Verwalten von Partitionen die vFlash-Funktion aktivieren. vFlash ist eine lizenzierte Funktion.

ANMERKUNG: Es gibt keine Beschränkung der Größe der SD-Karte. Sie können die werksseitig installierte SD-Karte öffnen und durch eine SD-Karte mit höherer Kapazität ersetzen. Da vFlash das FAT32-Dateisystem verwendet, ist die Dateigröße auf 4 GB beschränkt.

Wenn die Karte im vFlash SD-Kartensteckplatz des Systems nicht erkannt wird, wird die folgende Fehlermeldung in der iDRAC-Weboberfläche unter **Übersicht** > **Server** > **vFlash** angezeigt:

```
SD card not detected. Please insert an SD card of size 256MB or greater.
```

ANMERKUNG: Stellen Sie sicher, dass Sie nur eine mit vFlash kompatible SD-Karte in den iDRAC-vFlash-Kartensteckplatz einsetzen. Wenn Sie eine nicht kompatible SD-Karte einsetzen, wird die folgende Fehlermeldung angezeigt, wenn Sie die Karte initialisieren: Es ist *ein Fehler beim Initialisieren der SD-Karte aufgetreten.*

Zentrale Funktionen:

- Bereitstellung von Speicherplatz und Emulation von USB-Gerät(en).
- Erstellung von bis zu 16 Partitionen. Diese Partitionen werden dem System, wenn angeschlossen, je nach ausgewähltem Emulationsmodus als Diskettenlaufwerk, als Festplatte oder CD/DVD-Laufwerk bereitgestellt.
- Erstellung von Partitionen aus unterstützten Dateisystemtypen. Unterstützt das **.img**-Format für Floppy-Emulationstypen, das **.iso**-Format für CD/DVD-Emulationstypen und die Formate **.iso**- und **.img** für Festplatten-Emulationstypen.
- Erstellung von startfähigen USB-Geräten
- Einmalstart auf ein emuliertes USB-Gerät

  ANMERKUNG: Es kann vorkommen, dass eine vFlash-Lizenz während eines vFlash-Vorgangs abläuft. Wenn dies der Fall ist, werden die laufenden vFlash-Vorgänge normal abgeschlossen.

ANMERKUNG: Wenn der FIPS-Modus aktiviert ist, können Sie keine vFlash-Aktionen ausführen.

Themen:

- Konfigurieren der vFlash-SD-Karte
- vFlash-Partitionen verwalten

Konfigurieren der vFlash-SD-Karte

Bevor Sie vFlash konfigurieren, müssen Sie sicherstellen, dass die vFlash-SD-Karte auf dem System installiert ist. Weitere Informationen zum Installieren und Entfernen der Karte auf dem bzw. vom System finden Sie unter *Installations- und Service-Handbuch* verfügbar unter https://www.dell.com/poweredgemanuals.

ANMERKUNG: Sie müssen über die Berechtigung für den Zugriff auf virtuelle Datenträger verfügen, um die vFlash-Funktion aktivieren oder deaktivieren und die Karte initialisieren zu können.

Eigenschaften der vFlash-SD-Karte anzeigen

Nachdem die vFlash-Funktion aktiviert wurde, können Sie die SD-Karteneigenschaften über die iDRAC-Webschnittstelle oder über RACADM anzeigen.

vFlash SD-Karteneigenschaften über die Web-Schnittstelle anzeigen

Um die Eigenschaften der vFlash-SD-Karte anzuzeigen, gehen Sie in der iDRAC-Web-Schnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Hardware Settings (Hardwareeinstellungen)** > **vFlash**. Die Seite „Card Properties" (Karteneigenschaften) wird angezeigt. Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der *iDRAC-Online-Hilfe*.

vFlash SD-Karteneigenschaften über RACADM anzeigen

Um die Eigenschaften der vFlash SD-Karte unter Verwendung von RACADM anzuzeigen, verwenden Sie den Befehl `get` mit den folgenden Objekten:

- iDRAC.vflashsd.AvailableSize
- iDRAC.vflashsd.Health
- iDRAC.vflashsd.Licensed
- iDRAC.vflashsd.Size
- iDRAC.vflashsd.WriteProtect

Weitere Informationen zu diesen Objekten finden Sie unter *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

vFlash SD-Karteneigenschaften über das Dienstprogramm für die iDRAC-Einstellungen anzeigen

Gehen Sie im **Dienstprogramm für die iDRAC-Einstellungen** zu **Media and USB Port Settings (Medien und USB-Schnittstelleneinstellungen)**, um die Eigenschaften der vFlash-SD-Karte anzuzeigen. Die Seite **Media and USB Port Settings (Datenträger- und USB-Port-Einstellungen)** zeigt die Eigenschaften an. Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

Aktivieren oder Deaktivieren der vFlash-Funktionalität

Zum Ausführen der Partitionsverwaltung muss die vFlash-Funktionalität aktiviert sein.

vFlash-Funktionen über die Web-Schnittstelle aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die vFlash-Funktion:

1. Gehen Sie in der iDRAC-Web-Schnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Hardware Settings (Hardwareeinstellungen)** > **vFlash**.
   Die Seite **Eigenschaften der SD-Karte** wird angezeigt.
2. Aktivieren oder deaktivieren Sie die Option **vFLASH Enabled** (vFlash aktiviert), um die vFlash-Funktion zu aktivieren bzw. zu deaktivieren. Ist eine vFlash-Partition verbunden, können Sie die vFlash-Karte nicht deaktivieren, und es erscheint eine Fehlernachricht.

   ANMERKUNG: Wenn die vFlash-Funktion deaktiviert ist, werden die SD-Karteneigenschaften nicht angezeigt.
3. Klicken Sie auf **Anwenden**. Die vFlash-Funktion wird auf der Basis Ihrer Auswahl aktiviert oder deaktiviert.

vFlash-Funktionen über RACADM aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die vFlash-Funktion über RACADM:

```
racadm set iDRAC.vflashsd.Enable [n]
```

n=0

Deaktiviert

n=1

Aktiviert

ANMERKUNG: Die RACADM-Befehlsfunktionen sind nur verfügbar, wenn eine vFlash-SD-Karte vorhanden ist. Wenn keine Karte vorhanden ist, wird folgende Meldung angezeigt: *ERROR: SD Card not present (FEHLER: SD-Karte nicht vorhanden)*.

vFlash-Funktionen über das Dienstprogramm für die iDRAC-Einstellungen aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die vFlash-Funktion:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Datenträger- und USB-Port-Einstellungen**.
   Die Seite **iDRAC Settings (iDRAC-Einstellungen) Media and USB Port Settings (Datenträger- und USB-Port-Einstellungen)** wird angezeigt.
2. Wählen Sie im Abschnitt **vFlash-Datenträger** die Option **Aktiviert** aus, um die vFlash-Funktion zu aktivieren, oder wählen Sie **Deaktiviert** aus, um die vFlash-Funktion zu deaktivieren.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
   Die vFlash-Funktion wird auf der Basis Ihrer Auswahl aktiviert oder deaktiviert.

vFlash SD-Karte initialisieren

Durch den Initialisierungsvorgang wird die SD-Karte neu formatiert, und die anfänglichen vFlash-Systeminformationen auf der Karte werden konfiguriert.

ANMERKUNG: Wenn die SD-Karte schreibgeschützt ist, wird die Option „Initialisieren“ deaktiviert.

vFlash SD-Karte über die Web-Schnittstelle initialisieren

So initialisieren Sie die vFlash SD-Karte:

1. Gehen Sie in der iDRAC-Web-Schnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Hardware Settings (Hardwareeinstellungen)** > **vFlash**.
   Die Seite **Eigenschaften der SD-Karte** wird angezeigt.
2. Aktivieren Sie **vFLASH**, und klicken Sie auf **Initialisieren**.

   Alle vorhandenen Inhalt werden entfernt, und die Karte wird mit den neuen vFlash-Systeminformationen formatiert.

   Wenn eine vFlash-Partition verbunden wird, schlägt der Initialisierungsvorgang fehl, und es wird eine Fehlermeldung angezeigt.

Initialisieren der vFlash-SD-Karte mithilfe von RACADM

So initialisieren Sie die vFlash-SD-Karte mithilfe von RACADM:

```
racadm set iDRAC.vflashsd.Initialized 1
```

Sämtliche vorhandenen Partitionen werden gelöscht, und die Karte wird erneut formatiert.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

vFlash SD-Karte über das Dienstprogramm für die iDRAC-Einstellungen initialisieren

So initialisieren Sie die vFlash SD-Karte über das Dienstprogramm für die iDRAC-Einstellungen:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Datenträger- und USB-Port-Einstellungen**.
   Die Seite **iDRAC Settings (iDRAC-Einstellungen Media and USB Port Settings (Datenträger- und USB-Port-Einstellungen)** wird angezeigt.
2. Klicken Sie auf **vFlash initialisieren**.
3. Klicken Sie auf **Yes** (Ja). Der Initialisierungsvorgang wird gestartet.
4. Klicken Sie auf **Back** (Zurück) und navigieren Sie zur Seite **iDRAC Settings (iDRAC-Einstellungen) . Media and USB Port Settings (Datenträger- und USB-Port-Einstellungen)**, um die Meldung anzuzeigen, ob der Vorgang erfolgreich war.

Alle vorhandenen Inhalt werden entfernt, und die Karte wird mit den neuen vFlash-Systeminformationen formatiert.

Aktuellen Status über RACADM abrufen

So rufen Sie den Status des zuletzt an die vFlash SD-Karte gesendeten Initialisierungsbefehls ab:

1. Öffnen Sie eine SSH- oder serielle Konsole für das System und melden Sie sich an.
2. Geben Sie den folgenden Befehl `racadm vFlashsd status` ein.
   Daraufhin wird der Status der an die SD-Karte gesendeten Befehle angezeigt.
3. Verwenden Sie zum Abrufen des aktuellen Status für alle vflash-Partitionen den folgenden Befehl: `racadm vflashpartition status -a`
4. Um den letzten Status einer bestimmten Partition abzurufen, verwenden Sie den Befehl: `racadm vflashpartition status -i (index)`

ANMERKUNG: Wenn iDRAC zurückgesetzt wird, geht der Status des letzten Partitionsvorgangs verloren.

vFlash-Partitionen verwalten

Sie können die folgenden Schritte über die iDRAC-Web-Schnittstelle oder RACADM ausführen:

ANMERKUNG: Als Administrator können Sie alle Vorgänge auf den vFlash-Partitionen ausführen. Ansonsten benötigen Sie die Berechtigung **Access Virtual Media (Auf virtuelle Datenträger zugreifen)**, um die Inhalte auf der Partition erstellen, löschen, formatieren, verbinden, trennen oder kopieren zu können.

- Leere Partition erstellen
- Partition unter Verwendung einer Imagedatei erstellen
- Partition formatieren
- Verfügbare Partitionen anzeigen
- Partition modifizieren
- Partitionen verbinden oder trennen
- Vorhandene Partitionen löschen
- Partitionsinhalte herunterladen
- In eine Partition starten

ANMERKUNG: Wenn Sie auf den vFlash-Seiten auf eine beliebige Option klicken, wenn eine Anwendung wie WSMan, das Dienstprogramm für die iDRAC-Einstellungen oder RACADM vFlash verwendet, oder wenn Sie zu einer anderen Seite in der GUI navigieren, zeigt der iDRAC möglicherweise die folgende Meldung an: `vFlash is currently in use by another process. Try again after some time.`

vFlash kann eine schnelle Partitionserstellung durchführen, wenn kein anderer vFlash-Vorgang erfolgt (wie Formatieren, Anhängen von Partitionen usw.). Daher wird empfohlen, zunächst alle Partitionen zu erstellen, bevor Sie andere einzelne Partitionsvorgänge durchführen.

Leere Partition erstellen

Eine leere Partition, die mit dem System verbunden ist, verhält sich ähnlich wie ein leeres USB-Flash-Laufwerk. Sie können leere Partitionen auf einer vFlash-SD-Karte erstellen. Sie können die Partitionen des Typs *Diskette* oder *Festplatte* erstellen. Die Partitionstyp-CD wird nur im Rahmen der Erstellung von Partitionen auf der Basis von Images unterstützt.

Stellen Sie vor dem Erstellen einer leeren Partition Folgendes sicher:

- dass Sie über die Berechtigung **Zugriff auf virtuellen Datenträger** verfügen.
- Die Karte ist initialisiert.
- Die Karte ist nicht schreibgeschützt.
- Auf der Karte wird kein Initialisierungsvorgang ausgeführt.

Leere Partition über die Web-Schnittstelle erstellen

So erstellen Sie eine leere vFlash-Partition:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Configuration (Konfiguration)** > **Systems Settings (Systemeinstellungen)** > **Hardware Settings (Hardware-Einstellungen)** > **vFlash** > **Create Empty Partition (Leere Partition erstellen)**.
   Die Seite **Leere Partition erstellen** wird angezeigt.
2. Geben Sie die erforderlichen Informationen ein und klicken Sie auf **Anwenden**. Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

   Es wird eine neue, unformatierte, leere Partition erstellt, die standardmäßig schreibgeschützt ist. Es wird eine Seite eingeblendet, auf der der Status in Prozent angezeigt wird. In folgenden Fällen wird eine Fehlermeldung angezeigt:
   - Die Karte ist schreibgeschützt.
   - Der Kennzeichnungsname stimmt mit der Kennzeichnung einer vorhandenen Partition überein.
   - Ein nicht ganzzahliger Wert wurde als Partitionsgröße eingegeben, der Wert übersteigt den auf der Karte verfügbaren Speicherplatz oder die Partition ist größer als 4 GB.
   - Auf der Karte wird ein Initialisierungsvorgang ausgeführt.

Leere Partition über RACADM erstellen

So erstellen Sie eine leere Partition:

1. Melden Sie sich über SSH oder die serielle Konsole bei Ihrem System an.
2. Geben Sie den folgenden Befehl ein:

   ```
   racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s [n]
   ```

   wobei `[n]` die Partitionsgröße ist.

   Standardmäßig wird eine leere Partition als editierbare Partition erstellt.

   Wenn die Freigabe nicht mit Nutzername/Kennwort konfiguriert wurde, müssen Sie die Parameter festlegen, und zwar als

   ```
   -u anonymous -p anonymous
   ```

   .

Partition unter Verwendung einer Imagedatei erstellen

Sie können auf der vFlash-SD-Karte mithilfe einer Imagedatei eine neue Partition erstellen. Dabei werden die folgenden Imagedateiformate unterstützt: **.img** oder **.iso**. Die Partitionen liegen in den folgenden Emulationstypen vor: Diskette (**.img**), Festplatte (**.img**) oder CD (**.iso**). Die Größe der erstellten Partition entspricht der Größe der Imagedatei.

Vor der Erstellung einer Partition über eine Imagedatei müssen Sie Folgendes sicherstellen:

- Sie haben Berechtigungen für den Zugriff auf den virtuellen Datenträger.
- Die Karte ist initialisiert.
- Die Karte ist nicht schreibgeschützt.
- Auf der Karte wird kein Initialisierungsvorgang ausgeführt.
- Der Imagetyp und der Emulationstyp stimmen überein.

  ANMERKUNG: Das hochgeladene Image und der Emulationstyp stimmen überein. Es treten Probleme auf, wenn iDRAC ein Gerät mit einem falschen Imagetyp emuliert. Beispiel: Wenn die Partition unter Verwendung eines ISO-Images erstellt wird und der Emulationstyp als Festplatte festgelegt ist, wird das BIOS nicht in der Lage sein, über dieses Image zu starten.
- Die Größe der Image-Datei ist geringer als der auf der Karte verfügbare Speicherplatz oder gleich diesem Speicherplatz.
- Die Größe der Imagedatei ist kleiner oder gleich 4 GB, da die maximale unterstützte Partitionsgröße 4 GB ist. Bei der Erstellung einer Partition mit einem Web-Browser, muss die Größe der Imagedatei jedoch kleiner als 2 GB sein.

ANMERKUNG: Die vFlash-Partition ist eine Imagedatei auf einem FAT32-Dateisystem. Für die Imagedatei gilt daher die 4-GB-Einschränkung.

ANMERKUNG: Die Installation eines vollständigen BS wird unterstützt.

Partition unter Verwendung einer Imagedatei mithilfe der Webschnittstelle erstellen

So erstellen Sie eine vFlash-Partition über eine Imagedatei:

1. Gehen Sie auf der iDRAC-Web-Schnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Hardware Settings (Hardwareeinstellungen)** > **vFlash (VFlash)** > **Create From Image (Aus Image erstellen)**.
   Die Seite **Partition über Imagedatei erstellen** wird angezeigt.
2. Geben Sie die erforderlichen Informationen ein und klicken Sie auf **Anwenden**. Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

   Eine neue Partition wird erstellt. Für den Emulationstyp „CD“ wird eine schreibgeschützte Partition erstellt. Für den Emulationstyp „Diskette“ (Floppy) oder „Festplatte“ (Hard Disk) wird eine Lesen-Schreiben-Partition erstellt. In folgenden Fällen wird eine Fehlermeldung angezeigt:
   - Die Karte ist schreibgeschützt.
   - Der Kennzeichnungsname stimmt mit der Kennzeichnung einer vorhandenen Partition überein.
   - Die Imagedatei ist größer als 4 GB oder übersteigt den auf der Karte verfügbaren Speicherplatz.
   - Die Imagedatei existiert nicht oder die Erweiterung der Imagedatei ist weder .img noch .iso.
   - Auf der Karte wird bereits ein Initialisierungsvorgang ausgeführt.

Partition unter Verwendung einer Imagedatei mithilfe von RACADM erstellen

So erstellen Sie eine Partition aus einer Imagedatei über RACADM:

1. Melden Sie sich über SSH oder die serielle Konsole bei Ihrem System an.
2. Geben Sie den Befehl ein

```
racadm vflashpartition create -i 1 -o drive1 -e HDD -t image -l //myserver/sharedfolder/
foo.iso -u root -p mypassword
```

   Standardmäßig ist die erstellte Partition schreibgeschützt. Bei diesem Befehl wird die Groß-/Kleinschreibung für die Imagedateinamenerweiterung berücksichtigt. Ist die Dateinamenerweiterung in Großbuchstaben, z. b. FOO.ISO anstelle von FOO.iso, gibt der Befehl einen Syntaxfehler aus.

   ANMERKUNG: Diese Funktion wird im lokalen RACADM nicht unterstützt.

   ANMERKUNG: Die Erstellung einer vFlash-Partition aus einer Imagedatei, die sich auf dem CFS oder der für NFS IPv6 aktivierten Netzwerkfreigabe befindet, wird nicht unterstützt.

   Wenn die Freigabe nicht mit Nutzername/Kennwort konfiguriert wurde, müssen Sie die Parameter festlegen, und zwar als

```
-u anonymous -p anonymous
```

   .

Partition formatieren

Sie können eine vorhandene Partition auf der vFlash-SD-Karte auf Grundlage des Dateisystemtyps formatieren. Die unterstützten Dateisystemtypen sind EXT2, EXT3, FAT16 und FAT32. Sie können nur Partitionen des Typs „Festplatte“ oder „Diskette“, aber nicht „CD“ formatieren. Schreibgeschützte Partitionen können nicht formatiert werden.

Vor der Erstellung einer Partition über eine Imagedatei stellen Sie Folgendes sicher:

- Sie haben Berechtigungen für den **Zugriff auf den virtuellen Datenträger**.
- Die Karte ist initialisiert.
- Die Karte ist nicht schreibgeschützt.
- Auf der Karte wird kein Initialisierungsvorgang ausgeführt.

So formatieren Sie eine vFlash-Partition:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Hardware Settings (Hardware-Einstellungen)** > **vFlash** > **Format (Formatieren)**.
   Die Seite **Partition formatieren** wird angezeigt.
2. Geben Sie die erforderlichen Informationen ein und klicken Sie auf **Anwenden**.

Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC-Online-Hilfe*.

Es wird eine Warnungsmeldung angezeigt, die darauf hinweist, dass alle Daten auf der Partition gelöscht werden.

3. Klicken Sie auf **OK**.

   Die ausgewählte Partition wird gemäß dem angegebenen Dateisystemtyp formatiert. In folgenden Fällen wird eine Fehlermeldung angezeigt:

   - Die Karte ist schreibgeschützt.
   - Auf der Karte wird bereits ein Initialisierungsvorgang ausgeführt.

Verfügbare Partitionen anzeigen

Stellen Sie sicher, dass die vFlash-Funktion aktiviert ist, damit die Liste der verfügbaren Partitionen angezeigt wird.

Verfügbare Partitionen über die Web-Schnittstelle anzeigen

Um die verfügbaren vFlash-Partitionen über die iDRAC-Webschnittstelle anzuzeigen, navigieren Sie zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Hardware Settings (Hardwareeinstellungen)** > **vFlash** > **Manage (Verwalten)**. Die Seite **Manage Partitions** (Partitionen verwalten) wird angezeigt und zeigt die verfügbaren Partitionen sowie die zugehörigen Informationen für jede Partition. Weitere Informationen zu den Partitionen finden Sie in der *iDRAC-Online-Hilfe*.

Verfügbare Partitionen über RACADM anzeigen

So zeigen Sie die verfügbaren Partitionen und die dazugehörigen Eigenschaften über RACADM an:

1. Öffnen Sie eine SSH- oder serielle Konsole für das System und melden Sie sich an.
2. Geben Sie die folgenden Befehle ein:
   - So listen Sie alle vorhandenen Partitionen und deren Eigenschaften auf:

     ```
     racadm vflashpartition list
     ```

   - So rufen Sie den Status des Vorgangs auf Partition 1 ab:

     ```
     racadm vflashpartition status -i 1
     ```

   - So rufen Sie den Status sämtlicher vorhandener Partitionen ab:

     ```
     racadm vflashpartition status -a
     ```

     ANMERKUNG: Die Option „-a“ ist nur mit der Statusaktion gültig.

Partition modifizieren

Sie können eine schreibgeschützte Partition zu einer Partition mit Lese- und Schreibzugriff ändern und umgekehrt. Vor dem Ändern der Partition müssen Sie Folgendes sicherstellen:

- Die vFlash-Funktion ist aktiviert.
- Sie haben Berechtigungen für den **Zugriff auf den virtuellen Datenträger**.

ANMERKUNG: Standardmäßig wird eine schreibgeschützte Partition erstellt.

Partition über die Web-Schnittstelle ändern

So ändern Sie eine Partition:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Hardware Settings (Hardwareeinstellungen)** > **vFlash** > **Manage (Verwalten)**.
   Die Seite **Partitionen verwalten** wird angezeigt.
2. Führen Sie in der Spalte **Nur-Lesen** die folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen für die Partition(en), und klicken Sie für den Wechsel in den schreibgeschützten Modus auf **Anwenden**.

- Deaktivieren Sie das Kontrollkästchen für die Partition(en), und klicken Sie für den Wechsel des schreibgeschützten Modus auf **Anwenden**.

  Auf Grundlage der entsprechenden Auswahl werden die Partitionen zu Nur-Lesen oder Lesen-Schreiben geändert.

ANMERKUNG: Handelt es sich um eine Partition des Typs CD, ist der Status schreibgeschützt. Sie können den Zustand nicht zu Lesen-Schreiben ändern. Wenn die Partition verbunden ist, ist das Kontrollkästchen grau unterlegt.

Partition über RACADM ändern

So zeigen Sie die verfügbaren Partitionen und Eigenschaften auf der Karte an:

1. Melden Sie sich über SSH oder die serielle Konsole bei Ihrem System an.
2. Verwenden Sie eine der folgenden Optionen:
   - Verwenden Sie den Befehl `set` zum Ändern des Lese-Schreib-Status der Partition:
     - So ändern Sie eine schreibgeschützte Partition zu Lesen-Schreiben:

       ```
       racadm set iDRAC.vflashpartition.<index>.AccessType 1
       ```

     - So ändern Sie eine Lesen-Schreiben-Partition zu Nur-Lesen:

       ```
       racadm set iDRAC.vflashpartition.<index>.AccessType 0
       ```

   - Verwenden Sie den Befehl `set` zum Festlegen des Emulationstyps:

     ```
     racadm set iDRAC.vflashpartition.<index>.EmulationType <HDD, Floppy, or CD-DVD>
     ```

Partitionen verbinden oder trennen

Wenn Sie eine oder mehrere Partitionen anhängen, werden diese dem Betriebssystem und dem BIOS als USB-Massenspeichergeräte angezeigt. Wenn Sie mehrere Partitionen anhängen, werden diese auf Basis des zugewiesenen Index in aufsteigender Reihenfolge im Betriebssystem und im BIOS-Startreihenfolgemenü angezeigt.

