iDRAC10 Benutzerhandbuch

1.10.xx Series

Dezember 2024
Rev. A00

Hinweise, Vorsichtshinweise und Warnungen

ANMERKUNG: HINWEIS enthält wichtige Informationen, mit denen Sie Ihr Produkt besser nutzen können.

VORSICHT: ACHTUNG deutet auf mögliche Schäden an der Hardware oder auf den Verlust von Daten hin und zeigt, wie Sie das Problem vermeiden können.

WARNUNG: WARNUNG weist auf ein potenzielles Risiko für Sachschäden, Verletzungen oder den Tod hin.

© 2024 Dell Inc. oder deren Tochtergesellschaften. Alle Rechte vorbehalten. Dell Technologies, Dell und andere Marken sind Marken von Dell Inc. oder deren Tochtergesellschaften. Andere Marken sind Marken der jeweiligen Eigentümer.

Revisionsverlauf

Tabelle 1. Revisionsverlauf

Datum	Dokumentversionen	Beschreibung der Änderungen
Dezember 2024	A00	iDRAC10 Version 1.10.17.00

Inhaltsverzeichnis

Revisionsverlauf....3

Kapitel 1: Übersicht über den iDRAC....16
Vorteile der iDRAC-Verwendung....16
Wichtige Funktionen....17
Neue Funktionen hinzugefügt....19
Firmware-Version 1.10.17.00....19
Veraltete Funktionen....19
Funktionen, die in dieser ersten iDRAC10-Version nicht unterstützt werden....19
Verwendung dieses Benutzerhandbuchs....23
Unterstützte Webbrowser....23
Unterstützte Betriebssysteme und Hypervisoren....23
iDRAC-Lizenzen....23
Lizenztypen....23
Methoden zum Erwerb von Lizenzen....24
Erwerben von Lizenzschlüssel vom Dell digitalen Schließfach....24
Lizenzvorgänge....24
Lizenzierte Funktionen in iDRAC10....25
Schnittstellen und Protokoll für den Zugriff auf iDRAC....31
iDRAC-Schnittstelleninformationen....32
Weitere nützliche Dokumente....33
Kontaktaufnahme mit Dell....34
Zugriff auf Dokumente auf der Dell Supportwebsite....34
Zugriff auf die Redfish API....34

Kapitel 2: Anmelden bei iDRAC....35
Kennwortänderung erzwingen (FCP)....35
Anmelden als lokaler Nutzer, Active Directory-Nutzer oder LDAP-Nutzer bei iDRAC....36
Bei iDRAC über eine Smartcard als lokaler Nutzer anmelden....37
Bei iDRAC über eine Smartcard als Active Directory-Nutzer anmelden....38
Bei iDRAC über die einmalige Anmeldung anmelden....38
Bei iDRAC SSO über die iDRAC-Weboberfläche anmelden....38
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....39
Einfache Zwei-Faktor-Authentifizierung (einfache 2FA)....39
RSA SecurID 2FA....40
Systemzustand anzeigen....41
Anmeldung beim iDRAC mit Authentifizierung mit öffentlichem Schlüssel....42
Mehrere iDRAC-Sitzungen....42
Sicheres Standardkennwort....42
Lokales Zurücksetzen des standardmäßigen iDRAC-Kennworts....43
Remote-Zurücksetzen des standardmäßigen iDRAC-Kennworts....43
Ändern des standardmäßigen Anmeldekennworts....43

Ändern des standardmäßigen Anmeldekennworts über die Weboberfläche....43
Ändern des standardmäßigen Anmeldekennworts mithilfe von RACADM....43
Ändern des standardmäßigen Anmeldekennworts unter Verwendung des Dienstprogramms für iDRAC-Einstellungen....44
Aktivieren oder Deaktivieren der standardmäßigen Kennwortwarnungsmeldung....44
IP-Blockierung....44
Aktivieren und Deaktivieren eines Betriebssystems für iDRAC-Passthrough unter Verwendung der Weboberfläche....45
Warnungen über RACADM aktivieren oder deaktivieren....46

Kapitel 3: Open Server Manager 3.0.x....47
Vorbereiten des Systems auf ein OSM-Update....47
Aktualisieren von OSM auf dem System....47

Kapitel 4: Managed System einrichten....48
iDRAC-IP-Adresse einrichten....48
iDRAC-IP-Adresse über das Dienstprogramm für die iDRAC-Einstellungen einrichten....49
Auto-Ermittlung....52
Konfigurieren von Servern und Serverkomponenten mithilfe der automatischen Konfiguration....53
Verwenden von Hash-Kennwörtern für mehr Sicherheit....59
Einstellungen für lokales Administratorkonto ändern....60
Standort für das Managed System einrichten....60
Standort des Managed System über die Web-Schnittstelle einrichten....61
Standort für Managed System über RACADM einrichten....61
Standort für Managed System über das Dienstprogramm für die iDRAC-Einstellungen einrichten....61
Systemleistung und Stromverbrauch optimieren....61
Thermische Einstellungen über die iDRAC-Webschnittstelle ändern....62
Thermische Einstellungen unter Verwendung von RACADM ändern....64
Thermische Einstellungen unter Verwendung vom Dienstprogramm für die iDRAC-Einstellungen ändern....67
Ändern von PCIe Airflow-Einstellungen über die iDRAC-Weboberfläche....68
Management Station einrichten....68
Per Remote auf iDRAC zugreifen....68
Konfigurieren von unterstützten Webbrowsern....68
Konfiguration von Mozilla Firefox....69
Web-Browser für die Verwendung der virtuellen Konsole konfigurieren....69
Lokalisierte Versionen der Webschnittstelle anzeigen....70
Aktualisieren der Gerätefirmware....71
Firmware über die iDRAC-Webschnittstelle aktualisieren....74
Planung automatischer Firmware-Aktualisierungen....75
Aktualisieren der Gerätefirmware über RACADM....75
Firmware über DUP aktualisieren....75
Firmware über Remote-RACADM aktualisieren....76
Neustartfreie Updates....77
Anzeigen und Managen von gestuften Aktualisierungen....77
Anzeigen und Managen gestufter Aktualisierungen unter Verwendung von RACADM....78
Anzeigen und Managen gestufter Aktualisierungen unter Verwendung der iDRAC-Weboberfläche....78
Rollback der Geräte-Firmware durchführen....78
Rollback für die Firmware über die iDRAC-Webschnittstelle durchführen....79
Rollback der Firmware über RACADM durchführen....79
Easy Restore (Einfache Wiederherstellung)....79

iDRAC über andere Systemverwaltungs-Tools überwachen....80
Unterstützung des Serverkonfigurationsprofils – Import und Export....80
Importieren des Serverkonfigurationsprofils mithilfe der iDRAC-Webschnittstelle....81
Exportieren des Server-Konfigurationsprofils mithilfe der iDRAC-Webschnittstelle....82
Secure Boot-Konfiguration über BIOS-Einstellungen oder F2....82
BIOS recovery....83
iDRAC wiederherstellen....84

Kapitel 5: Datenverarbeitungseinheit (Data Processing Unit, DPU)....85

Kapitel 6: Plug-in-Management....87
Installieren eines Plug-ins....87
Deinstallieren eines Plug-ins....87
Ein Plug-in neu starten....87
Plug-in aktivieren oder deaktivieren....88
Anzeigen der Plug-in-Details....88

Kapitel 7: iDRAC konfigurieren....89
iDRAC-Informationen anzeigen....90
iDRAC-Informationen über die Webschnittstelle anzeigen....90
iDRAC-Informationen über RACADM anzeigen....91
Netzwerkeinstellungen ändern....91
Netzwerkeinstellungen über einen lokalen RACADM ändern....91
Netzwerkeinstellungen über die Weboberfläche ändern....91
Chiffresammlungs-Auswahl....92
Chiffresammlungs-Auswahl mithilfe von RACADM konfigurieren....92
Chiffresammlungs-Auswahl über die iDRAC-Weboberfläche konfigurieren....92
Modus FIPS (Konfiguration)....93
Deaktivieren des FIPS-Modus....93
FIPS-Modus aktivieren....93
Dienste konfigurieren....93
Dienste über RACADM konfigurieren....94
Services unter Verwendung der Weboberfläche konfigurieren....94
iLKM-Funktionen....95
SEKM-Funktionen....96
Aktivieren oder Deaktivieren der HTTPS-Umleitung....97
Verwenden des VNC-Client für die Remote-Server-Verwaltung....97
Konfigurieren von VNC-Server unter Verwendung der iDRAC-Webschnittstelle....98
VNC-Server unter Verwendung von RACADM konfigurieren....98
Einrichten von VNC Viewer mit SSL-Verschlüsselung....98
Einrichten von VNC Viewer ohne SSL-Verschlüsselung....98
Das Konfigurieren von Zeitzone und NTP....99
Konfigurieren von Zeitzone und NTP unter Verwendung der iDRAC- Web-Schnittstelle....99
Konfigurieren von Zeitzone und NTP unter Verwendung von RACADM....99
Erstes Startlaufwerk einstellen....99
Erstes Startgerät über die Web-Schnittstelle einrichten....100
Erstes Startgerät über RACADM festlegen....100
Einstellen des ersten Startgeräts unter Verwendung der virtuellen Konsole....100
Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough....100

Unterstützte Betriebssysteme für USB-NIC....101
Aktivieren und Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung von RACADM....102
Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung des Dienstprogramms für iDRAC-Einstellungen....102
Aktivieren und Deaktivieren eines Betriebssystems für iDRAC-Passthrough unter Verwendung der Weboberfläche....103
Zertifikate abrufen....103
SSL-Serverzertifikate....104
Neue Zertifikatsignierungsanforderung erstellen....105
Automatische Zertifikatregistrierung....106
Serverzertifikat hochladen....106
Serverzertifikat anzeigen....107
Hochladen eines nutzerdefinierten Signaturzertifikats....107
Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat herunterladen....108
Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat herunterladen....108
Mehrere iDRACs über RACADM konfigurieren....109
Zugriff zum Ändern der iDRAC-Konfigurationseinstellungen auf einem Host-System deaktivieren....110

Kapitel 8: Delegierte Autorisierung mithilfe von OAuth 2.0....111

Kapitel 9: Anzeigen von Informationen zu iDRAC und zum Managed System....112
Zustand und Eigenschaften des Managed System anzeigen....112
Konfigurieren der Assetnachverfolgung....112
System-Bestandsaufnahme anzeigen....113
Anzeigen der Systemkomponenten....115
Überwachen des Leistungsindex für CPU, Arbeitsspeicher und Eingabe-/Ausgabemodule....116
Überwachen des Leistungsindex für CPU-, Storage- und I/O-Module über RACADM....117
Überwachen des Leistungsindex für CPU-, Storage- und I/O-Module über die Weboberfläche....117
Lesen von Firmware- und Hardwarebeständen....117
Durchführen und Überprüfen des System-/Komponentenkonfigurationsstatus....118
Durchführen und Überprüfen des Firmwareupdatestatus....118
Erkennung eines Servers im Ruhezustand....119
GPU-Verwaltung (Beschleuniger)....119
Überprüfen der Frischlufttauglichkeit des Systems....122
Temperaturverlaufsdaten anzeigen....122
Temperaturverlaufsdaten über RACADM anzeigen....123
Anzeigen der Temperaturverlaufsdaten über die iDRAC-Webschnittstelle....123
Konfigurieren des Warnungsschwellenwerts für die Einlasstemperatur....124
Konfigurieren der Warnschwelle für die Einlasstemperatur über die Webschnittstelle....124
Anzeigen der auf dem Host-Betriebssystem verfügbaren Netzwerkschnittstellen....124
Anzeigen der auf dem Hostbetriebssystem verfügbaren Netzwerke über RACADM....125
Anzeigen von verfügbaren Netzwerkschnittstellen auf dem Host-Betriebssystem über die Webschnittstelle....125
Anzeigen und Beenden von iDRAC-Sitzungen....125
Beenden von iDRAC-Sitzungen über RACADM....125
Beenden der iDRAC-Sitzungen über die Webschnittstelle....125

Kapitel 10: Einrichten der iDRAC-Kommunikation....126
Mit iDRAC über eine serielle Verbindung über ein DB9-Kabel kommunizieren....127

BIOS für serielle Verbindung konfigurieren... 127
Serielle RAC-Verbindung aktivieren... 127
Grundlegenden seriellen IPMI-Verbindungs- und -Terminalmodus aktivieren... 128
Von der seriellen RAC-Verbindung auf die serielle Konsolenverbindung bei Verwendung eines DB9-Kabels umschalten... 130
Von der seriellen RAC-Verbindung auf die serielle Konsole umschalten... 130
Von der seriellen Konsole auf die serielle RAC-Verbindung umschalten... 130
Mit iDRAC über IPMI SOL kommunizieren... 130
BIOS für serielle Verbindung konfigurieren... 131
iDRAC für die Verwendung von SOL konfigurieren... 131
Unterstütztes Protokoll aktivieren... 132
Mit iDRAC über IPMI über LAN kommunizieren... 135
IPMI über LAN mithilfe des Dienstprogramms für die iDRAC-Einstellungen konfigurieren... 135
IPMI über LAN mithilfe von RACADM konfigurieren... 136
IPMI über LAN mithilfe der Weboberfläche konfigurieren... 136
Remote-RACADM aktivieren oder deaktivieren... 136
Remote-RACADM über RACADM aktivieren oder deaktivieren... 137
Remote-RACADM über die Weboberfläche aktivieren oder deaktivieren... 137
Lokalen RACADM deaktivieren... 137
Konfigurieren von Linux während des Starts in RHEL für die serielle Konsole... 137
Anmeldung an der virtuellen Konsole nach dem Start aktivieren... 138
Konfigurieren des seriellen Terminals in RHEL... 139
Steuern von GRUB von der seriellen Konsole... 140
Unterstützte SSH-Verschlüsselungssysteme... 141
Authentifizierung mit öffentlichen Schlüsseln für SSH verwenden... 141
SSH-Schlüssel hochladen... 142
SSH-Schlüssel löschen... 143
SSH-Schlüssel anzeigen... 144

Kapitel 11: Nutzerrollen und Nutzerkonten... 145
iDRAC-Benutzerrollen und -Berechtigungen... 145
Empfohlene Zeichen in Nutzernamen und Kennwörtern... 146
Erstellen von Benutzerrollen... 146
Lokale Nutzer konfigurieren... 147
Erstellen von lokalen Nutzern über die iDRAC UI... 147
Lokale Nutzer über RACADM konfigurieren... 147
Konfigurieren von Active Directory-Nutzern... 149
Voraussetzungen für die Verwendung der Active Directory-Authentifizierung für iDRAC... 149
Unterstützte Active Directory-Authentifizierungsmechanismen... 150
Übersicht des Standardschema-Active Directory... 151
Active Directory-Standardschema konfigurieren... 152
Übersicht über Active Directory mit erweitertem Schema... 154
Active Directory mit erweitertem Schema konfigurieren... 156
iDRAC-Nutzer und -Berechtigungen zu Active Directory hinzufügen... 160
Konfiguration des Active Directory mit erweitertem Schema unter Verwendung von RACADM... 162
Active Directory mit erweitertem Schema unter Verwendung der iDRAC-Webschnittstelle konfigurieren... 163
Active Directory-Einstellungen testen... 163
Generische LDAP-Nutzer konfigurieren... 164
Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mittels RACADM... 164
Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mit der iDRAC-Webschnittstelle... 164

Einstellungen für LDAP-Verzeichnisdienst testen....165
Testen der Einstellungen des LDAP-Verzeichnisdienstes über die iDRAC-Webschnittstelle....165

Kapitel 12: Systemkonfigurations-Sperrmodus....166

Kapitel 13: iDRAC für die einfache Anmeldung oder Smart Card-Anmeldung konfigurieren....168
Voraussetzungen für die einmalige Active Directory-Anmeldung oder die Smartcard-Anmeldung....168
iDRAC im Domänennamensystem registrieren....168
Active Directory-Objekte erstellen und Berechtigungen bereitstellen....169
iDRAC-SSO-Anmeldung für Active Directory-Nutzer konfigurieren....169
Erstellen eines Nutzers in Active Directory für SSO....169
Kerberos Keytab-Datei generieren....170
iDRAC-SSO-Anmeldung für Active Directory-Nutzer über die Webschnittstelle konfigurieren....171
iDRAC SSO-Anmeldung für Active Directory-Nutzer über RACADM konfigurieren....171
Management Station-Einstellungen....171
Smartcard-Anmeldung aktivieren oder deaktivieren....171
Smart Card-Anmeldung über die Web-Schnittstelle aktivieren oder deaktivieren....172
Smartcard-Anmeldung über RACADM aktivieren oder deaktivieren....172
Smart Card-Anmeldung über das Dienstprogramm für die iDRAC-Einstellungen aktivieren oder deaktivieren....172
Konfigurieren von Smart Card-Anmeldung....172
iDRAC-Smart-Card-Anmeldung für Active Directory-Nutzer konfigurieren....172
iDRAC-Smart Card-Anmeldung für lokale Nutzer konfigurieren....173
Anmelden mit Smartcard....174

Kapitel 14: iDRAC für das Versenden von Warnungen konfigurieren....175
Warnungen aktivieren und deaktivieren....175
Warnungen über die Web-Schnittstelle aktivieren oder deaktivieren....175
Warnungen über RACADM aktivieren oder deaktivieren....176
Warnungen über das Dienstprogramm für iDRAC-Einstellungen aktivieren oder deaktivieren....176
Ereigniswarnungen einrichten....176
Ereigniswarnungen über die Web-Schnittstelle einrichten....177
Ereigniswarnungen über RACADM einrichten....177
Alarmwiederholungsereignis einrichten....177
Alarmwiederholungsereignis über RACADM einrichten....177
Einrichten eines Alarmwiederholungsereignisses über die iDRAC-Weboberfläche....177
Ereignismaßnahmen festlegen....178
Ereignismaßnahmen über die Web-Schnittstelle einrichten....178
Ereignismaßnahmen über RACADM einrichten....178
Einstellungen für E-Mail-Warnungs-SNMP-Trap oder IPMI-Trap konfigurieren....178
IP-basierte Warnziele konfigurieren....178
Konfigurieren von E-Mail-Benachrichtigungen....180
Konfigurieren von Redfish-Ereignissen....182
Remote-Systemprotokollierung konfigurieren....182
Remote-Systemprotokollierung über die Web-Schnittstelle konfigurieren....183
Remote-Systemanmeldung über RACADM konfigurieren....183
IDs für Warnungsmeldung....183
CPU- und GPU-Leckerkennung....185
Konfigurieren der CPU-Leckerkennung....185

Konfigurieren der GPU-Leckerkennung....185

Kapitel 15: Managen von Protokollen....187
Systemereignisprotokoll anzeigen....187
Systemereignisprotokoll über RACADM anzeigen....187
Systemereignisprotokoll über die Web-Schnittstelle anzeigen....187
Anzeigen des Systemereignisprotokolls unter Verwendung des Dienstprogramms für die iDRAC-Einstellungen....188
Lifecycle-Protokoll anzeigen....188
Lifecycle-Protokoll über die Web-Schnittstelle anzeigen....189
Lifecycle-Protokoll über RACADM anzeigen....189
Exportieren der Lifecycle Controller-Protokolle....189
Exportieren von Lifecycle Controller-Protokollen mit RACADM....189
Exportieren von Lifecycle Controller-Protokollen mithilfe der Webschnittstelle....189
Verhindern eines Überlaufs von Lebenszyklusprotokollen....190
Arbeitsanmerkungen hinzufügen....190
Lifecycle-Protokoll anzeigen....190
Lifecycle-Protokoll über die Web-Schnittstelle anzeigen....191

Kapitel 16: Stromversorgung im iDRAC überwachen und managen....192
Stromversorgung überwachen....192
Überwachen des Leistungsindex für CPU-, Storage- und I/O-Module über die Weboberfläche....193
Überwachen des Leistungsindex für CPU-, Storage- und I/O-Module über RACADM....193
Festlegen des Warnungsschwellenwerts für den Stromverbrauch....193
Einrichten der Warnschwelle für den Stromverbrauch über die Webschnittstelle....193
Ausführen von Stromsteuerungsvorgängen....194
Ausführen von Stromsteuerungsvorgängen über die Web-Schnittstelle....194
Stromsteuerungsvorgänge über RACADM ausführen....194
Strombegrenzung....194
Strombegrenzungsrichtlinie anzeigen und konfigurieren....194
Netzteiloptionen konfigurieren....195
Netzteiloptionen über die Web-Schnittstelle konfigurieren....196
Netzteiloptionen über RACADM konfigurieren....196
Netzteiloptionen über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren....196
Netzschalter aktivieren oder deaktivieren....196
Multi-Vektor-Kühlung....197
Konfigurieren der Netzstromwiederherstellung....198

Kapitel 17: Direkte iDRAC-Updates....199

Kapitel 18: Durchführen einer Bestandsaufnahme, Überwachung und Konfiguration von Netzwerkgeräten....200
Bestandsaufnahme und Überwachung von FC-HBA-Geräten....200
Überwachung von FC-HBA-Geräten unter Verwendung von RACADM....200
FC-HBA-Geräte mit der Webschnittstelle überwachen....201
Bestandsaufnahme für Netzwerkgeräte erstellen und Netzwerkgeräte überwachen....201
Netzwerkgeräte über RACADM überwachen....201
Netzwerkgeräte über die Web-Schnittstelle überwachen....201
Verbindungsanzeige....201

Bestandsaufnahme und Überwachung von SFP-Transceiver-Geräten..... 203
SFP-Transceiver-Geräte mit der Webschnittstelle überwachen.....203
SFP-Transceiver-Geräte unter Verwendung von RACADM überwachen..... 204
Telemetrie-Streaming.....204
Metrische Berichtsdefinition.....206
Auslöser..... 206
Serielle Datenerfassung.....207
Dynamische Konfiguration von virtuellen Adressen, Initiator- und Speicherziel-Einstellungen.....207
Anzeigen der Unterstützung für die I/O-Identitätsoptimierung auf der Weboberfläche..... 208
Virtuelle oder Remote-zugewiesene Adresse und Persistenzrichtlinien-Verhalten, wenn iDRAC auf Remote-zugewiesenen Address-Modus oder Konsolenmodus eingestellt ist..... 208
Systemverhalten für FlexAddress und E/A-Identität.....210
Aktivieren oder Deaktivieren der E/A-Identitätsoptimierung.....210
SSD-Verschleiß-Schwellenwerte..... 211
Konfigurieren von SSD-Verschleißschwellenwert-Warnfunktionen über die Web-Schnittstelle.....211
SSD-Verschleißschwellen-Alarmfunktionen mit RACADM konfigurieren.....212
Konfigurieren der Einstellungen für die Beständigkeitsrichtlinie..... 212
Konfigurieren der Richtlinieneinstellungen für die Persistenz über die iDRAC-Webschnittstelle..... 213
Konfigurieren der Persistenz-Richtlinieneinstellungen über RACADM..... 213
Standardwerte für iSCSI-Initiator und Speicherziel.....213

Kapitel 19: Managen von Storage-Geräten..... 215
Zum Verständnis von RAID-Konzepten..... 217
Was bedeutet RAID?..... 217
Datenspeicher-Organisation zur erhöhten Verfügbarkeit und Leistung..... 218
Auswählen der RAID-Stufen.....219
RAID-Level-Leistung vergleichen.....224
Unterstützte Controller.....225
Unterstützte Gehäuse.....225
Übersicht über die unterstützten Funktionen für Speichergeräte.....225
Bestandsaufnahme für Storage-Geräte erstellen und Storage-Geräte überwachen..... 228
Netzwerkgeräte über die Weboberfläche überwachen..... 228
Speichergerät über RACADM überwachen..... 229
Überwachen der Verwendung der Rückwandplatine über das Dienstprogramm für iDRAC-Einstellungen....229
Anzeigen der Speichergerätetopologie..... 229
Managen von physischen Festplatten.....230
Zuweisen oder Aufheben der Zuweisung von dezidierten Hotspares.....230
Konvertieren einer physischen Festplatte in den RAID- und Nicht-RAID-Modus..... 231
Konvertierung von physischen Laufwerken in den RAID-fähigen oder nicht-RAID-Modus mithilfe der iDRAC-Weboberfläche..... 231
Konvertierung von physikalischen Festplatten in den RAID-fähigen oder nicht-RAID-Modus mithilfe von RACADM.....231
Löschen physischer Laufwerke.....231
Löschen von SED/ISE-Gerätedaten.....232
Löschen eines SED-Geräts unter Verwendung von RACADM..... 233
Löschen von SED/ISE-Gerätedaten über die Webschnittstelle.....233
Physisches Laufwerk neu erstellen.....234
Verwalten von virtuellen Festplatten.....234
Erstellen von virtuellen Laufwerken..... 234
Bearbeiten von Cache-Richtlinien für virtuelle Laufwerke.....236

Löschen von virtuellen Festplatten....237
Überprüfen der Übereinstimmung der virtuellen Festplatte....237
Initialisieren von virtuellen Festplatten....237
Verschlüsseln der virtuellen Laufwerke....238
Zuweisen oder Aufheben der Zuweisung von dezidierten Hotspares....239
Managen von virtuellen Festplatten über RACADM....241
Managen von virtuellen Laufwerken über die Webschnittstelle....241
RAID-Konfigurationsfunktionen....243
Managen von Controllern....244
Wechseln des Controller-Modus....250
HBA-Adaptervorgänge....251
Überwachen der voraussagenden Fehleranalyse auf Festplatten....252
Controller-Vorgänge im nicht-RAID-Modus oder HBA-Modus....252
Ausführen der RAID-Konfigurations-Jobs auf mehreren Storage-Controllern....252
Beibehaltenen Cache managen....253
Managen von PCIe-SSDs....253
Erstellen einer Bestandsaufnahme für und Überwachen von PCIe-SSDs....253
Vorbereiten auf das Entfernen von PCIe-SSDs....254
Löschen von PCIe-SSD-Gerätedaten....255
Managen von Gehäusen oder Rückwandplatinen....257
Konfigurieren des Rückwandplatinen-Modus....257
Einrichten des SGPIO-Modus....260
Gehäusebestandsnamen festlegen....260
Gehäuse-Bestands-Tag festlegen....260
Auswählen des Betriebsmodus zum Anwenden von Einstellungen....261
Anzeigen und Anwenden von ausstehenden Vorgängen....261
Storage-Geräte – Szenarien des Anwenden-Vorgangs....262
Blinken oder Beenden des Blinkens der Komponenten-LEDs....264
Blinken oder Beenden des Blinkens der Komponenten-LEDs über die Webschnittstelle....264
Blinken der Komponenten-LEDs über RACADM ein- oder ausschalten....264
Softwareneustart....265

Kapitel 20: BIOS-Einstellungen....266
BIOS Live Scan....267
BIOS-Wiederherstellung und Hardware-RoT (Root of Trust)....268

Kapitel 21: Virtuelle Konsole konfigurieren und verwenden....269
Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen....270
Konfigurieren einer virtuellen Konsole....271
Virtuelle Konsole über die Weboberfläche konfigurieren....271
Virtuelle Konsole über RACADM konfigurieren....271
Vorschau der virtuellen Konsole....271
Virtuelle Konsole starten....271
Virtuelle Konsole über die Weboberfläche starten....272
Virtuelle Konsole über eine URL starten....272
Anzeige der virtuellen Konsole verwenden....272
Verwenden der virtuellen Konsole....273

Kapitel 22: Verwenden des iDRAC Service Module....276

Installieren des iDRAC Service Module....276
Installieren des iDRAC Service Module von iDRAC Core....277
Installieren des iDRAC Service Module von iDRAC Enterprise....277
Unterstützte Betriebssysteme für das iDRAC Service Module....277
Überwachungsfunktionen des iDRAC-Servicemoduls....277
Verwendung des iDRAC Servicemoduls über die iDRAC-Weboberfläche....281
Verwenden des iDRAC Servicemodul von RACADM....281

Kapitel 23: Verwenden des Typ-C-USB-Dual-Mode-Ports für das Servermanagement....282
Konfigurieren von iDRAC über das Server-Konfigurationsprofil auf dem USB-Gerät....282
Konfigurieren der Type-C-USB-Dual-Mode-Porteinstellungen über die iDRAC-UI....282
Zugriff auf die iDRAC-Schnittstelle über eine direkte USB-Verbindung....283
Importieren des Serverkonfigurationsprofils von einem USB-Gerät....283
LC-Protokolle und Fehlermeldungen während USB-bezogener Vorgänge....284

Kapitel 24: Verwendung von Quick Sync 2....286
Konfigurieren von iDRAC Quick Sync 2....286
Konfigurieren von iDRAC Quick Sync 2-Einstellungen über RACADM....287
Konfigurieren von iDRAC Quick Sync 2-Einstellungen über die Weboberfläche....287
Konfigurieren der iDRAC Quick Sync 2-Einstellungen über das Dienstprogramm für die iDRAC-Einstellungen....287
Verwenden vom Mobilgerät zum Anzeigen von iDRAC-Informationen....287

Kapitel 25: Virtuelle Datenträger managen....288
Unterstützte Laufwerke und Geräte....289
Virtuellen Datenträger konfigurieren....289
Konfigurieren von virtuellen Datenträgern über die iDRAC-Webschnittstelle....289
Virtuelle Datenträger über RACADM konfigurieren....289
Virtuelle Datenträger über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren....289
Status des verbundenen Datenträgers und Systemantwort....290
Auf virtuellen Datenträger zugreifen....290
Virtuellen Datenträger über die virtuelle Konsole starten....290
Virtuelle Datenträger ohne virtuelle Konsole starten....291
Images von virtuellen Datenträgern hinzufügen....291
Details zum virtuellen Gerät anzeigen....291
USB-Gerät zurücksetzen....292
Virtuelles Laufwerk zuordnen....292
Zuordnung für virtuelles Laufwerk aufheben....293
Einmalstart für virtuelle Datenträger aktivieren....294
Remote-Dateifreigabe....294
Startreihenfolge über das BIOS festlegen....296
Zugriff auf Treiber....297

Kapitel 26: Betriebssysteme bereitstellen....298
Betriebssystem über eine Remote-Dateifreigabe bereitstellen....298
Managen der Remote-Dateifreigaben....298
Remote-Dateifreigabe über die Web-Schnittstelle konfigurieren....298
Remote-Dateifreigabe über RACADM konfigurieren....300
Betriebssystem über virtuelle Datenträger bereitstellen....301

Betriebssystem über mehrere Festplatten bereitstellen....302

Kapitel 27: Fehler auf Managed System über iDRAC beheben....303
Diagnosekonsole verwenden....303
iDRAC zurücksetzen und iDRAC auf Standardeinstellungen zurücksetzen....303
Planen von Automatischer Remote-Diagnose....304
Planen der automatisierten Remote-Diagnose und Exportieren der Ergebnisse über RACADM....304
POST-Codes anzeigen....305
Videos zum Startvorgang und zur Absturzerfassung anzeigen....305
Konfigurieren der Videoerfassungs-Einstellungen....306
Protokolle anzeigen....306
Bildschirm „Letzter Systemabsturz“ anzeigen....306
Anzeigen des Systemstatus....306
Status der LE-Anzeige auf der Frontblende des Systems anzeigen....306
Anzeigen für Hardwareprobleme....307
Systemzustand anzeigen....307
iDRAC-Neustart....307
Zurücksetzen des iDRAC über RACADM....308
Zurücksetzen des iDRAC über die iDRAC-Webschnittstelle....308
Löschen von System- und Nutzerdaten....308
Zurücksetzen des iDRAC auf die Standardeinstellungen....309
Zurücksetzen von iDRAC auf die Standardwerkseinstellungen unter Verwendung der iDRAC-Webschnittstelle....309
Zurücksetzen von iDRAC auf die Standardwerkseinstellungen unter Verwendung des Dienstprogramms für iDRAC-Einstellungen....309

Kapitel 28: Integration von SupportAssist im iDRAC....311
SupportAssist....311
SupportAssist....311
Erfassungsprotokoll....311
Generieren der SupportAssist-Erfassung....311
Manuelles Generieren der SupportAssist-Erfassung unter Verwendung der iDRAC-Webschnittstelle....312
Erfassungsprotokoll....313

Kapitel 29: Häufig gestellte Fragen....314
Betriebssystem....314
Active Directory....315
iDRAC Service Module....317
Netzwerksicherheit....318
RACADM....319
Benutzerdefinierte Absender-E-Mail-Konfiguration für iDRAC-Warnmeldungen....320
Smartcard-Anmeldung....320
SNMP-Authentifizierung....320
Single Sign-On....320
Speichergeräte....321
System-Ereignisprotokoll....321
Virtuelle Konsole....322
Virtueller Datenträger....324
Sonstiges....326
Proxyservereinstellungen....329

Standardkennwort dauerhaft auf „calvin“ setzen....330

Kapitel 30: Anwendungsfallszenarien....331
Fehler auf einem Managed System beheben, auf das nicht zugegriffen werden kann....331
Systeminformationen abrufen und Systemzustand bewerten....332
Einrichten von Warnungen und Konfigurieren von E-Mail-Warnungen....332
Anzeigen und Exportieren des Systemereignisprotokolls und Lifecycle-Protokolls....332
Schnittstellen zum Aktualisieren der iDRAC-Firmware....332
Ordnungsgemäßes Herunterfahren....332
Neues Administratorbenutzerkonto erstellen....333
Starten der Server-Remote-Konsole und Mounten eines USB-Laufwerks....333
Bare Metal-Betriebssystem über verbundenen virtuellen Datenträger und Remote-Dateifreigabe installieren....333
Rack-Dichte managen....333
Neue elektronische Lizenz installieren....334
Anwenden der E/A-Identitätskonfigurationseinstellungen für mehrere Netzwerkkarten über Einzel-Host-Systemneustart....334

Index....335

1

Übersicht über den iDRAC

Der Integrated Dell Remote Access Controller (iDRAC) wurde entwickelt, um die Arbeit von Systemadministratoren produktiver zu gestalten und die allgemeine Verfügbarkeit von Dell Servern zu verbessern. iDRAC weist auf Systemprobleme hin, unterstützt Sie bei der Ausführung von Remote-Verwaltungsaufgaben und reduziert die Notwendigkeit, physisch auf das System zuzugreifen.

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

ANMERKUNG: Das iDRAC-Verhalten ist möglicherweise nicht konsistent, wenn iDRAC mit Hardware verwendet wird, die nicht von Dell stammt.

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

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

Der iDRAC wird in den folgenden Varianten angeboten:

- IDRAC Core – standardmäßig auf allen Servern verfügbar
- iDRAC Enterprise – für alle Servermodelle verfügbar
- iDRAC Datacenter – für alle Servermodelle verfügbar

Themen:

- Vorteile der iDRAC-Verwendung
- Wichtige Funktionen
- Neue Funktionen hinzugefügt
- Veraltete Funktionen
- Funktionen, die in dieser ersten iDRAC10-Version nicht unterstützt werden
- Verwendung dieses Benutzerhandbuchs
- Unterstützte Webbrowser
- iDRAC-Lizenzen
- Lizenzierte Funktionen in iDRAC10
- Schnittstellen und Protokoll für den Zugriff auf iDRAC
- iDRAC-Schnittstelleninformationen
- Weitere nützliche Dokumente
- Kontaktaufnahme mit Dell
- Zugriff auf Dokumente auf der Dell Supportwebsite
- Zugriff auf die Redfish API

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.

Wichtige Funktionen

Zentrale Funktionen von iDRAC:

ANMERKUNG: Einige der Funktionen sind nur mit einer iDRAC Enterprise- oder Datacenter-Lizenz verfügbar. Informationen zu den verfügbaren Funktionen der verschiedenen Lizenzen finden Sie in Lizenzierte Funktionen in iDRAC10. Eine Liste der Funktionen, die in iDRAC10-Version 1.10.17.00 nicht unterstützt werden, finden Sie im Abschnitt Funktionen, in dieser Version nicht unterstützt werden.

Bestandsaufnahme und Überwachung

- Telemetriedaten-Streaming
- Zustand verwalteter Server anzeigen
- Netzwerkadapter zur Bestandsaufnahme und Überwachung und Speichersubsysteme (PERC und Direct Attached Storage) 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.
- Anzeigen von verfügbaren Netzwerk-Schnittstellen auf Hostbetriebssystemen.
- iDRAC10 bietet bessere Überwachungs- und -Managementfunktionen mit Quick Sync 2. Auf Ihrem Android- oder iOS-Mobilgerät muss die OpenManage Mobile-App konfiguriert sein.

Bereitstellung

- Managen von iDRAC-Netzwerkeinstellungen.
- Virtuelle Konsole und virtuelle Datenträger konfigurieren und verwenden
- Betriebssysteme mit Remote-Dateifreigabe und virtuellem Datenträger bereitstellen
- Aktivieren Sie die automatische Ermittlung.
- Führen Sie Änderungen an der Serverkonfiguration mithilfe der SCP-Funktion (Server Configuration Profile) durch. Weitere Informationen finden Sie im Referenzhandbuch für SCP.
- Konfigurieren der Persistenzrichtlinie für virtuelle Adressen, Initiator und Storage-Ziele
- 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 globalen 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 geplanten Zeitpunkt oder als einen ausstehenden Stapelvorgang an, der als Teil des einzelnen Jobs ausgeführt werden soll.

Update

- Managen 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.
- Managen gestufter Aktualisierungen.
- Zugriff auf die iDRAC-Schnittstelle über direkte USB-Verbindung.
- Konfigurieren von iDRAC unter Verwendung von Serverkonfigurationsprofilen auf einem USB-Gerät.

Wartung und Troubleshooting

- Stromversorgungsbezogene Vorgänge ausführen und Stromverbrauch überwachen
- Optimierte Systemleistung und Stromverbrauch durch Ändern der thermischen Einstellungen.
- 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
- Out-of-band-Performancemonitoring und Ausgabe von Warnmeldungen an den Leistungsindex von CPU, Storage und E/A-Modulen.
- Konfigurieren des Warnungsschwellenwerts für Einlasstemperatur und Stromverbrauch.
- Verwenden Sie das iDRAC-Servicemodul 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
  - Aktivieren von In-Band-iDRAC-SNMP-Warnmeldungen.
  - Zugriff auf iDRAC über das Host-BS (experimentelle Funktion)
  - Bestücken der Windows Management Instrumentation (WMI)-Informationen
  - Integration mit SupportAssist-Erfassung. Dies gilt nur, wenn das iDRAC-Servicemodul Version 2.0 oder höher installiert ist.

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 Technologies empfiehlt die Verwendung des dedizierten Gigabit-Ethernet-Anschlusses, der auf 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 Nutzer 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 einen Bereich mit Sicherheitsfunktionen, darunter:

- Nutzerdefinierte Signaturzertifikate für Secure Socket Layer (SSL).
- Signierte Firmwareupdates
- Nutzerauthentifizierung 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 Nutzer
- SNMPv3-Authentifizierung für Nutzerkonten, 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 jeder iDRAC-Veröffentlichung hinzugefügt wurden.

Firmware-Version 1.10.17.00

In iDRAC-Version 1.10.17.00 wurden iDRAC folgende Funktionen hinzugefügt:

- Verbesserte Sicherheit mit dediziertem Sicherheitsprozessor:
  - Verbesserte Sicherheitsleistung
  - Integrierte Root-of-Trust-Zertifizierung (RoT), Bestätigung auf Geräteebene und Verschlüsselung.
  - Stärkere Verschlüsselungsalgorithmen
- Aktualisierte Benutzeroberfläche:
  - Konsistentes Benutzererlebnis über alle Dell Technologies-Konsolen hinweg
  - Vereinfachte Schnittstelle
  - Einfachere Navigation
- Vereinfachte Lizenzstruktur in PowerEdge der 17. Generation
- Erstellen benutzerdefinierter iDRAC-Nutzerrollen
- Netzstromwiederherstellung durch iDRAC gesteuert (wurde in früheren Generationen im BIOS verwaltet)

Veraltete Funktionen

Die folgenden Funktionen sind in iDRAC10 veraltet:

- Group Manager
- WS-Verwaltung
- TLS 1.1
- vFlash

Funktionen, die in dieser ersten iDRAC10-Version nicht unterstützt werden

Die folgenden Funktionen werden in den iDRAC10-Firmwareversionen 1.1x nicht unterstützt.

Tabelle 2. Nicht unterstützte Funktionen

Funktion	Funktion
iDRAC-GUI	iDRAC-GUI-Unterstützung für andere internationale Sprachen
	Lokaler RACADM (BS bandintern)
	Remote-RACADM
	iDRAC-Tools
	Seriell – RAC seriell
	Lifecycle-Controller-UI

Tabelle 2. Nicht unterstützte Funktionen (fortgesetzt)

Funktion	Funktion
	Seriell – IPMI seriell
ANMERKUNG: Auf RACADM CLI kann über die SSH-Schnittstelle zugegriffen werden.	
Netzwerke und Konnektivität	IP-Blockierung
	IP-Bereich
	iDRAC Direct (USB) SCP-Konfiguration
	Quick Sync
	Ansicht „Netzwerkanbindung“
Fernverwaltung	Seriell über LAN mit SSH
	Virtuelle Ordner
	Remote-Dateifreigabe
	Qualität/Bandbreiten-Kontrolle
	Virtuelle Konsolenzusammenarbeit (bis zu sechs Nutzer gleichzeitig)
	Chat über virtuelle Konsole
	Virtuelle Zwischenablage
	Assetnachverfolgung
	Nachverfolgung der Verwendung auf dem Markt (MUT)
	Software Development Kit (SDK)
	Virtueller Datenträger – Einzelsitzung
iDRAC-Service-Moduls (iSM)	iDRAC-Hardware-Reset und andere Funktionen
	Netzwerkinformationen
	IBIA
	Virtuelles Aus- und Einschalten
	Vorbereitung zur Entfernung
	iDRAC SSO
	Details zum Betriebssystem
	Chipsatz-SATA-Überwachung
	Software-RAID
	Lifecycle-Controller-Protokollreplikation
	Bandinternes SNMP
	SupportAssist-Integration
	SDS Event Co-Relation
	iSM Installation
Warnmeldungen	Redfish Lifecycle-Ereignisse (RLCE)
	Remote-Syslog – unsicher
	Remote-Syslog – sicher
	Telemetrie-Streaming

Tabelle 2. Nicht unterstützte Funktionen (fortgesetzt)

Funktion	Funktion
	Telemetrie- Kennzahlenberichte
	Telemetrie-Auslöser
	ISM OS Metric Injection-Funktionen für Telemetrie
Plattformmanagement	Memory SDPM
	Memory NVDIMM
	Bandexterne Leistungsüberwachung
	Erkennung eines Servers im Ruhezustand
	Überwachung der Flüssigkeitskühlung
Strom und thermisch	Strombegrenzung
	Stromüberwachung – Leistungsmesser in Echtzeit
	Echtzeit-Stromdiagramme
	Historische Stromzähler
	OME Power Manager-Plug-in-Integration
	Eingangsstrombegrenzung
	Frischluft
	ASHERE
	Kundenspezifische Ablufttemperatur
	Temperatur-Diagramme
	Soundcap 1.0
	Luftstromverbrauch des Systems, benutzerdefinierte PCIe-Einlasstemperatur
	PCIe-Luftstrom-Anpassung
Storage Management	Externes Gehäusemanagement
	Secure-Enterprise-Key-Manager (SEKM) und iDRAC Local Key Management (iLKM)
	HBA-Echtzeit-Bestandsaufnahme und -Überwachung
	HBA-bereitgestellte Bestandsaufnahme
Kommunikationsmanagement	DPU-Echtzeit-Bestandsaufnahme, -Überwachung und -Konfiguration
	DPU-bereitgestellte Bestandsaufnahme und Konfiguration
	Virtuelle Adressverwaltung
	DPU-/SmartNIC-Funktionen
	FC-Echtzeit-Bestandsaufnahme und -Überwachung
	FC-bereitgestellte Bestandsaufnahme und Konfiguration
Accelerator-Management	FPGA-bereitgestellte Bestandsaufnahme
	FPGA-Echtzeit-Bestandsaufnahme, -Stromversorgung und -Temperatur
Bereitstellung der Serverkonfiguration	Treiberpaket
	Server-Konfigurationsprofil-Repository-Aktualisierung

Tabelle 2. Nicht unterstützte Funktionen (fortgesetzt)

Funktion	Funktion
	Serverkonfigurationsprofil – BS-Bereitstellung
	Lokale Konfiguration
	Zero-Touch-Konfiguration
Systemupdate	Katalogupdate
	Integrierte Update-Tools
	Automatische Aktualisierung
Werk, Diagnose, Dienste und Protokolle	Zurücksetzen des iDRAC auf die Standardeinstellungen
	Secure Erase
	Absturzbildschirm-Video – mit Agent
	Absturzbildschirm-Capture
	Serielle Datenprotokolle
	Absturzvideo-Erfassung – ohne Agent
	Arbeitsanmerkungen
	Remote-Syslog für Warnmeldungen
Authentifizierung und Autorisierung	Lokale/r NutzerIn – reserviertes Konto
	Verzeichnisdienste
	Active Directory – Standardschema
	Active Directory – Erweitertes Schema
	Single Sign-On (SSO)
	Zwei-Faktor-Authentifizierung (2FA) – Smartcard
	Zwei-Faktor-Authentifizierung (2FA) – einfach
	Secure Shell Authentifizierung mit öffentlichem Schlüssel (SSH PKA)
	RSA Multi-Faktor-Authentifizierung (RSA MFA)
	OAuth
	OpenID verbinden
Sicherheit	SSL-Zertifikat Benutzerdefiniertes Signierungszertifikat
	SSL-Zertifikat – Automatische Zertifikatregistrierung
	FIPS 140-2/FIPS 3
	Benutzerdefiniertes Banner für Sicherheits-Policy
	IP-Blockierung/Denial-of-Service (DOS)-Schutz
	QuickSync 2.0 zusätzliche Sicherheit
	System-Sperrmodus
	IP-Bereichsfilterung
	Nutzerdefinierte Verschlüsselungszeichenfolge
	Lokale Konfiguration
	iDRAC-Netzwerk – 802.1x-Sicherheit
	BIOS-Livescan

Tabelle 2. Nicht unterstützte Funktionen (fortgesetzt)

Funktion	Funktion
Temperaturmanagement	PCIe-Luftstrom-Anpassung (LFM)
	Benutzerdefinierte Abluftsteuerung
	Benutzerdefinierte Delta-T-Steuerung
	Nutzerdefinierte PCIe-Einlasstemperatur
	System-Luftstromverbrauch
Sonstiges	Adaptive ICA

Verwendung dieses Benutzerhandbuchs

Nutzeranweisungen

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

1. 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.
2. RACADM – Hier ist der RACADM-Befehl bzw. das zu verwendende Objekt enthalten. Weitere Informationen finden Sie im **Referenzhandbuch für iDRAC10 RACADM CLI** auf der Dell Support-Website.
3. Das Dienstprogramm für die iDRAC-Einstellungen - Hier sind nur die Task-bezogenen Informationen enthalten. Informationen zu den Feldern und Optionen finden Sie in der **Online-Hilfe zum Dienstprogramm für die 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**).
4. Redfish – Hier sind nur die Task-bezogenen Informationen enthalten. Weitere Informationen zu den Feldern und Optionen finden Sie im **Referenzhandbuch für iDRAC10 Redfish-API** im Entwicklerportal.