Wenn Sie eine Partition trennen, wird diese nicht mehr im Betriebssystem und im BIOS-Startreihenfolgemenü angezeigt.

Wenn Sie eine Partition anhängen oder trennen, wird der USB-Bus auf dem verwalteten System zurückgesetzt. Dies wirkt sich auch auf die Anwendungen aus, die vFlash verwenden. Außerdem werden die Sitzungen für den virtuellen iDRAC-Datenträger getrennt.

Vor dem Verbinden und Trennen einer Partition müssen Sie Folgendes sicherstellen:

- Die vFlash-Funktion ist aktiviert.
- Es wird nicht bereits ein Initialisierungsvorgang auf der Karte ausgeführt.
- Sie haben Berechtigungen für den **Zugriff auf den virtuellen Datenträger**.

Partitionen über die Web-Schnittstelle verbinden oder trennen

So werden Partitionen verbunden oder abgetrennt:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Hardware Settings (Hardwareeinstellungen)** > **vFlash** > **Manage (Verwalten)**.
   Die Seite **Partitionen verwalten** wird angezeigt.
2. Führen Sie in der Spalte **Verbunden** die folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen für die Partition(en), und klicken Sie zum Verbinden der Partition(en) auf **Anwenden**.
   - Aktivieren Sie das Kontrollkästchen für die Partition(en), und klicken Sie zum Trennen der Partition(en) auf **Anwenden**.

     Auf Grundlage der entsprechenden Auswahl werden die Partitionen verbunden oder abgetrennt.

Partitionen über RACADM verbinden oder trennen

So werden Partitionen verbunden oder abgetrennt:

1. Melden Sie sich über SSH oder die serielle Konsole bei Ihrem System an.

2. Verwenden Sie die folgenden Befehle:
   - So verbinden Sie eine Partition:

     ```
     racadm set iDRAC.vflashpartition.<index>.AttachState 1
     ```

   - So trennen Sie eine Partition ab:

     ```
     racadm set iDRAC.vflashpartition.<index>.AttachState 0
     ```

Verhalten des Betriebssystems bei verbundenen Partitionen

Windows- und Linux-Betriebssysteme:

- Das Betriebssystem kontrolliert die Laufwerksbuchstaben und weist sie den angeschlossenen Partitionen zu.
- Schreibgeschützte Partitionen sind schreibgeschützte Laufwerke auf dem Betriebssystem.
- Das Betriebssystem muss das Dateisystem einer verbundenen Partition unterstützen. Andernfalls können Sie die Inhalte der Partition über das Betriebssystem weder lesen noch ändern. In einer Windows-Umgebung kann das Betriebssystem beispielsweise den Partitionstyp EXT2 nicht lesen, da es sich hierbei um einen nativen Linux-Typ handelt. In einer Linux-Umgebung kann das Betriebssystem wiederum den Partitionstyp NTFS nicht lesen, da es sich hierbei um einen nativen Windows-Typ handelt.
- Die Kennzeichnung der vFlash-Partition weicht vom Volume-Namen des Dateisystems auf dem emulierten USB-Gerät ab. Sie können den Volume-Namen des emulierten USB-Geräts im Betriebssystem ändern. Der Kennzeichnungsname der Partition, der in iDRAC gespeichert ist, wird dadurch nicht geändert.

Vorhandene Partitionen löschen

Stellen Sie vor dem Löschen vorhandener Partitionen Folgendes sicher:

- Die vFlash-Funktion ist aktiviert.
- Die Karte ist nicht schreibgeschützt.
- Die Partition ist nicht verbunden.
- Auf der Karte wird kein Initialisierungsvorgang ausgeführt.

Vorhandene Partitionen über die Web-Schnittstelle löschen

Löschen einer bestehenden Partition:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Hardware Settings (Hardwareeinstellungen)** > **vFlash** > **Manage (Verwalten)**.
   Die Seite **Partitionen verwalten** wird angezeigt.
2. Klicken Sie in der Spalte **Löschen** auf das Symbol zum Löschen, um die gewünschte Partition zu löschen.
   Es wird eine Meldung angezeigt, aus der hervorgeht, dass die Partition durch diese Maßnahme endgültig gelöscht wird.
3. Klicken Sie auf **OK**.
   Die Partition ist damit gelöscht.

Vorhandene Partitionen über RACADM löschen

So löschen Sie Partitionen:

1. Öffnen Sie eine SSH- oder serielle Konsole für das System und melden Sie sich an.
2. Geben Sie die folgenden Befehle ein:
   - So löschen Sie eine Partition:

     ```
     racadm vflashpartition delete -i 1
     ```

   - Zum Löschen sämtlicher Partitionen ist die vFlash-SD-Karte erneut zu initialisieren.

Partitionsinhalte herunterladen

Sie können die Inhalte einer vFlash-Partition in den folgenden Formaten herunterladen: **.img** oder **.iso**:

- Managed System (über das iDRAC ausgeführt wird)
- Netzwerkstandort, der mit einer Management Station verknüpft ist.

Vor dem Herunterladen der Partitionsinhalte müssen Sie Folgendes sicherstellen:
- Sie haben Berechtigungen für den Zugriff auf den virtuellen Datenträger.
- Die vFlash-Funktion ist aktiviert.
- Auf der Karte wird kein Initialisierungsvorgang ausgeführt.
- Wenn eine Lesen-Schreiben-Partition vorliegt, darf diese nicht verbunden sein.

So laden Sie die Inhalte der vFlash-Partition herunter:

1. Gehen Sie in der iDRAC-Web-Schnittstelle zu **Configuration (Konfiguration)** > **System Settings (Systemeinstellungen)** > **Hardware Settings (Hardwareeinstellungen)** > **vFlash** > **Download (Herunterladen)**.
   Die Seite **Partition herunterladen** wird angezeigt.
2. Wählen Sie aus dem Drop-Down-Menü **Kennzeichnung** eine Partition aus, die Sie herunterladen möchten, und klicken Sie auf **Herunterladen**.

   ANMERKUNG: Alle vorhandenen Partitionen (mit Ausnahme der verbundenen Partitionen) werden in der Liste angezeigt. Standardmäßig ist die erste Partition ausgewählt.

3. Legen Sie den Speicherort fest, an dem die Datei gespeichert werden soll.
   Der Inhalt der ausgewählten Partition wird an den festgelegten Speicherort heruntergeladen.

   ANMERKUNG: Wenn nur der Ordnerspeicherort angegeben ist, wird die Partitionsbezeichnung mit dem Dateinamen und außerdem bei CD- und Festplattenpartitionen mit der Dateierweiterung **.iso** und bei Floppy- und Festplattenpartitionen mit der Dateierweiterung **.img** gekennzeichnet.

In eine Partition starten

Sie können eine verbundene vFlash-Partition als Startgerät für den nächsten Startvorgang einrichten.

Vor dem Starten einer Partition müssen Sie Folgendes sicherstellen:
- Die vFlash-Partition enthält ein startfähiges Image (in den Formaten **.img** oder **.iso**), um einen Start vom Gerät zu ermöglichen.
- Die vFlash-Funktion ist aktiviert.
- Sie haben Berechtigungen für den Zugriff auf den virtuellen Datenträger.

Über die Web-Schnittstelle auf eine Partition starten

Weitere Informationen zum Festlegen der vFlash-Partition als ein erstes Startgerät finden Sie unter Über die Web-Schnittstelle auf eine Partition starten auf Seite 337.

ANMERKUNG: Wenn die verbundene(n) vFlash-Partition(en) nicht im Drop-Down-Menü **Erstes Startlaufwerk** gelistet ist/sind, müssen Sie sicherstellen, dass das BIOS in der aktuellen Version vorliegt.

Über RACADM auf eine Partition starten

Um eine vFlash-Partition als erstes Startgerät einzustellen, verwenden Sie das Objekt `iDRAC.ServerBoot`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

ANMERKUNG: Wenn Sie diesen Befehl ausführen, wird die Kennzeichnung der vFlash-Partition automatisch auf Einmalstart eingestellt, `iDRAC.ServerBoot.BootOnce` wird auf `1` eingestellt. Der Einmalstart startet das Gerät auf der Partition nur einmal und behält es nicht dauerhaft als erstes Gerät in der Startreihenfolge.

26

SMCLP verwenden

ANMERKUNG: SMCLP wird nur in iDRAC-Versionen unterstützt, die älter als 4.00.00.00 sind.

Die Server Management Command Line Protocol (SMCLP)-Spezifikation aktiviert die CLI-basierte Systemverwaltung. Sie definiert ein Protokoll für die Verwaltungsbefehle, die über Standardzeichen-basierte Streams übertragen werden. Dieses Protokoll greift über einen von Hand eingegebenen Befehlssatz auf einen Common Information Model Object Manager (CIMOM) zu. Das SMCLP ist eine Unterkomponente der Distributed Management Task Force (DMTF)-Initiative, mit der die Systemverwaltung über mehrere Plattformen hinweg optimiert werden kann. In Verbindung mit der Spezifikation für verwaltete Elementadressierung und zahlreichen Profilen zu SMCLP-Zuordnungsspezifikationen beschreibt die SMCLP-Spezifikation die Standard-Verben und -Ziele zum Ausführen verschiedener Managementaufgaben.

ANMERKUNG: Es wird angenommen, dass Sie mit der SMASH-Initiative (Systemverwaltungsarchitektur für Serverhardware) und den SMWG SMCLP-Angaben vertraut sind.

Das SM-CLP ist eine Unterkomponente der Distributed Management Task Force (DMTF)-Initiative, mit der die Server-Verwaltung über mehrere Plattformen hinweg optimiert werden kann. In Verbindung mit der Spezifikation für verwaltete Elementadressierung und zahlreichen Profilen zu SM-CLP-Zuordnungsspezifikationen beschreibt die SM-CLP-Spezifikation die Standard-Verben und -Ziele zum Ausführen verschiedener Managementaufgaben.

Das SMCLP wird von der iDRAC-Controller-Firmware gehostet und unterstützt SSH- und serielle Anschlüssen. Die iDRAC SM-CLP-Schnittstelle basiert auf der SM-CLP-Spezifikation Version 1.0 der Organisation DMTF.

ANMERKUNG: Informationen zu den Profilen, Erweiterungen und MOFs können unter https://www.dell.com/support abgerufen werden, und die gesamten DMTF-Informationen können von **dmtf.org/standards/profiles/** abgerufen werden.

SM-CLP-Befehle nutzen eine Teilmenge der lokalen RACADM-Befehle. Die Befehle sind für die Skripterstellung nützlich, da sie von einer Befehlszeile der Management Station aus ausgeführt werden können. Sie können die Ausgabe von Befehlen in genau definierten Formaten, einschließlich XML, abrufen, was die Skripterstellung und die Integration mit bestehende Berichterstellungs- und Managementtools erleichtert.

Themen:

- System-Verwaltungsfunktionen über SMCLP
- SMCLP-Befehle ausführen
- iDRAC-SMCLP-Syntax
- MAP-Adressbereich navigieren
- Verb „show“ verwenden
- Anwendungsbeispiele

System-Verwaltungsfunktionen über SMCLP

Mit iDRAC SMCLP können Sie die folgenden Funktionen ausführen:

- Serverenergieverwaltung – System einschalten, herunterfahren oder neu starten
- Verwaltung des Systemereignisprotokolls (SEL) – SEL-Datensätze anzeigen oder löschen
- iDRAC-Benutzerkonten anzeigen
- Systemeigenschaften anzeigen

SMCLP-Befehle ausführen

Sie können die SMCLP-Befehle über die SSH-Schnittstelle ausführen. Öffnen Sie eine SSH-Sitzung und melden Sie sich bei iDRAC als Administrator an. Die SMCLP-Eingabeaufforderung (admin->) wird angezeigt.

SMCLP-Befehlseingaben:

- yx1x-Blade-Server verwenden – `$`.

- yx1x-Rack- und -Tower-Server verwenden `admin->`.
- yx2x-Blade-, -Rack- und -Tower-Server verwenden `admin->`.

Hier steht „y“ für ein alphanumerisches Zeichen wie „M“ (für Blade-Server), „R“ (für Rack-Server) und „T“ (für Tower-Server) und „x“ für eine Zahl. Die Zahl dient der Kennzeichnung der Dell PowerEdge-Servergeneration.

ANMERKUNG: Skripte, die `-$` verwenden, können diese für yx1x-Systeme verwenden, aber beginnend bei yx2x-Systemen kann ein Skript mit `admin->` für Blade-, Rack- und Tower-Server verwendet werden.

iDRAC-SMCLP-Syntax

iDRAC-SMCLP verwendet das Konzept von Verben und Zielen und stellt Systemverwaltungsfunktionen über die CLI bereit. Das Verb gibt den auszuführenden Vorgang an und das Ziel bestimmt die Entität (oder das Objekt), die den Vorgang ausführt.

Die SMCLP Befehlszeilensyntax:

```
<verb> [<options>] [<target>] [<properties>]
```

Die folgende Tabelle zeigt die Verben sowie ihre Definitionen.

Tabelle 62. SMCLP-Verben

Verb	Definition
cd	Navigiert durch den MAP mittels der Shell.
set	Stellt eine Eigenschaft auf einen bestimmten Wert ein.
Hilfe	Zeigt die Hilfe für ein bestimmtes Ziel an.
reset	Setzt das Ziel zurück.
show	Zeigt die Zieleigenschaften, Verben und Unterziele an.
start	Schaltet ein Ziel ein.
stop	Fährt ein Ziel herunter.
exit	Beendet die SMCLP-Shell-Sitzung
Version	Zeigt die Versionsattribute eines Ziels an.
load	Lädt ein Binärbild von einer URL zu einer bestimmten Zieladresse.

Die folgende Tabelle enthält eine Liste mit Zielen.

Tabelle 63. SMCLP-Ziele

Ziel	Definitionen
`admin1`	admin domain
`admin1/profiles1`	Registrierte Profile in iDRAC
`admin1/hdwr1`	Hardware
`admin1/system1`	Ziel des verwalteten Systems

Tabelle 63. SMCLP-Ziele (fortgesetzt)

Ziel	Definitionen
admin1/system1/capabilities1	SMASH-Erfassungsfunktionen des verwalteten Systems
admin1/system1/capabilities1/elecap1	Zielfunktionen des verwalteten Systems
admin1/system1/logs1	Datensatzprotokoll-Erfassungsziel
admin1/system1/logs1/log1	Systemereignisprotokoll (SEL) Datensatzeintrag
admin1/system1/logs1/log1/record*	Eine einzelne SEL-Datensatzinstanz auf dem verwalteten System
admin1/system1/settings1	SMASH-Erfassungseinstellungen des verwalteten Systems
admin1/system1/capacities1	SMASH-Erfassung der verwalteten Systemkapazitäten
admin1/system1/consoles1	SMASH-Erfassung der verwalteten Systemkonsolen
admin1/system1/sp1	Serviceprozessor
admin1/system1/sp1/timesvc1	Zeitansage des Serviceprozessors
admin1/system1/sp1/capabilities1	SMASH-Erfassung der Serviceprozessorfunktionen
admin1/system1/sp1/capabilities1/clpcap1	CLP-Dienstfunktionen
admin1/system1/sp1/capabilities1/pwrmgtcap1	Dienstfunktionen der Stromzustandsverwaltung auf dem System
admin1/system1/sp1/capabilities1/acctmgtcap*	Dienstfunktionen der Kontoverwaltung
admin1/system1/sp1/capabilities1/rolemgtcap*	Lokale rollenbasierte Verwaltungsfunktionen
admin1/system1/sp1/capabilities1/elecap1	Authentifizierungsfunktionen
admin1/system1/sp1/settings1	Sammlung von Serviceprozessoreinstellungen
admin1/system1/sp1/settings1/clpsetting1	CLP-Dienst-Einstellungsdaten
admin1/system1/sp1/clpsvc1	CLP-Dienst-Protokolldienst

Tabelle 63. SMCLP-Ziele (fortgesetzt)

Ziel	Definitionen
admin1/system1/sp1/clpsvc1/clpendpt*	CLP-Dienst-Protokollendpunkt
admin1/system1/sp1/clpsvc1/tcpendpt*	CLP-Dienst-Protokoll-TCP-Endpunkt
admin1/system1/sp1/jobq1	Auftragswarteschlange des CLP-Dienst-Protokolls
admin1/system1/sp1/jobq1/job*	CLP-Dienst-Protokollaufgabe
admin1/system1/sp1/pwrmgtsvc1	Stromzustandsverwaltungsdienst
admin1/system1/sp1/account1-16	Lokales Benutzerkonto
admin1/sysetm1/sp1/account1-16/identity1	Identitätskonto des lokalen Benutzers
admin1/sysetm1/sp1/account1-16/identity2	IPMI-Identitätskonto (LAN)
admin1/sysetm1/sp1/account1-16/identity3	IPMI-Identitätskonto (seriell)
admin1/sysetm1/sp1/account1-16/identity4	CLP-Identitätskonto
admin1/system1/sp1/acctsvc2	IPMI-Kontoverwaltungsdienst
admin1/system1/sp1/acctsvc3	CLP-Kontoverwaltungsdienst
admin1/system1/sp1/rolesvc1	Lokaler rollenbasierter Authentifizierungsdienst (RBA)
admin1/system1/sp1/rolesvc1/Role1-16	Lokale Rolle
admin1/system1/sp1/rolesvc1/Role1-16/ privilege1	Lokale Rollenberechtigung
admin1/system1/sp1/rolesvc2	IPMI-RBA-Dienst
admin1/system1/sp1/rolesvc2/Role1-3	IPMI-Rolle
admin1/system1/sp1/rolesvc2/Role4	IPMI Seriell-über-LAN-Rolle (SOL)
admin1/system1/sp1/rolesvc3	CLP-RBA-Dienst

Tabelle 63. SMCLP-Ziele (fortgesetzt)

Ziel	Definitionen
`admin1/system1/sp1/rolesvc3/Role1-3`	CLP-Rolle
`admin1/system1/sp1/rolesvc3/Role1-3/privilege1`	CLP-Rollenberechtigung

MAP-Adressbereich navigieren

Objekte, die mit SM-CLP verwaltet werden können, werden durch Ziele repräsentiert, die in einem hierarchischen Bereich namens Manageability Access Point(MAP)-Adressbereich angeordnet sind. Ein Adresspfad legt den Pfad vom Adressbereichsstamm zu einem Objekt im Adressbereich fest.

Das Stammziel wird durch einen Schrägstrich (/) oder einen umgekehrten Schrägstrich (\) dargestellt. Es ist der standardmäßige Ausgangspunkt, wenn Sie sich beim iDRAC anmelden. Navigieren Sie vom Stamm abwärts, indem Sie das Verb`cd` verwenden.

ANMERKUNG: Der Schrägstrich (/) und der umgekehrte Schrägstrich (\) sind in SM-CLP-Adresspfaden austauschbar. Mit einem umgekehrten Schrägstrich am Ende einer Befehlszeile wird jedoch der Befehl in der nächsten Zeile fortgesetzt und der Schrägstrich wird ignoriert, wenn der Befehl geparst wird.

Wenn Sie z. B. zum dritten Eintrag des Systemereignisprotokolls (SEL) wechseln möchten, geben Sie den folgenden Befehl ein:

```
->cd /admin1/system1/logs1/log1/record3
```

Geben Sie das Verb `cd` ohne Ziel ein, um Ihre aktuelle Position im Adressbereich zu ermitteln. Die Abkürzungen `..` und `.` funktionieren wie in Windows und Linux: `..` bezieht sich auf die übergeordnete Ebene und `.` auf die aktuelle Ebene.

Verb „show“ verwenden

Verwenden Sie zum Anzeigen weiterer Informationen zu einem Ziel das Verb `show`. Durch dieses Verb werden die Eigenschaften der Ziele, die Unterziele, die Verknüpfungen und eine Liste der SM-CLP-Verben angezeigt, die an einem bestimmten Standort zulässig sind.

Option -display verwenden

Mit der Option `show -display` können Sie in der Befehlsausgabe die folgenden Elemente einschränken: Eigenschaften, Ziele, Zuordnungen und Verben. Wenn Sie z. B. nur die Eigenschaften und Ziele des aktuellen Orts anzeigen möchten, verwenden Sie den folgenden Befehl:

```
show -display properties,targets
```

Wenn Sie nur bestimmte Eigenschaften aufführen möchten, qualifizieren Sie sie, wie im folgenden Befehl gezeigt wird:

```
show -d properties=(userid,name) /admin1/system1/sp1/account1
```

Wenn Sie nur eine Eigenschaft anzeigen möchten, können Sie die Klammern auslassen.

Option -level verwenden

Die Option `show -level` führt `show` über zusätzliche Ebenen unterhalb des festgelegten Ziels aus. Wenn Sie alle Ziele und Eigenschaften im Adressbereich anzeigen möchten, verwenden Sie die `-l all`-Option.

Option -output verwenden

Die Option `-output` legt eins von vier Formaten für die Ausgabe von SM-CLP-Verben fest: **text**, **clpcsv**, **keyword** und **clpxml**.

Das Standardformat ist **text**, die am einfachsten lesbare Ausgabe. Das Format **clpcsv** ist ein Format, bei dem Werte durch Kommas getrennt werden. Es eignet sich zum Laden in ein Tabellenkalkulationsprogramm. Das Format **keyword** gibt Informationen als Liste von keyword=value-Paaren (eins pro Zeile) aus. Das Format **clpxml** ist ein XML-Dokument, das ein **response**-XML-Element enthält. Die DMTF hat die Formate **clpcsv** und **clpxml** festgelegt, deren Spezifikationen auf der DMTF-Website unter **dmtf.org** verfügbar sind.

Das folgende Beispiel zeigt, wie der Inhalt des SEL in XML ausgegeben werden kann:

```
show -l all -output format=clpxml /admin1/system1/logs1/log1
```

Anwendungsbeispiele

In diesem Abschnitt werden die Fallbeispiele für SMCLP dargestellt:

- Server-Energieverwaltung auf Seite 343
- SEL-Verwaltung auf Seite 343
- MAP-Zielnavigation auf Seite 344

Server-Energieverwaltung

Die folgenden Beispiele stellen die Verwendung von SMCLP für die Ausführung von Energieverwaltungsaufgaben auf einem Managed System dar.

Geben Sie die folgenden Befehle an der SMCLP-Befehlseingabe ein:

- Ausschalten des Servers:

  ```
  stop /system1
  ```

  Die folgende Meldung wird angezeigt:

  ```
  system1 has been stopped successfully
  ```

- Einschalten des Servers:

  ```
  start /system1
  ```

  Die folgende Meldung wird angezeigt:

  ```
  system1 has been started successfully
  ```

- Neustart des Servers:

  ```
  reset /system1
  ```

  Die folgende Meldung wird angezeigt:

  ```
  system1 has been reset successfully
  ```

SEL-Verwaltung

Die folgenden Beispiele stellen die Verwendung von SMCLP für die Ausführung von SEL-bezogenen Aufgaben auf einem verwalteten System dar. Geben Sie die folgenden Befehle an der SMCLP-Befehlseingabe ein:

- So zeigen Sie das Systemereignisprotokoll (SEL) an:

  ```
  show/system1/logs1/log1
  ```

  Die folgende Ausgabe wird angezeigt:

  ```
  /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
```

- Zum Anzeigen des SEL-Datensatzes:

  ```
  show/system1/logs1/log1
  ```

  Die folgende Ausgabe wird angezeigt:

  ```
  /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-Zielnavigation

Die folgenden Beispiele zeigen, wie das cd-Verb für die Navigation des MAP verwendet werden kann. In allen Beispielen wird angenommen, dass das erste Standardziel „/“ ist.

Geben Sie die folgenden Befehle an der SMCLP-Befehlseingabe ein:

- Anhand des folgenden Befehls navigieren Sie für einen Neustart zum Systemziel:

  cd system1 reset – Das aktuelle Ziel lautet „/“.

- So wechseln Sie zum SEL-Ziel und zeigen die Protokolldatensätze an:

  ```
  cd system1
  cd logs1/log1
  show
  ```

- So zeigen Sie das aktuelle Ziel an:

  Geben Sie `cd .` ein.

- So gehen Sie eine Ebene nach oben:

  Geben Sie `cd ..` ein.

- So schließen Sie die Befehlseingabe:

  ```
  exit
  ```

27

Betriebssysteme bereitstellen

Sie können die folgenden Dienstprogramme verwenden, um Betriebssysteme auf Managed Systemen bereitzustellen:

- Remote-Dateifreigabe
- Konsole

Themen:

- Betriebssystem über eine Remote-Dateifreigabe bereitstellen
- Betriebssystem über virtuelle Datenträger bereitstellen
- Integriertes Betriebssystem auf SD-Karte bereitstellen

Betriebssystem über eine Remote-Dateifreigabe bereitstellen

Bevor Sie das Betriebssystem über eine Remote-Dateifreigabe (RFS, Remote File Share) bereitstellen, müssen Sie Folgendes sicherstellen:

- Die iDRAC-Berechtigungen **Benutzer konfigurieren** und **Zugriff auf virtuelle Datenträger** sind für den Benutzer aktiviert.
- Die Netzwerkfreigabe enthält Treiber und eine startfähige Imagedatei für das Betriebssystem in einem branchenüblichen Standardformat, wie z. B. **.img** oder **.iso**.

  ANMERKUNG: Folgen Sie während der Erstellung der Imagedatei den standardmäßigen, netzwerkbasierten Installationsvorgängen, und markieren Sie das Bereitstellungsimage als schreibgeschütztes Image, um sicherzustellen, dass jedes Zielsystem gestartet werden kann und gemäß dem gleichen Bereitstellungsverfahren ausgeführt wird.

So stellen Sie ein Betriebssystem mithilfe von RFS bereit:

1. Stellen Sie unter Verwendung der Remote-Dateifreigabe (RFS) die ISO- oder IMG-Imagedatei über NFS, CIFS, HTTP oder HTTPs im verwalteten System bereit.

   ANMERKUNG: RFS über HTTP-, Standard- oder Digest-Authentifizierung wird nicht unterstützt. Es ist keine Authentifizierung erforderlich. Für HTTPS wird die Standardauthentifizierung nicht unterstützt. Es wird nur Digest-Authentifizierung oder keine Authentifizierung unterstützt.

2. Gehen Sie zu **Konfiguration** > **Systemeinstellungen** > **Hardwareeinstellungen** > **Erstes Startgerät**.
3. Legen Sie die Startreihenfolge in der Drop-Down-Liste **Erstes Startgerät** fest, um einen virtuellen Datenträger wie z. B. Floppy, CD, DVD oder ISO auszuwählen.
4. Wählen Sie die Option **Einmalstart** aus, um das Managed System für den Neustart über die Imagedatei nur für die nächste Instanz zu aktivieren.
5. Klicken Sie auf **Anwenden**.
6. Starten Sie das Managed System neu, und folgen Sie den Anweisungen auf dem Bildschirm, um die Bereitstellung abzuschließen.

Managing remote file shares

Using Remote File Share (RFS) feature, you can set an ISO or IMG image file on a network share and make it available to the managed server's operating system as a virtual drive by mounting it as a CD or DVD using NFS, CIFS, HTTP or HTTPs. RFS is a licensed feature.

Remote file share supports only **.img** and **.iso** image file formats. A **.img** file is redirected as a virtual floppy and a **.iso** file is redirected as a virtual CDROM.

You must have Virtual Media privileges to perform an RFS mounting.

RFS and Virtual Media features are mutually exclusive.

- If the Virtual Media client is not active, and you attempt to establish an RFS connection, the connection is established and the remote image is available to the host operating system.

- If the Virtual Media client is active, and you attempt to establish an RFS connection, the following error message is displayed:

  Virtual Media is detached or redirected for the selected virtual drive.

The connection status for RFS is available in iDRAC log. Once connected, an RFS-mounted virtual drive does not disconnect even if you log out from iDRAC. The RFS connection is closed if iDRAC is reset or the network connection is dropped. The Web interface and command-line options are also available in CMCOME Modular and iDRAC to close the RFS connection. The RFS connection from CMC always overrides an existing RFS mount in iDRAC.

NOTE:

- CIFS and NFS supports both IPv4 and IPv6 addresses.
- When the iDRAC is configured with both IPv4 and IPv6, the DNS server can contain records associating the iDRAC hostname to both addresses. If IPv4 option is disabled in iDRAC, then iDRAC may not be able to access the external IPv6 share. This is because the DNS server may still contain IPv4 records, and DNS name resolution can return the IPv4 address. In such cases, it is recommended to delete the IPv4 DNS records from the DNS server, when disabling IPv4 option in iDRAC.
- If you are using CIFS and are part of an Active Directory domain, enter the domain name with the IP address in the image file path.
- If you want to access a file from an NFS share, configure the following share permissions. These permissions are required because iDRAC interfaces run in non-root mode.
  - Linux: Ensure that the share permissions are set to at least **Read** for the **Others** account.
  - Windows: Go to the **Security** tab of the share properties and add **Everyone** to **Groups or user names** field with **Read & execute** privilege.
- If ESXi is running on the managed system and if you mount a floppy image (**.img**) using RFS, the connected floppy image is not available to the ESXi operating system.
- iDRAC vFlash feature and RFS are not related.
- Only English ASCII characters are supported in network share file paths.
- The OS drive eject feature is not supported when virtual media is connected using RFS.
- RFS through HTTP or HTTPs feature is not available on CMC web interface.
- RFS may get disconnected when iDRAC IP is not reachable for more than 1 minute.

Remote-Dateifreigabe über die Web-Schnittstelle konfigurieren

So aktivieren Sie die Remote-Dateifreigabe:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Virtuelle Medien** > **Verbundener Datenträger**. Daraufhin wird die Seite **Verbundener Datenträger** angezeigt.
2. Wählen Sie unter **Verbundener Datenträger** die Option **Verbinden** oder **Automatisch Verbinden**aus.
3. Geben Sie unter **Remote File Share** (Remote-Dateifreigabe) den Abbilddateipfad, den Domänennamen, Benutzernamen und Kennwort an. Weitere Informationen zu den Feldern finden Sie in der *iDRAC Online-Hilfe*.

   Beispiel für einen Dateipfad:
   - 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>`

   ANMERKUNG: Zur Vermeidung von E/A-Fehlern bei CIFS-Freigaben auf Windows 7-Systemen, ändern Sie die folgenden Registrierungsschlüssel:
   - Legen Sie HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache auf `1` fest.
   - Legen Sie HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\Size auf `3` fset.

   ANMERKUNG: Für den Dateipfad kann sowohl das Zeichen '/' als auch '\' verwendet werden.

   CIFS unterstützt IPv4- und IPv6-Adressen, NFS jedoch nur IPv4-Adressen.

   Bei einer NFS-Freigabe muss der genaue <Dateipfad> und <Imagename> eingegeben werden, da zwischen Groß- und Kleinschreibung unterschieden wird.

ANMERKUNG: Informationen zu empfohlenen Zeichen für Benutzernamen und Kennwörter finden Sie unter Empfohlene Zeichen in Benutzernamen und Kennwörtern auf Seite 152.

ANMERKUNG: Die zulässigen Zeichen in Benutzernamen und Kennwörter für Netzwerkfreigaben ergeben sich aus der Netzwerkfreigabe. iDRAC unterstützt zulässige Zeichen in Anmeldeinformationen für die Netzwerkfreigabe dem Freigabetyp, außer < ,> und , (Komma).

4. Klicken Sie auf **Anwenden** und dann auf **Verbinden**.

   Nachdem die Verbindung eingerichtet wird, wird der **Verbindungsstatus** als **Verbunden** angezeigt.

   ANMERKUNG: Auch wenn Sie die Remote-Dateifreigabe konfiguriert haben, zeigt die Webschnittstelle die Benutzeranmeldedaten aus Sicherheitsgründen nicht an.

   ANMERKUNG: Wenn der Image-Pfad Benutzeranmeldeinformationen enthält, verwenden Sie HTTPS, um die Anzeige der Anmeldedaten in der GUI und RACADM zu vermeiden. Wenn Sie die Anmeldedaten in die URL eingeben, vermeiden Sie die Verwendung des Symbols „@“, da es sich um ein Trennzeichen handelt.

   Bei Linux-Distributionen kann diese Funktion einen Befehl zum manuellen Bereitstellen erfordern, wenn es mit runlevel init 3 betrieben wird. Die Syntax für den Befehl lautet:

   ```
   mount /dev/OS_specific_device / user_defined_mount_point
   ```

   Wobei `user_defined_mount_point` jedes Verzeichnis ist, das Sie für das Bereitstellen auswählen, ähnlich wie für jeden Bereitstellen-Befehl.

   Für RHEL ist das CD-Gerät (virtuelles Gerät **.iso**) `/dev/scd0` und das Floppy-Gerät (virtuelles Gerät **.img**) `/dev/sdc`.

   Für SLES ist das CD-Gerät `/dev/sr0` und das Floppy-Gerät /dev/sdc. Um beim Anschluss des virtuellen Gerätes die Verwendung des richtigen Gerätes sicherzustellen (jeweils SLES oder RHEL), müssen Sie auf dem Linux-Betriebssystem sofort folgenden Befehl ausführen:

   ```
   tail /var/log/messages | grep SCSI
   ```

   Hierbei wird der Text angezeigt, der das Gerät identifiziert (z. B. SCSI-Gerät sdc). Dieses Verfahren gilt auch für virtuelle Datenträger, wenn Sie Linux-Distributionen mit runlevel init 3 betrieben werden. Standardmäßig werden die virtuellen Datenträger nicht automatisch in init 3 bereitgestellt.

Remote-Dateifreigabe über RACADM konfigurieren

Verwenden Sie die folgenden Befehle, um die Remote-Dateifreigabe über RACADM zu konfigurieren:

`racadm remoteimage`

`racadm remoteimage <options>`

Die Optionen sind:

`-c` : Verbindung zum Abbild herstellen

`-d` : Verbindung zum Abbild trennen

`-u` <Benutzername>: Benutzername zum Zugriff auf die Netzwerkfreigabe

`-p` <Kennwort>: Kennwort zum Zugriff auf die Netzwerkfreigabe

`-l` <image_location>: Abbildspeicherort auf der Netzwerkfreigabe; verwenden Sie doppelte Anführungszeichen um den Speicherort. Beispiele für Abbilddateipfade finden Sie im Abschnitt „Remote-Dateifreigabe über die Web-Schnittstelle konfigurieren“.

`-s`: Aktuellen Status anzeigen

ANMERKUNG: Alle Zeichen einschließlich alphanumerischer Zeichen und Sonderzeichen sind als Teil des Benutzernamens, des Kennworts und des Imagespeicherorts zulässig, mit Ausnahme der folgenden Zeichen: ' (Apostroph), " (Anführungszeichen), , (Komma), < (kleiner als) und > (größer als).

ANMERKUNG: Zur Vermeidung von E/A-Fehlern bei CIFS-Freigaben auf Windows 7-Systemen, ändern Sie die folgenden Registrierungsschlüssel:

- Legen Sie HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache auf `1` fest.

- Legen Sie HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\Size auf 3 fset.

Betriebssystem über virtuelle Datenträger bereitstellen

Bevor Sie das Betriebssystem über einen virtuellen Datenträger bereitstellen können, müssen Sie Folgendes sicherstellen:

- Der virtuelle Datenträger befindet sich im Status *Verbunden*, damit die virtuellen Laufwerke in der Startsequenz angezeigt werden.
- Wenn sich ein virtueller Datenträger im Modus *Automatisch verbunden* befindet, müssen Sie zunächst die Anwendung für den virtuellen Datenträger starten, bevor das System gestartet wird.
- Die Netzwerkfreigabe enthält Treiber und eine startfähige Imagedatei für das Betriebssystem in einem branchenüblichen Standardformat, wie z. B. **.img** oder **.iso**.

So stellen Sie ein Betriebssystem über den virtuellen Datenträger bereit:

1. Do one of the following: (Die zweite SD-Karte ist nicht vorhanden, reagiert nicht oder ist schreibgeschützt. Führen Sie einen der folgenden Schritte aus:)
   - Legen Sie eine Betriebssystem-Installations-CD- oder DVD in das CD- oder DVD-Laufwerk der Management Station ein.
   - Verbinden Sie das Betriebssystem-Image.
2. Wählen Sie das Laufwerk auf der Management Station mit dem Image aus, mit dem eine Verknüpfung hergestellt werden soll.
3. Verwenden Sie eines der folgenden Verfahren, um das benötigte Gerät zu starten:
   - Legen Sie die Startreihenfolge so fest, dass über die iDRAC-Web-Schnittstelle einmal vom **virtuellen Floppy**- oder vom **virtuellen CD/DVD/ISO**-Laufwerk aus gestartet wird.
   - Legen Sie die Startreihenfolge über **System Setup (System-Setup)** > **System BIOS Settings (System-BIOS-Einstellungen)** fest, indem Sie während des Startvorgangs <F2> drücken.
4. Starten Sie das Managed System neu, und folgen Sie den Anweisungen auf dem Bildschirm, um die Bereitstellung abzuschließen.

Betriebssystem über mehrere Festplatten bereitstellen

1. Lösen Sie die bestehende CD/DVD-Verbindung.
2. Legen Sie die nächste CD/DVD in das optische Remote-Laufwerk ein.
3. Weisen Sie das CD/DVD-Laufwerk neu zu.

Integriertes Betriebssystem auf SD-Karte bereitstellen

So installieren Sie einen eingebetteten Hypervisor auf eine SD-Karte:

1. Setzen Sie zwei SD-Karten in die Steckplätze für das interne Dual-SD-Modul (IDSDM) auf dem System ein.
2. Aktivieren Sie das SD-Modul und die Redundanz (falls erforderlich) im BIOS.
3. Überprüfen Sie, ob die SD-Karte auf einem der Laufwerke verfügbar ist, indem Sie während des Startvorgangs auf die Taste <F11> drücken.
4. Stellen Sie das eingebettete Betriebssystem bereit, und folgen Sie den Anweisungen zur Installation des Betriebssystems.

SD-Modul und Redundanz im BIOS aktivieren

So aktivieren Sie das SD-Modul und die Redundanz im BIOS:

1. Drücken Sie während des Startvorgangs auf <F2>.
2. Gehen Sie zu **System-Setup** > **System-BIOS-Einstellungen** > **Integrierte Geräte**.
3. Legen Sie **Internal USB Port (Interner USB-Anschluss)** auf **On (Ein)** fest. Bei Einstellung auf **Off (Aus)** ist der IDSDM nicht als Startgerät verfügbar.
4. Wenn Redundanz nicht benötigt wird (einzelne SD-Karte), setzen Sie die **interne SD-Kartenschnittstelle** auf **Ein** und die **interne SD-Kartenredundanz** auf **Deaktiviert**.
5. Wenn Redundanz benötigt wird (zwei SD-Karten), setzen Sie die **interne SD-Kartenschnittstelle** auf **Ein** und die **interne SD-Kartenredundanz** auf **Spiegelung**.
6. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.

7. Klicken Sie zum Speichern der Einstellungen auf **Ja**, und drücken Sie auf <Esc>, um das **System-Setup** zu beenden.

Über IDSDM

IDSDM (Internal Dual SD Module) ist nur auf geeigneten Plattformen verfügbar. IDSDM sorgt für Redundanz auf der Hypervisor-SD-Karte, indem eine weitere SD-Karte verwendet wird, die die Inhalte der ersten SD-Karte spiegelt.

Eine der beiden SD-Karten die Master-Karte sein. Wenn z. B. zwei neue SD-Karten in das IDSDM eingesetzt werden, ist SD1 die aktive (Master-)Karte und SD2 die Standbykarte. Die Daten werden auf den beiden Karten geschrieben, gelesen werden die Daten jedoch von SD1. Wenn SD1 ausfällt oder entfernt wird, wird SD2 automatisch zur aktiven (Master-)Karte.

Sie können über die iDRAC-Webschnittstelle oder über RACADM Status, Funktionszustand und die Verfügbarkeit von IDSDM anzeigen. Der Redundanzstatus der SD-Karte und Fehlerereignisse werden im Systemereignisprotokoll erfasst, auf der Frontblende angezeigt und PET-Warnungen werden generiert, wenn Warnungen aktiviert sind.

28

Fehler auf Managed System über iDRAC beheben

Sie können Fehler auf einem Remote-Managed-System wie folgt analysieren und beheben:

- Diagnosekonsole
- POST-Code
- Videos zur Start- und Absturzerfassung
- Bildschirm zum letzten Absturz
- Systemereignisprotokolle
- Lifecycle-Protokolle
- Status auf der Frontblende
- Problemanzeigen
- Systemzustand

Themen:

- Diagnosekonsole verwenden
- POST-Codes anzeigen
- Viewing boot and crash capture videos
- Protokolle anzeigen
- Bildschirm „Letzter Systemabsturz“ anzeigen
- Anzeigen des Systemstatus
- Anzeigen für Hardwareprobleme
- Systemzustand anzeigen
- Serverstatusbildschirm auf Fehlermeldungen überprüfen
- iDRAC-Neustart
- Auf Standardeinstellungen zurücksetzen (RTD)
- Löschen von System- und Nutzerdaten
- Zurücksetzen des iDRAC auf die Standardeinstellungen

Diagnosekonsole verwenden

iDRAC bietet standardmäßige Netzwerkdiagnosetools, die den Tools auf Microsoft Windows- oder Linux-basierten Systemen ähneln. Über die iDRAC-Webschnittstelle können Sie auf die Netzwerk-Debugging-Tools zugreifen.

So rufen Sie die Diagnosekonsole auf:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Maintenance (Wartung)** > **Diagnostics (Diagnose)**.
   Daraufhin wird die Seite **Diagnostics Console Command** (Diagnosekonsolenbefehl) angezeigt.
2. Geben Sie im Textfeld **Befehl** einen Befehl ein, und klicken Sie auf **Senden**. Weitere Informationen zu den Befehlen finden Sie in der *iDRAC-Online-Hilfe*.
   Die Ergebnisse werden auf der gleichen Seite angezeigt.

iDRAC zurücksetzen und iDRAC auf Standardeinstellungen zurücksetzen

1. Gehen Sie in der iDRAC-Weboberfläche zu **Wartung** > **Diagnose**.
   Es stehen Ihnen folgende Optionen zur Verfügung:

- Klicken Sie auf **iDRAC zurücksetzen**, um den iDRAC zurückzusetzen. Es wird ein normaler Neustart auf dem iDRAC durchgeführt. Nach dem Neustart aktualisieren Sie den Browser, um die Verbindung zum iDRAC neu herzustellen und sich neu anzumelden.
- Klicken Sie auf **iDRAC auf Standardeinstellungen zurücksetzen**, um den iDRAC auf die Standardeinstellungen zurückzusetzen. Nach dem Klicken auf **iDRAC auf Standardeinstellungen zurücksetzen** wird das Fenster **iDRAC auf Werkseinstellungen zurücksetzen** angezeigt. Diese Aktion setzt den iDRAC auf die Werkseinstellungen zurück. Wählen Sie aus den folgenden Optionen aus:
  a. Nutzer- und Netzwerkeinstellungen beibehalten
  b. Alle Einstellungen verwerfen und Nutzer auf Versandwert zurücksetzen (Stamm-/Versandwert)
  c. Verwerfen Sie alle Einstellungen und setzen Sie Nutzernamen und Kennwort zurück.

2. Es wird eine Bestätigungsmeldung angezeigt. Klicken Sie auf **OK**, um fortzufahren.

Planen von Automatischer Remote-Diagnose

Sie können automatische Offlinediagnosen auf einem Server als einmaliges Ereignis remote aufrufen und die Ergebnisse zurückgeben. Falls ein Neustart für die Diagnosen erforderlich ist, können Sie diesen sofort ausführen oder einen späteren Neustart- oder Wartungszyklus planen (ähnlich wie bei Aktualisierungen). Wenn Diagnosen ausgeführt werden, werden die Ergebnisse gesammelt und im internen iDRAC-Speicher gespeichert. Sie können die Ergebnisse dann mit dem racadm-Befehl `diagnostics export` in eine NFS-, CIFS-, HTTP- oder HTTP-Netzwerkfreigabe exportieren. Sie können die Diagnosen auch mit den entsprechenden WSMan-Befehlen ausführen. Weitere Information finden Sie in der WSMan-Dokumentation.

Sie müssen über die iDRAC Express-Lizenz verfügen, um die automatische Remote-Diagnose verwenden zu können.

Sie können die Diagnose entweder sofort ausführen oder auf einen bestimmten Tag und eine Uhrzeit planen, wobei Sie auch die Art der Diagnose und den Neustarttyp festlegen können.

Für den Zeitplan können Sie Folgendes festlegen:

- Startzeit – Ausführen der Diagnose zu einem bestimmten Datum und einer bestimmten Uhrzeit. Wenn Sie TIME NOW (SOFORT) angeben, wird die Diagnose beim nächsten Neustart ausgeführt.
- Endzeit – Ausführen der Diagnose bis zu einem bestimmten Datum und einer bestimmten Uhrzeit nach der Startzeit. Wenn sie bis zur Endzeit nicht gestartet wurde, wird sie als „Failed with end time expired“ (Fehlgeschlagen aufgrund überschrittener Endzeit) markiert. Wenn Sie TIME NA (NZ) angeben, ist keine Wartezeit vorhanden.

Die verfügbaren Diagnosetypen sind:

- Schnelltest
- Erweiterter Test
- Beide in einer bestimmten Reihenfolge

Die verfügbaren Neustarttypen sind:

- Schalten Sie das System aus und wieder ein.
- Ordentliches Herunterfahren (Warten, bis das Betriebssystem herunterfährt, bevor der Neustart des Systems beginnt)
- Erzwungenes ordentliches Herunterfahren (Signalisiert dem Betriebssystem, dass es herunterfahren soll, und wartet 10 Minuten. Wenn das Betriebssystem nicht heruntergefahren wird, schaltet der iDRAC das System aus und wieder ein.)

Es kann jeweils nur eine Diagnose geplant oder ausgeführt werden. Eine Diagnose kann erfolgreich, mit Fehlern oder nicht erfolgreich abgeschlossen werden. Die Diagnose-Ereignisse, einschließlich der Ergebnisse, werden im Lifecycle Controller-Protokoll aufgezeichnet. Sie können die Ergebnisse der letzten Ausführung der Diagnose mithilfe von Remote-RACADM oder- WSMan abrufen.

Sie können die Diagnoseergebnisse der letzten abgeschlossenen Diagnosen, die remote geplant wurden, in eine Netzwerkfreigabe wie CIFS, NFS, HTTP oder HTTPS exportieren. Die maximal zulässige Dateigröße ist 5 MB.

Sie können eine Diagnose abbrechen, wenn der Job-Status „Unscheduled (Nicht geplant)“ oder „Scheduled (Geplant)“ lautet. Wenn die Diagnose ausgeführt wird, können Sie das System neu starten, um den Job abzubrechen.

Stellen Sie vor dem Ausführen des Remote-Diagnose Folgendes sicher:

- Lifecycle Controller ist aktiviert.
- Sie verfügen über Anmelde- und Serversteuerungsberechtigungen.

Planen von Automatischer Remote-Diagnose unter Verwendung von RACADM

- Verwenden Sie zum Ausführen der Remote-Diagnose und zum Speichern der Ergebnisse auf dem lokalen System den folgenden Befehl:

```
racadm diagnostics run -m <Mode> -r <reboot type> -s <Start Time> -e <Expiration Time>
```

- Verwenden Sie zum Exportieren der Ergebnisse der zuletzt ausgeführten Remote-Diagnose den folgenden Befehl:

```
racadm diagnostics export -f <file name> -l <NFS / CIFS / HTTP / HTTPs share> -u
<username> -p <password>
```

Weitere Informationen zu den Optionen finden Sie unter *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

POST-Codes anzeigen

POST-Codes zeigen den Fortschritt des System-BIOS an, kennzeichnen verschiedene Phasen der Startsequenz von Power-on-Reset und ermöglichen, Fehler bezüglich des Systemstarts zu diagnostizieren. Die Seite **Post Codes (POST-Codes)** zeigt den letzten POST-Code des Systems vor dem Start des Betriebssystems an.

Gehen Sie zu **Maintenance (Wartung)** > **Troubleshooting (Fehlerbehebung)** > **Post Code (POST-Code)**, um POST-Codes anzuzeigen.

Die Seite **POST-Code** blendet die Systemzustandsanzeige, einen Hexadezimalcode sowie eine Beschreibung des Codes ein.

Viewing boot and crash capture videos

You can view the video recordings of:

- Last three boot cycles — A boot cycle video logs the sequence of events for a boot cycle. The boot cycle videos are arranged in the order of latest to oldest.
- Last crash video — A crash video logs the sequence of events leading to the failure.

This is a licensed feature.

iDRAC records fifty frames during boot time. Playback of the boot screens occur at a rate of 1 frame per second. If iDRAC is reset, the boot capture video is not available as it is stored in RAM and is deleted.

NOTE:

- You must have Access Virtual Console or administrator privileges to playback the Boot Capture and Crash Capture videos.
- The video capture time displayed in the iDRAC GUI video player may differ from the video capture time displayed in other video players. The iDRAC GUI video player displays the time in the iDRAC time zone while all other video players display the time in the respective operating system time zones.

NOTE:

- The reason for the delay in boot capture file availability is because the boot capture buffer is not full after the host boot.
- Default /inbox SLES/RHEL video players do not support the MPEG-1 video decoder. You need to install a MPEG decoder supported video player and play the files.
- MPEG-1 format videos are not supported in MAC OS native player.

To view the **Boot Capture** screen, click **Maintenance** > **Troubleshooting** > **Video Capture**.

The **Video Capture** screen displays the video recordings. For more information, see the *iDRAC Online Help*.

NOTE: When embedded video controller is disabled and server has add-on video controller, then certain latency is expected with respect to boot capture. Hence, End of Post Messages of a video will be recorded in next capture.

Konfigurieren der Videoerfassungs-Einstellungen

So konfigurieren Sie die Videoerfassungs-Einstellungen:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Maintenance (Wartung)** > **Troubleshooting (Problembehebung)** > **Video Capture (Videoerfassung)**.
   Die Seite **Videoerfassung** wird angezeigt.
2. Wählen Sie aus dem Drop-Down-Menü **Videoerfassungs-Einstellungen** eine der folgenden Optionen:
   - **Deaktivieren** – Die Starterfassung ist deaktiviert.
   - **Erfassen, bis Puffer voll** – Die Startreihenfolge wird erfasst, bis die Größe des Pufferspeichers erreicht wird.
   - **Erfassen bis zum Ende des POST** – Die Startreihenfolge wird erfasst, bis das Ende des POST-Vorgangs erreicht wird.
3. Klicken Sie auf **Anwenden**, um die Einstellungen zu übernehmen.

Protokolle anzeigen

Sie können Systemereignisprotokolle (SELs) und Lifecycle-Protokolle anzeigen. Weitere Informationen finden Sie unter Systemereignisprotokoll anzeigen und Lifecycle-Protokoll anzeigen.

Bildschirm „Letzter Systemabsturz“ anzeigen

Die Funktion „Bildschirm Letzter Absturz“ erfasst einen Screenshot des letzten Systemabsturzes, speichert diesen und zeigt ihn in iDRAC an. Hierbei handelt es sich um eine lizenzierte Funktion.

So zeigen Sie den Bildschirm „Letzter Absturz“ an:

1. Stellen Sie sicher, dass die Funktion „Bildschirm Letzter Absturz“ aktiviert ist.
2. Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **Server** > **Fehlerbehebung** > **Bildschirm „Letzter Absturz“**.

   Auf der Seite **Bildschirm „Letzter Absturz“** wird der Bildschirm für den letzten Absturz auf dem Managed System angezeigt.

   Klicken Sie auf **Löschen**, um den Bildschirm für den letzten Absturz zu löschen.

   ANMERKUNG: Sobald iDRAC zurückgesetzt wird oder ein Aus- und Einschaltvorgang durchgeführt wird, werden die erfassten Absturzdaten gelöscht.

   ANMERKUNG: Die Auflösung des Bildschirms „Letzter Absturz“ ist unabhängig von der Auflösung des Host-Betriebssystems immer 1024x768.

Anzeigen des Systemstatus

Der Systemstatus fasst den Status der folgenden Komponenten im System zusammen:

- Zusammenfassung
- Batterien
- des Doppelmantels
- CPUs
- Frontblende
- Eingriff
- Speicher
- Netzwerkgerät
- Netzteile
- Spannungen
- Wechselbarer Flash-Datenträger
- Gehäuse-Controller

Sie können den Status des verwalteten Systems anzeigen:

- Bei Rack- und Tower-Servern: Über den Status der LC-Anzeige auf der Frontblende und die System-ID-LED oder über den Status der LE-Anzeige auf der Frontblende und die System-ID-LED.

- Bei Blade-Servern: Nur über die System-ID-LEDs.

Status der LC-Anzeige auf der Frontblende des Systems anzeigen

Um den Status der LCD-Anzeige auf der Frontblende für die jeweiligen Rack- und Tower-Server anzuzeigen, gehen Sie in der iDRAC-Webschnittstelle zu **System** > **Übersicht** > **Frontblende**. Die Seite **Frontblende** wird angezeigt.

Der Abschnitt **Frontblende** zeigt den Live-Feed der Meldungen an, die derzeit auf der LCD-Anzeige auf der Frontblende angezeigt werden. Wenn das System normal ausgeführt wird (gekennzeichnet durch eine stetig blaue Anzeige auf der LCD-Anzeige der Frontblende), sind sowohl **Fehler ausblenden** als auch **Fehler einblenden** ausgegraut.

ANMERKUNG: Sie können die Fehler nur für Rack- und Tower-Server ein- und ausblenden.

Auf Grundlage der Auswahl erscheint im Textfeld der gegenwärtige Wert. Wenn Sie Benutzerdefiniert auswählen, geben Sie die erforderliche Nachricht in das Textfeld ein. Es können maximal 62 Zeichen eingegeben werden. Wenn Sie Keine auswählen, wird die Nachricht auf der Startseite nicht auf der LCD-Anzeige angezeigt.

Verwenden Sie zum Anzeigen des Status der LCD-Frontblende mit RACADM die Objekte in der Gruppe `System.LCD`. Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Status der LE-Anzeige auf der Frontblende des Systems anzeigen

Um den Status der aktuellen System-ID-LED anzuzeigen, gehen Sie in der iDRAC-Webschnittstelle zu **System** > **Übersicht** > **Frontblende**. Der Abschnitt **Frontblende** zeigt den aktuellen Status der Anzeige auf der Frontblende an:

- Dauerhaft blau – Auf dem Managed System liegen keine Probleme vor.
- Blau blinkend – Der Identifizierungsmodus ist aktiviert (unabhängig davon, ob ein Fehler auf dem Managed System vorhanden ist).
- Dauerhaft gelb – Das Managed System befindet sich im Failsafe-Modus.
- Gelb blinkend – Auf dem Managed System sind Fehler vorhanden.

Wenn das System normal ausgeführt wird (erkennbar am blauen Statussymbol auf der LED-Anzeige der Frontblende), werden die Optionen **Fehler ausblenden** und **Fehler einblenden** ausgegraut dargestellt. Sie können die Fehler nur für Rack- und Tower-Server ein- und ausblenden.

Um den Status der System-ID-LED unter Verwendung von RACADM anzuzeigen, verwenden Sie den Befehl `getled`.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

Anzeigen für Hardwareprobleme

Die Hardware-bezogenen Probleme lauten:

- Gerät kann nicht hochgefahren werden
- Laute Lüfter
- Verlust der Netzwerkkonnektivität
- Festplattenfehler
- Fehler des USB-Datenträgers
- Physischer Schaden

Verwenden Sie auf der Basis des Problems die folgenden Verfahren, um das Problem zu beheben:

- Setzen Sie das Modul oder die Komponente neu ein, und starten Sie das System neu.
- Setzen Sie bei einem Blade-Server das Modul in einen anderen Schacht des Gehäuses ein.
- Tauschen Sie die Festplatten oder die USB-Flash-Laufwerke aus.
- Schließen Sie die Strom- und Netzwerkkabel erneut an, oder tauschen Sie sie aus

Sollte das Problem fortbestehen, finden Sie weitere Informationen zum Beheben von spezifischen Fehlern auf dem Hardware-Gerät unter *Installations- und Service-Handbuch* verfügbar unter https://www.dell.com/poweredgemanuals.

VORSICHT: Maßnahmen zur Fehlerbehebung oder einfache Reparaturen sollten Sie nur dann selbst durchführen, wenn dies laut Produktdokumentation genehmigt ist, oder wenn Sie vom Team des Online- oder Telefonsupports dazu aufgefordert werden. Schäden durch nicht von Dell genehmigte Wartungsarbeiten werden durch die Garantie nicht abgedeckt. Lesen und beachten Sie die Sicherheitshinweise, die Sie zusammen mit Ihrem Produkt erhalten haben.

Systemzustand anzeigen

Sie können den Status für die folgenden Komponenten auf den iDRAC-, CMC- und OME-Modular-Webschnittstellen anzeigen:

- Batterien
- CPUs
- Kühlung
- Eingriff
- Speicher
- Netzteile
- Wechselbarer Flash-Datenträger
- Spannungen
- Verschiedenes

Klicken Sie einen beliebigen Komponentennamen im Abschnitt **Server-Zustand**, um die Details zu den jeweiligen Komponenten anzuzeigen.

Serverstatusbildschirm auf Fehlermeldungen überprüfen

Wenn eine LED gelb blinkt und ein bestimmter Server einen Fehler aufweist, zeigt der Serverstatushauptbildschirm auf der LCD-Anzeige den betroffenen Server in Orange an. Verwenden Sie die LCD-Navigationstasten, um den betroffenen Server zu kennzeichnen, und klicken Sie dann auf die mittlere Taste. Fehler- und Warnmeldungen werden jetzt in der zweiten Zeile angezeigt. Im Server-Benutzerhandbuch finden Sie eine Liste der auf der LC-Anzeige angezeigten Fehlermeldungen.

iDRAC-Neustart

Sie können einen harten oder weichen iDRAC-Neustart ausführen, ohne den Server auszuschalten:

- Harter Neustart – Halten Sie auf dem Server die LED-Schaltfläche für 15 Sekunden gedrückt.
- Weicher Neustart – Über die iDRAC-Webschnittstelle oder RACADM.

Auf Standardeinstellungen zurücksetzen (RTD)

Sie können die Funktion „Auf benutzerdefinierte Standardeinstellungen zurücksetzen“ verwenden, um eine benutzerdefinierte Konfigurationsdatei und RTD in die Einstellungen hochzuladen. Die neuen Einstellungen werden unter Beibehaltung der Nutzer- und Netzwerkeinstellungen angewendet.

Die Funktion „Zurücksetzen auf benutzerdefinierte Standardeinstellungen“ hat folgende Optionen:

- Benutzerdefinierte Standardeinstellungen hochladen:
  - Sie können eine Datei für benutzerdefinierte Standardeinstellungen hochladen. Diese Datei kann abgerufen werden, indem das Server-Konfigurationsprofil (SCP) im XML-Format exportiert wird (das JSON-Format wird für diese Funktion nicht unterstützt). Der Inhalt der Datei kann vom Kunden geändert werden, um Einstellungen hinzuzufügen oder zu löschen.
  - Sie können die SCP-XML-Datei über die iDRAC-GUI oder die RACADM-Schnittstellen hochladen.
  - Die hochgeladenen Konfigurationen werden in der Standarddatenbank gespeichert.
- Aktuelle Einstellungen als benutzerdefinierte Standardeinstellungen speichern:
  - Dieser Vorgang speichert die aktuellen Einstellungen als Standardeinstellungen.
  - Dies wird nur über die RACADM-Schnittstelle unterstützt.
- Benutzerdefinierte Standardeinstellungen herunterladen:
  - Sie können die Datei SCP.XML für alle Standardeinstellungen herunterladen.
  - Dies wird nur über die RACADM-Schnittstelle unterstützt.
- Zurücksetzen auf benutzerdefinierte Standardeinstellungen starten:
  - Die hochgeladenen/gespeicherten Standardeinstellungen werden angewendet.

Zurücksetzen des iDRAC über die iDRAC-Webschnittstelle

Führen Sie zum Zurücksetzen von iDRAC einen der folgenden Schritte über die iDRAC-Webschnittstelle aus:

- Datei mit benutzerdefinierten Standardeinstellungen hochladen:
  - Gehen Sie zu **Konfiguration** > **Server-Konfigurationsprofil** > **benutzerdefinierte Standardeinstellungen** > **benutzerdefinierte Standardeinstellungen hochladen**
  - Laden Sie die angepasste Datei *CustomConfigured.xml* aus dem lokalen Freigabepfad hoch.
  - Klicken Sie auf **Anwenden**. Ein neuer Job zum Hochladen der benutzerdefinierten Standardeinstellungen wird erstellt.
- Auf die Standardeinstellungen zurücksetzen:
  - Wenn der Job zum Hochladen der benutzerdefinierten Standardeinstellungen erfolgreich ist, wechseln Sie zu **Wartung** > **Diagnose** und klicken Sie auf **iDRAC auf Werkseinstellungen zurücksetzen**.
  - Wählen Sie **Alle Einstellungen löschen** und anschließend die **Standardkonfiguration** aus.
  - Klicken Sie auf **Weiter**, um die Konfiguration auf benutzerdefinierte Voreinstellungen zurückzusetzen.

Zurücksetzen des iDRAC über RACADM

Verwenden Sie zum Neustarten von iDRAC den Befehl **racreset**. Weitere Informationen finden Sie unter *Chassis Management Controller RACADM CLI – Handbuch* verfügbar unter https://www.dell.com/cmcmanuals.Weitere Informationen finden Sie unter *OME - Modular für PowerEdge MX7000-Gehäuse RACADM CLI – Handbuch* verfügbar unter https://www.dell.com/openmanagemanuals

Zum Zurücksetzen auf Standardbetrieb verwenden Sie die folgenden Befehle:

- Datei mit benutzerdefinierten Standardeinstellungen hochladen: `racadm –r <iDracIP> -u <username> -p <Password> set -f <filename> -t xml --customdefaults`
- Aktuelle Einstellungen als Standardeinstellungen speichern: `racadm –r <iDracIP> -u <username> -p <Password> set --savecustomdefaults`
- Benutzerdefinierte Standardeinstellungen herunterladen: `racadm –r <iDracIP> -u <username> -p <Password> get -f <filename> -t xml --customdefaults`
- Auf die Standardeinstellungen zurücksetzen: `Racadm –r <iDracIP> -u <username> -p <Password> racresetcfg -custom`

Löschen von System- und Nutzerdaten

ANMERKUNG: Löschen von System- und Nutzerdaten wird von iDRAC-GUI nicht unterstützt.

Sie können System-Komponente(n) und die Nutzerdaten für die folgenden Komponenten löschen:

- Zurücksetzen des BIOS auf die Standardeinstellungen
- Integrierte Diagnosefunktionen
- Integriertes BS-Treiberpaket
- Lifecycle-Controller-Daten
- Zurücksetzen des iDRAC auf die Standardeinstellungen
- Überschreiben von Festplattenlaufwerken, die keine Unterstützung für Instant Secure Erase (ISE) bieten
- Controller-Cache zurücksetzen
- vFLASH zurücksetzen
- Löschen von Festplatten, SSDs und NVMes mit Unterstützung von ISE
- Löschen aller Betriebssystemanwendungen

Stellen Sie vor der Durchführung einer Systemlöschung Folgendes sicher:

- Sie verfügen über iDRAC-Serversteuerung-Berechtigungen.
- Lifecycle Controller ist aktiviert.

Die Option „Lifecycle-Controller-Daten“ löscht jeden Inhalt, wie z. B. das LC-Protokoll, die Konfigurations-Datenbank, die Werk-Protokolle wie ab Werk geliefert und die Konrigurations-Informationen aus dem FP-SPI (oder die Verwaltungs-Riser).

ANMERKUNG: Das Lifecycle Controller-Protokoll enthält die Informationen über die Anfrage zur Systemlöschung und alle Informationen, die erzeugt werden, wenn der iDRAC neu startet. Alle vorherigen Informationen werden entfernt.

Sie können einzelne oder mehrere Systemkomponenten mithilfe des **SystemErase**-Befehls löschen:

```
racadm systemErase <BIOS | DIAG | DRVPACK | LCDATA | IDRAC >
```

wobei

- bios – BIOS wird auf die Standardeinstellung zurückgesetzt
- diag – Integrierte Diagnosefunktionen
- drvpack – Integriertes BS-Treiberpaket
- lcdata – Löscht die Lifecycle-Controller-Daten
- idrac – iDRAC wird auf die Standardeinstellung zurückgesetzt
- overwritepd – Überschreiben von Festplattenlaufwerken, die keine Unterstützung für Instant Secure Erase (ISE) bieten
- percnvcache – Controller-Cache wird zurückgesetzt
- vflash – vFlash wird zurückgesetzt
- secureerasepd – Löschen von Festplatten, SSDs und NVMes mit Unterstützung von ISE
- allapps – Löscht alle BS-Anwendungen

ANMERKUNG: Stellen Sie beim Löschen von vFlash sicher, dass alle Partitionen auf der vFlash-Karte getrennt sind, bevor Sie den Vorgang ausführen.

ANMERKUNG: Wenn SEKM auf dem Server aktiviert ist, deaktivieren Sie SEKM mithilfe des Befehls `racadm sekm disable`, bevor Sie diesen Befehl verwenden. Somit kann verhindert werden, dass Storage-Geräte gesperrt werden, die durch iDRAC gesichert sind, wenn SEKM-Einstellungen aus iDRAC gelöscht werden, indem Sie den Befehl ausführen.

Weitere Informationen finden Sie im *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

ANMERKUNG: Der Dell Tech Center-Link wird in der iDRAC-GUI auf Systemen der Marke Dell angezeigt. Wenn Sie Systemdaten mit dem WSMan-Befehl löschen und die Verknüpfung erneut angezeigt werden soll, starten Sie den Host manuell neu und warten Sie, bis CSIOR ausgeführt wird.

ANMERKUNG: Nachdem Sie die Systemlöschung ausgeführt haben, werden die VDs möglicherweise weiterhin angezeigt. Führen Sie CSIOR aus, nachdem die Systemlöschung abgeschlossen ist und der iDRAC neu gestartet wurde.

Zurücksetzen des iDRAC auf die Standardeinstellungen

Sie können iDRAC mithilfe des Dienstprogramms für die iDRAC-Einstellungen oder der iDRAC-Webschnittstelle auf die Werkseinstellungen zurücksetzen.

Zurücksetzen von iDRAC auf die Standardwerkseinstellungen unter Verwendung der iDRAC-Webschnittstelle

So setzen Sie iDRAC mithilfe der iDRAC-Webschnittstelle auf die Standardwerkseinstellungen zurück:

1. Gehen Sie zu **Maintenance (Wartung)** > **Diagnostics (Diagnose)**.
   Daraufhin wird die Seite **Diagnoseprogramm Konsole** angezeigt.
2. Klicken Sie auf **iDRAC auf Standardeinstellungen zurücksetzen**.
   Der Status der Fertigstellung wird in Prozent angezeigt. iDRAC startet neu und wird auf Werkseinstellungen zurückgesetzt. Die iDRAC-IP wird zurückgesetzt und es ist kein Zugriff auf diese möglich. Sie können die IP mithilfe der Frontblende oder des BIOS konfigurieren.

Zurücksetzen von iDRAC auf die Standardwerkseinstellungen unter Verwendung des Dienstprogramms für iDRAC-Einstellungen

So setzen Sie iDRAC über das Dienstprogramm für die iDRAC-Einstellungen auf die werksseitigen Standardeinstellungen zurück:

1. Gehen Sie zu **iDRAC Konfigurationen auf Standard zurücksetzen**.
   Daraufhin wird die Seite **iDRAC-Einstellungen – iDRAC-Konfigurationen auf Standardeinstellungen zurücksetzen** angezeigt.
2. Klicken Sie auf **Yes** (Ja).

Die iDRAC Zurücksetzung startet.

3. Klicken Sie auf **Zurück**, und navigieren Sie erneut zur Seite **iDRAC-Einstellungen – iDRAC-Konfigurationen auf Standardeinstellungen zurücksetzen**, um die Erfolgsmeldung anzuzeigen.

29

Integration von SupportAssist im iDRAC

SupportAssist ermöglicht Ihnen die Erstellung von SupportAssist-Sammlungen und die Nutzung anderer Funktionen von SupportAssist zur Überwachung Ihres Systems und Rechenzentrums. iDRAC bietet einen Anwendungsschnittstelle für die Sammlung von Plattforminformationen, die es Supportservices ermöglicht, Plattform- und Serverprobleme zu beheben. Mit iDRAC können Sie eine SupportAssist-Sammlung des Servers generieren und die Sammlung anschließend an einen Speicherort in einer Management Station (lokal) oder an einen Netzwerkfreigabespeicherort exportieren, zum Beispiel FTP, Trivial File Transfer Protocol (TFTP), HTTP, HTTPS, Common Internet File System (CIFS) oder Network File Share (NFS). Die Erfassung wird im Standard-ZIP-Format erstellt. Sie können diese Erfassung zur Fehlersuche oder Inventarsammlung an den technischen Support senden.

Themen:

- Registrierung von SupportAssist
- Installieren des Servicemoduls
- Server-BS-Proxy-Informationen
- SupportAssist
- Portal für Service-Anforderungen
- Sammlung Melden
- Generating SupportAssist Collection
- Einstellungen
- Einstellungen für Datenerfassung
- Kontaktinformationen

Registrierung von SupportAssist

Um die Vorteile der automatisierten, proaktiven und vorausschauenden Funktionen von SupportAssist nutzen zu können, müssen Sie Ihr System bei SupportAssist registrieren.

Sie können eine Sammlung lokal oder in einem Netzwerk erstellen und speichern und auch ohne Registrierung an Dell EMC senden.

ANMERKUNG: Einige OEM-Kunden haben keinen Modellnamen. SupportAssist im Back-End erlaubt keine Registrierung solcher Systeme bei Dell.

Kontakt- und Versandinformationen

Um die Registrierung abzuschließen, müssen Sie die Kontakt- und Versandinformationen angeben.

Informationen zur primären Kontaktperson

Geben Sie Firmennamen, Land, Vornamen*, Nachnamen*, Telefonnummer*, zusätzliche Telefonnummer und E-Mail-Adresse* ein. Überprüfen Sie, ob die Details korrekt angezeigt werden und nehmen Sie bei Bedarf Änderungen an den Feldern vor.

*kennzeichnet Pflichtfelder.

Informationen zur sekundären Kontaktperson

Geben Sie den Vornamen, Nachnamen, die Telefonnummer, die alternative Telefonnummer sowie die E-Mail-Adresse ein und überprüfen Sie, ob die Angeben richtig angezeigt werden. Nehmen Sie Bei Bedarf Änderungen an den Feldern vor.

ANMERKUNG: Sie können die Angaben zur sekundären Kontaktperson jederzeit entfernen.

Automatischer Versand

Wenn Dell EMC über iDRAC ein kritisches Ereignis gemeldet wird, der bei SupportAssist registriert ist, wird der automatische Versand initialisiert. Dieser Arbeitsablauf basiert auf dem weitergeleiteten Ereignis und der Garantiestufe des bei SupportAssist registrierten Geräts. Sie müssen die **Versandinformationen** während der SupportAssist-Registrierung eingeben, um den automatischen Versand zu aktivieren. Wenn Vor-Ort-Support zusammen mit der Versendung von Ersatzteilen erforderlich ist, wählen Sie **Teileversand mit Vor-Ort-Support** aus.

ANMERKUNG: Der automatische Versand ist in Systemen mit iDRAC-Servicemodul (iSM) v3.4.0 für Windows aktiviert. Zukünftige iSM-Versionen werden den automatischen Versand auch in weiteren Betriebssystemen unterstützen.

Versandadresse

Geben Sie die Adresse und die Zeit ein, zu der Sie am besten erreichbar sind.

Endbenutzer-Lizenzvereinbarung

Nachdem Sie alle erforderlichen Informationen angegeben haben, müssen Sie die Endbenutzer-Lizenzvereinbarung (EULA) akzeptieren, um die Registrierung abzuschließen. Sie haben die Möglichkeit, die EULA für weitere Referenzzwecke auszudrucken. Sie können den Registrierungsvorgang jederzeit abbrechen und beenden.

Installieren des Servicemoduls

Um SupportAssist zu registrieren und zu verwenden, muss iDRAC Service Module (iSM) auf dem System installiert sein. Nach dem **Inititiieren der Service Module-Installation** werden die Installationsanweisungen anzeigt. Die Schaltfläche **Next (Weiter)** bleibt deaktiviert, bis Sie iSM erfolgreich installiert haben.

Server-BS-Proxy-Informationen

Für den Fall, dass ein Problem bei der Verbindung besteht, wird der Benutzer aufgefordert, BS-Proxy-Informationen anzugeben. Geben Sie **Server, Port, Benutzername** und **Kennwort** ein, um die Proxy-Einstellungen zu konfigurieren.

SupportAssist

Nach der Konfiguration von SupportAssist können Sie das SupportAssist Dashboard anzeigen und **Serviceanfrage-Zusammenfassung**, **Garantiestatus**, **SupportAssist-Überblick**, **Serviceanfragen** und das **Erfassungsprotokoll** anzeigen. Eine Registrierung ist nicht erforderlich, um das Erfassungsprotokoll einzusehen oder zu versenden.

Portal für Service-Anforderungen

Serviceanfrage zeigt Details zu **Status** (Offen/Geschlossen), **Beschreibung**, **Quelle** (Ereignis/Telefon), **Serviceanfrage-ID**, **Öffnungsdatum** und **Abschlussdatum** für jedes Ereignis an. Sie können weitere Details für jedes Ereignis auswählen und anzeigen. Sie haben die Option, im Portal für Service-Anforderungen zu einem einzelnen Fall zusätzlichen Informationen anzuzeigen.

Sammlung Melden

Das **Erfassungsprotokoll** zeigt Details zu **Erfassungsdatum und -zeit**, **Erfassungstyp** (Manuell, Geplant, Ereignisbasiert), **Erfassten Daten** (Benutzerdefinierte Auswahl, Alle Daten), **Erfassungsstatus** (Mit Fehlern abgeschlossen, Abgeschlossen), **Job-ID**, **Sendestatus** und **Sendedatum und -zeit** an. Sie können die letzte beständige Sammlung in iDRAC an Dell senden.

ANMERKUNG: Nach der Generierung können die Details des Erfassungsprotokolls gefiltert werden, um die persönlich identifizierbaren Informationen (PII) basierend auf der Benutzerauswahl zu entfernen.

Generating SupportAssist Collection

For generating the OS and Application logs:

- iDRAC Service Module must be installed and running in Host Operating System.
- OS Collector, which comes factory installed in iDRAC, if removed must be installed in iDRAC.

NOTE: SupportAssist Collection takes more than 10 minutes to complete when performed from OS/iDRAC while OMSA 10.1.0.0 is running with it.

If you have to work with Tech Support on an issue with a server but the security policies restrict direct internet connection, then you can provide Tech Support with necessary data to facilitate troubleshooting of the problem without having to install software or download tools from Dell and without having access to the Internet from the server operating system or iDRAC.

You can generate a health report of the server and then export the Collection log:

- To a location on the management station (local).
- To a shared network location such as Common Internet File System (CIFS) or Network File Share (NFS). To export to a network share such as CIFS or NFS, direct network connectivity to the iDRAC shared or dedicated network port is required.
- To Dell EMC.

The SupportAssist Collection is generated in the standard ZIP format. The collection may contain the following information:

- Hardware inventory for all components (includes system component configuration and firmware details, Motherboard System Event Logs, iDRAC state information and Lifecycle Controller logs).
- Operating system and application information.
- Storage Controller logs.
- iDRAC Debug Logs.
- It contains an HTML5 viewer, that can be accessed once the collection is complete.
- The collection provides a massive amount of detailed system information and logs in a user friendly format that can be viewed without uploading the collection to the Tech Support site.

After the data is generated, you can view the data which contains multiple XML files and log files.

Each time the data collection is performed, an event is recorded in the Lifecycle Controller log. The event includes information such as the user who initiated the report, interface used, and the date and time of export.

On Windows, If WMI is disabled, OS Collector collection stops with an error message.

Check the appropriate privilege levels and make sure there is no firewall or security settings that may prevent from collecting the registry or software data.

Before generating the health report, make sure:

- Lifecycle Controller is enabled.
- Collect System Inventory On Reboot (CSIOR) is enabled.
- You have Login and Server Control privileges.

Manuelles Generieren der SupportAssist-Erfassung unter Verwendung der iDRAC-Webschnittstelle

So generieren Sie die SupportAssist-Erfassung manuell:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Maintenance (Wartung)** > **SupportAssist**.
2. Wenn der Server nicht für SupportAssist registriert ist, wird der SupportAssist Registration Wizard (SupportAssist-Registrierungsassistent) angezeigt. Klicken Sie auf **Abbrechen** > **Registrierung abbrechen**.
3. Klicken Sie auf **Start a Collection** (Erfassung starten).
4. Wählen Sie die Datensätze aus, die in die Sammlung aufgenommen werden müssen.
5. Sie können festlegen, die Sammlung nach personenbezogenen Daten (PII) zu filtern.
6. Wählen Sie das Ziel, in der die Erfassung gespeichert werden soll.
   a. Wenn der Server mit dem Internet verbunden ist und die Option **Jetzt senden** aktiviert ist, wird bei Auswahl dieser Option das Sammelprotokoll an Dell EMC SupportAssist gesendet.

b. Mit der Option **Save locally** (Lokal speichern) können Sie die generierte Erfassung auf dem lokalen System speichern.
c. Mit der Option **Save to Network** (Im Netzwerk speichern) wird die generierte Erfassung in einer benutzerdefinierten CIFS- oder NFS-Netzwerkfreigabe gespeichert.

ANMERKUNG: Wenn *Save to Network (Im Netzwerk speichern)* ausgewählt ist und kein standardmäßiger Speicherort verfügbar ist, werden die angegebenen Netzwerkdetails als Standardspeicherort für zukünftige Sammlungen gespeichert. Wenn ein Standardspeicherort bereits vorhanden ist, dann werden für die Sammlung die nur einmal angegebenen Details verwendet.

Wenn die Option **Save to Network** (Im Netzwerk speichern) ausgewählt ist, werden die vom Benutzer bereitgestellten Netzwerkdetails als Standardwerte (falls keine Netzwerkfreigabe zuvor gespeichert wurde) für künftige Erfassungen gespeichert.

7. Klicken Sie auf **Collect** (Erfassen), um mit der Erfassung fortzufahren.
8. Wenn Sie dazu aufgefordert werden, akzeptieren Sie die **End User Agreement (EULA) (Endbenutzer-Lizenzvertrag)**, um fortzufahren.

Die Option für Betriebssystem- und Anwendungsdaten ist ausgegraut und kann nicht ausgewählt werden, wenn Folgendes zutrifft:

- iSM ist nicht installiert oder wird nicht unter dem Host-BS ausgeführt,
- OS Collector wurde von iDRAC entfernt,
- OS-BMC-Passthrough ust auf dem iDRAC deaktiviert oder
- im Cache gespeicherte OS-Anwendungsdaten von einer früheren Erfassung sind nicht in iDRAC verfügbar.

Einstellungen

Auf dieser Seite können Sie die Einstellungen des Sammelprotokolls konfigurieren, und wenn Sie registriert sind, können Sie die Kontaktdaten aktualisieren, E-Mail-Benachrichtigungen aktivieren oder deaktivieren und die Spracheinstellungen ändern.

Einstellungen für Datenerfassung

Sie können die erfassten Daten an einem beliebigen Speicherort im Netzwerk speichern. Verwenden Sie **Set Archive Directory** (Archivverzeichnis festlegen), um den Speicherort im Netzwerk festzulegen. Sie können die erfassten Daten an einem bevorzugten Speicherort im Netzwerk speichern. Verwenden Sie die Option "Set Archive Directory" (Archivverzeichnis festlegen), um den Speicherort im Netzwerk einzustellen. Geben Sie den gewünschten Protokolltyp (CIFS/NFS) sowie die entsprechende IP-Adresse, den Freigabenamen, Domänennamen, Benutzernamen und Kennwort an, bevor Sie die Netzwerkverbindung testen. Mit der Schaltfläche "Test Network Connection" (Netzwerkverbindung testen) wird eine Verbindung zum Zielfreigabeort bestätigt.

Wenn Sie registriert sind, können Sie in den Einstellungen für Datenerfassung die Option wählen, beim Senden der Daten an Dell Identifizierungsinformationen einzuschließen.

Sie können die Optionen für die **automatische Erfassung** aktivieren oder planen, um manuelles Eingreifen zu vermeiden und eine regelmäßige Überprüfung des Systems zu gewährleisten. Standardmäßig ist SupportAssist so konfiguriert, dass bei der Auslösung eines Ereignisses und der Erstellung eines Support-Falls automatisch die Systemprotokolle von dem Gerät, das die Warnung generiert hat, erfasst und an Dell gesendet werden. Sie können die automatische Erfassung basierend auf Ereignissen aktivieren oder deaktivieren Sie können einen Zeitplan für die automatische Erfassung basierend auf entsprechenden Voraussetzungen erstellen. Die verfügbaren Optionen sind: wöchentlich, monatlich, vierteljährlich oder nie. Sie können auch das Datum und die Uhrzeit für die regelmäßig geplanten Ereignisse festlegen. Sie haben die Möglichkeit, die Option **ProSupport Plus Recommendation Report (ProSupport Plus Empfehlungsbericht)** bei der Konfiguration der automatischen Erfassung zu aktivieren oder zu deaktivieren.

Kontaktinformationen

Diese Seite zeigt die Details zu den Kontaktinformationen, die während der Registrierung von SupportAssist hinzugefügt wurden, und ermöglicht Ihnen deren Aktualisierung.

30

Häufig gestellte Fragen

In diesem Abschnitt werden häufig gestellte Fragen zu den folgenden Themen aufgelistet:

- System-Ereignisprotokoll
- Netzwerksicherheit
- Active Directory
- Einfache Anmeldung
- Smart Card-Anmeldung
- Virtuelle Konsole
- Virtueller Datenträger
- vFlash-SD-Karte
- SNMP-Authentifizierung
- Speichergeräte
- iDRAC-Service-Modul
- RACADM
- Verschiedenes

Themen:

- System-Ereignisprotokoll
- Benutzerdefinierte Absender-E-Mail-Konfiguration für iDRAC-Warnmeldungen
- Netzwerksicherheit
- Telemetrie-Streaming
- Active Directory
- Einmaliges Anmelden
- Smart Card-Anmeldung
- Virtuelle Konsole
- Virtueller Datenträger
- vFlash-SD-Karte
- SNMP-Authentifizierung
- Speichergeräte
- GPU (Beschleuniger)
- iDRAC-Service-Modul
- RACADM
- Standardkennwort dauerhaft auf „calvin“ setzen
- Verschiedenes

System-Ereignisprotokoll

Warum verwendet SEL während der Verwendung der iDRAC-Webschnittstelle über den Internet Explorer nicht die Option „Speichern unter“?

Der Grund dafür liegt in einer Browser-Einstellung. So können Sie das Problem lösen:

1. Wechseln Sie im Internet Explorer zu **Tools** > **Internetopionen** > **Sicherheit** und wählen Sie die Zone, in die Sie versuchen herunterzuladen.

   Wenn sich das iDRAC-Gerät z. B. in Ihrem lokalen Intranet befindet, wählen Sie **Lokales Intranet** und klicken Sie auf **Stufe anpassen**....

2. Im Fenster **Sicherheitseinstellungen** müssen unter **Downloads** die folgenden Optionen aktiviert sein:
   - Automatische Eingabeaufforderung für Datei-Downloads (falls diese Option verfügbar ist)
   - Dateien herunterladen

VORSICHT: Um sicherzustellen, dass der Computer, der für den Zugriff auf iDRAC verwendet wird, sicher ist, aktivieren Sie unter Verschiedenes nicht die Option Anwendungen und unsichere Dateien starten.

Benutzerdefinierte Absender-E-Mail-Konfiguration für iDRAC-Warnmeldungen

Die generierte E-Mail-Benachrichtigung ist nicht von der benutzerdefinierten Absender-E-Mail auf dem cloudbasierten E-Mail-Service.

Sie müssen Ihre Cloud-E-Mail über diesen Prozess registrieren: Support.google.com.

Netzwerksicherheit

Während des Zugriffs auf die iDRAC-Webschnittstelle wird eine Sicherheitswarnung angezeigt, aus der hervorgeht, dass das durch die Zertifizierungsstelle ausgestellte SSL-Zertifikat nicht vertrauenswürdig ist.

iDRAC ist mit einem standardmäßigen iDRAC-Serverzertifikat ausgestattet, das die Netzwerksicherheit gewährleistet, während der Zugriff über die Webschnittstelle oder ein Remote-RACADM erfolgt. Dieses Zertifikat wird nicht von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt. Um dieses Problem zu beheben, laden Sie ein iDRAC-Serverzertifikat hoch, das von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde (z. B. Microsoft Zertifizierungsstelle, Thawte oder Verisign).

Warum führt der DNS-Server keine Registrierung von iDRAC durch?

Einige DNS-Server registrieren ausschließlich iDRAC-Namen mit bis zu 31 Zeichen.

Wenn Sie auf die iDRAC-Webschnittstelle zugreifen, wird eine Sicherheitswarnung angezeigt, aus der hervorgeht, dass der SSL-Zertifikat-Hostname nicht mit dem iDRAC-Hostnamen übereinstimmt.

iDRAC ist mit einem standardmäßigen iDRAC-Serverzertifikat ausgestattet, das die Netzwerksicherheit gewährleistet, während der Zugriff über die Webschnittstelle oder ein Remote-RACADM erfolgt. Wenn dieses Zertifikat verwendet wird, zeigt der Webbrowser eine Sicherheitswarnung an, da das für iDRAC ausgestellte Standardzertifikat nicht mit dem iDRAC-Hostnamen übereinstimmt (z. B. mit der IP-Adresse).

Um dieses Problem zu lösen, laden Sie ein iDRAC-Server-Zertifikat hoch, das auf die IP-Adresse oder den iDRAC-Host-Namen ausgestellt wurde. Im Rahmen der Generierung der Zertifikatsignierungsanforderung (für die Ausstellung des Zertifikats) müssen Sie sicherstellen, dass der allgemeine Name (CN) der Zertifikatsignierungsanforderung mit der iDRAC-IP-Adresse (wenn auf die IP-Adresse ausgestellt) oder mit dem registrierten DNS-iDRAC-Namen (wenn auf den registrierten iDRAC-Namen ausgestellt) übereinstimmt.

So stellen Sie sicher, dass die Zertifikatsignierungsanforderung mit dem registrierten DNS-iDRAC-Namen übereinstimmt:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Übersicht** > **iDRAC-Einstellungen** > **Netzwerk**. Die Seite **Netzwerk** wird angezeigt.
2. Im Abschnitt **Allgemeine Einstellungen**:
   - Wählen Sie die Option **iDRAC auf DNS registrieren** aus.
   - Geben Sie den iDRAC-Namen in das Feld **DNS-iDRAC-Name** ein.
3. Klicken Sie auf **Anwenden**.

Warum kann ich von meinem Webbrowser nicht auf iDRAC zugreifen?

Dieses Problem kann auftreten, wenn HTTP Strict Transport Security (HSTS) aktiviert ist. HSTS ist ein Internetsicherheitsmechanismus, der es Webbrowsern ermöglicht, ausschließlich über das sichere HTTPS-Protokoll und nicht über HTTP zu interagieren.

Aktivieren Sie HTTPS auf Ihrem Browser und melden Sie sich bei iDRAC an, um das Problem zu beheben.

Warum kann ich Vorgänge nicht abschließen, die eine Remote-CIFS-Freigabe durchführen?

Importieren/Exportieren oder ein beliebiger anderer Remote-Dateifreigabevorgang, der eine CIFS-Freigabe durchführt, schlägt fehl, wenn sie nur SMBv1 verwenden. Stellen Sie sicher, dass das SMBv2-Protokoll auf dem Server aktiviert ist und die SMB/CIFS-Freigabe bereitstellt. Informationen zum Aktivieren des SMBv2-Protokolls finden Sie in der Betriebssystemdokumentation.

Telemetrie-Streaming

Einige Berichtsdaten fehlen, während die Telemetrie-Berichte für Rsyslog-Server gestreamt werden.

Bei älteren Versionen von Rsyslog-Servern fehlen möglicherweise gelegentlich einige Berichtsdaten in einigen Berichten. Sie können ein Upgrade auf eine neuere Version durchführen, um dieses Problem zu vermeiden.

Active Directory

Active Directory-Anmeldung fehlgeschlagen. Wie kann ich dieses Problem lösen?

Klicken Sie für eine Diagnose des Problems auf der Seite **Active Directory Configuration and Management** (Active Directory-Konfiguration und -Verwaltung) auf **Test Settings** (Einstellungen testen). Überprüfen Sie die Testergebnisse und beheben Sie das Problem. Ändern Sie die Konfiguration und führen Sie den Test solange aus, bis der Testbenutzer den Autorisierungsschritt erfolgreich bestanden hat.

Überprüfen Sie allgemein die folgenden Aspekte:

- Stellen Sie bei der Anmeldung sicher, dass Sie den korrekten Benutzerdomänennamen statt des NetBIOS-Namens verwenden. Wenn Sie über ein lokales iDRAC-Benutzerkonto verfügen, melden Sie sich bei iDRAC mit den lokalen Anmeldeinformationen an. Stellen Sie nach der Anmeldung Folgendes sicher:
  - Die Option **Active Directory aktivieren** ist auf der Seite **Aktive Directory-Konfiguration und -Verwaltung** markiert.
  - Die DNS-Einstellung auf der **iDRAC-Netzwerkkonfigurationsseite** ist korrekt.
  - Sie haben das richtige Stamm-CA-Zertifikat des Active Directory auf den iDRAC hochgeladen, falls Überprüfung des Zertifikats aktiviert wurde.
  - Der iDRAC-Name und der iDRAC-Domänenname stimmen mit der Active Directory-Umgebungskonfiguration überein, wenn Sie das erweiterte Schema verwenden.
  - Der Gruppenname und der Gruppendomänenname stimmen mit der Active Directory-Konfiguration überein, wenn Sie das Standardschema verwenden.
  - Wenn sich der Benutzer und das iDRAC-Objekt in unterschiedlichen Domänen befinden, wählen Sie die Option **User Domain from Login** (Benutzerdomäne von Anmeldung) nicht aus. Wählen Sie stattdessen die Option **Specify a Domain** (Domäne angeben) aus und geben Sie den Namen der Domäne ein, in der sich das iDRAC-Objekt befindet.
- Überprüfen Sie die SSL-Zertifikate des Domänen-Controllers, um sicherzustellen, dass die iDRAC-Zeit innerhalb der Gültigkeitsdauer des Zertifikats liegt.

Die Anmeldung bei Active Directory schlägt selbst dann fehl, wenn die Zertifikatüberprüfung aktiviert ist. In den Testergebnissen wird die folgende Fehlmeldung angezeigt: Warum tritt dieses Problem auf und wie kann es gelöst werden?