Unterstützte Webbrowser

Eine Liste der unterstützten Versionen finden Sie in den **iDRAC10-Versionshinweisen** auf der Dell Support-Website.

Unterstützte Betriebssysteme und Hypervisoren

Eine Liste der unterstützten Betriebssystem- und Hypervisor-Versionen finden Sie in den **iDRAC10-Versionshinweisen** auf der Dell Support-Website.

iDRAC-Lizenzen

IDRAC-Funktionen sind basierend auf dem Lizenztyp verfügbar. Die iDRAC Core-Lizenz ist standardmäßig installiert. Die iDRAC Enterprise-Lizenz ist als Upgrade verfügbar und kann 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 iDRAC10.

Lizenztypen

Die iDRAC-Standardlizenz ist standardmäßig auf Ihrem System verfügbar. Die iDRAC Enterprise- und Datacenter-Lizenzen umfassen alle lizenzierten Funktionen und können jederzeit erworben werden. Die folgenden Upsell-Typen sind verfügbar:

- 30-Tage-Testlizenz – Testlizenzen gelten für eine bestimmte Zeit ab dem Moment, in dem das System mit Strom versorgt wird. Diese Lizenz kann nicht verlängert werden.
- Dauerlizenz – Die Lizenz ist an die Service-Tag-Nummer gebunden und damit dauerhaft.

In der folgenden Tabelle sind die Standardlizenzen aufgeführt, die für die folgenden Systeme verfügbar sind:

Tabelle 3. Standardlizenzen

iDRAC Core-Lizenz	iDRAC Enterprise-Lizenz	iDRAC Datacenter-Lizenz
• Für alle Server verfügbar. • Bietet wichtige Core-Systemmanagementfunktionen.	• Verfügbar als Upselling auf allen Servern • Umfasst alle Core-, Automatisierungs-, virtuelle Konsolen- und Sicherheitsfunktionen. • Im Paket mit Lizenzen für Secure Enterprise Key Management (SEKM) und Secure Component Verification (SCV).	• Verfügbar als Upselling auf allen Servern • Umfasst alle Core- und Enterprise-Funktionen. • Umfasst wichtige Funktionen wie Telemetrie und Temperaturmanagement. • Umfasst fortschrittliche Accelerators (GPU und DPU), Systemmanagement und fortschrittliche Luft- und Flüssigkeitskühlung.

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 Supportcenter 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, 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.

- 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.

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 RACADM managen

Lizenzverwaltung

1. Um Lizenzen über RACADM zu managen, verwenden Sie den Unterbefehl **license**.
2. Weitere Informationen finden Sie unter RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller

Lizenzen über die iDRAC-Weboberfläche managen

Um Lizenzen über die iDRAC-Webschnittstelle zu verwalten, navigieren Sie zu **Konfiguration** > **Lizenzen**.

Die Seite **Lizenzierung** zeigt die Lizenzen, die mit den Geräten verknüpft sind, oder solche Lizenzen, die zwar installiert sind, für die 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**.

Lizenzierte Funktionen in iDRAC10

In der folgenden Tabelle werden die iDRAC10-Funktionen aufgeführt, die gemäß der erworbenen Lizenz aktiviert sind:

Tabelle 4. Lizenzierte Funktionen in iDRAC10

Funktion	IDRAC 10-Core	iDRAC 10 Enterprise	IDRAC 10-Datacenter
Schnittstellen und Standards			
iDRAC RESTful-API und Redfish	Ja	Ja	Ja
IPMI 2,0	Ja	Ja	Ja
DCMI 1,5	Ja	Ja	Ja
Webbasierte GUI	Ja	Ja	Ja
RACADM-Befehlszeile (lokal/ Remote)	Ja	Ja	Ja
SSH	Ja	Ja	Ja

Tabelle 4. Lizenzierte Funktionen in iDRAC10 (fortgesetzt)

Funktion	IDRAC 10-Core	iDRAC 10 Enterprise	IDRAC 10-Datacenter
Serielle Umleitung	Ja	Ja	Ja
Network Time Protocol (NTP)	Ja	Ja	Ja
Konnektivität			
Gemeinsam genutzte NIC (LOM)	Ja	Ja	Ja
Dedizierte NIC	Ja	Ja	Ja
VLAN-Tagging	Ja	Ja	Ja
IPv4	Ja	Ja	Ja
IPv6	Ja	Ja	Ja
DHCP	Ja	Ja	Ja
DHCP mit Zero-Touch	Nein	Ja	Ja
Dynamisches DNS	Ja	Ja	Ja
BS-Pass-Through	Ja	Ja	Ja
iDRAC Direct (USB-Frontblende)	Ja	Ja	Ja
Verbindungsanzeige	Ja	Ja	Ja
DPU	Nein	Ja	Ja
Sicherheit			
Rollenbasierte Autorität	Ja	Ja	Ja
Lokale Nutzer	Ja	Ja	Ja
SSL-Verschlüsselung	Ja	Ja	Ja
Secure-Enterprise-Key-Management und iDRAC Local Key Manager	Nein	Ja (mit SEKM-Lizenz)	Ja (mit SEKM-Lizenz)
Blockieren von IP-Adressen	Nein	Ja	Ja
Verzeichnisdienste (AD, LDAP)	Nein	Ja	Ja
Zwei-Faktor-Authentifizierung (Smartcard)	Nein	Ja	Ja
Einmaliges Anmelden	Nein	Ja	Ja
PK-Authentifizierung (für SSH)	Ja	Ja	Ja
OAuth-Integration in webbasierte Authentifizierungsservices	Nein	Nein	Ja
Portbasierte Netzwerkzugriffskontrolle (IEEE 802.1x)	Nein	Nein	Ja
OpenID Connect für Dell Konsolen	Nein	Nein	Ja
FIPS 140-2	Ja	Ja	Ja
Secure Boot (UEFI) – Zertifikatsverwaltung	Ja	Ja	Ja
Systemsperre	Nein	Ja	Ja

Tabelle 4. Lizenzierte Funktionen in iDRAC10 (fortgesetzt)

Funktion	IDRAC 10-Core	iDRAC 10 Enterprise	IDRAC 10-Datacenter
Eindeutiges iDRAC-Standardkennwort	Ja	Ja	Ja
Nutzerdefinierte Banner für Sicherheitsrichtlinie – Anmeldeseite	Ja	Ja	Ja
Einfache Multifaktor-Authentifizierung	Nein	Ja	Ja
Automatische Zertifikatregistrierung (SSL-Zertifikate)	Nein	Nein	Ja
iDRAC Quick Sync 2 – optionale Authentifizierung für Lesevorgänge	Ja	Ja	Ja
iDRAC Quick Sync 2 – Nummer des Mobilgeräts zu LCL hinzufügen	Ja	Ja	Ja
Secure Erase	Ja	Ja	Ja
BIOS Live Scan	Nein	Ja	Ja
Automatische SSL-Zertifikatregistrierung	Nein	Ja	Ja
Zwei-Faktor-Authentifizierung von RSA SecurID (2FA)	Nein	Ja	Ja
Device RoT	Ja	Ja	Ja
Angriffserkennung	Ja	Ja	Ja
USB-Zugriffskontrolle	Ja	Ja	Ja
Secured Component Verification	Nein	Ja	Ja
Remote-Präsenz			
Betriebsschalter	Ja	Ja	Ja
Boot-Steuerung	Ja	Ja	Ja
Seriell-über-LAN	Ja	Ja	Ja
Virtueller Datenträger	Nein	Ja	Ja
Virtuelle Ordner	Nein	Ja	Ja
Remote-Dateifreigabe	Nein	Ja	Ja
HTML5-Zugriff auf die virtuelle Konsole	Nein	Ja	Ja
Virtuelle Konsole	Nein	Ja	Ja
Virtuelle Zwischenablage	Nein	Ja	Ja
VNC-Verbindung zum Betriebssystem	Nein	Ja	Ja
Qualität/Bandbreiten-Kontrolle	Nein	Ja	Ja
Virtuelle Konsolenzusammenarbeit (bis zu sechs Nutzer gleichzeitig)	Nein	Ja	Ja

Tabelle 4. Lizenzierte Funktionen in iDRAC10 (fortgesetzt)

Funktion	IDRAC 10-Core	iDRAC 10 Enterprise	IDRAC 10-Datacenter
Chat über virtuelle Konsole	Nein	Ja	Ja
HTTP/HTTPS-Unterstützung mit NFS/CIFS	Ja	Ja	Ja
Strom und thermisch			
Innovative Temperatursteuerung	Nein	Ja	Ja
Echtzeit-Leistungsmesser	Ja	Ja	Ja
Stromschwellenwerte und Warnungen	Ja	Ja	Ja
Echtzeit-Stromdiagramme	Nein	Ja	Ja
Historische Stromzähler	Nein	Ja	Ja
Strombegrenzung	Nein	Ja	Ja
Power Center-Integration	Nein	Ja	Ja
Temperatur-Diagramme	Ja	Ja	Ja
PCIe-Luftstrom-Anpassung (LFM)	Nein	Ja	Ja
Nutzerdefinierte Auslasssteuerung	Nein	Ja	Ja
Nutzerdefinierte Delta-T-Steuerung	Nein	Ja	Ja
System-Luftstromverbrauch	Nein	Ja	Ja
Nutzerdefinierte PCIe-Einlasstemperatur	Nein	Ja	Ja
Health			
Vollständig Agent-freies Monitoring	Ja	Ja	Ja
Temperaturüberwachung	Ja	Ja	Ja
Vorhergesagte Fehler-Überwachung	Ja	Ja	Ja
Unterstützung von SNMP v1, v2 und v3 (Traps und Gets)	Ja	Ja	Ja
E-Mail-Warnungen	Nein	Ja	Ja
Konfigurierbare Schwellenwerte	Ja	Ja	Ja
Überwachung des Lüfters	Ja	Ja	Ja
Überwachung der Stromversorgung	Ja	Ja	Ja
Speicherüberwachung	Ja	Ja	Ja
GPU	Nein	Ja	Ja
CPU-Überwachung	Ja	Ja	Ja
CPU- und GPU-Leckerkennung	Ja	Ja	Ja
Storage-Controller	Ja	Ja	Ja
NIC-Überwachung	Ja	Ja	Ja

Tabelle 4. Lizenzierte Funktionen in iDRAC10 (fortgesetzt)

Funktion	IDRAC 10-Core	iDRAC 10 Enterprise	IDRAC 10-Datacenter
Optisches Inventar	Ja	Ja	Ja
Optische Statistiken	Nein	Nein	Ja
Festplattenüberwachung	Ja	Ja	Ja
Out-of-Band-Performancemonitoring	Nein	Ja	Ja
Warnungen für übermäßige SSD-Abnutzung	Ja	Ja	Ja
Nutzerdefinierte Einstellungen für die Eintrittstemperatur	Ja	Ja	Ja
Serielle Datenprotokolle	Nein	Ja	Ja
SMART-Protokolle für Speicherlaufwerke	Nein	Ja	Ja
Erkennung spannungsloser Server	Nein	Ja	Ja
Telemetrie	Nein	Ja	Ja
Funktionszustands-Rollup	Ja	Ja	Ja
Update			
Remote-Agent-freies Update	Ja	Ja	Ja
Integrierte Update-Tools	Ja	Ja	Ja
Update über Repository	Ja	Ja	Ja
Update über Repository (automatisches Update)	Ja	Ja	Ja
Firmware-Aktualisierungen	Ja	Ja	Ja
Bereitstellung und Konfiguration			
Lokale Konfiguration über F2	Nein	Ja	Ja
Integrierte BS-Bereitstellungs-Tools	Ja	Ja	Ja
Integrierte Konfigurations-Tools	Ja	Ja	Ja
Auto-Ermittlung	Nein	Ja	Ja
Remote BS-Bereitstellung	Nein	Ja	Ja
Integriertes Treiberpaket	Ja	Ja	Ja
Vollständige Konfigurationsbestandsaufnahme	Ja	Ja	Ja
Inventar exportieren	Ja	Ja	Ja
Remote-Konfiguration	Ja	Ja	Ja
Berührungslose Konfiguration	Nein	Ja	Ja
Außerbetriebnahme oder Neuzuweisung des Systems	Ja	Ja	Ja
Server-Konfigurationsprofil exportieren	Ja	Ja	Ja

Tabelle 4. Lizenzierte Funktionen in iDRAC10 (fortgesetzt)

Funktion	IDRAC 10-Core	iDRAC 10 Enterprise	IDRAC 10-Datacenter
Server-Konfigurationsprofil importieren	Nein	Ja	Ja
Vorschau des Server-Konfigurationsprofils	Ja	Ja	Ja
BIOS-Konfiguration	Ja	Ja	Ja
Storage-Konfiguration	Nein	Ja	Ja
Diagnose, Dienste und Protokolle			
Assetnachverfolgung	Ja	Ja	Ja
Integrierte Diagnosetools	Ja	Ja	Ja
Teilersetzung	Ja	Ja	Ja
Einfache Wiederherstellung (Systemkonfiguration)	Ja	Ja	Ja
LED-Anzeigen zum Funktionszustand	Ja	Ja	Ja
iDRAC Quick Sync 2 (BLE/Wi-Fi-Hardware)	Ja	Ja	Ja
iDRAC Direkt (Vordere USB-Verwaltungsschnittstelle)	Ja	Ja	Ja
iDRAC Service Module (iSM) integriert	Ja	Ja	Ja
iSM in In-Band-Warnungsweiterleitung auf Konsolen	Ja	Ja	Ja
SupportAssist-Sammlung(integriert)	Ja	Ja	Ja
Absturzbildschirm-Erfassung	Ja	Ja	Ja
Absturzvideo-Erfassung	Nein	Ja	Ja
Agentenlose Absturzvideo-Erfassung (nur Windows)	Nein	Nein	Ja
Start-Erfassung	Ja	Ja	Ja
Remote-Zurücksetzung für iDRAC (erfordert iSM)	Ja	Ja	Ja
Virtuelles NMI	Ja	Ja	Ja
2FA	Nein	Ja	Ja
Gerätebestandsaufnahme und -überwachung	Ja	Ja	Ja
Arbeitsanmerkungen	Ja	Ja	Ja
BS-Watchdog	Ja	Ja	Ja
System-Ereignisprotokoll	Ja	Ja	Ja
Lifecycle-Protokoll	Ja	Ja	Ja
Erweiterte Protokollierung im Lifecycle Controller-Protokoll	Ja	Ja	Ja
Remote-Syslog	Nein	Ja	Ja

ANMERKUNG: Eine Liste der Funktionen, die in dieser Version nicht unterstützt werden, finden Sie im Abschnitt Funktionen, die in dieser Version nicht unterstützt werden.

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 5. 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 auf 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**.
iDRAC-Weboberfläche	Über die iDRAC-Weboberfläche können Sie iDRAC managen 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 Nutzerzugriff basiert auf Nutzerberechtigungen.
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 In-Band-IPMI-Hostschnittstelle mit iDRAC. Da es auf dem lokal verwalteten System installiert ist, müssen sich Nutzer zum Ausführen dieses Dienstprogramms beim Betriebssystem anmelden. Ein Nutzer muss über umfassende Administratorrechte verfügen oder ein Root-Nutzer sein, um dieses Dienstprogramm zu verwenden. ● Remote-RACADM ist ein Client-Dienstprogramm, das auf einer Management Station ausgeführt wird. Es verwendet die Out-of-Band-Netzwerkschnittstelle, um die RACADM-Befehle auf dem Managed System 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 Out-of-Band-Systemverwaltung verwendet. Sie ist für zahlreiche Server geeignet, von eigenständigen Servern bis hin zu Rack-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. Siehe das iDRAC-Handbuch zur Redfish-API.
USB-Port (Typ C)	Greifen Sie über den Type-C-USB-Anschluss auf den gekennzeichneten iDRAC zu.
SSH	Verwenden Sie SSH, um entweder RACADM-Befehle auszuführen oder eine Konsolenumleitungssitzung zu starten. Der SSH-Dienst ist standardmäßig für iDRAC aktiviert. Der SSH-Dienst kann in iDRAC deaktiviert werden. iDRAC

Tabelle 5. Schnittstellen und Protokoll für den Zugriff auf iDRAC (fortgesetzt)

Schnittstelle oder Protokoll	Beschreibung
	unterstützt nur SSH-Version 2 mit dem RSA-Host-Schlüssel-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**. **ANMERKUNG:** IPMI Version 1.5 wird nicht unterstützt.
NTLM	iDRAC bietet für NTLM die Authentifizierung, Integrität und Vertraulichkeit für Nutzer. NT LAN Manager (NTLM) ist eine Suite von Microsoft-Sicherheitsprotokollen und funktioniert in einem Windows-Netzwerk.
SMB	iDRAC unterstützt das SMB-Protokoll (Server Message Block). Dies ist ein Netzwerk-Dateifreigabeprotokoll. Die unterstützten SMB-Versionen sind 2.0 bis 3.11. SMBv1 wird nicht mehr unterstützt.
NFS	iDRAC unterstützt das Network File System (NFS). Dies ist ein verteiltes Dateisystemprotokoll, das es NutzerInnen ermöglicht, Remoteverzeichnisse auf den Servern bereitzustellen.
TFTP	iDRAC verwendet Trivial File Transfer Protocol (TFTP) für Firmwareupdates und Zertifikatinstallationen.
CIFS	iDRAC verwendet das CIFS-Protokoll (Common Internet File System), um Dateien remote freizugeben. CIFS mountet ISO- oder IMG-Image-Dateien von einer Netzwerkfreigabe als virtuelle Laufwerke auf das Betriebssystem des verwalteten Servers.
HTTP und HTTPS	iDRAC unterstützt sowohl HTTP (Hyper-Text Transfer Protocol) als auch HTTPS (Hyper-Text Transfer Protocol Secure) für das Remotemanagement von Dell Servern.

iDRAC-Schnittstelleninformationen

In der folgenden Tabelle sind die Ports aufgeführt, die für den Remotezugriff auf iDRAC durch die Firewall erforderlich sind. Dies sind die standardmäßigen Schnittstellen, auf die iDRAC für Verbindungen wartet. Optional können Sie die meisten Ports ändern. Informationen zum Ändern von Ports finden Sie unter Konfigurieren von Services.

Tabelle 6. Ports, die iDRAC für Verbindungen überwacht

Portnummer	Typ	Funktion	Konfigurierbarer Port	Maximale Verschlüsselungsebene
22	TCP	SSH	Ja	256-Bit-SSL
80	TCP	HTTP	Ja	Keine
161	UDP	SNMP-Agent	Ja	Keine
443	TCP	HTTPS	Ja	256-Bit-SSL
623	UDP	RMCP/RMCP+	Nein	128-Bit-SSL
5000	TCP	iDRAC zu iSM	Nein	256-Bit-SSL
5901	TCP	VNC	Ja	128-Bit-SSL
ANMERKUNG: Port 5901 wird geöffnet, wenn die VNC-Funktion aktiviert ist.				

In der folgenden Tabelle sind die Ports aufgeführt, die iDRAC als Client verwendet:

Tabelle 7. Von iDRAC als Client verwendete Ports

Portnummer	Typ	Funktion	Konfigurierbarer Port	Maximale Verschlüsselungsebene
25	TCP	SMTP	Ja	Keine
53	UDP	DNS	Nein	Keine

Tabelle 7. Von iDRAC als Client verwendete Ports (fortgesetzt)

Portnummer	Typ	Funktion	Konfigurierbarer Port	Maximale Verschlüsselungsebene
68	UDP	IP-Adresse des DHCP-assigned	Nein	Keine
69	TFTP	TFTP	Nein	Keine
123	UDP	Network Time Protocol (NTP)	Nein	Keine
162	UDP	SNMP-Trap	Ja	Keine
445	TCP	CIFS (Common Internet File System)	Nein	Keine
636	TCP	LDAP über SSL (LDAPS)	Nein	256-Bit-SSL
2049	TCP	NFS (Network File System)	Nein	Keine
3269	TCP	LDAPS für globalen Katalog (GK)	Nein	256-Bit-SSL
5353	UDP	mDNS	Nein	Keine
514	UDP	Remote-Syslog	Ja	Keine

Weitere nützliche Dokumente

Die iDRAC-UI unterstützt die integrierte **Online-Hilfe**, auf die Sie über die Registerkarte **Hilfe und Feedback** zugreifen können. Die **Onlinehilfe** enthält ausführliche Informationen zu den in der Webschnittstelle verfügbaren Feldern und den dazugehörigen Beschreibungen. Zusätzlich bieten die folgenden, auf der Dell Supportwebsite über **dell.com/support** verfügbaren Dokumente zusätzliche Informationen zum Setup und Betrieb des iDRAC auf Ihrem System.

- Das **iDRAC Redfish API-Handbuch** enthält Informationen über die Redfish API.
- Das RACADM-CLI-Handbuch für den Integrated Dell Remote Access Controller enthält Informationen zu den RACADM-Unterbefehlen, unterstützten Schnittstellen und iDRAC-Eigenschaftendatenbankgruppen sowie Objektdefinitionen.
- Unter *Systemmanagementübersicht-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 das Ermitteln von iDRAC-IP-Adressen in Ihrem Netzwerk und zum Ausführen von 1-zu-n-Firmwareupdates 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** enthalten aktuelle Änderungen am System oder der Dokumentation oder technischen Referenzmaterialen, die für erfahrene NutzerInnen oder TechnikerInnen gedacht sind.
- Die **Integrated Dell Remote Access Controller 10-Attributregistrierung** enthält die Details zu den Gruppen und Objekten in der iDRAC-Eigenschaftsdatenbank.