```
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.
```

Wenn die Zertifikatüberprüfung aktiviert ist, wenn iDRAC die SSL-Verbindung mit dem Verzeichnisserver aufbaut, verwendet iDRAC das hochgeladene Zertifizierungsstellenzertifikat, um das Zertifikat des Verzeichnisservers zu überprüfen. Die häufigsten Gründe für das Scheitern der Zertifizierung sind:

- Das iDRAC-Datum liegt nicht innerhalb des Gültigkeitszeitraums des Serverzertifikats oder des Zertifizierungsstellenzertifikats. Überprüfen Sie die iDRAC-Zeit und den Gültigkeitszeitraum Ihres Zertifikats.
- Die in iDRAC konfigurierten Domänen-Controller-Adressen stimmen nicht mit dem Servernamen oder dem alternativen Servernamen des Verzeichnisserverzertifikats überein. Falls Sie eine IP-Adresse verwenden, lesen Sie bitte die folgende Frage. Wenn Sie einen FQDN verwenden, stellen Sie bitte sicher, dass Sie den FQDN des Domänen-Controllers verwenden und nicht den der Domäne. Zum Beispiel **servername.beispiel.com**, und nicht **beispiel.com**.

Die Zertifikatüberprüfung schlägt fehl, auch wenn die IP-Adresse als Domänen-Controller-Adresse verwendet wird. Wie kann ich dieses Problem lösen?

Prüfen Sie die Angaben für Servername und alternativer Servername Ihres Domänen-Controller-Zertifikats. Active Directory verwendet in der Regel den Hostnamen, und nicht die IP-Adresse, des Domänen-Controllers als Servernamen oder alternativen Servernamen des Domänen-Controller-Zertifikats. Führen Sie die folgenden Schritte aus, um dieses Problem zu lösen:

- Konfigurieren Sie den Hostnamen (FQDN) des Domänen-Controllers als *Adresse(n) des Domänen-Controllers* auf dem iDRAC, damit er mit dem Servernamen oder alternativen Servernamen des Server-Zertifikats übereinstimmt.
- Erstellen Sie das Server-Zertifikat erneut, damit im Feld "Servername" oder "Alternativer Servername" eine IP-Adresse verwendet wird, die auf dem iDRAC konfiguriert ist.

- Deaktivieren Sie die Überprüfung des Zertifikats, wenn Sie dem Domänen-Controller beim SSL-Handshake ohne diese Überprüfung vertrauen.

Wie werden die Domänen-Controller-Adressen konfiguriert, wenn das erweiterte Schema in einer Umgebung mit mehreren Domänen verwendet wird?

Es musste der Host-Name (FQDN) oder die IP-Adresse des Domänen-Controllers sein, der die Domäne bedient, in der sich das iDRAC-Objekt befindet.

Wann muss ich Adressen des globalen Katalogs konfigurieren?

Wenn Sie das Standardschema verwenden und die Benutzer und Rollengruppen verschiedenen Domänen angehören, sind Adressen des globalen Katalogs erforderlich. In diesem Fall können Sie nur die Universalgruppe verwenden.

Wenn Sie das Standardschema verwenden und alle Benutzer und Rollengruppen derselben Domäne angehören, sind keine Adressen des globalen Katalogs erforderlich.

Wenn Sie ein erweitertes Schema verwenden, wird die Adresse des globalen Katalogs nicht verwendet.

Wie funktioniert die Abfrage im Standardschema?

iDRAC stellt zunächst eine Verbindung mit den konfigurierten Domänen-Controller-Adressen her. Wenn Benutzer und Rollengruppen dieser Domäne angehören, wenden die Berechtigungen gespeichert.

Wenn globale Controller-Adressen konfiguriert sind, fragt iDRAC weiterhin den globalen Katalog ab. Wenn zusätzliche Berechtigungen vom globalen Katalog abgerufen werden, werden diese Berechtigungen kumuliert.

Verwendet iDRAC immer LDAP über SSL?

Ja. Der gesamte Transfer erfolgt über den geschützten Anschluss 636 und/oder 3269. Unter „Test settings“ (Einstellungen testen) führt iDRAC einen LDAP CONNECT durch, um das Problem zu isolieren, er führt jedoch keinen LDAP BIND auf einer unsicheren Verbindung aus.

Warum ist in der Standardkonfiguration des iDRAC die Überprüfung des Zertifikats aktiviert?

iDRAC erzwingt hohe Sicherheit, um die Identität des Domänen-Controllers zu sichern, mit dem iDRAC eine Verbindung herstellt. Ohne die Überprüfung des Zertifikats kann ein Hacker mithilfe eines gefälschten Domänen-Controllers die SSL-Verbindung hacken. Wenn Sie alle Domänen-Controller in Ihrer Sicherheitsbegrenzung ohne Überprüfung des Zertifikats als vertrauenswürdig festlegen, können Sie die Überprüfung über die Webschnittstelle oder RACADM deaktivieren.

Unterstützt iDRAC den NetBIOS-Namen?

Nicht in dieser Version.

Warum dauert es bis zu vier Minuten, sich über die Active Directory-basierte Einmal- oder Smart Card-Anmeldung bei iDRAC anzumelden?

Die Active Directory-basierte Einmal- oder Smart Card-Anmeldung dauert in der Regel weniger als 10 Sekunden, sie kann jedoch bis zu vier Minuten dauern, wenn Sie den bevorzugten DNS-Server und den alternativen DNS-Server angegeben haben und der bevorzugte DNS-Server ausfällt. DNS-Zeitüberschreitungen sind zu erwarten, wenn ein DNS-Server ausgeschaltet ist. iDRAC meldet Sie unter Verwendung des alternativen DNS-Servers an.

Active Directory wird für eine Domäne in Windows Server 2008 Active Directory konfiguriert. Eine untergeordnete Domäne bzw. Unterdomäne ist für die Domäne vorhanden, der Benutzer und die Gruppe gehören derselben untergeordneten Domäne an und der Benutzer ist Mitglied dieser Gruppe. Bei dem Versuch, sich mit dem Benutzer bei iDRAC anzumelden, der derselben untergeordneten Domäne angehört, schlägt das einmalige Anmelden über Active Directory fehl.

Dies kann möglicherweise auf den falschen Gruppentyp zurückzuführen sein. Auf dem Active Directory-Server gibt es zwei Arten von Gruppentypen:

- Sicherheit – Sicherheitsgruppen ermöglichen Ihnen, den Benutzer- und Computerzugriff auf freigegebene Ressourcen zu verwalten und Gruppenrichtlinieneinstellungen zu filtern.
- Verteilung – Verteilungsgruppen sind nur als E-Mail-Verteilerlisten vorgesehen.

Stellen Sie immer sicher, dass der Gruppentyp „Security“ (Sicherheit) lautet. Sie können zum Zuweisen von Berechtigungen für Objekte keine Verteilergruppen verwenden. Verwenden Sie diese jedoch zum Filtern von Gruppenrichtlinieneinstellungen.

Einmaliges Anmelden

Die SSO-Anmeldung schlägt auf Windows Server 2008 R2 x64 fehl. Welche Einstellungen sind zum Lösen dieses Problems erforderlich?

1. Führen Sie **http://technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** für den Domänen-Controller und die Domänenregel aus.

2. Konfigurieren Sie die Computer zur Verwendung der DES-CBC-MD5-Cipher-Suite.

   Diese Einstellungen haben möglicherweise Auswirkungen auf die Kompatibilität mit Client-Computern oder -Diensten und -Anwendungen in Ihrer Umgebung. Die für die Kerberos-Richtlinieneinstellung zulässigen konfigurierbaren Verschlüsselungstypen sind unter **Computer Configuration (Computerkonfiguration)** > **Security Settings (Sicherheitseinstellungen)** > **Local Policies (Lokale Richtlinien)** > **Security Optionen (Sicherheitsoptionen)** verfügbar.

3. Stellen Sie sicher, dass die Domänen-Clients über das aktualiserte GPO verfügen.
4. Geben Sie in der Befehlszeile den Befehl `gpupdate /force` ein und löschen Sie die alte Keytab mit dem Befehl `klist purge`.
5. Nachdem das GPO aktualisiert wurde, erstellen Sie die neue Keytab.
6. Laden Sie das Keytab zu iDRAC hoch.

Sie können sich jetzt unter Verwendung der SSO am iDRAC anmelden.

Warum scheitert die SSO-Anmeldung bei Active Directory-Benutzern auf Windows 7 und Windows Server 2008 R2?

Sie müssen die Verschlüsselungstypen für Windows 7 und Windows Server 2008 R2 aktivieren. So aktivieren Sie die Verschlüsselungstypen:

1. Melden Sie sich als Administrator oder als Benutzer mit Administratorrechten an.
2. Gehen Sie zu **Start** und führen Sie **gpedit.msc** aus. Das Fenster **Local Group Policy Editor** (Editor für lokale Gruppenrichtlinien) wird angezeigt.
3. Wechseln Sie zu **Local Computer Settings (Lokale Computereinstellungen)** > **Windows Settings (Windows-Einstellungen)** > **Security Settings (Sicherheitseinstellungen)** > **Local Policies (Lokale Richtlinien)** > **Security Options (Sicherheitsoptionen)**.
4. Klicken Sie mit der rechten Maustaste auf **Netzwerksicherheit: Für Kerberos genehmigte Verschlüsselungstypen konfigurieren** und wählen Sie **Eigenschaften** aus.
5. Aktivieren Sie alle Optionen.
6. Klicken Sie auf **OK**. Sie können sich jetzt unter Verwendung der SSO am iDRAC anmelden.

Führen Sie die folgenden zusätzlichen Einstellungen für das erweiterte Schema aus:

1. Navigieren Sie im Fenster **Local Group Policy Editor** (Editor für lokale Gruppenrichtlinien) zu **Local Computer Settings (Lokale Computereinstellungen)** > **Windows Settings (Windows-Einstellungen)** > **Security Settings (Sicherheitseinstellungen)** > **Local Policies (Lokale Richtlinien)** > **Security Options (Sicherheitsoptionen)**.
2. Klicken Sie mit der rechten Maustaste auf **Netzwerksicherheit: NTLM einschränken: Ausgehender NTLM-Verkehr zu Remote-Server** und wählen Sie **Eigenschaften** aus.
3. Wählen Sie **Alle zulassen**, klicken Sie auf **OK** und schließen Sie das Fenster **Editor für lokale Gruppenrichtlinien**.
4. Gehen Sie zu **Start** und führen Sie cmd aus. Das Eingabeaufforderungsfenster wird angezeigt.
5. Führen Sie den Befehl `gpupdate /force` aus. Die Gruppenrichtlinien werden aktualisiert. Schließen Sie das Eingabeaufforderungsfenster.
6. Gehen Sie zu **Start** und führen Sie regedit aus. Das Fenster **Registrierungseditor** wird angezeigt.
7. Navigieren Sie zu **HKEY_LOCAL_MACHINE** > **System** > **CurrentControlSet** > **Control (Steuerung)** > **LSA**.
8. Klicken Sie mit der rechten Maustaste in den rechten Fensterbereich und wählen Sie **New (Neu)** > **DWORD (32-bit) Value (DWORD (32-Bit) Wert)** aus.
9. Geben Sie dem neuen Schlüssel den Namen **SuppressExtendedProtection**.
10. Klicken Sie mit der rechten Maustaste auf **SuppressExtendedProtection** und klicken Sie dann auf **Ändern.**.
11. Geben Sie in das Feld **Wertdaten** die Zahl **1** ein und klicken Sie auf **OK**.
12. Schließen Sie das Fenster **Registry Editor** (Registrierungseditor). Sie können sich jetzt unter Verwendung der SSO am iDRAC anmelden.

Wenn Sie SSO für iDRAC aktiviert haben und Internet Explorer zum Anmelden bei iDRAC verwenden, schlägt SSO fehl, und Sie werden aufgefordert, Ihren Benutzernamen und Ihr Kennwort einzugeben. Wie kann ich dieses Problem lösen?

Stellen Sie sicher, dass die iDRAC-IP-Adresse unter **Tools (Extras)** > **Internet Options (Internetoptionen)** > **Security (Sicherheit)** > **Trusted sites (Vertrauenswürdige Sites)** aufgeführt ist. Wenn sie nicht aufgelistet ist, schlägt das einmalige Anmelden fehl und Sie werden aufgefordert, Ihren Benutzernamen und Ihr Kennwort einzugeben. Klicken Sie auf **Cancel** (Abbrechen) und fahren Sie fort.

Smart Card-Anmeldung

Bei Verwendung der Active Directory Smart-Card-Anmeldung dauert es vbs zu vier Minuten, um sich am iDRAC anzumelden.

Die normale Active Directory-Smart Card-Anmeldung dauert weniger als zehn Sekunden, es kann jedoch bis zu vier Minuten dauern, wenn Sie den bevorzugten DNS-Server und den alternativen DNS-Server auf der Seite **Netzwerk** angegeben haben und der bevorzugte DNS-Server ausgefallen ist. DNS-Zeitüberschreitungen sind zu erwarten, wenn ein DNS-Server ausgeschaltet ist. Der iDRAC meldet Sie unter Verwendung des alternativen DNS-Servers an.

Das ActiveX-Plugin kann das Smart Card-Laufwerk nicht erkennen.

Stellen Sie sicher, dass die Smart Card auf dem Microsoft Windows-Betriebssystem unterstützt wird. Windows unterstützt eine begrenzte Anzahl von Cryptographic Service Providers (CSP) für die Smart Card.

Sie können generell überprüfen, ob die Smart Card-CSPs auf einem bestimmten Client vorhanden sind, indem Sie die Smart Card beim Windows-Anmeldebildschirm (Strg-Alt-Entf) in das Laufwerk einlegen, um zu sehen, ob Windows die Smart Card erkennt und das PIN-Dialogfeld einblendet.

Falsche Smart Card-PIN

Prüfen Sie, ob die Smart Card aufgrund zu vieler Versuche mit einer falschen PIN gesperrt wurde. In solchen Fällen kann Ihnen der Aussteller der Smart Card in der Organisation helfen, eine neue Smart Card zu beschaffen.

Virtuelle Konsole

Welche Java-Version ist zum Starten der virtuellen Konsole erforderlich?

Zur Nutzung dieser Funktion und zum Starten der virtuellen iDRAC-Konsole über ein IPv6-Netzwerk ist Java 8 oder höher erforderlich.

Die Sitzung für die virtuelle Konsole ist aktiv, auch wenn Sie sich von der iDRAC-Weboberfläche abgemeldet haben. Ist dies das erwartete Verhalten?

Ja. Schließen Sie das Fenster mit dem Viewer für die virtuelle Konsole, um sich von der entsprechenden Sitzung abzumelden.

Kann eine neue Remote-Konsolenvideositzung gestartet werden, wenn das lokale Video auf dem Server ausgeschaltet ist?

Ja.

Warum dauert es 15 Sekunden, um das lokale Video auf dem Server auszuschalten, nachdem eine Aufforderung zum Ausschalten des lokalen Videos eingereicht wurde?

Hierdurch wird einem lokalen Benutzer die Gelegenheit gegeben, Maßnahmen durchzuführen, bevor das Video ausgeschaltet wird.

Tritt beim Einschalten des lokalen Videos eine Zeitverzögerung auf?

Nein. Sobald der iDRAC eine Anforderung zum Einschalten des lokalen Videos erhält, wird das Video sofort eingeschaltet.

Kann der lokale Benutzer das Video aus- oder einschalten?

Wenn die lokale Konsole deaktiviert ist, kann der lokale Benutzer das Video nicht aus- oder einschalten.

Werden beim Ausschalten des lokalen Videos auch die lokale Tastatur und Maus ausgeschaltet?

Nein.

Wird durch das Ausschalten der lokalen Konsole auch das Video der Remote-Konsolensitzung ausgeschaltet?

Nein, das Ein- oder Ausschalten des lokalen Videos ist von der Remote-Konsolensitzung unabhängig.

Welche Berechtigungen sind für einen iDRAC-Benutzer erforderlich, um das lokale Server-Video ein- oder auszuschalten?

Sämtliche Benutzer mit iDRAC-Konfigurationsberechtigungen können die lokale Konsole ein- oder ausschalten.

Wie kann ich den aktuellen Status des lokalen Servervideos abrufen?

Der Status wird auf der Seite „Virtuelle Konsole“ angezeigt.

Verwenden Sie zur Anzeige des Status des Objekts `iDRAC.VirtualConsole.AttachState` den folgenden Befehl:

```
racadm get idrac.virtualconsole.attachstate
```

Verwenden Sie alternativ den folgenden Befehl über eine SSH- oder eine Remote-Sitzung:

```
racadm -r (iDrac IP) -u (username) -p (password) get iDRAC.VirtualConsole.AttachState
```

Der Status wird auch auf der OSCAR-Anzeige der virtuellen Konsole angezeigt. Wenn die lokale Konsole aktiviert ist, wird neben dem Servernamen ein grüner Status angezeigt. Wenn sie deaktiviert ist, zeigt ein gelber Punkt an, dass iDRAC die lokale Konsole gesperrt hat.

Warum wird der untere Bereich des Systembildschirms nicht im Fenster für die virtuelle Konsole angezeigt?

Stellen Sie sicher, dass die Bildschirmauflösung der Management Station auf 1280x1024 eingestellt ist.

Warum wird das Fenster für den Viewer der virtuellen Konsole auf Linux-Betriebssystemen unkenntlich dargestellt?

Für den Konsolen-Viewer ist unter Linux ein UTF-8-Zeichensatz erforderlich. Überprüfen Sie Ihre Spracheinstellungen und setzen Sie den Zeichensatz bei Bedarf zurück.

Warum wird die Maus unter der Linux-Textkonsole in Lifecycle Controller nicht synchronisiert?

Die virtuelle Konsole benötigt den USB-Maustreiber, der USB-Maustreiber ist jedoch nur im X-Window-Betriebssystem verfügbar. Führen Sie im Viewer für die virtuelle Konsole die folgenden Schritte aus:

- Navigieren Sie zur Registerkarte **ExtrasSitzungsoptionen** > **Maus**. Wählen Sie unter **MausbeschleunigungLinux** aus.
- Wählen Sie im Menü **Extras** die Option **Einzel-Cursor** aus.

Wie kann der Mauszeiger im Fenster für den Viewer für die virtuelle Konsole synchronisiert werden?

Bevor Sie eine Sitzung für eine virtuelle Konsole starten, stellen Sie sicher, dass Sie die richtige Maus für Ihr Betriebssystem ausgewählt haben.

Stellen Sie außerdem sicher, dass die Option **Einzel-Cursor** unter **Extras** im Menü für die virtuelle iDRAC-Konsole auf dem Client für die Konsole ausgewählt ist. Standardmäßig ist der Zwei-Cursor-Modus eingestellt.

Kann eine Tastatur oder eine Maus verwendet werden, während ein Microsoft-Betriebssystem remote über die virtuelle Konsole installiert wird?

Nein. Wenn Sie remote ein unterstütztes Microsoft-Betriebssystem auf einem System installieren, auf dem die virtuelle Konsole im BIOS aktiviert ist, wird eine EMS-Verbindungsnachricht gesendet, bei der Sie remote **OK** auswählen müssen. Sie müssen entweder **OK** auf dem lokalen System auswählen oder den remote verwalteten Server neu starten, eine Neuinstallation vornehmen und die virtuelle Konsole im BIOS deaktivieren.

Diese Nachricht wird durch Microsoft erstellt, um den Benutzer darauf hinzuweisen, dass die virtuelle Konsole aktiviert ist. Um sicherzustellen, dass diese Meldung nicht angezeigt wird, müssen Sie die virtuelle Konsole im Dienstprogramm für die iDRAC-Einstellungen ausschalten, bevor Sie ein Betriebssystem remote installieren.

Warum zeigt die Nummernblockanzeige auf der Management Station nicht den Status des Nummernblocks auf dem Remote-Server an?

Wenn Sie über iDRAC auf den Nummernblock auf der Management Station zugreifen, stimmt dieser nicht unbedingt mit dem Status des Nummernblocks auf dem Remote-Server überein. Der Status des Nummernblocks hängt von der Einstellung zum Zeitpunkt der Verbindungsherstellung der Remote-Sitzung ab. Dabei ist der Status des Nummernblocks auf der Management Station nicht von Belang.

Warum werden mehrere Session Viewer-Fenster eingeblendet, wenn vom lokalen Host aus eine Sitzung der virtuellen Konsole aufgebaut wird?

Sie konfigurieren eine virtuelle Konsole über das lokale System. Dieser Vorgang wird nicht unterstützt.

Wenn eine Sitzung für eine virtuelle Konsole aktiv ist und ein lokaler Benutzer auf den Managed Server zugreift, wird dem ersten Benutzer eine Warnmeldung angezeigt?

Nein. Wenn ein lokaler Benutzer auf das System zugreift, haben beide Kontrolle über das System.

Wie viel Bandbreite ist für die Ausführung einer Sitzung für eine virtuelle Konsole erforderlich?

Für eine gute Leistung wird eine Verbindung mit einer Bandbreite von 5 Mbit/s empfohlen. Eine Verbindung mit einer Bandbreite von 1 Mbit/s stellt die Mindestanforderung dar.

Was sind die Mindestsystemanforderungen der Management Station zum Ausführen der virtuellen Konsole?

Die Management Station benötigt einen Intel Pentium III 500-MHz-Prozessor mit mindestens 256 MB RAM.

Warum zeigt das Fenster mit dem Viewer für die virtuelle Konsole manchmal die Meldung „Kein Signal“ an?

Diese Meldung wird angezeigt, da das iDRAC-Plug-in für die virtuelle Konsole das Remote-Server-Desktop-Video nicht empfängt. Im Allgemeinen kann dieses Verhalten auftreten, wenn der Remote-Server ausgeschaltet ist. Manchmal wird diese Meldung aufgrund einer Empfangsfehlfunktion des Remote-Server-Desktop-Videos angezeigt.

Warum zeigt das Fenster für den Viewer der virtuellen Konsole gelegentlich die Meldung „Außerhalb des Bereichs“ an?

Diese Meldung wird möglicherweise angezeigt, weil ein Parameter, der für die Videoerfassung erforderlich ist, sich außerhalb des Bereichs befindet, für den iDRAC das Video erfassen kann. Wenn bestimmte Parameter, z. B. die Anzeigeauflösung oder die Bildwiederholfrequenz, zu hoch eingestellt sind, ist es möglich, dass die Meldung „Out of range“ (Außerhalb des Bereichs) angezeigt wird. In der Regel wird der maximale Bereich der Parameter durch physische Begrenzungen definiert, wie z. B. die Größe des Videospeichers oder der Bandbreite.

Warum wird, wenn eine Sitzung für eine virtuelle Konsole von der iDRAC-Weboberfläche aus gestartet wird, ein ActiveX-Sicherheits-Pop-up-Fenster angezeigt?

iDRAC ist möglicherweise nicht in der Liste der vertrauenswürdigen Sites enthalten. Um zu verhindern, dass das Sicherheits-Pop-up-Fenster bei jedem Start einer Sitzung einer virtuellen Konsole aufgerufen wird, fügen Sie iDRAC wie folgt zur Liste der vertrauenswürdigen Sites im Client-Browser hinzu:

1. Klicken Sie auf **Extras** > **Internetoptionen** > **Sicherheit** > **Vertrauenswürdige Sites**.
2. Klicken Sie auf **Sites**, und geben Sie die IP-Adresse oder den DNS-Namen des iDRAC ein.
3. Klicken Sie auf **Hinzufügen**.

4. Klicken Sie auf **Stufe anpassen**.
5. Wählen Sie im Fenster **Sicherheitseinstellungen** die Option **Bestätigen** unter **Unsignierte ActiveX-Steuerelemente herunterladen** aus.

Warum ist das Fenster für den Viewer der virtuellen Konsole leer?

Wenn Sie über Berechtigungen für virtuelle Datenträger verfügen, nicht aber für die virtuelle Konsole, können Sie den Viewer für den Zugriff auf die Funktion für virtuelle Datenträger starten, die Konsole des verwalteten Servers wird jedoch nicht angezeigt.

Warum wird die Maus nicht unter DOS synchronisiert, wenn die virtuelle Konsole ausgeführt wird?

Das Dell BIOS emuliert den Maustreiber als PS/2-Maus. Die PS/2-Maus ist so konzipiert, dass sie die relative Position für den Mauszeiger verwendet, was die Verzögerung in der Synchronisation verursacht. iDRAC verfügt über einen USB-Maustreiber, mit dem eine absolute Position und damit eine engere Verfolgung des Mauszeigers möglich ist. Selbst wenn iDRAC die absolute Position der USB-Maus an das Dell BIOS weiterleitet, konvertiert die BIOS-Emulation sie zurück in die relative Position und das Verhalten bleibt unverändert. Um dieses Problem zu beheben, stellen Sie auf dem Bildschirm „Configuration“ (Konfiguration) den Mausmodus auf „USC/Diags“ ein.

Nach dem Start der virtuellen Konsole ist der Mauszeiger auf der virtuellen Konsole aktiv, jedoch nicht auf dem lokalen System. Warum tritt dieses Verhalten auf und wie kann es behoben werden?

Dieser Fehler tritt auf, wenn für **Mausmodus USC/Diags** eingestellt ist. Drücken Sie die Tastenkombination **Alt+M**, um die Maus auf dem lokalen System zu verwenden. Drücken Sie **Alt+M** erneut, um die Maus auf der virtuellen Konsole zu verwenden.

Warum kommt es bei der GUI-Sitzung zu einem Timeout, nachdem die virtuelle Konsole über die iDRAC-Schnittstelle gestartet wurde, die wiederum über CMC gestartet wurde?

Wenn die virtuelle Konsole über die CMC-Weboberfläche für iDRAC gestartet wird, wird ein Pop-up-Fenster zum Starten der virtuellen Konsole geöffnet. Dieses Pop-up-Fenster wird kurz nach dem Öffnen der virtuellen Konsole geschlossen.

Wenn sowohl die GUI als auch die virtuelle Konsole auf das gleiche iDRAC-System auf einer Management Station gestartet werden, tritt ein Sitzungs-Timeouts für die iDRAC-GUI auf, wenn die GUI vor dem Schließen des Pop-up-Fensters gestartet wird. Wenn die iDRAC-GUI über die CMC-Weboberfläche nach dem Schließen des Pop-up-Fensters der virtuellen Konsole gestartet wird, tritt dieses Problem nicht auf.

ANMERKUNG: Gilt nicht für MX-Plattformen.

Warum kann der Linux S-Abf-Schlüssel nicht mit Internet Explorer verwendet werden?

Das Verhalten der S-Abf-Taste ändert sich, wenn die virtuelle Konsole über Internet Explorer verwendet wird. Um die S-Abf-Taste zu nutzen, drücken Sie die Taste **Druck** und lassen Sie sie los, während Sie die Tasten **Strg** und **Alt** gedrückt halten. So nutzen Sie die S-Abf-Taste für einen Remote-Linux-Server über iDRAC bei Verwendung des Internet Explorers:

1. Aktivieren Sie die Funktion für die magische Taste auf dem Remote-Linux-Server. Sie können den folgenden Befehl verwenden, sie auf dem Linux-Terminal zu aktivieren:

   ```
   echo 1 > /proc/sys/kernel/sysrq
   ```

2. Aktivieren Sie den Tastaturdurchgangsmodus von Active X Viewer.
3. Drücken Sie **Strg+Alt+Druck**.
4. Lassen Sie nur die Taste **Druck** wieder los.
5. Drücken Sie die Tastenkombination **Druck+Strg+Alt**.

ANMERKUNG: Die S-Abf-Funktion wird derzeit nicht für Internet Explorer und Java unterstützt.

Warum wird die Meldung „Verknüpfung unterbrochen“ unten auf der virtuellen Konsole angezeigt?

Wenn Sie während des Neustarts eines Servers den freigegebenen Netzwerkport verwenden, wird iDRAC getrennt, während das BIOS die Netzwerkkarte zurücksetzt. Dieser Vorgang dauert auf Karten mit 10 Gbit länger und dauert außerdem außergewöhnlich lange, wenn auf dem angeschlossenen Netzwerkswitch das Spanning Tree Protocol (STP) aktiviert ist. In diesem Fall wird empfohlen, die Option „portfast“ für den Switch-Port zu verwenden, der mit dem Server verbunden ist. In den meisten Fällen stellt sich die virtuelle Konsole selbst wieder her.

Starten der virtuellen Konsole mit Java-Plug-in schlägt fehl, nachdem die iDRAC-Firmware aktualisiert wurde.

Löschen Sie den Java-Cache und starten Sie anschließend die virtuelle Konsole.

So aktivieren Sie die Konsolenumleitung über den Webserver-Port (443)

```
racadm>>set iDRAC.VirtualConsole.WebRedirect Enabled
```

Um den externen virtuellen Konsolen-Port (5900) zu schließen, legen Sie die folgende iDRAC-Eigenschaft fest.

Um den externen virtuellen Konsolen-Port (5900) zu schließen, muss sowohl `iDRAC.VirtualConsole.WebRedirect` als auch `iDRAC.VirtualConsole.CloseUnusedPort` aktiviert sein.