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**. Gewährleistungsinformationen 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

Dell bietet mehrere Online- und auf Telefon basierende Support- und Service-Optionen an. Die Verfügbarkeit ist je nach Land oder Region und Produkt unterschiedlich und bestimmte Services sind in Ihrer Region eventuell nicht verfügbar. Kontaktdaten für den Vertrieb, technischen Support und Customer Service von Dell finden Sie auf Kontaktaufnahme mit Dell.

ANMERKUNG: Wenn Sie nicht über eine aktive Internetverbindung verfügen, können Sie Kontaktinformationen auch auf Ihrer Auftragsbestätigung, dem Lieferschein, der Rechnung oder im Dell Produktkatalog finden.

Zugriff auf Dokumente auf der Dell Supportwebsite

Klicken Sie auf die folgenden Links, um auf die Dokumente auf der Dell Supportwebsite zuzugreifen:

- Dokumente zu Enterprise Systems Management und OpenManage Connections
- OpenManage-Dokumente
- Dokumente zu iDRAC und Lifecycle Controller
- Dokumente zu Serviceability Tools
- Dokumente zu Client Command Suite Systems Management

Zugriff auf Dokumente über die Produktsuche

1. Rufen Sie die Website Dell Support auf.
2. Geben Sie in das Suchfeld **Geben Sie ein Service-Tag**, **eine Seriennummer… ein** den Produktnamen ein. Zum Beispiel **PowerEdge** oder **iDRAC**. Eine Liste von passenden Produkten 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. Rufen Sie die Seite Dell Support auf.
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 anschließend 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 die Redfish API

Das Redfish API-Handbuch ist jetzt auf dem Dell API Marketplace verfügbar.

1. Gehen Sie zum Entwicklerportal
2. Klicken Sie auf **APIs durchsuchen** und klicken Sie dann auf **APIs**.
3. Klicken Sie unter iDRAC10 Redfish API auf **Mehr anzeigen**.

2

Anmelden bei iDRAC

Sie können sich beim iDRAC als iDRAC-Nutzer, als Microsoft Active Directory-Nutzer oder als Lightweight Directory Access Protocol-Nutzer (LDAP-Nutzer) anmelden. Sie können sich auch mit OpenID Connect und Single Sign-On oder Smartcard 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 Nutzernamen 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-UI unterstützt keine Browser Schaltflächen wie z. B. **Zurück**, **Vorwärts** oder **Aktualisieren**.
- Nachdem die iDRAC-IP-Adresse erkannt wurde, kann es maximal fünf Minuten dauern, bis Sie sich beim iDRAC anmelden. Wenn Sie sich nicht anmelden können, wenden Sie sich an das Team des technischen Supports.

Nutzerdefinierbare Sicherheitsbanner

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

Themen:

- Kennwortänderung erzwingen (FCP)
- Anmelden als lokaler Nutzer, Active Directory-Nutzer oder LDAP-Nutzer bei iDRAC
- 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
- Sicheres Standardkennwort
- Ändern des standardmäßigen Anmeldekennworts
- Aktivieren oder Deaktivieren der standardmäßigen Kennwortwarnungsmeldung
- IP-Blockierung
- Aktivieren und Deaktivieren eines Betriebssystems für iDRAC-Passthrough unter Verwendung der Weboberfläche
- 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 Nutzer 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-Nutzer 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.

Anmelden als lokaler Nutzer, Active Directory-Nutzer oder LDAP-Nutzer bei iDRAC

Stellen Sie vor der Anmeldung beim iDRAC über die Weboberfläche sicher, dass Sie einen unterstützten Webbrowser konfiguriert haben und dass das Nutzerkonto mit den erforderlichen Berechtigungen erstellt wurde.

Sie können den Nutzernamen, das Kennwort und die Zugriffsberechtigungen für neue oder vorhandene iDRAC-NutzerInnen mithilfe der Option **Nutzer hinzufügen/bearbeiten** in der iDRAC-Benutzeroberfläche konfigurieren.

Um NutzerInnen zu konfigurieren, verwenden Sie einen eindeutigen Nutzernamen. Dieser sollte 16 Zeichen lang sein, einschließlich Leerstellen. Die folgenden Zeichen sind zulässig:

- 0-9
- A-Z
- a-z
- Sonderzeichen: + %) > $ [| ! & = * . , - {] # (? < ; _ } I ^

Wird der Nutzername geändert, erscheint der neue Name erst nach der nächsten Nutzeranmeldung auf der Weboberfläche.

ANMERKUNG: Geben Sie vor und nach dem Nutzernamen keine Leerstelle ein.

Das Kennwortfeld kann bis zu 127 Zeichen lang sein. Die Zeichen sind maskiert. Die folgenden Zeichen sind zulässig:

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

ANMERKUNG: Zur Erhöhung der Sicherheit wird empfohlen, komplexe Kennwörter zu verwenden, die 8 oder mehr Zeichen sowie Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen enthalten. Es wird außerdem empfohlen, die Kennwörter regelmäßig zu ändern (sofern möglich).

ANMERKUNG: Der Nutzername unterscheidet nicht zwischen Groß- und Kleinschreibung für einen Active Directory-Nutzer. Beim Kennwort wird für alle Nutzer zwischen Groß- und Kleinschreibung unterschieden.

ANMERKUNG: Neben Active Directory openLDAP, openDS, Novell eDir werden auch die auf Fedora basierenden Verzeichnisdienste unterstützt.

ANMERKUNG: Die LDAP-Authentifizierung mit OpenDS wird unterstützt. Der DH-Schlüssel muss größer als 768 bit sein.

ANMERKUNG: Die RSA-Funktion kann für LDAP-NutzerInnen konfiguriert und aktiviert werden, aber RSA bietet keine Unterstützung, wenn LDAP im Microsoft Active Directory konfiguriert ist. Daher schlägt die LDAP-Nutzeranmeldung fehl. RSA wird nur für OpenLDAP unterstützt.

So melden Sie sich als lokaler Nutzer, Active Directory-Nutzer oder LDAP-Nutzer bei iDRAC an:

1. Öffnen Sie einen unterstützten Webbrowser.
2. Geben Sie in das Feld **Adresse** die folgende URL ein und drücken Sie die Eingabetaste: `https://[iDRAC-IP-address]`.

ANMERKUNG: Wenn die standardmäßige HTTPS-Portnummer (Port 443) geändert wird, geben Sie Folgendes ein: `https://[iDRAC-IP-address]:[port-number]` wobei `[iDRAC-IP-address]` die iDRAC-IPv4- oder -IPv6-Adresse und `[port-number]` die HTTPS-Portnummer ist.

Die Seite für die **Anmeldung** wird angezeigt.

3. Bei einem lokalen Nutzer:
   - Geben Sie in die Felder **Nutzername** und **Kennwort** Ihre Daten für den iDRAC-Nutzernamen und das Kennwort ein.
   - Wählen Sie aus dem Drop-Down-Menü **Domäne** die Option **Dieser iDRAC** aus.
4. Geben Sie für einen Active Directory-Nutzer in den Feldern **Nutzername** und **Kennwort** den Active Directory-Nutzernamen und das -Kennwort ein. Wenn Sie den Domänennamen als Teil des Nutzernamens festgelegt haben, wählen Sie **Dieser iDRAC** aus dem Drop-down-Menü aus. Das Format des Nutzernamens kann wie folgt lauten: <domain>\<username>, <domain>/<username> oder <user>@<domain>.

   Beispiele: dell.com\Markus_Bauer oder Markus_Bauer@dell.com.

   Die Active Directory-Domain aus dem Drop-down-Menü **Domain** zeigt die zuletzt verwendete Domain an.
5. Geben Sie für einen LDAP-Nutzer in die Felder **Nutzername** und **Kennwort** den LDAP-Nutzernamen und das -Kennwort ein. Der Domänenname ist für die LDAP-Anmeldung nicht erforderlich. Standardmäßig ist **Dieser iDRAC** im Drop-down-Menü ausgewählt.
6. Klicken Sie auf **Senden**. Sie werden mit den erforderlichen Nutzerberechtigungen beim iDRAC angemeldet.

   Wenn Sie sich mit Berechtigungen „Nutzer konfigurieren“ und den standardmäßigen Kontenanmeldeinformationen anmelden und die standardmäßige Kennwortwarnungsfunktion aktiviert ist, wird Ihnen die Seite **Standardmäßige Kennwortwarnung** angezeigt, die es Ihnen ermöglicht, das Kennwort auf einfache Art und Weise zu ändern.

Bei iDRAC über eine Smartcard als lokaler Nutzer anmelden

Bevor Sie sich als lokaler Nutzer 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 Nutzer an, die für die Verwendung der Smartcard konfiguriert wurden.

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 Smartcard als Active Directory-Nutzer anmelden

Bevor Sie sich über eine Smartcard als Active Directory-NutzerIn anmelden, müssen Sie folgendes sicherstellen:

- 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.
- Smartcard-Anmeldung aktivieren

So melden Sie sich über eine Smartcard als Active Directory-Nutzer bei iDRAC an:

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

   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 iDRAC-IP-Adresse und `[port number]` die HTTPS-Portnummer ist.

2. Legen Sie die Smartcard ein und klicken Sie auf **Anmeldung**.
   Sie werden daraufhin aufgefordert, die **PIN** für die Smartcard einzugeben.
3. Geben Sie die PIN ein und klicken Sie auf **Senden**.

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

   ANMERKUNG: Wenn der Smartcard-Nutzer in Active Directory vorhanden ist, wird kein Active Directory-Kennwort benötigt.

   ANMERKUNG: Bei Client-Workstations, die Teil der Active-Directory-Domain sind, beschränkt die Smartcard-Nutzung die Zertifikatskettentiefe auf 10. Die Verwendung von Smartcards auf Client-Workstations ohne Domain beschränkt jedoch nicht die Tiefe der Clientzertifikatketten.

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-Nutzerauthentifizierung (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-Weboberfläche anmelden

Bevor Sie sich beim iDRAC über Single Sign-On anmelden, stellen Sie Folgendes sicher:

- 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 standardmäßige HTTPS-Portnummer (Port 443) geändert wird, geben Sie Folgendes ein: `https://[FQDN address]:[port number]`, wobei `[FQDN address]` der iDRAC-FQDN (iDRACdnsname.domain.name) und `[port number]` die HTTPS-Portnummer ist.

   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.

Über Remote-RACADM auf iDRAC zugreifen

Remote und lokale RACADM, die Teil der RACADM-CLI sind, sind in der iDRAC10 1.10.17.00-Version nicht verfügbar. Sie können jedoch die RACADM-CLI über die iDRAC-SSH-Schnittstelle verwenden.

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Wenn die Managementstation 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. Beispiel: Der Speicherort für RHEL 64 Bit ist **/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

Remote oder lokale RACADM, die Teil von RACADM CLI sind, sind in der iDRAC10-Version 1.10.17.00 nicht verfügbar. Sie können RACADM CLI jedoch über die iDRAC-SSH-Schnittstelle verwenden. Weitere Informationen zum Zugriff auf iDRAC unter Verwendung des lokalen RACADM finden Sie unter RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Einfache Zwei-Faktor-Authentifizierung (einfache 2FA)

Um die Sicherheit zu verbessern, bietet iDRAC eine einfache 2-Faktor-Authentifizierungsoption für lokale NutzerInnen. 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.

Zu jedem Zeitpunkt wird unabhängig vom Zeitintervall nur eine Quell-IP-Adresse für die Anmeldung gespeichert.

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.

Es kann ein Timeout festgelegt werden, sodass sich 2FA-NutzerInnen unabhängig von der IP-Änderung regelmäßig authentifizieren müssen. Die NutzerInnen können den Timeout-Bereich festlegen.

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 dem konfigurierten Zeitintervall 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 die 2FA aktiviert ist, werden folgende Aktionen nicht zugelassen:

- Anmelden bei iDRAC über eine beliebige Benutzeroberfläche mit Standardnutzerzugangsdaten
- Anmelden bei iDRAC über die OMM-App über Quick Sync-2

ANMERKUNG: RACADM, Redfish, 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 kann für die Authentifizierung mit jeweils einem einzelnen RSA AM-Server konfiguriert werden. Die globalen Einstellungen auf dem RSA AM-Server gelten für alle lokalen iDRAC-Nutzer sowie AD- und LDAP-Nutzer.

ANMERKUNG: Die RSA SecurID 2FA-Funktion ist nur mit einer Datacenter-Lizenz verfügbar.

Nachfolgend sind die Voraussetzungen aufgeführt, die vor der Konfiguration von iDRAC zur Aktivierung von RSA SecurID erfüllt werden müssen:

- Konfigurieren Sie den Microsoft Active Directory-Server.
- Wenn Sie versuchen, RSA SecurID für alle AD-Nutzer zu aktivieren, fügen Sie den AD-Server zum RSA AM-Server als Identitätsquelle hinzu.
- Stellen Sie sicher, dass Sie über einen generischen LDAP-Server verfügen.
- Für alle LDAP-Nutzer muss die Identitätsquelle für den LDAP-Server dem RSA AM-Server hinzugefügt werden.

Um RSA SecurID auf iDRAC zu aktivieren, sind die folgenden Attribute vom RSA AM-Server erforderlich:

1. **RSA-Authentifizierungs-API-URL**: Die URL-Syntax lautet `https://<rsa-am-server-hostname>:<port>/mfa/v1_1` und der Port ist standardmäßig 5555.
2. **RSA-Client-ID**: Standardmäßig ist die RSA-Client-ID identisch mit dem RSA-AM-Server-Hostnamen. Die RSA Client-ID ist auf der Konfigurationsseite des Authentifizierungs-Agenten für den RSA AM-Server zu finden.
3. **RSA Zugriffsschlüssel**: Der Zugriffsschlüssel kann auf dem RSA AM-Server abgerufen werden, indem Sie zum Abschnitt **Setup** > **Systemeinstellungen** > **RSA SecurID** > **Authentifizierungs-API** navigieren und wird in der Regel als `198cv5x195fdi86u43jw0q069byt0x37umlfwxc2gnp4s0xk11ve2lffum4s8302` angezeigt. So konfigurieren Sie die Einstellungen über die iDRAC-GUI:
   - Gehen Sie zu **iDRAC-Einstellungen Nutzer**.
   - Wählen Sie im Bereich **Lokale Nutzer** einen vorhandenen lokalen Nutzer aus und klicken Sie auf **Bearbeiten**.
   - Scrollen Sie bis zum Ende der Konfigurationsseite.
   - Klicken Sie im Abschnitt **RSA SecurID** auf den Link **RSA SecurID-Konfiguration**, um die Einstellungen anzuzeigen oder zu bearbeiten.

   Sie können die Einstellungen auch wie folgt konfigurieren:
   - Gehen Sie zu **iDRAC-Einstellungen Nutzer**.
   - Wählen Sie im Abschnitt **Verzeichnisdienste Microsoft Active Service** oder **Generischer LDAP-Verzeichnisdienst** aus und klicken Sie auf **Bearbeiten**.
   - Klicken Sie im Abschnitt **RSA SecurID** auf den Link **RSA SecurID-Konfiguration**, um die Einstellungen anzuzeigen oder zu bearbeiten.
4. **RSA AM-Server-Zertifikat (Kette)**

Sie können sich bei iDRAC über die iDRAC-GUI und SSH mit dem RSA SecurID-Token anmelden.

RSA SecurID-Token-App

Sie müssen die RSA SecurID-Token-App auf Ihrem System oder Smartphone installieren. Wenn Sie versuchen, sich bei iDRAC anzumelden, werden Sie aufgefordert, den in der App angezeigten Passcode einzugeben.

Wenn ein falscher Passcode eingegeben wird, fordert der RSA AM-Server den/die NutzerIn auf, das „Nächste Token“ bereitzustellen. Dies kann auch passieren, wenn der/die NutzerIn möglicherweise den richtigen Passcode eingegeben hat. Dieser Eintrag weist darauf hin, dass der Nutzer das richtige Token besitzt, das den richtigen Passcode erzeugt.

Sie können das **Nächste Token** aus der RSA SecurID-Token-App durch Klicken auf **Optionen** abrufen. Wählen Sie das **Nächste Token** aus und der nächste Passcode ist verfügbar. In diesem Schritt kommt es auf die Zeit an. Andernfalls kann die Verifizierung des nächsten Tokens auf dem iDRAC fehlschlagen. Wenn bei der iDRAC-Nutzeranmeldesitzung ein Timeout auftritt, muss ein weiterer Anmeldeversuch durchgeführt werden.

Wenn ein falscher Passcode eingegeben wird, fordert der RSA AM-Server den/die NutzerIn auf, das „Nächste Token“ bereitzustellen. Dies kann auch passieren, wenn der/die NutzerIn möglicherweise später den richtigen Passcode eingegeben hat. Dieser Eintrag weist darauf hin, dass der Nutzer das richtige Token besitzt, das den richtigen Passcode erzeugt.

Um das nächste Token in der RSA SecurID-Token-App abzurufen, klicken Sie auf **Optionen** und wählen Sie **Nächstes Token** aus. Daraufhin wird ein neues Token generiert. In diesem Schritt kommt es auf die Zeit an. Andernfalls kann die Verifizierung des nächsten Tokens auf dem iDRAC fehlschlagen. Wenn bei der iDRAC-Nutzeranmeldesitzung ein Timeout auftritt, muss ein weiterer Anmeldeversuch durchgeführt werden.

Systemzustand anzeigen

Bevor Sie eine Aufgabe ausführen oder ein Ereignis auslösen, können Sie über RACADM überprüfen, ob sich das System in einem geeigneten Zustand befindet. Verwenden Sie den Befehl `getremoteservicesstatus`, um den Remote-Servicestatus über RACADM anzuzeigen.

ANMERKUNG: Der Echtzeitstatus wird als **Nicht zutreffend** angezeigt, wenn auf dem System keine Echtzeit-fähigen Controller vorhanden sind.

Tabelle 8. Mögliche Werte für den Systemstatus

Hostsystem	Lifecycle-Controller (LC)	Echtzeitstatus	Allgemeiner Status
• Ausgeschaltet • In POST • Außerhalb von POST • Erfassen der Systembestandaufnahme • Automatisierte Task-Ausführung • Lifecycle Controller Unified Server Configurator • Server wurde bei fehlerhafter F1/F2-Aufforderung aufgrund eines POST-Fehlers angehalten • Der Server wurde bei der F1/F2/F11-Eingabeaufforderung angehalten, da keine startfähigen Geräte verfügbar sind. • Server hat das F2-Setup-Menü aufgerufen • Server hat das F11-Start-Manager-Menü aufgerufen	• Bereit • Nicht initialisiert • Erneutes Laden von Daten • Deaktiviert • Wird wiederhergestellt • In Use	• Bereit • Nicht bereit • Nicht anwendbar	• Bereit • Nicht bereit

1. Lesen/Schreiben: Schreibgeschützt
2. Nutzerberechtigung: Nutzer anmelden
3. Lizenz erforderlich: iDRAC Express oder iDRAC Enterprise
4. Abhängigkeit: Keine

Anmeldung beim iDRAC mit Authentifizierung mit öffentlichem Schlüssel

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

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 9. 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.

Sicheres Standardkennwort

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 Dell Supportseite.

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 physischen Zugriff auf das System haben, können Sie das Kennwort wie folgt zurücksetzen:

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

Remote-Zurücksetzen des standardmäßigen iDRAC-Kennworts

Wenn Sie keinen physischen Zugriff auf das System haben, können Sie das Standardkennwort per Remotezugriff zurücksetzen.

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 „Nutzer 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.

Ändern des standardmäßigen Anmeldekennworts über die Weboberfläche

Wenn Sie sich bei der iDRAC-Webschnittstelle anmelden und die Seite **Standardkennwort – Warnung** angezeigt wird, können Sie das Kennwort ändern. Gehen Sie hierfür folgendermaßen vor:

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

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

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

   Das neue Kennwort wird konfiguriert und Sie werden beim iDRAC 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 standardmäßigen Anmeldekennworts mithilfe von RACADM

Um das Kennwort zu ändern, führen Sie den folgenden RACADM-Befehl aus:

```
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 nutzerdefinierte Kennwort ist.

ANMERKUNG: Der Index für das Standardkonto ist 2.

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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

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

So ändern Sie das standardmäßige Anmeldekennwort über das Dienstprogramm für die 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.

3. Klicken Sie auf **Zurück**, dann auf **Fertig stellen** und anschließend auf **Ja**.
   Die Details werden gespeichert.

Aktivieren oder Deaktivieren der standardmäßigen Kennwortwarnungsmeldung

Sie können die Anzeige der standardmäßigen Kennwortwarnmeldung aktivieren oder deaktivieren. Hierfür müssen Sie über die Berechtigung zum Konfigurieren von NutzerInnen verfügen.

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 iDRAC10 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 Nutzer 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 10. 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 eines Betriebssystems für iDRAC-Passthrough unter Verwendung der Weboberfläche

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

1. Gehen 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 Link zwischen dem iDRAC und dem Hostbetriebssystem für Betriebssystem-zu-iDRAC-PassThrough wird über das LOM oder die OCP hergestellt.
   - **USB-NIC**: Der Link zwischen dem iDRAC und dem Hostbetriebssystem für Betriebssystem-zu-iDRAC-PassThrough wird über den internen USB hergestellt.

   ANMERKUNG: Wenn Sie den Pass-Through-Modus auf LOM einstellen, stellen Sie Folgendes sicher:
   - Das Betriebssystem und der iDRAC befinden sich im selben 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 Hostbetriebssystem nach dem Kaltstart zu starten.
   - Der LOM-Passthrough wird unter Verwendung der Funktion „dedizierter Modus“ 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 IPs sind für den USB-NIC-Anschluss an der Vorderseite, wenn ein Type-C-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.

ANMERKUNG: Wenn Sie die statische IP-Adresse der USB-NIC ändern, wird der DHCP-Adressbereich automatisch an die neue statische IP angepasst. Wenn Sie beispielsweise die statische IP-Adresse auf 169.254.1.1 festlegen, wird die DHCP-Adresse auf 169.254.1.2 aktualisiert. Diese Änderung ist kompatibel mit dem Netzwerkmanager Wicked, der die neue DHCP-Adresse akzeptiert.

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 Hostbetriebssystem hergestellt ist.

Warnungen über RACADM aktivieren oder deaktivieren

Verwenden Sie den folgenden Befehl:

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

n=0 – Deaktiviert

n=1 – Aktiviert

3

Open Server Manager 3.0.x

Sie können ein Update auf Open Server Manager (OSM) 3.0.x von iDRAC10 durchführen.

Themen:

- Vorbereiten des Systems auf ein OSM-Update
- Aktualisieren von OSM auf dem System

Vorbereiten des Systems auf ein OSM-Update

Sorgen Sie dafür, dass die entsprechenden Voraussetzungen erfüllt sind und das System auf ein OSM-Update vorbereitet ist.

- Überprüfen Sie, ob OSM auf der Zielplattform unterstützt wird.
- OSM-Lizenz ist verfügbar.
- OSM DUP ist verfügbar.

1. Sorgen Sie dafür, dass die neueste iDRAC-, FPGA- und BIOS-Firmware auf Ihrem System ausgeführt wird.
2. Laden Sie die bei Dell erworbene OSM-Lizenz hoch.
3. Sorgen Sie dafür, dass OSM in der Firmwarebestandsliste von Redfish URI (**redfish/v1/UpdateService/FirmwareInventory**) und auf der iDRAC-Benutzeroberfläche (**System** > **Inventory** > **Firmware Inventory**) verfügbar ist.

Aktualisieren von OSM auf dem System

1. Laden Sie das OSM-DUP hoch und initiieren Sie ein Update.
   Der Host schaltet sich automatisch aus, bevor das Update beginnt. Wenn der Host nicht heruntergefahren wird, fahren Sie den Host über die verfügbare Schnittstelle (UI, Redfish, IPMI) manuell herunter, damit das Update fortgesetzt werden kann.
2. Nachdem das Update abgeschlossen ist, startet iDRAC neu und startet mit OSM.
3. Im aktuellen Dell Open Server Manager auf Basis von OpenBMC™-Benutzerhandbuch finden Sie Schritte zum Zugriff auf die OSM-Benutzeroberfläche und SSH.

4

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

ANMERKUNG: Für alle Aktualisierungen, die iDRAC zurücksetzen/neu starten müssen, oder für den Fall, dass iDRAC neu gestartet wird, wird empfohlen, zu überprüfen, ob der iDRAC vollständig bereit ist. Warten Sie hierfür einige Sekunden im Intervall mit einer maximalen Zeitüberschreitung von 5 Minuten, bevor Sie einen anderen Befehl verwenden.

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
- Lokalisierte Versionen der Webschnittstelle anzeigen
- Aktualisieren der Gerätefirmware
- Anzeigen und Managen von gestuften Aktualisierungen
- Rollback der Geräte-Firmware durchführen
- Easy Restore (Einfache Wiederherstellung)
- iDRAC über andere Systemverwaltungs-Tools überwachen
- Unterstützung des Serverkonfigurationsprofils – Import und Export
- Secure Boot-Konfiguration über BIOS-Einstellungen oder F2
- BIOS recovery
- iDRAC wiederherstellen

iDRAC-IP-Adresse einrichten

Sie müssen die anfänglichen Netzwerkeinstellungen auf der Basis Ihrer Netzwerkinfrastruktur konfigurieren, um die Kommunikation zum und vom iDRAC zu ermöglichen. Sie können die IP-Adresse über eine der folgenden Schnittstellen einrichten:

- Dienstprogramm für die iDRAC-Einstellungen
- Lifecycle Controller (Siehe *Benutzerhandbuch für Dell Lifecycle Controller*)

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.

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 Dell Supportseite 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 <F2 > während des Einschaltselbsttests (POST).
3. Klicken Sie auf der Seite **System Setup Main Menu** auf **iDRAC Settings**.
   Die Seite **iDRAC-Einstellungen** wird angezeigt.
4. Klicken Sie auf **Network**.
   Die Seite **Netzwerk** wird angezeigt.
5. Legen Sie die folgenden Einstellungen fest:
   - 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 verfügbaren 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 der Liste **NIC-Auswahl** auf der Basis der Netzwerkanforderung eine der folgenden Schnittstellen aus:
   - **Dediziert** – Aktiviert das Remote-Zugriffsgerät, um die auf dem Remote-Access-Controller (RAC) verfügbare dedizierte Netzwerkschnittstelle zu verwenden. Diese Schnittstelle wird nicht an das Hostbetriebssystem freigegeben und leitet den Managementverkehr auf ein separates physisches Netzwerk um, wodurch eine Trennung vom Anwendungsdatenverkehr erfolgt.

     ANMERKUNG: 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.

   - **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.

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

   - **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** gesetzt wird.

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.

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 Mbit/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 Hostbetriebssystem 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 **Aktiviert** unter **IPv4 aktivieren** aus.
2. Wählen Sie die Option **Aktiviert** unter **DHCP aktivieren** aus, so dass DHCP die IP-Adresse, das Gateway und die Subnetzmaske automatisch iDRAC zuweisen kann. Wählen Sie andernfalls **Deaktiviert** aus und geben Sie die Werte für Folgendes ein:
   - Statische IP-Adresse
   - Statisches Gateway
   - Statische Subnetzmaske

Die Optionen **DHCP zum Abrufen von DNS-Serveradressen verwenden**, **DHCPv6 zum Abrufen von DNS-Serveradressen verwenden** und **Domänenname automatisch konfigurieren** sind standardmäßig aktiviert.

Konfigurieren der IPv6-Einstellungen

Sie können auf der Basis der Einrichtung der Infrastruktur das IPv6-Adressprotokoll verwenden.

So konfigurieren Sie die IPv6-Einstellungen:

ANMERKUNG: Wenn IPv6 auf statisch eingestellt ist, stellen Sie sicher, dass Sie den IPv6-Gateway manuell konfigurieren, was im Falle von dynamischem IPv6 nicht nötig ist. Wenn bei statischem IPv6 keine manuelle Konfiguration vorgenommen wird, führt dies zum Verlust der Kommunikation.

1. Wählen Sie die Option **Aktiviert** unter **IPv6 aktivieren** aus.
2. Damit der DHCPv6-Server dem iDRAC automatisch IP-Adresse und Präfixlänge zuweist, aktivieren Sie die Option **Aktiviert** unter **Automatische Konfiguration aktivieren**.

   ANMERKUNG: Sie können gleichzeitig statische IP-Adressen und DHCP-IP-Adressen konfigurieren.

3. Geben Sie in das Feld **Statische IP-Adresse 1** die statische IPv6-Adresse ein.
4. Geben Sie in das Feld **Statische Präfixlänge** einen Wert zwischen 1 und 128 ein.
5. Geben Sie in das Feld **Statisches Gateway** die Gateway-Adresse ein.

   ANMERKUNG: Wenn Sie statische IP konfigurieren, zeigt die aktuelle IP-Adresse 1 statische IP und die IP-Adresse 2 dynamische IP an. Wenn Sie die statischen IP-Einstellungen löschen, zeigt die aktuelle IP-Adresse 1 die dynamische IP an.

   Die Optionen **DHCP zum Abrufen von DNS-Serveradressen verwenden**, **DHCPv6 zum Abrufen von DNS-Serveradressen verwenden** und **Domänenname automatisch konfigurieren** sind standardmäßig aktiviert.
6. Konfigurieren Sie bei Bedarf Folgendes:
   - Geben Sie in das Feld **Statischer bevorzugter DNS-Server** die statische DNS-Server-IPv6-Adresse ein.
   - Geben Sie in das Feld **Statischer alternativer DNS-Server** den statischen alternativen DNS-Server ein.
7. Wenn DNS-Informationen weder durch DHCPv6 noch durch eine statische Konfiguration ermittelt werden können, können Sie RFC 8106 „IPv6 Router-Ankündigungsoptionen“ für die DNS-Konfiguration verwenden. Dies wird vom IPv6-Router identifiziert. Die Verwendung der RA-DNS-Konfiguration hat keine Auswirkungen auf vorhandene DNS-Konfigurationen (DHCPv6 oder statisch).
   - Der iDRAC kann DNS-Namensserver- und DNS-Suchdomaininformationen aus IPv6-Router-Ankündigungsmeldungen abrufen. Bitte lesen Sie RFC 8106 und das Benutzerhandbuch Ihres IPv6-Routers, um zu erfahren, wie Sie den Router für die Ankündigung dieser Informationen konfigurieren.
   - Wenn DNS-Informationen sowohl vom DHCPv6-Server als auch von der IPv6-Router-Ankündigung verfügbar sind, verwendet der iDRAC beides. Im Falle eines Konflikts haben die DNS-Informationen des DHCPv6-Servers In den Einstellungen /etc/resolv.conf des iDRAC Vorrang.

   ANMERKUNG: Damit iDRAC RA-DNS-Informationen verwenden kann: IPv6. Enable und IPv6.Autoconfig müssen aktiviert sein. Wenn die automatische Konfiguration deaktiviert ist, verarbeitet der iDRAC keine IPv6-RA-Meldungen, sondern verwendet nur statische DNS-Einstellungen entsprechend der Konfiguration.

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 **Nutzer** aus.
3. Geben Sie in das Feld **Verschlüsselungsschlüssel** den Verschlüsselungsschlüssel mit hexadezimalen Zeichen von 0 bis 40 (ohne Leerzeichen) ein. Der Standardwert besteht ausschließlich aus Nullen.

VLAN-Einstellungen

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

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.

Portbasierte Netzwerkzugriffskontrolle (IEEE 802.1x)

IDRAC bietet Anschluss-basierte Netzwerkzugriffskontrolle (IEEE802.1x). Es bietet einen sicheren Authentifizierungsmechanismus für Geräte, die mit einem LAN verbunden werden möchten.

Für diese Funktion wird eine iDRAC Datacenter-Lizenz benötigt.

Sie können über die iDRAC-GUI auf diese Funktion zugreifen, indem Sie zu **iDRAC-Einstellungen** > **Konnektivität** > **Netzwerk** > **Erweiterte Netzwerkeinstellungen** > **802.1x Sicherheit** navigieren. Sie können die Option über das Dropdown-Menü aktivieren oder deaktivieren. Diese Funktion ist standardmäßig aktiviert.

ANMERKUNG: Die Auswirkung von 802.1x funktioniert nicht im Modus „Gemeinsames LOM“ mit aktiviertem VLAN.

Die portbasierte Netzwerkzugriffskontrolle bietet drei Möglichkeiten zum Konfigurieren der Authentifizierungszertifikate:

- **Standard-IDevID** – Dies ist das standardmäßige iDRAC-Zertifikat, das werkseitig installiert wird.
- **Nutzerdefinierte Signatur-LDevID** – Mit dieser Option können Sie eine Zertifikatsignierungsanforderung (CSR) definieren, die vom hochgeladenen LDEVID-Signierungszertifikat signiert wird.
- **Nutzerdefinierte LDevID** – Mit dieser Option können Sie ein nutzerdefiniertes Zertifikat ihrer Wahl hochladen.

Es gibt die Möglichkeit, das **Authentifizierungsserverzertifikat** zu aktivieren oder zu deaktivieren, um die erforderlichen Informationen zur Validierung des Zertifikats bereitzustellen. Diese Option ist standardmäßig deaktiviert.

ANMERKUNG:

- Diese Funktion ist in modularen Servern standardmäßig deaktiviert.
- Alle Änderungen an der 802.1x-Konfiguration, einschließlich Zertifikat-Uploads und Aktivieren/Deaktivieren von Einstellungen, werden beim nächsten iDRAC-Start wirksam.
- Das Wechseln des iDRAC-Netzwerks zwischen 802.1x-aktiviertem Switch und Nicht-802.1x-Switch erfordert einen iDRAC-Neustart.
- Wenn die Anschlüsse auf dem Ethernetswitch, die mit den LOM-Anschlüssen des Servers verbunden sind, für 802.1X-Sicherheit aktiviert sind, müssen alle Downstream-Geräte auf diesen Anschlüssen für die 8021.X-Sicherheit aktiviert werden. Dies bedeutet, dass der Host beeinträchtigt ist, wenn er nicht für 802.1X-Sicherheit aktiviert wurde.

Auto-Ermittlung

Mit der Funktion „Automatische Ermittlung“ können neu installierte Server automatisch die Remote-Verwaltungskonsole ermitteln, die den Bereitstellungsserver hostet. Der **Bereitstellungsserver** stellt dem iDRAC nutzerdefinierte Administrator-Anmeldeinformationen zur Verfügung, damit der nicht bereitgestellte Server durch die Managementkonsole ermittelt und gemanagt werden kann.

Die automatische Ermittlung arbeitet mit einer statischen IP-Adresse. Die automatische Ermittlungsfunktion auf dem iDRAC wird verwendet, um den Bereitstellungsserver mithilfe von DHCP/Unicast DNS/mDNS zu finden.

- Wenn iDRAC die Konsolenadresse hat, sendet es sein eigenes Service-Tag, IP-Adresse, Redfish-Portnummer, Web-Zertifikat usw.
- Diese Informationen werden periodisch auf Konsolen veröffentlicht.

DHCP, DNS-Server oder der Standard-DNS-Host-Name ermitteln den Bereitstellungsserver. Wenn DNS angegeben ist, wird die IP-Adresse für den Bereitstellungsserver aus DNS abgerufen; die DHCP-Einstellungen werden nicht benötigt. Wenn automatische Ermittlung angegeben ist, wird die Ermittlung übersprungen, sodass weder DHCP noch DNS erforderlich sind.

Die automatische Ermittlung kann auf folgende Weise aktiviert werden:

1. Verwenden der iDRAC-UI: **iDRAC-Einstellungen** > **Konnektivität** > **Automatische iDRAC-Ermittlung**
2. RACADM verwenden: `racadm set iDRAC.AutoDiscovery.EnableIPChangeAnnounce 1`

So aktivieren Sie die automatische Ermittlung über das Dienstprogramm für die iDRAC-Einstellungen:

1. Schalten Sie das verwaltete System ein.
2. Drücken Sie während des POST die Taste F2, und wechseln Sie dann zu **iDRAC-Einstellungen** > **Remote-Aktivierung**. Daraufhin wird die Seite **iDRAC-Einstellungen – Remote-Aktivierung** angezeigt.

3. Aktivieren Sie die automatische Ermittlung, geben Sie die IP-Adresse für den Bereitstellungs-Server ein, und klicken Sie auf **Zurück**.

   ANMERKUNG: Die Angabe der IP-Adresse für den Bereitstellungsserver ist optional. Wenn Sie diese Adresse nicht angeben, wird sie über die DHCP- oder DNS-Einstellungen ermittelt (Schritt 7).

4. Klicken Sie auf **Network**.
   Die Seite **iDRAC-Einstellungen Netzwerk** wird angezeigt.
5. NIC aktivieren
6. IPv4 aktivieren

   ANMERKUNG: IPv6 wird für automatische Ermittlung nicht unterstützt.

7. Aktivieren Sie DHCP, und rufen Sie den Domänennamen, die DNS-Server-Adresse und den DNS-Domänennamen von DHCP ab.

   ANMERKUNG: Schritt 7 ist optional, wenn die IP-Adresse des Bereitstellungs-Servers in Schritt 3 angegeben wurde.

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 für iDRAC 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 11. 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 Zeichenkettenwerts aufgeführt:

`-f (Filename)`: Name der exportierten Server-Profil Datei.

`-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.

`-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 unterstützt, um die Konfiguration der HTTP-Proxy-Parameter zu ermöglichen und das Wiederholungs-Timeout 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 das Wiederholungs-Timeout in Minuten für das Beziehen der Konfigurationsdatei an (die Standardeinstellung ist 60 Minuten).

Profildateien im JSON-Format werden 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:

- 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 15/16G-Systemen verwendet werden. Die Datei kann `config.json` heißen.

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.

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. Der iDRAC meldet beim Abrufen der IP-Adresse die Anbieterklassen-Kennung. (Option 60)
5. Der DHCP-Server vergleicht die Anbieterklasse mit der Anbieteroption in der Datei `dhcpd.conf` und sendet den Speicherort und, falls angegeben, den Namen der SCP-Datei an den iDRAC.
6. Der iDRAC verarbeitet die SCP-Datei und konfiguriert alle in der Datei aufgeführten Attribute.

DHCP-Optionen

DHCPv4 ermöglicht die Übergabe zahlreicher global definierter Parameter an die DHCP-Clients. Jeder Parameter wird als DHCP-Option bezeichnet. Jede Option wird durch ein Options-Tag gekennzeichnet, bei dem es sich um einen 1-Byte-Wert handelt. Die Options-Tags 0 und 255 sind für das Auffüllen bzw. das Ende von Optionen reserviert. Alle anderen Werte stehen für die Definition von Optionen zur Verfügung.

Die DHCP-Option 43 wird verwendet, um Informationen vom DHCP-Server an den DHCP-Client zu senden. Die Option wird als Textzeichenfolge definiert. Diese Textzeichenfolge enthält die Werte für den SCP-Dateinamen, den Freigabespeicherort und die Zugangsdaten 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 identifiziert einen DHCP-Client und ordnet ihn einem bestimmten Anbieter zu. Für jeden DHCP-Server, der für die Ausführung von Maßnahmen basierend auf der Anbieter-ID eines Clients konfiguriert ist, sollten Option 60 und Option 43 konfiguriert werden. Bei Dell PowerEdge-Servern identifiziert sich der iDRAC mit der Anbieter-ID: **iDRAC**. Daher müssen Sie eine neue „Anbieterklasse“ hinzufügen und darunter eine „Bereichsoption“ für Code 60 erstellen und die neue Bereichsoption dann 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 auf **Start** > **Administrationstools** > **DHCP**, um die DHCP-Serveradministrationstools 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 **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 zu **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 aus der Liste **Anbieterklasse** die Option **iDRAC** aus.
    `060 Idrac` wird in der Spalte **Verfügbare Optionen** angezeigt.
16. Wählen Sie die Option **060 iDRAC** aus.
17. Geben Sie die Zeichenfolge ein, die (zusammen mit einer Standard-DHCP-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)` – Gibt den Namen der exportierten Serverkonfigurationsprofil-Datei (SCP) an.
    - `Sharename (-n)` – Gibt den Namen der Netzwerkfreigabe ein.
    - `ShareType (-s)` – Neben der Unterstützung von NFS- und CIFS-basierter Dateifreigabe unterstützt iDRAC-Firmware auch den Zugriff auf Profildateien mithilfe von HTTP und HTTPS. Die Markierung `-s option` wird wie folgt aktualisiert: `-s (ShareType)`: Geben Sie für NFS nfs oder 0, für CIFS cifs oder 2, für HTTP http oder 5 und für HTTPS https oder 6 ein.
    - `IPAddress (-i)` – Gibt die IP-Adresse der Dateifreigabe an.

      ANMERKUNG: `Sharename (-n)`, `IPAddress (-i)` und `ShareType (-s)` sind erforderliche Attribute, die übergeben werden müssen. -n ist für HTTP oder HTTPS nicht erforderlich.
    - `Username (-u)` – Gibt den Benutzernamen für den Zugriff auf die Netzwerkfreigabe an. Diese Informationen sind nur für CIFS erforderlich.
    - `Password (-p)` – Gibt das Kennwort für den Zugriff auf die Netzwerkfreigabe 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 lautet 0.
    - `Timetowait (-t)` – Gibt die Zeitspanne an, die das Hostsystem bis zum Herunterfahren wartet. Die Standardeinstellung lautet 300.
    - `EndHostPowerState (-e)` – Gibt den aktuellen Stromversorgungszustand 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 <**NUTZERNAME**> -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 den Richtlinien von Dateinamen finden Sie unter Konfigurieren von Servern und Serverkomponenten mithilfe der automatischen Konfiguration.

- 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`

    ANMERKUNG: 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 lautet 0.

- Timetowait (Wartezeit) (-t) – Gibt die Zeitspanne an, die das Host-System vor dem Herunterfahren wartet. Die Standardeinstellung lautet 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:

- Die unterstützte Netzwerkfreigabe (NFS, CIFS, HTTP und HTTPS) ist im selben Subnetz wie der iDRAC und DHCP-Server verfügbar. Testen Sie die Netzwerkfreigabe, um sicherzustellen, dass darauf zugegriffen werden kann und dass die Firewall und Nutzerberechtigungen korrekt festgelegt sind.
- Das Serverkonfigurationsprofil wurde in die Netzwerkfreigabe exportiert. Stellen Sie außerdem sicher, dass an der SCP-Datei die notwendigen Änderungen vorgenommen wurden, sodass die richtigen Einstellungen angewendet werden, sobald der Vorgang zur automatischen Konfiguration 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. Navigieren Sie auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Konnektivität** > **Netzwerk** > **Automatische Konfiguration**.
   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 einmalig unter Verwendung der SCP-Datei, auf die der DHCP-Server verweist. Danach wird die automatische Konfiguration deaktiviert.
   - **Einmal nach Reset aktivieren** – Konfiguriert nach dem iDRAC-Reset die Komponente einmalig unter Verwendung der SCP-Datei, auf die der DHCP-Server verweist. Danach wird die automatische Konfiguration 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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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 Dell Supportseite.

Verwenden von Hash-Kennwörtern für mehr Sicherheit

Sie können Nutzerkennwörter und BIOS-Kennwörter in einem einseitigen Hash-Format festlegen. 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 hinterlegen. Wenn Sie die Kennwortwerte für SHA256 bereitstellen, ist eine Authentifizierung über SNMPv3 und IPMI nicht möglich.

  ANMERKUNG: Remote RACADM 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 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 Nutzer fehl, die die Hash-Passwortwerte festgelegt haben.
- Die anderen Schnittstellen, z. B. die IDRAC-UI, 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 Nutzer 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 des Serverkonfigurationsprofils können Sie die Auskommentierung des vorhandenen Kennwortattributs oder des neuen Kennwort-Hash-Attributs aufheben. Wenn beide nicht auskommentiert sind, wird ein Fehler erzeugt und das Kennwort wird nicht festgelegt. Ein kommentiertes Attribut wird während eines Imports nicht angewendet.

Hash-Kennwort ohne SNMPv3- und IPMI-Authentifizierung erstellen

Das Hash-Kennwort kann ohne SNMPv3- und IPMI-Authentifizierung und mit oder ohne Salt erzeugt werden. Für beides ist SHA256 erforderlich.

So erzeugen Sie ein Hash-Kennwort mit Salt:

1. Für iDRAC-Nutzerkonten müssen Sie das Kennwort mithilfe von Salt über SHA256 erzeugen.
   - Wenn Sie das Kennwort mit Salt erzeugen, wird eine binäre Zeichenfolge mit 16 Byte angehängt. Die Salt-Zeichenfolge muss 16 Byte lang sein, falls verwendet. Nach dem Anhängen wird sie zu einer 32-stelligen Zeichenfolge. Das Format ist „Kennwort“+„Salt“, z. B.:
     - Kennwort = SOMEPASSWORD
     - Salt = ALITTLEBITOFSALT – 16 Zeichen werden angehängt.
2. Öffnen Sie eine Linux-Eingabeaufforderung und führen Sie die folgenden Befehle 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 oder in Redfish bereit.

   ANMERKUNG: Wenn Sie ein zuvor mit Salt erstelltes Kennwort löschen möchten, stellen Sie sicher, dass die Kennwort-Salt-Zeichenfolge explizit auf eine leere Zeichenfolge gesetzt wird.

```
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 SNMP-v3- und IPMI-Authentifizierung für iDRAC-Nutzerkonten 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 Nutzerln 2) über das Dienstprogramm für die iDRAC-Einstellungen ändern.

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Benutzerkonfiguration**.
   Die Seite zur **Benutzerkonfiguration der iDRAC-Einstellungen** wird 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 **Fertig stellen** und anschließend 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. Gehen Sie auf der iDRAC-Weboberfläche zu **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 im 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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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 verwaltete 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 **Fertig stellen** und anschließend 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 nutzerdefinierte Kühlung der Karten von Drittanbietern.