```
racadm>>set iDRAC.VirtualConsole.CloseUnusedPort Enabled
```

ANMERKUNG:

- Wenn der virtuelle Datenträger-Port deaktiviert ist, sind eigenständige virtuelle Datenträger nicht zugänglich und Sie können die virtuellen Datenträger über die virtuelle Konsole verwenden.
- Während „CloseUnusedPort“ aktiviert ist, funktionieren die Java- und die ActiveX-basierte virtuelle Konsole und die virtuellen Datenträger nicht, da Sie einen dedizierten externen Port benötigen. Die virtuelle Konsole und die virtuellen Datenträger, die das HTML5-Plug-in verwenden, funktionieren auf dem iDRAC-Webserver-Port (443).

Virtueller Datenträger

Warum wird die Verbindung mit dem Client für den virtuellen Datenträger manchmal getrennt?

Wenn ein Netzwerk-Timeout eintritt, trennt die iDRAC-Firmware die Verbindung und unterbricht die Verbindung zwischen dem Server und dem virtuellen Datenträger.

Wenn Sie die CD im Client-System ändern, weist die neue CD eventuell eine Autostart-Funktion auf. In diesem Fall kann es zu einem Timeout der Firmware kommen und die Verbindung verloren gehen, wenn das Client-System zu lange braucht, um die CD zu lesen. Wenn eine Verbindung verloren geht, stellen Sie die Verbindung über die GUI wieder her und fahren Sie mit dem vorherigen Vorgang fort.

Wenn die Konfigurationseinstellungen des virtuellen Datenträgers in der iDRAC-Weboberfläche oder durch Befehle des lokalen RACADM geändert werden, wird die Verbindung aller verbundener Datenträger bei Übernahme der Konfigurationsänderung unterbrochen.

Verwenden Sie zum erneuten Verbinden des virtuellen Datenträgers das Fenster „Virtueller Datenträger – **Client-Ansicht**“.

Warum dauert eine Windows-Betriebssysteminstallation über einen virtuellen Datenträger länger?

Wenn Sie das Windows-Betriebssystem mithilfe der DVD *Dell Systems Management Tools and Documentation* und über eine langsame Netzwerkverbindung installieren, kann es sein, dass das Installationsverfahren aufgrund von Netzwerklatenz für den Zugriff auf die iDRAC-Weboberfläche mehr Zeit erfordert. Das Installationsfenster zeigt den Installationsfortschritt nicht an.

Wie kann das virtuelle Gerät als Startlaufwerk konfiguriert werden?

Öffnen Sie auf dem verwalteten System das BIOS-Setup und navigieren Sie zum Startmenü. Suchen Sie die virtuelle CD, virtuelle Diskette oder vFlash und ändern Sie die Startreihenfolge des Geräts nach Bedarf. Drücken Sie außerdem die Leertaste in der Startreihenfolge im CMOS-Setup, um das virtuelle Gerät startbar zu machen. Um beispielsweise von einem CD-Laufwerk zu starten, konfigurieren Sie das CD-Laufwerk als erstes Gerät in der Startreihenfolge.

Welche Datenträgertypen können als Startlaufwerk festgelegt werden?

Mit dem iDRAC können Sie von den folgenden startfähigen Datenträgern aus starten:

- CD-ROM/DVD-Datenträger
- ISO 9660-Image
- 1,44 Zoll-Diskette oder Disketten-Image
- USB-Schlüssel, der vom Betriebssystem als Wechsellaufwerk erkannt wird
- Ein USB-Schlüssel-Image

Wie kann der USB-Schlüssel in ein Startlaufwerk umkonfiguriert werden?

Sie können auch über eine Windows 98-Startdiskette starten und Systemdateien von der Startdiskette auf den USB-Schlüssel kopieren. Geben Sie z. B. an der DOS-Eingabeaufforderung den folgenden Befehl ein:

```
sys a: x: /s
```

wobei „x:“ für den USB-Schlüssel steht, der als Startlaufwerk konfiguriert werden soll.

Der virtuelle Datenträger ist verbunden und mit der Remote-Diskette verbunden. Das virtuelle Diskettenlaufwerk/virtuelle CD-Gerät kann auf einem System, auf dem Red Hat Enterprise Linux oder SuSE Linux Betriebssystem ausgeführt wird, aber nicht gefunden werden. Wie kann dieses Problem behoben werden?

Einige Linux-Versionen laden das virtuelle Diskettenlaufwerk und das virtuelle CD-Laufwerk nicht automatisch auf dieselbe Weise. Um das virtuelle Diskettenlaufwerk zu laden, machen Sie den Geräteknoten ausfindig, den Linux dem virtuellen Diskettenlaufwerk zuweist. So laden Sie das virtuelle Diskettenlaufwerk:

1. Öffnen Sie eine Linux-Eingabeaufforderung, und führen Sie den folgenden Befehl aus:

   ```
   grep "Virtual Floppy" /var/log/messages
   ```

2. Machen Sie den letzten Eintrag zu dieser Meldung ausfindig, und notieren Sie die Zeit.
3. Führen Sie an der Linux-Eingabeaufforderung den folgenden Befehl aus:

   ```
   grep "hh:mm:ss" /var/log/messages
   ```

   wobei, hh:mm:ss der Zeitstempel der Meldung ist, die von grep in Schritt 1 zurückgegeben wurde.
4. Lesen Sie in Schritt 3 das Ergebnis des grep-Befehls und finden Sie den Gerätenamen, der dem virtuellen Diskettenlaufwerk zugeordnet wurde.
5. Stellen Sie sicher, dass das virtuelle Diskettenlaufwerk angeschlossen ist und eine Verbindung dazu besteht.
6. Führen Sie an der Linux-Eingabeaufforderung den folgenden Befehl aus:

   ```
   mount /dev/sdx /mnt/floppy
   ```

   wobei `/dev/sdx` für den in Schritt 4 ermittelten Gerätenamen steht und `/mnt/floppy` der Einhängepunkt ist.

Um das virtuelle CD-Laufwerk zu laden, machen Sie den Geräteknoten ausfindig, den Linux dem virtuellen CD-Laufwerk zuweist. Um das virtuelle CD-Laufwerk zu laden:

1. Öffnen Sie eine Linux-Eingabeaufforderung, und führen Sie den folgenden Befehl aus:

   ```
   grep "Virtual CD" /var/log/messages
   ```

2. Machen Sie den letzten Eintrag zu dieser Meldung ausfindig, und notieren Sie die Zeit.
3. Führen Sie an der Linux-Eingabeaufforderung den folgenden Befehl aus:

   ```
   grep "hh:mm:ss" /var/log/messages
   ```

   wobei, hh:mm:ss der Zeitstempel der Meldung ist, die von grep in Schritt 1 zurückgegeben wurde.
4. Lesen Sie in Schritt 3 das Ergebnis des grep-Befehls und machen Sie den Gerätenamen ausfindig, der der *virtuellen Dell-CD* zugeordnet wurde.
5. Stellen Sie sicher, dass das virtuelle CD-Laufwerk vorhanden und verbunden ist.
6. Führen Sie an der Linux-Eingabeaufforderung den folgenden Befehl aus:

   ```
   mount /dev/sdx /mnt/CD
   ```

   wobei `/dev/sdx` für den in Schritt 4 ermittelten Gerätenamen steht und `/mnt/floppy` der Einhängepunkt ist.

Warum werden die mit dem Server verbundenen virtuellen Laufwerke nach einem Remote-Firmwareupdate über die iDRAC-Weboberfläche entfernt?

Firmwareupdates bewirken, dass der iDRAC eine Rücksetzung durchführt, die Remote-Verbindung verwirft und die virtuellen Laufwerke aufhebt. Die Laufwerke werden wieder angezeigt, wenn der iDRAC-Reset abgeschlossen ist.

Warum werden nach dem Anschließen eines USB-Geräts alle USB-Geräte abgetrennt?

Virtuelle Datenträgergeräte und vFlash-Geräte werden als Composite-USB-Gerät mit dem Host-USB-Bus verbunden und nutzen einen gemeinsamen USB-Port. Immer, wenn ein virtueller Datenträger oder ein vFlash-USB-Gerät mit dem Host-USB-Bus verbunden oder vom Host getrennt wird, werden alle virtuellen Datenträger und vFlash-Geräte kurzzeitig vom Host-USB-Bus getrennt und dann erneut verbunden. Verbinden oder trennen Sie keine virtuellen Medien oder vFlash-Geräte, wenn das Hostbetriebssystem ein virtuelles Datenträgergerät verwendet. Es wird empfohlen, dass Sie alle erforderlichen USB Geräte anschließen, bevor Sie sie verwenden.

Welche Funktion hat das USB-Reset?

Sie setzt die Remote- und lokalen USB-Geräte zurück, die an den Server angeschlossen sind.

Wie lässt sich die Leistung des virtuellen Datenträgers maximieren?

Starten Sie zum Maximieren der Leistung des virtuellen Datenträgers den virtuellen Datenträger bei deaktivierter virtueller Konsole, oder führen Sie eine der folgenden Schritte aus:

- Stellen Sie den Schieberegler für die Leistung auf die maximale Geschwindigkeit.
- Deaktivieren Sie die Verschlüsselung sowohl für den virtuellen Datenträger als auch für die virtuelle Konsole.

  ANMERKUNG: In diesem Fall wird die Datenübertragung zwischen dem verwalteten Server und iDRAC für den virtuellen Datenträger und für die virtuelle Konsole nicht gesichert.

- Wenn Sie ein Windows Server-Betriebssystem verwenden, beenden Sie den Windows-Dienst mit dem Namen Windows Event Collector. Navigieren Sie dazu zu **Start** > **Verwaltung** > **Dienste**. Klicken Sie mit der rechten Maustaste auf **Windows Event Collector** und anschließend auf **Beenden**.

Während der Betrachtung der Inhalte eines Diskettenlaufwerks oder eines USB-Schlüssels wird ein Verbindungsfehler angezeigt, wenn das gleiche Laufwerk über den virtuellen Datenträger angeschlossen ist. Warum?

Der gleichzeitige Zugriff auf virtuelle Diskettenlaufwerke ist nicht erlaubt. Schließen Sie die Anwendung, die zum Anzeigen der Laufwerksinhalte verwendet wird, bevor Sie versuchen, das Laufwerk zu virtualisieren.

Welche Dateisystemtypen werden auf dem virtuellen Diskettenlaufwerk unterstützt?

Ihr virtuelles Diskettenlaufwerk unterstützt FAT16- oder FAT32-Dateisysteme.

Warum wird eine Fehlermeldung angezeigt, wenn man versucht, ein DVD-Laufwerk/einen USB-Schlüssel über einen virtuellen Datenträger zu verbinden, auch wenn der virtuelle Datenträger derzeit nicht verwendet wird?

Die Fehlermeldung wird angezeigt, wenn auch die Remote-Dateifreigabe (RFS) verwendet wird. Sie können RFS und virtuelle Datenträger nicht gleichzeitig verwenden.

Der Zugriff auf virtuelle Datenträger ist nicht möglich, obwohl iDRAC den *Verbindungsstatus* des virtuellen Datenträgers als *Verbunden* anzeigt.

Wenn Sie versuchen, über ActiveX- oder Java-Plug-ins auf den virtuellen Datenträger zuzugreifen, während der **Verbindungsmodus** in iDRAC auf **Trennen** eingestellt ist, wird der Verbindungsstatus möglicherweise als **Verbunden** angezeigt. Ändern Sie den **Verbindungsmodus** entweder auf **Automatisch verbinden** oder **Verbinden**, um auf den virtuellen Datenträger zuzugreifen.

vFlash-SD-Karte

Wann ist die vFlash SD-Karte gesperrt?

Die vFlash-SD-Karte ist gesperrt, wenn ein Vorgang läuft. Z. B. während der Initialisierung.

SNMP-Authentifizierung

Warum wird die Meldung „Remote-Zugriff: SNMP-Authentifizierungsfehler“ angezeigt?

Im Rahmen der Erkennung versucht IT Assistant, die get- und set-Community-Namen des Geräts zu überprüfen. In IT Assistant ist der get-Community-Name „public“ und der set-Community-Name „private“. Standardmäßig ist der SNMP-Agent-Community-Name für den iDRAC-Agenten „public“. Wenn IT Assistant eine set-Anforderung sendet, generiert der iDRAC-Agent den SNMP-Authentifizierungsfehler, weil er nur Anforderungen von Community = public akzeptiert.

Um zu verhindern, dass SNMP-Authentifizierungsfehler generiert werden, müssen Sie Community-Namen eingeben, die vom Agenten akzeptiert werden. Da der iDRAC nur einen einzigen Community-Namen zulässt, müssen Sie denselben get- und set-Community-Namen für das IT Assistant-Erkennungs-Setup eingeben.

Speichergeräte

Die OpenManage-Speicherverwaltung zeigt mehr Speichergeräte als iDRAC an, wobei keine Informationen für alle Speichergeräte angezeigt werden, die mit dem System verbunden sind. Warum?

iDRAC zeigt Informationen nur für die von Comprehensive Embedded Management (CEM) unterstützten Geräte an.

Für externe JBODs/Einblicke in die HBA wird die EEMI-Meldung für die Entfernung des SAS-Konnektors/IOM mit der EEMI-Meldungs-ID ENC42 generiert, allerdings wird die EEMI-Meldung ENC41 für die Wiederherstellung des SAS-Konnektors/IOM nicht erzeugt.

So bestätigen Sie die Wiederherstellung des IOM in der iDRAC-Weboberfläche:

1. Gehen Sie zu **Speicher** > **Übersicht** > **Gehäuse**
2. Wählen Sie das Gehäuse aus.
3. Stellen Sie unter **Erweiterte Eigenschaften** sicher, dass der Wert für **Redundanter Pfad** auf **Vorhanden** eingestellt ist, dann wird die IOM-Wiederherstellung bestätigt.

GPU (Beschleuniger)

Der Abschnitt „Beschleuniger“ unter CPU/Beschleuniger in der iDRAC GUI ist grau unterlegt.

Auf einigen Seiten in der GUI wird möglicherweise keine erwartete Reaktion angezeigt, wenn das entsprechende Attribut in Redfish deaktiviert ist.

iDRAC-Service-Modul

iSM-Details fehlen/werden auf der iDRAC-GUI-Seite einiger PowerEdge-Server nicht korrekt aktualisiert

Wenn ein Nutzer SUB NIC unter Teaming hinzufügt, ist die Konfiguration ungültig. Dies führt dazu, dass iSM nicht richtig mit iDRAC kommuniziert.

Sollte vor der Installation und dem Ausführen des iDRAC Service Module der OpenManage Server Administrator deinstalliert werden?

Nein, Sie müssen den Server Administrator nicht deinstallieren. Stellen Sie vor der Installation oder Ausführung des iDRAC Service Module sicher, dass Sie die Funktionen des Server Administrator, die das iDRAC Service Module bereitstellt, gestoppt haben.

Wie wird überprüft, ob das iDRAC Service Module auf dem System installiert ist?

Um herauszufinden, ob das iDRAC Service Module auf Ihrem System installiert ist, gehen Sie folgendermaßen vor:

- Auf Systemen, die Windows ausführen:

  Öffnen Sie die **Systemsteuerung**, und überprüfen Sie, ob das iDRAC-Service-Modul in der Liste der installierten Programme angezeigt wird.

- Auf Systemen, die Linux ausführen:

  Führen Sie den Befehl `rpm –qi dcism` aus. Wenn das iDRAC Service Module installiert ist, ist der Status **Installiert**.

- Auf Systemen, die ESXi ausführen: Führen Sie den Befehl `esxcli software vib list|grep -i open` auf dem Host aus. Das iDRAC-Servicemodul wird angezeigt.

ANMERKUNG: Um zu überprüfen, ob das iDRAC Service Module unter Red Hat Enterprise Linux 7 installiert ist, verwenden Sie den Befehl `systemctl status dcismeng.service` anstelle des Befehls `init.d`.

Wie wird die Versionsnummer des iDRAC Service Module überprüft, die im System installiert ist?

Zum überprüfen der Version des iDRAC Service Module im System führen Sie eine der folgenden Aktionen aus:

- Klicken Sie auf **Start** > **Systemsteuerung** > **Programme und Funktionen**. Die Version des installierten iDRAC Service Module wird auf der Registerkarte **Version** aufgelistet.
- Gehen Sie zu **Arbeitsplatz** > **Programm deinstallieren oder ändern**.

Welche Berechtigungsebene muss ein Nutzer mindestens haben, um das iDRAC Service Module installieren zu können?

Zum Installieren des iDRAC Service Module müssen Sie über Administratorrechte verfügen.

In iDRAC Service Module Version 2.0 und früher wird bei der Installation des iDRAC Service Module eine Fehlermeldung angezeigt, dass es sich um einen nicht unterstützten Server handelt. Weitere Informationen über unterstützte Server finden Sie in der Nutzerdokumentation. Wie kann ich diesen Fehler beheben?

Stellen Sie vor der Installation des iDRAC Service Module sicher, dass der Server ein PowerEdge-Server der 12. Generation oder höher ist. Stellen Sie außerdem sicher, dass Sie ein 64-Bit-System verwenden.

Die folgende Meldung wird in der BS-Protokolldatei angezeigt, selbst wenn Pass-through vom BS zum iDRAC über USBNIC ordnungsgemäß konfiguriert ist. Warum?

The iDRAC Service Module is unable to communicate with iDRAC using the OS to iDRAC Pass-through channel

Das iDRAC Service Module verwendet den Pass-through vom BS zum iDRAC über die USB-NIC-Funktion, um die Kommunikation mit dem iDRAC einzurichten. Manchmal wird die Kommunikation nicht eingerichtet, obwohl die USB-NIC-Schnittstelle mit den korrekten IP-Endpunkten konfiguriert ist. Dies kann eintreten, wenn die Routing-Tabelle des Host-Betriebssystems mehrere Einträge für dieselbe Zielmaske aufweist und das USB-NIC-Ziel nicht als erstes Ziel in der Routing-Reihenfolge aufgelistet ist.

Tabelle 64. Beispiel für eine Routing-Reihenfolge

Ziel	Gateway	Genmask	Flags	Metrik	Ref.	Iface verwenden
Standardeinstellung	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	B	0	0	0 em1
Link-lokal	0.0.0.0	255.255.255.0	B	0	0	0 em1
Link-lokal	0.0.0.0	255.255.255.0	B	0	0	0 enp0s20u12u3

In diesem Beispiel ist **enp0s20u12u3** die USB-NIC-Schnittstelle. Die Zielmaske „link-local (Link-lokal)“ wird wiederholt und die USB NIC ist nicht das erste Ziel in der Reihenfolge. Dies führt zu dem Konnektivitätsproblem zwischen dem iDRAC-Servicemodul und iDRAC über das Betriebssystem zu iDRAC-Passthrough. Um das Konnektivitätsproblem zu beheben, stellen Sie sicher, dass die iDRAC-USBNIC-IPv4-Adresse (die Standardeinstellung lautet 169.254.1.1) über das Hostbetriebssystem erreichbar ist.

Wenn nicht:

- Ändern Sie die iDRAC-USBNIC-Adresse auf einer eindeutigen Ziel-Maske.
- Löschen Sie die Einträge, die Sie nicht benötigen, aus der Routingtabelle, um sicherzustellen, dass die USB-NIC durch die Route ausgewählt wird, wenn der Host die iDRAC-USB-NIC-IPv4-Adresse erreichen möchte.

Auf iDRAC Service Module Version 2.0 wird beim Deinstallieren eines iDRAC Service Module von einem VMware ESXi-Server der virtuelle Switch auf dem vSphere-Client als vSwitchiDRACvusb und die Port-Gruppe als iDRAC-Netzwerk benannt. Wie können sie gelöscht werden?

Bei der Installation des iDRAC Service Module-VIB auf einem VMware ESXi-Server erstellt das iDRAC Service Module den vSwitch und die Port-Gruppe, um mit dem iDRAC über den Pass-through vom OS zum iDRAC im USB-NIC-Modus zu kommunizieren. Nach Abschluss der Deinstallation werden der virtuelle Switch **vSwitchiDRACvusb** und die Port-Gruppe **iDRAC-Netzwerk** nicht gelöscht. Um sie manuell zu löschen, führen Sie einen der folgenden Schritte aus:

- Gehen Sie zum Assistenten für die Konfiguration des vSphere-Clients, und löschen Sie die Einträge.
- Wechseln Sie zur Esxcli, und geben Sie die folgenden Befehle ein:
  - Zum Entfernen der Port-Gruppe: `esxcfg-vmknic -d -p "iDRAC Network"`
  - Zum Entfernen des vSwitch: `esxcfg-vswitch -d vSwitchiDRACvusb`

  ANMERKUNG: Sie können das iDRAC-Service-Modul auf dem VMware ESXi-Server neu installieren, da es sich dabei für den Server nicht um ein funktionsbezogenes Problem handelt.

Wo befindet sich das replizierte Lifecycle-Protokoll im Betriebssystem?

So zeigen Sie die replizierten Lifecycle-Protokolle an:

Tabelle 65. Speicherort für Lifecycle-Protokolle

Betriebssystem	Speicherort
Microsoft Windows	**Ereignisanzeige** > **Windows-Protokolle** > **System**. Alle Lifecycle-Protokolle für das iDRAC Service Module werden unter dem Quellnamen **iDRAC Service Module** repliziert. **ANMERKUNG:** In iSM Version 2.1 und höher werden Lifecycle-Protokolle unter dem Quellnamen des Lifecycle Controller-Protokolls repliziert. In iSM Version 2.0 und niedriger werden Protokolle unter dem Quellnamen des iDRAC Service Module repliziert. **ANMERKUNG:** Der Speicherort der Lifecycle-Protokolle kann unter Verwendung des Installationsprogramms für das iDRAC Service Module konfiguriert werden. Sie können beim Installieren des iDRAC Service Module oder beim Bearbeiten des Installationsprogramms den Speicherort konfigurieren.
Red Hat Enterprise Linux, SUSE Linux, CentOS und Citrix XenServer	`/var/log/messages`
VMware ESXi	`/var/log/syslog.log`

Was sind die abhängigen Linux-Pakete oder ausführbaren Dateien, die während der Vollendung der Linux-Installation verfügbar sind?

Die Liste der abhängigen Linux-Pakete finden Sie im Abschnitt *Linux-Abhängigkeiten* unter *iDRAC-Servicemodul-Benutzerhandbuch* verfügbar unter https://www.dell.com/idracmanuals.

Wie kann die GPU-Leistung für bestimmte Konfigurationen erhöht werden?

BIOS-System-Performance Profil auf Performance eingestellt

Legen Sie unter Prozessoreinstellungen NPS auf 4 und CCX auf Auto fest.

Mindestens 1 DIMM pro Kanal

IOmmu = Passthrough auf Linux OS

RACADM

Wenn nach dem Zurücksetzen eines iDRAC (über den Befehl „racadm racreset“) ein Befehl ausgegeben wird, wird die folgende Meldung angezeigt. Wofür steht diese Meldung?