Thermische Einstellungen über die iDRAC-Webschnittstelle ändern

So ändern Sie die Standardeinstellungen:

1. Gehen Sie in der iDRAC-Weboberfläche 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 nutzerdefinierten Algorithmus auswählen, der unabhängig vom BIOS-Profil ist. Die folgenden Optionen sind verfügbar:
     - **Maximale Leistung (Leistung wird optimiert)** :
       - Geringere Wahrscheinlichkeit von Arbeitsspeicher- oder CPU-Drosselung.
       - Höhere Wahrscheinlichkeit der Turbo-Modus-Aktivierung.
       - Im Allgemeinen höhere Lüftergeschwindigkeiten im Leerlauf und bei Spannungsladungen.

       ANMERKUNG: Die Lüftergeschwindigkeit ändert sich nicht, selbst wenn für einige bestimmte Konfigurationen maximale Leistung ausgewählt ist.
     - **Minimalstrom (optimierte Leistung pro Watt)**:
       - Optimiert für den geringsten Stromverbrauch 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.

     ANMERKUNG: 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 Überwachung 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.

     ANMERKUNG:
     - 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 Gesamtstromverbrauch 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.

- **Grenzwerte**
  - **Maximale PCIe-Einlasstemperatur** – Der Standardwert ist 55 °C. Wählen Sie die niedrigere Temperatur von 45 °C für PCIe-Karten von Drittanbietern aus, die eine niedrigere Einlasstemperatur benötigen.
  - **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 nutzerdefinierte Lüftergeschwindigkeitsoptionen nicht zu den erforderlichen höheren Lüftergeschwindigkeiten führen.
    - **Standardeinstellung** – Legt die Mindestlüftergeschwindigkeit auf einen Standardwert fest, der durch den Systemkühlungsalgorithmus bestimmt wird.
    - **Benutzerdefiniert** – Geben Sie den Prozentsatz ein, um den Sie die Lüftergeschwindigkeit ändern möchten. Der zulässige Bereich liegt zwischen 9 und 100.

    ANMERKUNG:
    - 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).
    - Für alle SAS/SATA-Storage-Konfigurationen wird die Lüftergeschwindigkeit auf 95 % begrenzt.
    - 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.
    - 0 % PWM bedeutet nicht, dass der Lüfter ausgeschaltet ist. Dies ist die niedrigste Geschwindigkeit, mit der der Lüfter betrieben werden kann.
    - Auf Servern mit mehreren Zonen führt ein Lüfterausfall in einer beliebigen Zone wie Host Processor Module (HPM) und PCIe Baseboard (PCB) dazu, dass alle Lüfter mit einer maximalen Geschwindigkeit laufen.

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 nutzerdefinierten Kühlungsoptionen werden möglicherweise nicht auf allen Servern unterstützt. Wenn die Optionen nicht unterstützt werden, werden sie nicht angezeigt, oder Sie können keinen nutzerdefinierten 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: Die Lüfteraktivierung hängt von der entsprechenden thermischen Konfiguration (offene Schleife) ab, die wiederum von den jeweiligen Hardwarekonfigurationen im Setup abhängt. Beispiel: Die erforderlichen hinteren Festplattenlaufwerke.

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 12. 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
		• 255 – Zeigt 70 °C an (Standard)
			• So prüfen Sie die vorhandenen Einstellungen auf dem System:
			`racadm get system.thermalsettings.AirExhaustTemp`
			• Das Ergebnis ist Folgendes:
			`AirExhaustTemp=70`
			• 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“.	Werte zwischen 0 und 100	`racadm get system.thermalsettings FanSpeedHighOffsetVal` Dies gibt einen numerischen Wert wie 66 zurück. Das bedeutet, dass, wenn Sie den folgenden Befehl verwenden,

Tabelle 12. Temperatureinstellungen (fortgesetzt)

Objekt	Beschreibung	Verwendung	Beispiel
	• Dieser Wert richtet sich nach dem System. • Verwenden Sie das Objekt `FanSpeedOffset`, um diesen Wert unter Verwendung von Indexwert 1 festzulegen.		ein hoher Lüftergeschwindigkeits-Offset (66 % des PWM) über der Baseline-Lüftergeschwindigkeit 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 Objekt `FanSpeedOffset`, um diesen Wert unter Verwendung von Indexwert 0 festzulegen.
		Werte zwischen 0 und 100	`racadm get system.thermalsettings FanSpeedLowOffsetVal`
			Dies gibt einen numerischen Wert wie 23 zurück. Das bedeutet, dass, wenn Sie den folgenden Befehl verwenden, ein niedriger Lüftergeschwindigkeits-Offset (23 % des PWM) über der Baseline-Lüftergeschwindigkeit 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 Objekt `FanSpeedOffset`, um diesen Wert unter Verwendung von Indexwert 3 festzulegen.
		Werte zwischen 0 und 100	`racadm get system.thermalsettings FanSpeedMaxOffsetVal`
			Dies gibt einen numerischen Wert wie 100 zurück. Das bedeutet, dass, wenn Sie den folgenden Befehl verwenden, der maximale Lüftergeschwindigkeits-Offset (100 % des PWM) angewendet wird. In der Regel führt dieser Offset dazu, dass die Lüftergeschwindigkeit auf die volle Drehzahl ansteigt.
			`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.
	• Verwenden Sie das Objekt `FanSpeedOffset`, um diesen Wert unter Verwendung von Indexwert 2 festzulegen.
		Werte zwischen 0 und 100	`racadm get system.thermalsettings FanSpeedMediumOffsetVal`
			Dies gibt einen numerischen Wert wie 47 zurück. Das bedeutet, dass, wenn Sie den folgenden Befehl verwenden, ein mittlerer Lüftergeschwindigkeits-Offset (47 % des PWM) über der Baseline-Lüftergeschwindigkeit angewendet wird.
			`racadm set system.thermalsettings FanSpeedOffset 2`

Tabelle 12. Temperatureinstellungen (fortgesetzt)

Objekt	Beschreibung	Verwendung	Beispiel

`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 festgelegt) sind die Werte, die für den Offset angewendet werden.
		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`
			ANMERKUNG: So legen Sie den Lüftergeschwindigkeits-Offset-Wert (wie in `FanSpeedHighOffsetVal` festgelegt) 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 Option `MinimumFanSpeed` eingestellt werden kann: `racadm get system.thermalsettings.MFSMaximumLimit`
`MFSMinimumLimit`	Minimalwerte für MFS lesen	Werte von 0 bis `MFSMaximumLimit` Standard ist 255 (bedeutet „Keiner“)	So zeigen Sie den niedrigsten Wert an, der mithilfe der Option `MinimumFanSpeed` eingestellt werden kann: `racadm get system.thermalsettings.MFSMinimumLimit`
`MinimumFanSpeed`	• Ermöglicht die Konfiguration der Mindest-Lüftergeschwindigkeit, die erforderlich ist, damit das System betrieben werden kann. • 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	Werte von `MFSMinimumLimit` bis `MFSMaximumLimit` Wenn der „get“-Befehl 255 meldet, bedeutet dies, dass der benutzerdefinierte Offset nicht angewendet wurde.	Gehen Sie wie folgt vor, um sicherzustellen, dass die Systemmindestgeschwindigkeit nicht unter 45 % des PWM fällt (45 muss ein Wert zwischen `MFSMinimumLimit` und `MFSMaximumLimit` sein): `racadm set system.thermalsettings.MinimumFanSpeed 45`

Tabelle 12. Temperatureinstellungen (fortgesetzt)

Objekt	Beschreibung	Verwendung	Beispiel
	die Lüftergeschwindigkeit, angegeben in Prozent.		

`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`
			ANMERKUNG: 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, 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. Einige Dell Server bieten möglicherweise keine Unterstützung für einige oder alle dieser nutzerdefinierten Kühlungsoptionen. Wenn die Optionen nicht unterstützt werden, werden sie nicht angezeigt, oder Sie können keinen nutzerdefinierten Wert festlegen.
3. Klicken Sie auf **Zurück**, dann auf **Fertig stellen** und anschließend auf **Ja**.
   Die Konfiguration der Temperatureinstellungen ist damit abgeschlossen.

Ändern von PCIe Airflow-Einstellungen über die iDRAC-Weboberfläche

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

ANMERKUNG: PCIe-Airflow-Einstellungen sind nicht für M.2-Laufwerke verfügbar, die über direkte Riser oder BOSS verbunden sind.

So ändern Sie die PCIe Airflow-Einstellungen:

1. Gehen Sie in der iDRAC-Weboberfläche zu **Konfiguration** > **Systemeinstellungen** > **Hardwareeinstellungen** > **Kühlungskonfiguration**.
   Die Seite **PCIe Airflow-Einstellungen** wird im Abschnitt „Lüftereinstellungen“ angezeigt.
2. Geben Sie folgendes an:
   - **LFM-Modus**: Wählen Sie den Modus **Benutzerdefiniert** aus, um die nutzerdefinierte 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: Starten Sie das System neu, um die Einstellungen anzuwenden.

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 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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.
4. Installieren Sie nach Bedarf auch die folgenden Komponenten:
   - SSH-Client
   - TFTP
   - Dell OpenManage Essentials

Per Remote auf iDRAC zugreifen

Um remote von einer Verwaltungsstation auf die iDRAC-Benutzeroberfläche zuzugreifen, muss iDRAC NIC auf **Dedicated** oder **LOM1** eingestellt werden, damit die Verwaltungsstation im gleichen Netzwerk wie iDRAC ist.

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 iDRAC-Handbücher.

Auf die meisten Funktionen der iDRAC-Weboberfläche kann mit diesen Browsern mit Standardeinstellungen zugegriffen werden. Damit bestimmte Funktionen funktionieren, müssen Sie einige Einstellungen ändern. Diese Einstellungen umfassen das Deaktivieren von Pop-up-Blockern, das Aktivieren von eHTML5-Plug-In-Support usw.

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

ANMERKUNG: Wenn Sie Firefox zum Zugriff auf die iDRAC-Weboberfläche 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.

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 „Weiße Liste“-Sicherheitsfunktion, die eine Benutzerberechtigung zum Installieren von Plugins für jede Site erfordert, die ein Plugin hostet. Ist die Weiße Liste-Funktion aktiviert, ist die Installation eines Virtuelle Konsole-Viewers für jeden besuchten iDRAC erforderlich, obwohl 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 die <Eingabetaste>.
3. Machen Sie in der Spalte **Einstellungsname** den Eintrag **xpinstall.whitelist.required** ausfindig und doppelklicken Sie darauf.
   Die Werte für **Einstellungsname**, **Status**, **Typ** und **Wert** werden fett formatiert. Der Wert für **Status** ändert sich auf „Vom Nutzer festgelegt“ und der **Wert** ändert sich auf „false“.
4. Machen Sie in der Spalte **Einstellungs**name den Eintrag xpinstall.enabled ausfindig.
   Stellen Sie sicher, dass für **Wert true** festgelegt ist. Wenn nicht, doppelklicken Sie auf **xpinstall.enabled**, um **Wert** auf **true** festzulegen.

Firefox für die Aktivierung von Active Directory SSO konfigurieren

So konfigurieren Sie die Browser-Einstellungen für Firefox:

1. Geben Sie in die Firefox-Adresszeile `about:config` ein.
2. Geben Sie unter **Filter** den Wert `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

ANMERKUNG: Die virtuelle Konsole verwendet nur eHTML5. Java und ActiveX werden nicht mehr unterstützt.

So verwenden Sie die virtuelle Konsole auf Ihrer Management Station:

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

ANMERKUNG: Im RHEL-BS mit Mozilla-Browser wurde folgende Beobachtung während des Netzwerkausfalls (Entfernen und erneutes Einsetzen des Netzwerkkabels) gemacht:

- Die Meldung zum Wiederaufbau der Verbindung wird in vConsole möglicherweise erst angezeigt, wenn das Netzwerk aktiv ist.
- Möglicherweise wird die Pop-up-Meldung **Anmeldung abgelehnt** anstelle des Fehlers **Wiederherstellung der Verbindung fehlgeschlagen** angezeigt, wenn das Netzwerk länger als 180 Sekunden ausgefallen ist.

ANMERKUNG: Bei Verwendung des Safari-Browsers wird empfohlen, die Auswahl der **NSURLSession WebSocket**-Optionen aufzuheben, wenn sie ausgewählt wurden, und dann die vConsole zu öffnen. Heben Sie zum Deaktivieren des **NSURLSession WebSocket** in Safari die Auswahl von **Safari** > **Entwickeln** > **Optionale Funktionen** > **Optionale Funktionen** auf.

Weitere Informationen zu den unterstützten Browserversionen finden Sie in den **Versionshinweisen** auf iDRAC-Handbücher.

ANMERKUNG: Es wird als Best Practice empfohlen, die virtuelle Suchfunktion im Edge-Browser zu deaktivieren. Sie ist standardmäßig aktiviert. Es besteht möglicherweise das Risiko, dass Bilder ohne Ihr Wissen durchsucht werden. Daher können Sie dieses Verhalten deaktivieren, indem Sie die Edge-Browsereinstellungen konfigurieren.

2. Wenn Sie Microsoft Edge verwenden, setzen Sie den Browser auf **Als Administrator ausführen**.
3. Konfigurieren Sie den Web-Browser, um das eHTML5-Plug-in zu verwenden.
4. Importieren Sie die Stammzertifikate auf das Managed System, um Pop-up-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.

Zertifizierungsstellenzertifikate auf die Management Station importieren

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

Weitere Informationen über die automatische Zertifikatregistrierung (ACE) finden Sie im Abschnitt Automatische Zertifikatregistrierung.

Zertifizierungsstellenzertifikat in den Storage für vertrauenswürdige Java-Zertifikate importieren

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

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 **Java-Einstellungen**-Fenster wird geschlossen.

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-Kennungen in Klammern geben die unterstützten Sprachvarianten an. Bei einigen unterstützten Sprachen muss die Größe des Browserfensters auf 1024 Pixel geändert werden, um alle Funktionen anzuzeigen.

Die iDRAC-Weboberfläche wurde für die Verwendung mit lokalisierten Tastaturen für die unterstützten Sprachvarianten entwickelt. Einige Funktionen der iDRAC-Weboberfläche, wie z. B. die virtuelle Konsole, erfordern möglicherweise zusätzliche Schritte für den Zugriff auf bestimmte Funktionen oder Buchstaben. Andere Tastaturen werden nicht unterstützt und können 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.

Aktualisieren der Gerätefirmware

Sie können iDRAC, BIOS und alle Gerätefirmware aktualisieren, z. B.:

- Fibre Channel (FC)-Karten
- Diagnose
- Treiberpaket des Betriebssystems
- Netzwerkschnittstellenkarte (NIC)
- RAID-Controller
- Netzteil (PSU)
- Accelerator (GPU)
- NVMe PCIe-Geräte
- SAS-/SATA-Festplatten
- Rückwandplatinenupdate für interne und externe Gehäuse

VORSICHT: Das Netzteil-Firmwareupdate kann je nach Systemkonfiguration und Netzteilmodell mehrere Minuten dauern. Um Schäden am Netzteil zu vermeiden, unterbrechen Sie während des Firmwareupdates des Netzteils den Aktualisierungsvorgang nicht und schalten Sie das System nicht ein.

ANMERKUNG:

- Das LC-Protokoll meldet möglicherweise Warnmeldungen zu verlorener Kommunikation und Wiederherstellung während des GPU-Firmware-Updates.
- Nach dem Firmwareupdate des PSU wird ein virtuelles Aus- und Wiedereinschalten des Netzteils durch das System initiiert.

ANMERKUNG:

- Wenn ein Firmware-Update auf einer Hot-Plug-fähigen Festplatte versucht wird, wird erwartet, dass eine doppelte PR7-Meldung in den Lifecycle-Protokollen angezeigt wird.
- Wenn der Jobstatus **Wird ausgeführt** ist und kein Status-Update von den Update-Modulen vorhanden ist, wird nach 6 Stunden ein Zeitüberschreitung für den Job ausgegeben und er wird als fehlgeschlagen gekennzeichnet.
- Wenn der Jobstatus **Wird ausgeführt** ist, wird der Firmware-Update-Job nach einem iDRAC-Neustart möglicherweise als **Fehlgeschlagen** gekennzeichnet.
- Verwenden Sie bei der Durchführung der Updates keine IP-Adresse von der Website downloads.dell.com. Dies funktioniert möglicherweise nicht wie erwartet. Wenn downloads.dell.com als HTTPS-Adresse angegeben ist, muss kein Katalogpfad angegeben werden. Der entsprechende Katalog wird automatisch aufgenommen.

Die benötigte Firmware muss zu iDRAC hochgeladen werden. Nach dem Hochladen werden die aktuelle auf dem Gerät installierte Version der Firmware sowie die nun aufgespielte Version angezeigt. Wenn die hochgeladene Firmwareversion nicht gültig ist, wird eine Fehlermeldung angezeigt. Aktualisierungen, bei denen kein Neustart erforderlich ist, werden sofort übernommen. Aktualisierungen, bei denen ein Neustart des Systems erforderlich ist, werden stufenweise durchgeführt und beim nächsten Systemneustart übernommen. Es ist nur ein Systemneustart erforderlich, um alle Aktualisierungen durchzuführen.

Wenn in einem Echtzeit-Firmwareupdateszenario von iDRAC der Jobstatus mit **Abgeschlossen, Virtuelles Aus- und Einschalten ausstehend** abgeschlossen ist, führen Sie das physische Aus- und Einschalten oder das virtuelle Aus- und Einschalten des Servers durch. Verwenden Sie für ein virtuelles Aus- und Einschalten den folgenden Redfish-URI. Wenn eine andere Methode zum Aus- und Einschalten verwendet wird, schlägt der Echtzeitjob möglicherweise fehl. Die aktualisierte Version spiegelt jedoch weiterhin das Aus- und Einschalten des Netzstroms wider.

ANMERKUNG:

- Wenn der iLKM-Modus auf einem Controller aktiviert ist, schlägt das Downgrade/Upgrade der iDRAC-Firmware fehl, wenn versucht wird, dieses von einer iLKM- auf eine nicht-iLKM-iDRAC-Version durchzuführen.
- Wenn der SEKM-Modus auf einem Controller aktiviert ist, schlägt das Downgrade/Upgrade der iDRAC-Firmware fehl, wenn versucht wird, dieses von einer SEKM- auf eine nicht-SEKM-iDRAC-Version durchzuführen.
- Das Herabstufen der PERC-Firmware schlägt fehl, wenn SEKM aktiviert ist.

Nachdem die Firmware aktualisiert wurde, zeigt die Seite **System-Bestandsaufnahme** die aktualisierte Firmwareversion und aufgezeichnete Protokolle an.

Die unterstützten Firmware-Image-Dateitypen sind:

- `.exe`– Windows-basiertes Dell Update Package (DUP) Sie müssen über die Berechtigung zum Steuern und Konfigurieren verfügen, um diesen Imagedateityp verwenden zu können.
- `.d10`– Enthält iDRAC- und Lifecycle Controller-Firmware

Für Dateien mit der Erweiterung `.exe` müssen Sie über die Berechtigung zur Systemsteuerung verfügen. Die lizenzierte Remote-Firmwareupdatefunktion und Lifecycle Controller müssen aktiviert sein. Dies gilt für RACADM-Updates, Redfish Simple-Updates und iDRAC-UI-Updates.

Für Dateien mit der Erweiterung `.d10` müssen Sie über Berechtigungen zur Konfiguration verfügen. Dies gilt nur für die `racadm fwupdate`-Methode.

ANMERKUNG: Stellen Sie sicher, dass alle Nodes im System ausgeschaltet sind, bevor Sie die PSU-Firmware aktualisieren.

ANMERKUNG: Möglicherweise stellen Sie nach dem Update der iDRAC-Firmware Unterschiede im Zeitstempel des Lifecycle Controller-Protokolls fest. Die im LC-Protokoll angezeigte Uhrzeit unterscheidet sich von NTP/BIOS-Uhrzeit für einige Protokolle während des iDRAC-Reset.

Sie können Firmwareupdates mithilfe der folgenden Methoden ausführen:

- Hochladen eines unterstützten Imagetyps einer nach dem anderen von einem lokalen System oder einer Netzwerkfreigabe.
- Verbindung zu einer FTP-, TFTP-, HTTP- oder HTTPS-Seite oder zu einem Netzwerk-Repository, das Windows-DUPs und eine entsprechende Katalogdatei enthält. Mithilfe von Dell Repository Manager können Sie Nutzerdefinierte Repositories erstellen. Weitere Informationen finden Sie im **Benutzerhandbuch für Dell Repository Manager Data Center**. iDRAC kann einen Bericht über die Unterschiede zwischen dem/der auf dem System installierten BIOS und Firmware und den im Repository verfügbaren Updates liefern. Alle im Repository enthaltenen verfügbaren Updates werden auf das System angewandt. Diese Funktion ist mit einer iDRAC Enterprise- oder Datacenter-Lizenz verfügbar.

  ANMERKUNG: Firmware-Updates mithilfe eines FTP schlagen fehl, wenn der verwendete HTTP-Proxy ohne Authentifizierung konfiguriert ist. Stellen Sie sicher, dass Sie die Proxykonfiguration ändern, damit die CONNECT-Methode Nicht-SSL-Ports verwenden kann. Wenn Sie beispielsweise einen Squid-Proxy verwenden, entfernen Sie die Zeile „http_access deny CONNECT ! SSL_ports“, die die Verwendung der CONNECT-Methode auf Nicht-SSL-Ports einschränkt.

  ANMERKUNG: HTTP/HTTPS unterstützt entweder nur Digest-Authentifizierung oder keine Authentifizierung.

- Das Planen wiederkehrender, automatischer Firmwareupdates mithilfe der Katalogdatei und Nutzerdefiniertem Repository.

Es gibt mehrere Tools und Schnittstellen, die verwendet werden können, um die iDRAC-Firmware zu aktualisieren. Die folgende Tabelle gilt nur für die iDRAC-Firmware. In der Tabelle werden die unterstützten Schnittstellen und Image-Dateitypen aufgelistet und es wird auch aufgelistet, ob sich der Lifecycle Controller im aktivierten Zustand befinden muss, damit die Firmware aktualisiert werden kann:

Tabelle 13. Firmware-Image-Dateitypen und -Abhängigkeiten

	.D10-Image		iDRAC DUP	
Schnittstelle	**Unterstützt**	**Erfordert LC aktiviert**	**Unterstützt**	**Erfordert LC aktiviert**
RACADM-Update (neu)	Ja	Ja	Ja	Ja
iDRAC UI	Ja	Ja	Ja	Ja
Bandinternes Betriebssystem-DUP	Nein	k. A.	Ja	Nein

Tabelle 13. Firmware-Image-Dateitypen und -Abhängigkeiten (fortgesetzt)

.D10-Image			iDRAC DUP	
Schnittstelle	**Unterstützt**	**Erfordert LC aktiviert**	**Unterstützt**	**Erfordert LC aktiviert**
ANMERKUNG: Wenn das Update nach dem Durchführen eines bandinternen DUP-Updates nicht auf iDRAC bereitgestellt wird, wird ein Multipart: Rollback-Job erstellt.				
Redfish	Ja	k. A.	Ja	k. A.
Diagnose	Nein	Nein	Nein	Nein
Treiberpaket des Betriebssystems	Nein	Nein	Nein	Nein
iDRAC	Ja	Nein	Nein*	Ja
BIOS	Ja	Ja	Ja	Ja
RAID-Controller	Ja	Ja	Ja	Ja
BOSS	Ja	Ja	Ja	Ja
NVDIMM	Nein	Ja	Ja	Ja
Rückwandplatinen	Ja	Ja	Ja	Ja
ANMERKUNG: Für aktive Rückwandplatinen (Expander) ist ein Neustart des Systems erforderlich.				
Gehäuse	Ja	Ja	Nein	Ja
Netzwerkadapter	Ja	Ja	Ja	Ja
Stromversorgungseinheit	Ja	Ja	Ja	Ja
ANMERKUNG: Wenn ein manueller Neustart durchgeführt wird oder wenn das Update über das Betriebssystem durchgeführt wird, erfordert das PSU-Update einen Kaltneustart, damit das Update gestartet werden kann.				Ja
FPGA	Nein	Ja	Ja	Ja
ANMERKUNG: Nach Abschluss des FPGA-Firmwareupdate startet iDRAC automatisch neu. **ANMERKUNG:** Das Repo-Update wird für FPGA nicht unterstützt, während das FPGA-Update allein oder FPGA mit anderen Updates durchgeführt wird. **ANMERKUNG:** Wenn ein A/C-Zyklus durchgeführt wird, warten Sie, bis der Stromabfluss abgeschlossen ist (ca. 20 Sekunden), um ein ordnungsgemäßes Zurücksetzen des Systems sicherzustellen. Andernfalls wird möglicherweise in LCL und SEL Folgendes angezeigt: • SWC9016: FPGA kann aufgrund eines Problems mit einer nicht erfolgreichen kryptografischen Authentifizierung oder der Integrität nicht authentifiziert werden • SWC9018: Automatischer FPGA-Recovery-Vorgang kann aufgrund eines internen Fehlers nicht wiederhergestellt werden.				
FC-Karten	Ja	Ja	Ja	Ja
NVMe-PCIe-SSD-Festplatten	Ja	Nein	Ja	Nein
SAS-/SATA-Festplatten	Nein	Ja	Ja	Nein
TPM-Modul	Nein	Ja	Ja	Ja
Anwendung für Nicht-SDL-Software und -Peripheriegeräte	Nein	Nein	Nein	Nein

Firmware über die iDRAC-Webschnittstelle aktualisieren

Verwenden Sie die Firmware-Images vom lokalen System oder von einem Repository auf einer Netzwerkfreigabe (CIFS, NFS, HTTP, HTTPS oder FTP).

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 zum Update 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**. Die erforderliche Firmware wird auf iDRAC hochgeladen.
4. Nachdem der Hochladevorgang abgeschlossen ist, wird im Abschnitt **Aktualisierungsdetails** jede auf iDRAC hochgeladene Firmware-Datei mit ihrem Status angezeigt.

   ANMERKUNG: 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 Firmware-Datei aus und nehmen Sie einen der folgenden Schritte vor:
   - 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**. Aktualisierungen, bei denen ein Neustart des Systems erforderlich ist, werden stufenweise durchgeführt und beim nächsten Systemneustart übernommen. Es ist nur ein Systemneustart erforderlich, um alle Aktualisierungen durchzuführen.
   - Um die Aktualisierung der Firmware abzubrechen, klicken Sie auf **Abbrechen**.

   ANMERKUNG: 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 managen, 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 Firmwaredatei abgelaufen ist, können Sie nicht fortfahren. Dieses Problem kann nur über RACADM `reset` behoben werden.

   ANMERKUNG: Nachdem das Firmwareupdate abgeschlossen ist, 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 auf die Anmeldeseite weitergeleitet.

7. Wenn der Jobstatus **Abgeschlossen, virtuelles Ein-/Ausschalten ausstehend** ist, schalten Sie den Server physisch bzw. virtuell aus und ein.

   ANMERKUNG: Verwenden Sie die Redfish-URI (Redfish/v1/Chassis/System.Embedded.1/Actions/OEM/DellOemChassis.ExtendedReset mit ResetType=PowerCycle und FinalState=Ein/Aus (um das System nach abgeschlossenem

VAC einzuschalten oder im ausgeschalteten Zustand zu belassen), um den virtuellen Aus- und Einschaltvorgang durchzuführen. Wenn eine andere Methode zum Aus- und Einschalten verwendet wird, schlägt der Echtzeitjob möglicherweise fehl. Die aktualisierte Version spiegelt jedoch weiterhin das Aus- und Einschalten des Netzstroms wider.

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 OpenManage Handbücher > Repository Manager.

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.

Aktualisieren der Gerätefirmware über RACADM

Verwenden Sie zum Update der Gerätefirmware mit RACADM den Unterbefehl `update`. Weitere Informationen finden Sie im **Benutzerhandbuch für die Integrated Dell Remote Access Controller-RACADM-CLI**, verfügbar auf iDRAC-Handbücher.

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 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.

Ziehen Sie einen Server in Betracht, der über ein oder mehrere Geräte aus jeder der Gruppen A, B und C verfügt. Werden die DUPs nacheinander verwendet, sollte das erfolgreich sein. Wenn Sie NDT09 selbst verwenden, werden die Geräte in Gruppe A und Gruppe B aktualisiert. Wenn Sie 8J1P7 allein verwenden, werden Geräte in Gruppe B und Gruppe C aktualisiert. Wenn Sie jedoch versuchen, beide DUPs gleichzeitig zu verwenden, wird möglicherweise versucht, zwei Updates 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.d10`
2. Führen Sie den folgenden RACADM-Befehl aus:

   TFTP-Server

   - 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, an dem `firmimg.d10` gespeichert ist.
   - Verwendung des Befehls `update`:

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

   FTP-Server

   - 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, an dem `firmimg.d10` gespeichert ist.
   - Verwendung des Befehls `update`:

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

   Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Neustartfreie Updates

iDRAC unterstützt neustartfreie Updates. Mit dieser Funktion können Sie ein Firmwareupdate von iDRAC aus ohne Neustart des Hostservers durchführen, um das Update vor dem Laden des BETRIEBSSYSTEMS zu initiieren und durchzuführen. Um zu ermitteln, ob das DUP Seitenband-Updates unterstützt, gibt es Tags, mit denen festgestellt werden kann, ob die DUP-Firmware das direkte Seitenband-Update (PLDM, NVMe-MI usw.) und/oder die UEFI-FMP-Updatemethode und die Art der im DUP vorhandenen Payload unterstützt.

Wenn iDRAC die Komponenten inventarisiert, entscheidet es, ob die jeweilige Komponente direkte Seitenband-Updates oder UEFI-FMP-basierte Legacy-Updates unterstützt und einen Hostneustart erfordert oder nicht.

ANMERKUNG: Einige Geräte wie Netzwerkadapter benötigen möglicherweise ein Aus- und Einschalten für das Firmwareupdate.

Zwei für PLDM-Firmwareupate-Funktionen spezifische Eigenschaften sind im Softwarebestand aufgeführt: **PLDMCapabilitiesDuringUpdate** und **PLDMFDPCapabilitiesDuringUpdate**. Diese Parameter sind nur für Geräte verfügbar, die PLDM-Firmwareupdates unterstützen.

ANMERKUNG: Die PLDM-basierte Updatefunktion wird nur auf Plattformen mit 1 GB iDRAC-Speicher unterstützt.

Die iDRAC/LC-Updatemodule verarbeiten die Neustart- oder neustartlosen Methoden basierend auf dem Support. Im Folgenden sind die verschiedenen Updatemethoden aufgeführt:

- Direktes Seitenband-Update, Neustart zur Laufzeit identifiziert
- Direktes Seitenband-Update ohne Neustart
- SSM (UEFI FMP-basiert)/SMA-basiertes Update
- Redstone FPGA-Update von iDRAC
- FPGA-Update von iDRAC

ANMERKUNG: Im Falle von Repository-Updates müssen die Anwendungsupdates, für die kein Neustart des Hosts erforderlich ist, sofort durchgeführt werden.

ANMERKUNG: Für direkte Updates (Echtzeit-FW-Updates) von iDRAC gibt es einen LCLOG (SUP200, SUP0518, SUP516) mit einer Gerätebeschreibung (nutzerfreundliche FQDD-Informationen) anstelle der Produktbeschreibung.

ANMERKUNG: Wenn NVMe-Laufwerke hinter PERC (vorne) und direkt in der hinteren Rückwandplatine oder umgekehrt angeschlossen sind, funktioniert das Update ohne Neustart der direkt angeschlossenen Laufwerke nicht.

ANMERKUNG: Wenn Sie Firmwareupdates über die LC-Benutzeroberfläche für Storage-Komponenten durchführen, die ohne Neustart updatefähig sind, schlagen die Updates fehl. Verwenden Sie daher iDRAC-Schnittstellen für alle Firmwareupdates.

Anzeigen und Managen von gestuften Aktualisierungen

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

ANMERKUNG: Während der Durchführung von Updates oder anderen Aufgaben und Jobs darf der Host oder der iDRAC auf keine Weise neu gestartet, heruntergefahren oder aus- und eingeschaltet werden (manuell, mit den Tasten „Strg+Alt+Entf“ oder auf andere Weise über die iDRAC-Schnittstellen). Das System (Host und iDRAC) sollte immer ordnungsgemäß neu gestartet/heruntergefahren werden, wenn keine Aufgaben oder Jobs in iDRAC oder Host ausgeführt werden. Ein nicht ordnungsgemäßes Herunterfahren oder Unterbrechen eines Vorgangs kann zu unvorhersehbaren Ergebnissen wie Firmwarebeschädigung, Erzeugung von Core-Dateien, RSODs, YSODs, Fehlerereignissen in LCL usw. führen.

ANMERKUNG: Für alle Aktualisierungen, die iDRAC zurücksetzen/neu starten müssen, oder für den Fall, dass iDRAC neu gestartet wird, wird empfohlen, zu überprüfen, ob der iDRAC vollständig bereit ist. Warten Sie hierfür einige Sekunden im Intervall mit einer maximalen Zeitüberschreitung von 5 Minuten, bevor Sie einen anderen Befehl verwenden.

Anzeigen und Managen gestufter Aktualisierungen unter Verwendung von RACADM

Zur Anzeige der gestuften Updates über RACADM verwenden Sie den Unterbefehl `jobqueue`. Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Anzeigen und Managen gestufter Aktualisierungen unter Verwendung der iDRAC-Weboberfläche

Um die Liste der geplanten Jobs auf der iDRAC-Weboberfläche anzuzeigen, gehen Sie zu **Wartung** > **Jobwarteschlange**. Die Seite **Jobwarteschlange** zeigt den Status von Jobs in der Lifecycle Controller-Jobwarteschlange an. Weitere Informationen zu den angezeigten Feldern finden Sie in der **iDRAC-Online-Hilfe**.

Wählen Sie zum Löschen von Jobs die jeweiligen Jobs aus und klicken Sie auf **Löschen**. Die Seite wird aktualisiert, und der ausgewählte Job wird aus der Jobwarteschlange des Lifecycle Controller entfernt. Sie können alle Jobs in der Warteschlange löschen, die beim nächsten Neustart ausgeführt werden sollten. Sie können aktive Jobs, d. h. Jobs mit dem Status **Wird ausgeführt** oder **Wird heruntergeladen**, nicht löschen.

Sie brauchen Berechtigungen zur Serversteuerung, um Jobs zu löschen.

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 UI von Lifecycle Controller durchgeführt wurde, können Sie die Firmware über die iDRAC-Weboberfläche zurücksetzen. Sie können die Firmware für mehrere Geräte gleichzeitig im Rahmen eines einzigen Systemneustarts zurücksetzen.

Es wird empfohlen, die Firmware zu aktualisieren, um sicherzustellen, dass Sie über die neuesten Funktionen und Sicherheitsupdates verfügen. Setzen Sie das Update zurück oder installieren Sie eine frühere Version, wenn nach einem Update 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.

Sie können die Firmware der folgenden Komponenten zurücksetzen:

- Integrated Dell Remote Access Controller
- BIOS
- Netzwerkschnittstellenkarte (NIC)
- Netzteil (PSU)
- Speicher-Controller
- Rückwandplatine
- Softwarebasierter persistenter Speicher (SDPM)

ANMERKUNG: Für Lifecycle Controller, das Diagnoseprogramm, Treiberpakete und FGPA 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
- OME-Modular-Webschnittstelle
- iDRAC RACADM CLI
- Lifecycle-Controller-UI
- Redfish API

Rollback für die Firmware über die iDRAC-Webschnittstelle durchführen

So führen Sie einen Rollback der Geräte-Firmware aus:

1. Gehen Sie auf der iDRAC-Weboberfläche zu **Wartung** > **Systemupdate** > **Rollback**.
   Auf der Seite **Rollback** werden die Geräte aufgelistet, für die Sie ein Rollback der Firmware durchführen können. Sie können den Gerätenamen, die zugehörigen Geräte, die derzeit installierte Firmware-Version und die zum Zurücksetzen verfügbare Firmware-Version einsehen.
2. Wählen Sie eines oder mehrere Geräte aus, für die Sie einen Firmware-Rollback ausführen möchten.
3. Auf Grundlage der ausgewählten Geräten klicken Sie auf **Installieren und Neustart** oder **Beim nächsten Neustart installieren**.
   Wenn nur iDRAC ausgewählt wurde, klicken Sie auf **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 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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Easy Restore (Einfache Wiederherstellung)

Easy Restore verwendet den Easy Restore-Flash-Storage, um die Daten zu sichern. Wenn Sie das Secure Control Modul (SCM)) 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 das Service-Tag 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.

- Easy Restore (Einfache Wiederherstellung) sichert keine anderen Daten (z. B. Firmware-Images oder Erweiterungskarten-Daten).
- Durch den Austausch des Host Processor Memory Module (HPM) wird der Easy Restore-Prozess nicht initiiert.

ANMERKUNG: Beim Austausch des SCM müssen Sie manuell **Flüssigkeitsgekühlt** oder **Luftgekühlt** auswählen. Eine falsche Auswahl dieser Optionen führt zu thermischen Problemen auf der Plattform. In diesem Fall wenden Sie sich für die Wiederherstellung an den technischen Support von Dell.

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

- Service-Tag-Nummer des Systems
- Bestands-Tag
- Daten zu Lizenzen
- UEFI-Diagnoseanwendung
- Systemkonfigurationseinstellungen – BIOS, iDRAC
- Systemereignisprotokoll (SEL)
- OEM-ID-Modul

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) kann mehrere Minuten in Anspruch nehmen, manchmal 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 mithilfe der Dell Management Console oder Dell OpenManage Essentials ermitteln und überwachen. Sie können auch das Dell Remote Access Configuration Tool (DRACT) verwenden, um iDRACs zu ermitteln, Firmware zu aktualisieren und das Active Directory einzurichten. Weitere Informationen finden Sie im jeweiligen Benutzerhandbuch.

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.

ANMERKUNG: Für den SCP-Import sind Enterprise- oder Datacenter-Lizenzen erforderlich. Mit der Core-Lizenz können Sie nur SCP-Exporte durchführen.

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 UI initiiert wurde. Der Aufgabenstatus kann auf der Seite „Job Queue“ (Job-Warteschlange) angezeigt werden.

ANMERKUNG:

- Es sind nur der Hostname oder die IP-Adressen als Zieladresse zulässig.

- Sie können zum Importieren der Serverkonfigurationsdateien zu einem bestimmten Speicherort navigieren. Wählen Sie die Serverkonfigurationsdatei aus, 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.
- Um sicherzustellen, dass Benutzerrollen korrekt importiert werden, legen Sie den Wert **PasswordHashSaltset** und den Wert **Set on Import** in der SCP-Exportdatei auf **true** fest.

SCP ermöglicht Ihnen die Durchführung der Betriebssystembereitstellung (Operating System Deployment, 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 Hostbetriebssystem heruntergefahren.

   ANMERKUNG: Nur CIFS- und NFS-Freigaben werden für das Hosten von Betriebssystemdatenträgern unterstützt.

7. Der SCP-Orchestrator initiiert OSD durch Anhängen der Treiber für das ausgewählte Betriebssystem und initiiert dann einen Neustart des Betriebssystemdatenträgers, derin NFS/Share vorhanden ist.
8. LCL zeigt den Fortschritt des Jobs an.
9. Nach dem Starten des BIOS auf dem Betriebssystemdatenträger wird der SCP-Job als abgeschlossen angezeigt.
10. Der angeschlossene Betriebssystemdatenträger wird nach 65.535 Sekunden oder nach der durch das Attribut `OSD.1#ExposeDuration` angegebenen Dauer automatisch getrennt.

Detaillierte Informationen zur Gesamtfunktion zusammen mit dem Bereitstellungsworkflow finden Sie unter Verwenden von Serverkonfigurationsprofilen zur Bereitstellung von Betriebssystemen auf Dell PowerEdge-Servern.

Weitere Informationen zu SCP finden Sie unter Serverkonfigurationsprofile: Referenzhandbuch.

Importieren des Serverkonfigurationsprofils mithilfe der iDRAC-Webschnittstelle

Vor dem Importieren der SCP-Datei wird empfohlen, die Importvorschau durchzuführen. Dieser Vorgang ermittelt mögliche Formatierungsprobleme oder ungültige Attributeinstellungen, ohne den Zustand des Servers zu beeinträchtigen.

So importieren Sie das Serverkonfigurationsprofil:

1. Navigieren Sie zu **Konfiguration** > **Serverkonfigurationsprofil**.
   Die Seite **Serverkonfigurationsprofil** wird angezeigt.
2. Wählen Sie eine der folgenden Optionen aus, um den Standorttyp vorzugeben:
   - **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- oder HTTPS-Dateiübertragung.

   ANMERKUNG: Je nach Speicherorttyp müssen Sie die Netzwerkeinstellungen oder HTTP- oder HTTPS-Einstellungen eingeben. Wenn Proxy für HTTP oder HTTPS konfiguriert ist, sind auch die Proxy-Einstellungen erforderlich.
3. Wählen Sie die in der Option **Komponenten importieren** aufgeführten Komponenten aus.

4. Wählen Sie die Registerkarte **Shutdown** 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** > **Serverkonfigurationsprofil**.
   Die Seite **Serverkonfigurationsprofil** wird angezeigt.
2. Klicken Sie auf **Exportieren**.
3. Wählen Sie eine der folgenden Optionen aus, um den Standorttyp vorzugeben:
   - **Local** zum Speichern der Konfigurationsdatei auf einem lokalen Laufwerk.
   - **Network Share**, um das Sicherungsdatei-Image auf einer CIFS- oder NFS-Freigabe zu speichern.
   - **HTTP or HTTPS**, um das Sicherungsdatei-Image in einer lokalen Datei mittels HTTP/HTTPS-Dateiübertragung zu speichern.

   ANMERKUNG: Je nach Standorttyp 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, für die Sie die Konfiguration sichern möchten.
5. Wählen Sie den **Exporttypen** aus. Die folgenden Optionen sind verfügbar:
   - **Basic**: erstellt einen zerstörungsfreien Snapshot der Konfiguration.
   - **Ersatzexport**: ersetzt die Servereinstellungen durch neue Einstellungen oder stellt die Servereinstellungen auf eine bekannte Baseline wieder her.
   - **Klonexport**: klont die Einstellungen von einem Server auf einen anderen Server mit identischer Hardware. Alle Einstellungen außer I/O-Identität werden aktualisiert. Die Einstellungen in diesem Export sind destruktiv, wenn sie auf ein anderes System hochgeladen werden.
6. Wählen Sie ein **Export file format** aus.
7. Wählen Sie **Additional export items** aus.
8. Klicken Sie auf **Exportieren**.

Secure Boot-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 (Betriebssystem) 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 Betriebssystem-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.

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), Storage für öffentliche Schlüssel	1. `.cer` 2. `.der` 3. `.crt` 4. `.pbk`	Mehr als einer
DB und DBX	X.509-Zertifikat (nur binäres DER-Format), EFI-Image (System-BIOS berechnet und importiert 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.
- Zum Support 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-Policy auf „Nutzerdefiniert“ eingestellt werden.

Ist die Secure Boot-Richtlinie auf Nutzerdefiniert 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 „Nutzerdefiniert“ können die Optionen zur Verwaltung des Zertifikatsspeichers mit verschiedenen Aktionen wie Exportieren, Importieren, Löschen, Alle löschen, Zurücksetzen und Alles zurücksetzen für PK, KEK, Datenbank 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 Import-, Export-, Lösch- und Zurücksetzen-Vorgänge 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 Policies aus. „Alle löschen“ löscht alle Zertifikate und Image-Digests in der nutzerdefinierten 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 und Redfish einleiten. Informationen zum Durchführen

einer manuellen BIOS-Wiederherstellung finden Sie im Referenzhandbuch für die iDRAC RACADM-Befehlszeilenschnittstelle unter iDRAC-Handbücher.

iDRAC wiederherstellen

iDRAC unterstützt zwei Betriebssystem-Images, sodass immer ein startfähiger iDRAC verfügbar ist. Während eines unvorhergesehenen katastrophalen Fehlers, wenn Sie beide Startpfade verlieren, erkennt der iDRAC-Bootloader, dass kein startfähiges Image vorhanden ist. Der Bootloader zeigt die Early Boot-Videomeldungen auf dem angeschlossenen Monitor an.

Führen Sie die folgenden Schritte aus, um ein iDRAC wiederherzustellen:

1. Formatieren Sie eine USB-Karte mit FAT mit einem Windows-Betriebssystem oder EXT4 mit einem Linux Betriebssystem.
2. Kopieren Sie **firmimg.d10** oder DUP.exe in den Speicherort des USB-Laufwerks **/scm/Images/**.
3. Schließen Sie das USB-Laufwerk an den hinteren oberen USB-Anschluss des Servers an und schalten Sie den Servers ein und aus. Der Bootloader erkennt das USB-Laufwerk, liest die Payload, programmiert iDRAC neu und startet iDRAC neu.

5

Datenverarbeitungseinheit (Data Processing Unit, DPU)

Eine Datenverarbeitungseinheit (DPU) ist ein System auf einem Chip, das aus ARM-Cores, einer NIC-ASIC und Beschleunigungs-Engines besteht. Eine DPU ist programmierbar und kann potenziell ein Betriebssystem ausführen. DPUs kombinieren Netzwerkkonnektivität mit CPU-Cores, unabhängig vom Hypervisor oder Betriebssystem, sodass Beschleunigungs- und Offload-Services möglich sind. DPUs unterscheiden sich von herkömmlichen Offload-Engines durch ihre Flexibilität, Programmierbarkeit und die Fähigkeit, eine Vielzahl von Services zu hosten.

ANMERKUNG: DPUs erfordern eine iDRAC10 Enterprise- oder Datacenter-Lizenz.