```
ERROR: Unable to connect to RAC at specified IP address
```

Die Meldung gibt an, dass Sie warten müssen, bis der iDRAC-Reset abgeschlossen ist, bevor Sie einen anderen Befehl ausgeben.

Wenn Sie RACADM-Befehle und -Unterbefehle verwenden, werden einige Fehler nicht behoben.

Bei der Verwendung von RACADM-Befehlen können ein oder mehrere der folgenden Fehler auftreten:

- Lokale RACADM-Fehlermeldungen - Probleme wie Syntax, typografische Fehler und falsche Namen.
- Remote RACADM-Fehlermeldungen – Probleme wie falsche IP-Adresse, falscher Benutzername oder falsches Kennwort.

Wenn während eines PING-Tests auf dem iDRAC der Netzwerkmodus von „Dediziert“ in „Freigegeben“ geändert wird, wird keine PING-Antwort generiert.

Löschen Sie die ARP-Tabelle auf dem System.

Remote-RACADM ist nicht in der Lage, eine Verbindung zu iDRAC über SUSE Linux Enterprise Server (SLES) 11 SP1 herzustellen.

Stellen Sie sicher, dass Sie die offiziellen openssl- und libopenssl-Versionen installiert haben. Führen Sie den folgenden Befehl aus, um die RPM-Pakete zu installieren:

```
rpm -ivh --force < filename >
```

Hierbei ist `filename` die openssl- oder libopenssl-RPM-Paketdatei.

Zum Beispiel:

```
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
```

Warum sind die Remote-RACADM- und webbasierten Dienste nach einer Eigenschaftsänderung nicht verfügbar?

Es kann eine Weile dauern, bis die Remote-RACADM-Dienste und die webbasierte Schnittstelle nach einem Reset des iDRAC-Web Servers verfügbar sind.

Der iDRAC Web-Server wird zurückgesetzt, wenn:

- Die Netzwerkkonfiguration oder Netzwerk-Sicherheitseigenschaften werden mittels der webbasierten iDRAC-Benutzeroberfläche geändert.
- Die Eigenschaft „iDRAC.Webserver.HttpsPort“ wird geändert, einschließlich wenn `racadm set -f <config file>` sie ändert.
- Der Befehl `racresetcfg` wird verwendet.
- iDRAC wurde zurückgesetzt.
- Ein neues SSL-Serverzertifikat wird hochgeladen.

Warum wird eine Fehlermeldung angezeigt, wenn Sie versuchen, eine Partition zu löschen, nachdem Sie sie über den lokalen RACADM erstellt haben?

Dies geschieht, da gerade eine Partition erstellt wird. Die Partition wird jedoch nach einer Weile gelöscht und der Löschvorgang durch eine entsprechende Meldung bestätigt. Warten Sie andernfalls, bis die Partitionserstellung abgeschlossen ist, und löschen Sie die Partition anschließend.

Standardkennwort dauerhaft auf „calvin“ setzen

Wenn Ihr System mit einem eindeutigen Standard-iDRAC-Kennwort geliefert wurde, Sie jedoch *calvin* als Standardkennwort festlegen möchten, müssen Sie die auf der Systemplatine verfügbaren Jumper verwenden.

VORSICHT: Durch das Ändern der Jumper-Einstellungen wird das Standardkennwort dauerhaft in *calvin* geändert. Sie können das eindeutige Kennwort nicht wiederherstellen, auch wenn Sie den iDRAC auf die Werkseinstellungen zurücksetzen.

Weitere Informationen über die Position des Jumpers und das Verfahren finden Sie in der Dokumentation zum Server unter https://www.dell.com/support.

Verschiedenes

Das Upgrade schlägt bei der Aktualisierung auf die neueste Version fehl.

ANMERKUNG: 3.30.30.30 ist die minimale iDRAC-Version, die für ein Upgrade auf 4.00.00.00/4.10.10.10 des späteren Builds erforderlich ist.

Nach dem Zurücksetzen von iDRAC werden in der iDRAC GUI möglicherweise nicht alle Werte angezeigt.

ANMERKUNG: Wenn Sie iDRAC aus irgendeinem Grund zurücksetzen, stellen Sie sicher, dass Sie mindestens zwei Minuten warten, nachdem Sie iDRAC zurückgesetzt haben, um Einstellungen in iDRAC aufzurufen oder zu ändern.

Wenn ein Betriebssystem installiert ist, wird der Hostname möglicherweise gar nicht angezeigt oder wird nicht automatisch geändert.

Es gibt zwei Szenarien:

- Szenario 1: iDRAC zeigt nicht den aktuellen Hostnamen nach der Installation eines Betriebssystems an. Sie müssen OMSA oder iSM zusammen mit iDRAC installieren, damit der aktuelle Hostname abgerufen wird.
- Szenario 2: iDRAC hatte einen Hostnamen für ein spezifisches Betriebssystem und es wurde ein anderes Betriebssystem installiert, es erscheint jedoch weiterhin der alte Hostname. Der Grund hierfür ist, dass der Hostname eine Informationen darstellt, die vom Betriebssystem kommt, iDRAC speichert nur diese Informationen. Nach Installation eines neuen Betriebssystems setzt iDRAC den Wert des Hostnamens nicht zurück. Neuere Betriebssystemversionen können den Hostnamen in iDRAC beim ersten Betriebssystemstart aktualisieren.

Wie kann man eine iDRAC-IP-Adresse für einen Blade-Server ausfindig machen?

ANMERKUNG: Die CMC-Option (Chassis Management Controller) ist nur für Blade-Server anwendbar.

- **Mit der CMC-Webschnittstelle**.

  Gehen Sie zu **Gehäuse** > **Server** > **Setup** > **Installieren**. In der angezeigten Tabelle wird die IP-Adresse für den Server angezeigt.

- **Über die virtuelle Konsole**: Starten Sie den Server neu, um die iDRAC-IP-Adresse im Rahmen eines POST zu betrachten. Wählen Sie in der OSCAR-Schnittstelle die „Dell CMC“-Konsole aus, um sich über eine lokale serielle Verbindung am CMC anzumelden. CMC-RACADM-Befehle können über diese Verbindung gesendet werden.

  Weitere Informationen zu CMC-RACADM-Befehlen finden Sie unter *Chassis Management Controller RACADM CLI – Handbuch* verfügbar unter https://www.dell.com/cmcmanuals.

Weitere Informationen zu iDRAC-RACADM-Befehlen finden Sie unter *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

- **Unter Verwendung lokaler RACADM**

  Verwenden Sie den folgenden Befehl: `racadm getsysinfo` Beispiel:

```
$ 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 verwenden**:

  Markieren Sie im Hauptmenü den Server, klicken Sie auf die Schaltfläche zum Markieren, wählen Sie den gewünschten Server aus und klicken Sie auf die Schaltfläche zum Markieren.

Wie kann man eine iDRAC-IP-Adresse für einen Blade-Server ausfindig machen?

ANMERKUNG: Die OME-Modular-Webschnittstellenoption gilt nur für MX-Plattformen.

- **Mit der OME-Modular-Webschnittstelle**:

  Navigieren Sie zu **Geräte** > **Rechner**. Wählen Sie den Rechnerschlitten aus. Die iDRAC-IP-Adresse wird als **Verwaltungs-IP** angezeigt.

- **OMM-Anwendung verwenden**: siehe *Dell EMC OpenManage Mobile – Benutzerhandbuch* verfügbar unter https://www.dell.com/openmanagemanuals
- **Verwendung der seriellen Verbindung**
- **Über die LC-Anzeige**: Markieren Sie im Hauptmenü den Server, klicken Sie auf die Schaltfläche zum Markieren, wählen Sie den gewünschten Server aus, und klicken Sie auf die Schaltfläche zum Markieren.

Wie kann man die CMC-IP-Adresse ausfindig machen, die sich auf den Blade-Server bezieht?

ANMERKUNG: Gilt nicht für MX-Plattformen.

- **Von der iDRAC-Webschnittstelle**:

  Gehen Sie zu **iDRAC-Einstellungen** > **CMC**. Auf der Seite **CMC-Zusammenfassung** wird die CMC-IP-Adresse angezeigt.

- **Von der virtuellen Konsole**:

  Wählen Sie in der OSCAR-Schnittstelle die „Dell CMC"-Konsole aus, um sich über eine lokale serielle Verbindung am CMC anzumelden. CMC-RACADM-Befehle können über diese Verbindung ausgegeben werden.

```
$ 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
```

ANMERKUNG: Sie können diesen Vorgang außerdem über den Remote-RACADM ausführen.

Weitere Informationen zu CMC-RACADM-Befehlen finden Sie unter *Chassis Management Controller RACADM CLI – Handbuch* verfügbar unter https://www.dell.com/cmcmanuals.

Weitere Informationen zu iDRAC-RACADM-Befehlen finden Sie unter *iDRAC-RACADM-CLI-Handbuch* verfügbar unter https://www.dell.com/idracmanuals.

So finden Sie die OME Modular-IP-Adresse

ANMERKUNG: Gilt nur für MX-Plattformen.

- **Von der iDRAC-Webschnittstelle**:

  Navigieren Sie zu **iDRAC-Einstellungen** > **Managementmodul**. Auf der Seite **Managementmodul** wird die OME Modular-IP-Adresse angezeigt.

Wie kann man die iDRAC-IP-Adresse für Rack- und Tower-Server ausfindig machen?

- **Von lokalem RACADM**:

  Verwenden Sie den Befehl `racadm getsysinfo`.

- **Über die LCD**:

  Verwenden Sie auf dem physikalischen Server zum Anzeigen der iDRAC-IP-Adresse die LCD-Navigationstasten. Gehen Sie zu **Setupansicht** > **Anzeigen** > **iDRAC-IP** > **IPv4** oder **IPv6** > **IP**.

- **Vom OpenManage Server Administrator**:

  Wechseln Sie in der Server Administrator-Web-Schnittstelle zu **Modulares Gehäuse** > **System-/Server-Modul** > **Hauptsystemgehäuse/Hauptsystem** > **Remote-Zugriff**.

Die iDRAC-Netzwerkverbindung funktioniert nicht.

Für Blade-Server:

- Stellen Sie sicher, dass das LAN-Kabel am CMC angeschlossen ist. (Nicht für MX-Plattformen)
- Stellen Sie sicher, dass NIC-Einstellungen, IPv4- oder IPv6-Einstellungen und entweder Statisch oder DHCP für das Netzwerk aktiviert sind.

Für Rack- und Tower-Server:

- Stellen Sie im freigegebenen Modus sicher, dass das LAN-Kabel mit der NIC-Schnittstelle verbunden ist, die mit einem Schraubenschlüsselsymbol gekennzeichnet ist.
- Stellen Sie im dedizierten Modus sicher, dass das LAN-Kabel mit der iDRAC-LAN-Schnittstelle verbunden ist.
- Stellen Sie sicher, dass NIC-Einstellungen, IPv4- und IPv6-Einstellungen und entweder „Statisch“ oder „DHCP“ für das Netzwerk aktiviert sind.

iDRAC nicht zugänglich im freigegebenen LOM

Auf iDRAC kann möglicherweise nicht zugegriffen werden, wenn es kritische Fehler im Host-BS gibt, z. B. einen BSOD-Fehler in Windows. Um auf iDRAC zuzugreifen, starten Sie den Host neu, um die Verbindung wiederherzustellen.

Shared LOM nicht funktionsfähig, nachdem Link Aggregation Control Protocol (LACP) aktiviert wurde.

Der Host-Betriebssystemtreiber für den Netzwerkadapter muss geladen werden, bevor LACP aktiviert wird. Wenn jedoch eine passive LACP-Konfiguration verwendet wird, kann das gemeinsame LOM funktionsfähig sein, bevor der Host-Betriebssystemtreiber geladen wird. Informationen zur LACP-Konfiguration finden Sie in der Switch-Dokumentation.

ANMERKUNG: Shared LOM IP von iDRAC ist im Pre-Boot-Zustand nicht zugänglich, wenn der Switch mit LACP konfiguriert ist.

Der Blade-Server wurde in das Gehäuse eingesetzt, der EIN-/AUS-Schalter wurde gedrückt, der Server konnte jedoch nicht eingeschaltet werden.

- iDRAC benötigt bis zu 2 Minuten zum Initialisieren, bevor der Server hochgefahren werden kann.
- Überprüfen Sie das Strombudget von CMC undOME-Modul (nur für MX-Plattformen). Das Gehäusestrombudget wurde möglicherweise überschritten.

Wie ruft man einen iDRAC-Administrator-Benutzernamen und das zugehörige Kennwort ab?

Sie müssen die Standardeinstellungen des iDRAC wiederherstellen. Weitere Informationen finden Sie unter Zurücksetzen des iDRAC auf die Standardeinstellungen auf Seite 358.

Wie kann man den Namen des Steckplatzes für das System in einem Gehäuse ändern?

ANMERKUNG: Gilt nicht für MX-Plattformen.

1. Melden Sie sich bei der CMC-Webschnittstelle an und gehen Sie zu **Gehäuse** > **Server** > **Setup** .
2. Geben Sie den neuen Namen für den Steckplatz in die Zeile für den Server ein und klicken Sie auf **Anwenden**.

Der iDRAC auf Blade-Server reagiert während des Startvorgangs nicht.

Enfernen Sie den Server und setzen Sie ihn erneut ein.

Überprüfen Sie die CMC (nicht für MX-Plattformen)OME Modular (gültig für MX-Plattformen)-Webschnittstelle, um zu sehen, ob iDRAC als aktualisierbare Komponente angezeigt wird. Ist dies der Fall, folgen Sie den Anweisungen unter Firmware über die CMC-Web-Schnittstelle aktualisieren auf Seite 84 Aktualisieren der Firmware.

ANMERKUNG: Diese Aktualisierungsfunktion gilt nicht für MX-Plattformen.

Wenn das Problem weiterhin besteht, setzen Sie sich mit dem technischen Support in Verbindung.

Beim Versuch, den verwalteten Server zu starten, ist die Betriebsanzeige grün, aber es ist kein POST bzw. kein Video vorhanden.

Dies kann eintreten, wenn einer oder mehrere der folgenden Zustände zutreffen:

- Speicher ist nicht installiert oder ist unzugänglich.
- Die CPU ist nicht installiert oder ist unzugänglich.
- Die Video-Riser-Karte fehlt oder ist falsch eingesteckt.

Weitere Informationen finden Sie, wenn Sie über die iDRAC-Webschnittstelle oder die Server-LC-Anzeige die Fehlermeldungen im iDRAC-Protokoll aufrufen.

Fehler beim Anmelden an der iDRAC-Webschnittstelle über Firefox Browser unter Linux oder Ubuntu. Kennwort kann nicht eingegeben werden.

Um dieses Problem zu beheben, installieren oder aktualisieren Sie den Firefox-Browser.

Kein Zugriff auf iDRAC über USB-NIC in SLES und Ubuntu

ANMERKUNG: Stellen Sie in SLES die iDRAC-Schnittstelle auf DHCP ein.

Verwenden Sie in Ubuntu das Netplan-Dienstprogramm zum Konfigurieren der iDRAC-Schnittstelle zum DHCP-Modus. So konfigurieren Sie DHCP:

1. Verwenden Sie `/etc/netplan/01-netcfg.yaml`.
2. Legen Sie „Ja“ für iDRAC-DHCP fest.
3. Wenden Sie die Konfiguration an.

Abbildung 5. Konfigurieren von iDRAC-Schnittstelle zum DHCP-Modus in Ubuntu

Modell, Hersteller und andere Eigenschaften werden nicht für eingebettete Netzwerkadapter in Redfish aufgeführt.

FRU-Details für eingebettete Geräte werden nicht angezeigt. Für Geräte, die auf der Hauptplatine eingebettet sind, gibt es kein FRU-Objekt. Daher wird die abhängige Eigenschaft nicht vorhanden sein.

31

Anwendungsszenarien

In diesem Abschnitt erhalten Sie Erläuterungen zum Navigieren zu bestimmten Abschnitten innerhalb des Handbuchs, um typische Anwendungsszenarien auszuführen.

Themen:

- Fehler auf einem Managed System beheben, auf das nicht zugegriffen werden kann
- Systeminformationen abrufen und Systemzustand bewerten
- Einrichten von Warnungen und Konfigurieren von E-Mail-Warnungen
- Anzeigen und Exportieren des Systemereignisprotokoll und Lifecycle-Protokolls
- Schnittstellen zum Aktualisieren der iDRAC-Firmware
- Ordnungsgemäßes Herunterfahren durchführen
- Neues Administratorbenutzerkonto erstellen
- Starten einer Server-Remote-Konsole und Mounten eines USB-Laufwerks
- Bare Metal-Betriebssystem über verbundenen virtuellen Datenträger und Remote-Dateifreigabe installieren
- Rack-Dichte verwalten
- Neue elektronische Lizenz installieren
- Übernehmen der E/A-Identitätskonfigurationseinstellungen für mehrere Netzwerkkarten bei einem Einzel-Host-System-Neustart

Fehler auf einem Managed System beheben, auf das nicht zugegriffen werden kann

Nach dem Eingang von Warnungen aus OpenManage Essentials, Dell Management Console oder einem lokalen Trap-Kollektor sind fünf Server in einem Rechenzentrum aufgrund von Problemen wie einem nicht mehr reagierenden Betriebssystem oder Server nicht mehr zugänglich. Es ist daher erforderlich, den Grund für diesen Fehler zu ermitteln, um den Fehler zu beheben und den Server über den iDRAC zu reaktivieren.

Bevor der Fehler in Bezug auf ein nicht zugreifbares System behoben werden kann, müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind:

- Bildschirm „Letzter Absturz“ ist aktiviert
- Warnungen auf iDRAC sind aktiviert

Um den Grund für den Fehler zu identifizieren, müssen Sie Folgendes auf der iDRAC-Web-Schnittstelle überprüfen und die Verbindung zum System wiederherstellen:

ANMERKUNG: Wenn Sie nicht auf die iDRAC-Webschnittstelle zugreifen können, gehen Sie zum Server, rufen Sie das LCD-Bedienfeld auf, notieren Sie sich die IP-Adresse oder den Host-Namen, und führen Sie von Ihrer Management-Station aus die folgenden Vorgänge über die iDRAC-Webschnittstelle aus:

- Server-LED-Status – Blinkt gelb oder leuchtet dauerhaft gelb.
- LCD-Bedienfeld auf der Frontblende oder Fehlermeldung – Gelbe LC-Anzeige oder Fehlermeldung.
- Das Betriebssystem-Image wird in der virtuellen Konsole angezeigt. Wenn das Image angezeigt wird, starten Sie das System über einen Warmstart neu und melden Sie sich wieder an. Wenn die Anmeldung erfolgreich war, ist der Fehler behoben.
- Bildschirm „Letzter Absturz“
- Capture-Video beim Startvorgang
- Absturzvideo-Capture
- Serverzustand – Rote *x*-Symbole für die Systemkomponenten, bei denen Fehler vorliegen.
- Speicher-Array-Status – Array möglicherweise offline oder ausgefallen
- Lifecycle-Protokoll für kritische Ereignisse in Bezug auf die Hardware und die Firmware auf dem System und die Protokolleinträge, die beim Systemabsturz erfasst wurden.
- Tech Support-Report erstellen und die erfassten Daten anzeigen.
- Verwenden Sie die vom iDRAC Service Module bereitgestellten Überwachungsfunktionen.

Systeminformationen abrufen und Systemzustand bewerten

So rufen Sie Systeminformationen ab und bewerten den Systemzustand:

- Gehen Sie in der iDRAC-Web-Schnittstelle zu **Overview (Übersicht)** > **Summary (Zusammenfassung)**, um die Systeminformationen anzuzeigen und auf verschiedene Links auf dieser Seite zur Bewertung des Systemzustands zuzugreifen. Sie können beispielsweise den Zustand des Gehäuselüfters überprüfen.
- Sie können außerdem die Gehäuseortungs-LED konfigurieren und auf der Basis der Farbe den Systemzustand bewerten.
- Wenn das iDRAC Service Module installiert ist, werden die Host-Informationen zum Betriebssystem angezeigt.

Einrichten von Warnungen und Konfigurieren von E-Mail-Warnungen

So richten Sie Warnungen ein und konfigurieren E-Mail-Warnungen:

1. Aktivieren Sie Warnungen.
2. Konfigurieren Sie die E-Mail-Warnung und markieren Sie die Schnittstellen.
3. Führen Sie einen Neustart aus, schalten Sie das Gerät aus, oder führen Sie einen Aus- und Einschaltvorgang auf dem Managed System durch.
4. Senden Sie die Testwarnung.

Anzeigen und Exportieren des Systemereignisprotokoll und Lifecycle-Protokolls

So zeigen Sie das Lifecycle-Protokoll und das Systemereignisprotokoll (SEL) an und exportieren diese:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Maintenance (Wartung)** > **System Event Logs (Systemereignisprotokolle)**, um das Systemereignisprotokoll anzuzeigen, und zu **Lifecycle Log (Lifecycle-Protokoll)**, um das Lifecycle-Protokoll anzuzeigen.

   ANMERKUNG: Das Systemereignisprotokoll wird auch im Lifecycle-Protokoll erfasst. Über die Filteroptionen können Sie das Systemereignisprotokoll anzeigen.

2. Exportieren Sie das Systemereignisprotokoll oder das Lifecycle-Protokoll im XML-Format an einem externen Speicherort (z. B. Management Station, USB, Netzwerkfreigabe). Alternativ können Sie die Remote-Systemprotokollierung aktivieren, damit alle in das Lifecycle-Protokoll geschriebenen Protokolle ferner gleichzeitig auf die konfigurierten Remote-Server geschrieben werden.
3. Wenn Sie das iDRAC-Servicemodul verwenden, exportieren Sie das Lifecycle-Protokoll in das Betriebssystemprotokoll.

Schnittstellen zum Aktualisieren der iDRAC-Firmware

Verwenden Sie zum Aktualisieren der iDRAC-Firmware die folgenden Schnittstellen:

- iDRAC-Web-Schnittstelle
- Redfish API
- RACADM-CLI (iDRAC_) und CMC (gilt nicht für MX-Plattformen))
- Dell Update Package (DUP)
- CMC (gilt nicht für MX-Plattformen)OME-Modul (gilt nur für MX-Plattformen)-Webschnittstelle
- Lifecycle-Controller–Remote-Dienste
- Lifecycle-Controller
- Dell Remote Access Configuration Tool (DRACT)

Ordnungsgemäßes Herunterfahren durchführen

Um ein ordnungsgemäßes Herunterfahren durchzuführen, gehen Sie in der iDRAC-Webschnittstelle zu einem der folgenden Standorte:

- Wählen Sie unter **Dashboard** die Option **Graceful Shutdown** (Ordentliches Herunterfahren) und klicken Sie auf **Apply** (Anwenden).

Weitere Informationen finden Sie in der *iDRAC-Online-Hilfe*.

Neues Administratorbenutzerkonto erstellen

Sie können das standardmäßige lokale Administratorkonto ändern oder ein neues Administratorkonto erstellen. Informationen zum Ändern des lokalen Administratorkontos finden Sie unter Einstellungen für lokales Administratorkonto ändern.

Weitere Informationen zum Erstellen eines neuen Administratorkontos finden Sie in den folgenden Abschnitten:

- Lokale Benutzer konfigurieren
- Konfigurieren von Active Directory-Benutzern
- Generische LDAP-Benutzer konfigurieren

Starten einer Server-Remote-Konsole und Mounten eines USB-Laufwerks

So starten Sie die Remote-Konsole und mounten ein USB-Laufwerk:

1. Schließen Sie ein USB-Flash-Laufwerk (mit dem erforderlichen Image) an die Management Station an.
2. Starten Sie die virtuelle Konsole über die folgende Methode über die iDRAC-Webschnittstelle:
   - Gehen Sie zu **Dashboard** > **Virtual Console (Virtuelle Konsole)** und klicken Sie auf **Launch Virtual Console (Virtuelle Konsole starten)**.

   Daraufhin wird der **Viewer für die virtuelle Konsole** angezeigt.
3. Klicken Sie im Menü **File** (Datei) auf **Virtual Media (Virtueller Datenträger)** > **Launch Virtual Media (Virtuellen Datenträger starten)**.
4. Klicken Sie auf **Image hinzufügen**, und wählen Sie das Image aus, das sich auf dem USB-Flash-Laufwerk befindet. Das Image wird zur Liste der verfügbaren Laufwerke hinzugefügt.
5. Wählen Sie das Laufwerk aus, dem das Image zugeordnet werden soll. Das Image auf dem USB-Flash-Laufwerk wird dem verwalteten System zugeordnet.

Bare Metal-Betriebssystem über verbundenen virtuellen Datenträger und Remote-Dateifreigabe installieren

Siehe Abschnitt Betriebssystem über eine Remote-Dateifreigabe bereitstellen.

Rack-Dichte verwalten

Vor der Installation zusätzlicher Server in einem Rack müssen Sie die verbleibende Kapazität im Rack ermitteln.

So bewerten Sie die Kapazität eines Rack in Bezug auf das Hinzufügen weiterer Server:

1. Zeigen Sie die aktuellen und historischen Stromverbrauchsdaten für die Server an.
2. Aktivieren Sie auf der Basis dieser Daten, der Stromversorgungsinfrastruktur und der Kühlungsbeschränkungen für das System die Strombegrenzungsrichtlinie, und legen Sie die Strombegrenzungswerte fest.

   ANMERKUNG: Es wird empfohlen, die Begrenzung nahe des zulässigen Höchstwertes festzulegen und über diese begrenzte Stufe dann die verbliebene Kapazität auf dem Rack für das Hinzufügen weiterer Server zu bestimmen.

Neue elektronische Lizenz installieren

Weitere Informationen finden Sie unter Lizenzvorgänge.

Übernehmen der E/A-Identitätskonfigurationseinstellungen für mehrere Netzwerkkarten bei einem Einzel-Host-System-Neustart

Wenn Sie über mehrere Netzwerkkarten eines Servers verfügen, der Teil einer Storage Area Network (SAN)-Umgebung ist, und Sie andere virtuelle Adressen- sowie Initiator- und Ziel-Konfigurationseinstellungen auf diese Karten anwenden möchten, verwenden Sie die Funktion zur E/A-Identitätsoptimierung, um den Zeitaufwand für die Konfiguration dieser Einstellungen zu reduzieren. Führen Sie dazu folgende Schritte durch:

1. Stellen Sie sicher, dass BIOS, iDRAC und Netzwerk-Karten auf die neueste Firmware aktualisiert sind.
2. Aktivieren Sie die E/A-Identitätsoptimierung.
3. Exportieren Sie die Serverkonfigurationsprofildatei von iDRAC.
4. Bearbeiten Sie die E/A-Identitätsoptimierungseinstellungen in der SCP-Datei.
5. Importieren Sie die SCP-Konfigurationsdatei nach iDRAC.