Die Verwendung einer DPU bietet die folgenden Vorteile:

- Isoliert Infrastrukturservices vom Hostbetriebssystem und den Anwendungen.
- Ermöglicht einer Umgebung die Bereitstellung neuer Services unabhängig von der Hostanwendungsumgebung.
- Ermöglicht Hardwarebeschleunigung für datenintensive Vorgänge mit Kabelgeschwindigkeit.
- Gibt Server-/x86-CPU-Cores für die Unterstützung von Edge-Plattformen mit einem Sockel und Small Form Factor für Kundenanwendungen frei

Nachdem das DPU-Betriebssystem gestartet wurde, können zusätzliche PCIe-Funktionen initialisiert werden. Die BIOS-PCIe-Aufzählung (und der Hostbetriebssystem-/Hypervisor-Startprozess) erfolgt erst, nachdem das DPU-Betriebssystem gestartet wurde oder bereit ist.

Mit iDRAC können Sie die Einstellungen für den Modus „DPU OS Ready“ (Startsynchronisation) für jeden DPU-fähigen Steckplatz konfigurieren. Zu den möglichen Werten gehören:

- **Aktiviert:** DPU nimmt an der Durchführung der BIOS-PCIe-Aufzählung und des Hostbetriebssystem-/Hypervisor-Startprozesses teil.
- **Deaktiviert:** DPU nimmt nicht an der Durchführung der BIOS-PCIe-Aufzählung und des Hostbetriebssystem-/Hypervisor-Startprozesses teil.

Zu berücksichtigende Punkte zur DPU:

- Nur wenige Steckplätze sind DPU-fähig. Mit iDRAC können Sie die DPU-Startsynchronisation nur für diese Steckplätze konfigurieren.
- Die DPU-Startsynchronisationseinstellungen sind steckplatzbasiert (nicht identitätsbasiert). Wenn das DPU-Gerät also in einen anderen Steckplatz verschoben wird, verhält sich das Gerät gemäß der neuen Steckplatzkonfiguration.
- Die DPU-Startsynchronisationseinstellungen können auch ohne Vorhandensein eines DPU-Geräts konfiguriert werden.
- Wenn nach der Erkennung im Steckplatz kein DPU-Gerät installiert ist, sind die DPU-Startsynchronisationskonfigurationen NICHT wirksam.
- „Individual DPU OS Ready“ und „Overall DPU OS Ready“ werden in der LCL gemeldet.
- Auf einer nicht unterstützten DPU-Plattform zeigen die DPU-LC-Protokolle während der Durchführung einer Systemlöschung die SYS560-Meldung (`some of the DPU devices failed to reset`)) an. Wenn auf einer unterstützten DPU-Plattform die DPU nicht vorhanden ist und eine Systemlöschung durchgeführt wird, zeigen die Protokolle die SYS564-Meldung (`unable to perform system erase of DPU because there is no DPU available in the system`) an.
- Wenn die NVIDIA BF3-Karten in der BIOS-Konfiguration deaktiviert sind, wird der **Status** auf der Seite **Netzwerkgeräte** angezeigt. (**System** > **Übersicht** > **Netzwerkgeräte** > **Zusammenfassung**) in der iDRAC-Benutzeroberfläche wird grün angezeigt.
- Wenn die PCIe-Steckplätze der DPU BF3 DPU-Karten in der BIOS-Konfiguration (**System-BIOS-Einstellungen** > **Integrierte Geräte** > **Steckplatzdeaktivierung) Mit Starttreiber deaktiviert** sind, werden PR7- und PR8-Protokolle in den iDRAC-LC-Protokollen angezeigt.
- Der Gerätehardwarebestand wird für die NVIDIA BF3-Karten angezeigt, wenn für den PCIe-Steckplatz in der BIOS-Konfiguration **Startlaufwerk deaktiviert** ausgewählt ist.
- Wenn die Nokia RAN DPU-Karte auf den Energiesparmodus eingestellt ist, werden kritische LC-Protokolle angezeigt.

Folgendes sind die Hauptfunktionen der DPU:

- Sie können die DPU-Startsynchronisation für jeden DPU-fähigen Steckplatz konfigurieren.
- Sie können den Timeout-Wert für „DPU OS Ready“ in Minuten konfigurieren (von 0 bis 30).
- Basierend auf der Nutzerkonfiguration erfolgen die BIOS-PCIe-Aufzählung und der Hostbetriebssystem-/Hypervisor-Startprozess erst, nachdem jede **Startsynchronisierungs-aktivierte DPU** gemeldet hat, dass das DPU Betriebssystem bereit ist.

- Andere PCIe-Funktionen, die vom DPU Betriebssystem verfügbar gemacht werden, werden vom BIOS aufgelistet und in der iDRAC-Hardware-Bestandsaufnahme gemeldet.
- Das BIOS zeigt verschiedene DPU-bezogene Meldungen während des POST an:
  - **Erkennen von Datenverarbeitungseinheiten ...**: Beim Erkennen der DPU-Geräte
  - **Erkennen von Datenverarbeitungseinheiten ... Fertig**: Wenn die DPU-Erkennung abgeschlossen ist.
  - **Initialisieren der Datenverarbeitungseinheit (Starten Sie das System NICHT neu)**: Wenn die Startsynchronisation zu 0, 10, 20, 30, 40, 50, 60, 70, 80, 90 und 100% abgeschlossen ist
  - **Initialisieren der Datenverarbeitungseinheit ... Fertig**: Wenn die Startsynchronisation zu 100 % abgeschlossen und erfolgreich ist.
- Einzelne und allgemeine Meldungen zu „DPU OS Ready“ werden in LCL gemeldet.

  ANMERKUNG: Das Flag „DPU OS Ready“ bleibt während der Hostneustarts bestehen, und die Meldung „DPU OS Ready“ wird für jeden Hostneustart protokolliert.

- Wenn eine LC-SSM-Aufgabe vorhanden ist, überspringt das BIOS das Warten auf die DPU-Startsynchronisation.

Bestandsaufnahme und Überwachung von DPUs

Bei der iDRAC-Systembestandsaufnahme werden die Marke und das Modell der DPU während der Überwachung des Funktionszustands der DPU-Cores, Peripheriegeräte und des installierten Betriebssystems angezeigt. `GET` wird verwendet, um Bestandsinformationen abzurufen. Dadurch wird sichergestellt, dass keine nicht autorisierten Geräte in böswilliger Absicht installiert werden. Mithilfe des GET-Vorgangs können Sie die DPU-Integrität regelmäßig überprüfen. Wenn das System fehlerfrei ist, gibt es eine Payload-Antwort und eine Statusaktualisierung zurück, um Funktionszustandsaktualisierungen bereitzustellen.

Um bösartige oder versehentliche DPU-Betriebssysteminstallationen zu erkennen, verwenden Sie den GET-Vorgang. Mit dem GET-Vorgang können Sie den Namen des Betriebssystems, den Herstellernamen, die Version und den Status des DPU Betriebssystems abrufen.

Sie können die installierte DPU über die iDRAC UI anzeigen: **System** > **Bestandsaufnahme** > **Firmware-Bestandsaufnahme**.

Redfish

Mithilfe von Redfish können Sie eine einmalige Startkonfiguration festlegen, die verwendet wird, um die DPU nach dem Neustart mit dem konfigurierten Wert zu starten. Beim nächsten Neustart basiert der DPU-Start auf der konfigurierten Startreihenfolge. Redfish ermöglicht auch ARM-UEFI- und BMC-Firmware-Aktualisierungen. Weitere Informationen finden Sie unter developer.dell.com.

Serielle Konsole

Um über RACADM auf die serielle Steuerung zuzugreifen, melden Sie sich bei iDRAC SSH an und führen Sie den folgenden Befehl aus:

```
Racadm> console dpu
```

Koordiniertes Herunterfahren

Durch das interne Herunterfahren des ESXi-Betriebssystems wird DPU ESXio heruntergefahren, um die ESXio-Datei vor Beschädigung zu schützen.

6

Plug-in-Management

Plug-ins sind Softwarekomponenten, die die Funktionalität von iDRAC erweitern. Plug-ins werden einzeln in einem DUP verpackt. Plug-ins werden bei iDRAC-Neustart, -Reset oder -Ausschalt-Zyklen nicht gelöscht. Der iDRAC-Bereinigungsvorgang oder LC-Löschvorgang wird verwendet, um die Plug-ins zu entfernen. Sie können Plug-ins aktivieren oder deaktivieren.

Um Plug-ins über die iDRAC-UI zu managen, navigieren Sie zu **iDRAC-Einstellungen** > **Einstellungen** > **Plug-ins**.

ANMERKUNG: Für Installation, Update und Entfernung der Plug-ins benötigen Sie die Berechtigung zum Anmelden sowie Steuerungs- und Konfigurationsberechtigungen. Sie können die installierten Plug-ins mit Anmeldeberechtigung nur anzeigen.

Themen:

- Installieren eines Plug-ins
- Deinstallieren eines Plug-ins
- Ein Plug-in neu starten
- Plug-in aktivieren oder deaktivieren
- Anzeigen der Plug-in-Details

Installieren eines Plug-ins

Installieren Sie ein Plug-in, wenn Sie die Funktionalität von iDRAC erweitern möchten. Einige Plug-ins sind ab Werk von Dell in iDRAC für 15G, 16G und spätere Generationen von PowerEdge-Servern vorinstalliert.

Wenn eine Non-SDL-Karte (Non-Standard Device List) installiert ist, kann iDRAC kein SDK-Plug-in erkennen. Suchen und installieren Sie das SDK-Plug-in manuell. Aktualisierung, Downgrade oder Rollback des iDRAC-Firmware-Updates haben keine Auswirkungen auf die Funktionalität von Plug-Ins.

1. Laden Sie das Plug-in von Dell.com herunter.
2. Navigieren Sie zu **iDRAC-Einstellungen** > **Einstellungen** > **Plug-ins**
3. Klicken Sie auf **Hinzufügen/Update**.
4. Wählen Sie den **Speicherorttyp** aus, klicken Sie auf **Datei auswählen** und wählen Sie die Plug-in-Datei aus.
5. Klicken Sie auf **Hochladen**.
   Wenn ein Plug-in gültig ist, wird nach der Installation des Plug-ins eine Erfolgsmeldung angezeigt. Wenn die Hardware nicht vorhanden ist, wird eine LC-Meldung protokolliert, die darauf hinweist, dass das Plug-in nicht gestartet wurde. Wenn das Plug-in ungültig ist, wird eine Fehlermeldung angezeigt.

Deinstallieren eines Plug-ins

1. Gehen Sie zu **iDRAC-Einstellungen** > **Einstellungen** > **Plug-ins**.
2. Wählen Sie den/die NutzerIn aus und klicken Sie auf **Weiter**.
   Das Plug-in für Services wird deinstalliert.

Ein Plug-in neu starten

Sie können ein Plug-in neu starten, das in iDRAC installiert ist.

1. Gehen Sie zu **iDRAC-Einstellungen** > **Einstellungen** > **Plug-ins**.
2. Klicken Sie auf **Neustart.**

Plug-in aktivieren oder deaktivieren

Sie können Plug-ins aktivieren oder deaktivieren.

1. Gehen Sie zu **iDRAC-Einstellungen** > **Einstellungen** > **Plug-ins**.
2. Wählen Sie das Plug-in aus und klicken Sie auf **Aktivieren** oder **Deaktivieren**.

Anzeigen der Plug-in-Details

Sie können die Details der installierten Plug-ins anzeigen.

1. Gehen Sie zu **iDRAC-Einstellungen** > **Einstellungen** > **Plug-ins**.
2. Wählen Sie das Plug-in aus und klicken Sie auf **Details**.
   Die Details zum Plug-in werden angezeigt.

7

iDRAC konfigurieren

Mit iDRAC können Sie iDRAC-Eigenschaften konfigurieren, Nutzer 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.

Sie können iDRAC über die folgenden Komponenten konfigurieren:

- iDRAC-Weboberfläche
- RACADM
- IPMITool (siehe **Benutzerhandbuch zu den Dienstprogrammen des Dell OpenManage Baseboard Management Controller**)

ANMERKUNG: Während der Durchführung von Aufgaben und Jobs darf der Host oder der iDRAC auf keine Weise neu gestartet, heruntergefahren oder aus- und eingeschaltet werden (manuell, mit den Tasten „Strg+Alt+Entf“ oder auf andere Weise über die iDRAC-Schnittstellen). Das System (Host und iDRAC) sollte immer ordnungsgemäß neu gestartet oder heruntergefahren werden, wenn keine Aufgaben oder Jobs in iDRAC oder Host ausgeführt werden. Ein nicht ordnungsgemäßes Herunterfahren oder Unterbrechen eines Vorgangs kann zu unvorhersehbaren Ergebnissen wie Firmwarebeschädigung, Erzeugung von Core-Dateien, RSODs, YSODs, Fehlerereignissen in LCL usw. führen.

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. Richten Sie ggf. das erste Startlaufwerk ein.
15. Stellen Sie das Betriebssystem ggf. auf iDRAC-Passthrough.

Themen:

- iDRAC-Informationen anzeigen
- Netzwerkeinstellungen ändern
- Chiffresammlungs-Auswahl
- Modus FIPS (Konfiguration)
- Dienste konfigurieren
- Verwenden des VNC-Client für die Remote-Server-Verwaltung
- 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 auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Übersicht**, um die folgenden Informationen im Zusammenhang mit iDRAC anzuzeigen. Weitere Informationen zu den Eigenschaften finden Sie in der **iDRAC-Online-Hilfe**.

iDRAC-Informationen

- Gerätetyp
- Hardwareversion
- Firmware-Version
- Firmwareupdate
- RAC-Uhrzeit
- IPMI-Version
- Anzahl von möglichen Sitzungen
- Anzahl von aktuellen Sitzungen
- IPMI-Version

iDRAC Service Module

- Status

Verbindungsanzeige

- Status
- Switch-Verbindungs-ID
- Switch-Portverbindungs-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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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 einen lokalen RACADM ändern

Um eine Liste verfügbarer Netzwerkeigenschaften zu erstellen, verwenden Sie den Befehl

```
racadm get iDRAC.Nic
```

Wenn DHCP zum Abrufen 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.

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 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.

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 und die RACADM-Befehlszeilenschnittstellen konfiguriert werden.

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 **Referenzhandbuch zu Befehlszeilenschnittstellen für iDRAC RACADM** auf der Seite iDRAC-Handbücher.

Chiffresammlungs-Auswahl über die iDRAC-Weboberfläche 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 Cipher Suite-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.

ANMERKUNG: Unabhängig von der in iDRAC konfigurierten TLS-Version ermöglicht der FF-Browser in RHEL das Starten der iDRAC-UI.

ANMERKUNG: Um die Liste der Chiffren für einen bestimmten Port abzurufen, führen Sie das Tool „nmap“ aus.

So fügen Sie nutzerdefinierte Verschlüsselungszeichenfolgen (Cipher Strings) hinzu:

1. Gehen Sie in der iDRAC-Weboberfläche 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 finden Sie auf der Seite OpenSSL.
   - TLS 1.3 wird nicht unterstützt.

4. Klicken Sie auf **Anwenden**.
   Durch Einstellen der nutzerdefinierten Verschlüsselungszeichenfolge wird die aktuelle iDRAC-Sitzung beendet. Warten Sie ein paar Minuten, bevor Sie eine neue iDRAC-Sitzung öffnen.

Modus FIPS (Konfiguration)

FIPS ist ein Computersicherheitsstandard, den US-amerikanische Regierungsbehörden und deren Contractor verwenden müssen. iDRAC unterstützt die Aktivierung 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 Cryptographic Module Validation Program validiert wurde, wird als FIPS-validiert bezeichnet. Aufgrund des Zeitaufwands für die FIPS-Validierung 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“ auf der NIST-Website.

Deaktivieren des FIPS-Modus

Zum Deaktivieren des FIPS-Modus müssen Sie einen Reset von iDRAC auf die werksseitigen Voreinstellungen durchführen.

FIPS-Modus aktivieren

VORSICHT: Beim Aktivieren des FIPS-Modus werden die Standardeinstellungen von iDRAC wiederhergestellt. Wenn Sie die Einstellungen wiederherstellen möchten, sichern Sie das Serverkonfigurationsprofil (Server Configuration Profile, SCP), bevor Sie den FIPS-Modus aktivieren, und stellen Sie das SCP nach dem Neustart des iDRAC wieder her.

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.

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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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 beim Erstellen einer SSL-Zertifikatanforderung mindestens eine der IP-Adressen oder den DNS-Namen des Schlüsselverwaltungsservers in das Feld **Alternativer Name des Inhabers** aufnehmen. Stellen Sie sicher, dass die IP-Adresse das Format IP:xxx.xxx.xxx.xxx hat.

iLKM-Funktionen

iDRAC Local Key Management (iLKM) ist eine Sicherheitslösung, die dem Secure Enterprise Key Management (SEKM) ähnelt. Diese Lösung eignet sich ideal für NutzerInnen, die SEKM nicht verwenden, aber Geräte über den iDRAC sichern möchten. KundInnen können jedoch zu einem späteren Zeitpunkt zu SEKM migrieren. Weitere Informationen finden Sie im Whitepaper „Aktivieren von iLKM auf Dell PowerEdge-Servern“

.

Bei Verwendung von iLKM fungiert iDRAC als Key Manager und erzeugt Authentifizierungsschlüssel, die zum Sichern von Storage-Geräten verwendet werden. Um iLKM als Key-Management-System zu verwenden, navigieren Sie zu **iDRAC-Einstellungen** > **Services** > **iDRAC-Key-Management** und wählen Sie iLKM aus dem Drop-down-Menü aus.

ANMERKUNG: iLKM erfordert eine Kombination aus einer SEKM-Lizenz und iDRAC Enterprise-Lizenz oder einer SEKM-Lizenz und iDRAC Datacenter-Lizenz.

Sie müssen eine Passphrase und eine Schlüssel-ID angeben, um iLKM zu aktivieren. Die Länge der Passphrase und der Schlüssel-ID sollte maximal 255 Zeichen betragen.

ANMERKUNG:

- iLKM kann über die iDRAC-UI, RACADM- und Redfish-Schnittstelle angezeigt und konfiguriert werden.
- Es ist möglich, die Sicherheit auf unterstützten NVMe-SED zu aktivieren oder zu deaktivieren, wenn sich iDRAC im iLKM-Sicherheitsmodus befindet.
- Es ist nicht möglich, iLKM im Systemsperrmodus zu aktivieren, zu deaktivieren oder einen neuen Schlüssel zu erstellen.
- iLKM unterstützt derzeit nur Direct-Attached-NVMe-SEDs, die das TCG Opal 2.0-Protokoll und höher unterstützen.
- iLKM bietet eine Neuverschlüsselungsoption, bei der Sie die Passphrase und die Schlüssel-ID für die Authentifizierung angeben müssen.

Automatisches Sichern sicherungsfähiger Laufwerke

- Option zum Anfordern von iDRAC zur automatischen Sicherung nicht PERC-verbundener NVMe-SED und SAS-SED hinter einem geschützten SAS-HBA. Laufwerke werden bei einem Hostneustart oder auf einem Hot-Plug-Laufwerk automatisch gesichert.
- Die Option aktiviert nicht automatisch die Sicherheit auf Controllern wie PERC und SAS HBA.
- Die Option ist standardmäßig aktiviert und kann von NutzerInnen mithilfe des RACADM-Befehls deaktiviert werden.
- Deaktivieren Sie die Option, bevor Sie ein Laufwerk über die Option für kryptografisches Löschen (oder die PSID-Rücksetzoption) neu verwenden, wenn das Laufwerk nicht mehr durch iDRAC gesichert werden muss.

ANMERKUNG: Direct-Attached-NVMe-Laufwerke können verschlüsselungsfähig und nicht verschlüsselungsfähig sein. Für nicht verschlüsselungsfähige Laufwerke werden SEKM-044-Protokolle erzeugt, da der Plug-in-Status während des automatischen Sicherungsvorgangs für beide Direct-Attached-NVMe-Laufwerke überprüft wird.

ANMERKUNG: PSID-basiertes Zurücksetzen kann nur auf gesperrten oder fremden Laufwerken durchgeführt werden. PSID-basiertes Zurücksetzen kann nicht auf den Laufwerken durchgeführt werden, die mit dem PERC-Controller verbunden sind.

ANMERKUNG: Führen Sie den Aus- und Einschaltvorgang auf dem Hostsystem nicht unmittelbar nach dem Aktivieren der Option **Automatisches Sichern sicherungsfähiger Laufwerke** durch. Dies kann die Sicherheitsaktivierung auf den Laufwerken unterbrechen und die Laufwerke in den Sicherheitsstatus „nicht festgelegt“ versetzen.

Umstellung von iLKM auf SEKM

Sie müssen die iLKM-Passphrase zur Authentifizierung der Umstellung zusammen mit den SEKM-Konfigurationsdetails angeben. Wenn die Authentifizierung erfolgreich ist, wird SEKM auf dem iDRAC aktiviert und die vorherige iLKM-Schlüssel-ID wird gelöscht. Gehen Sie wie folgt vor, um von iLKM auf SEKM umzustellen:

1. Richten Sie das CSA-Zertifikat ein.
2. Konfigurieren Sie die SEKM-Einstellungen.

3. Führen Sie die Umstellung von iLKM zu SEKM durch.

SEKM-Funktionen

Nachfolgend sind die in iDRAC verfügbaren SEKM-Funktionen aufgelistet:

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 die folgenden zwei Optionen in der Benutzeroberfläche 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 und -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-UI erfolgen – **iDRAC-Einstellungen** > **Services** > **SEKM-Konfiguration** > **Schlüsselneuerstellung**. Nach der Durchführung 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 Storage-Controller kann auch über die iDRAC-UI erfolgen: **Storage** > **Controller** > **<Controller FQDD>** > **Aktionen** > **Bearbeiten** > **Sicherheit** > **Sicherheit (Verschlüsselung)** > **Schlüsselneuerstellung**.

     ANMERKUNG: Wenn Sie eine Schlüsselneuerstellung auf PERC ausführen, während die Controller- und iDRAC-Schlüssel synchronisiert sind, wird beim Ausführen des Jobs möglicherweise ein **Konfigurationsjobfehler** angezeigt, oder der Konfigurationsjob wird ausgeführt, doch der Schlüssel wird nicht geändert. Sie können die Option zur iDRAC-Schlüsselneuerstellung verwenden, um dieses Problem zu beheben.

5. **SEKM-Schlüsselneuerstellung nur von Redfish**: Die folgenden beiden SEKM-Schlüsselneuerstellungsoptionen werden von Redfish unterstützt:
   - **SEKM-Schlüsselneuerstellung über iDRAC-Zeitplan**: Sendet eine Anfrage zur Schlüsselneuerstellung von iDRAC zur automatischen Änderung der SEKM-Schlüssel, basierend auf einem vom Nutzer konfigurierten Wiederholungsintervall.
   - **Regelmäßige-iDRAC-SEKM-Synchronisierung mit Schlüsselmanagement-Server (KMS)**: Aktiviert die automatische Änderung der SEKM-Schlüssel entsprechend dem auf dem KMS-Server konfigurierten Wiederholungsintervall. IDRAC fragt jeden neuen Schlüssel ab, der vom KMS-Server erzeugt wird.

Detaillierte Informationen zu allen unterstützten SEKM-Funktionen und Bereitstellungsworkflows finden Sie im Whitepaper Aktivieren von OpenManage Secure EnterpriseKey Manager (SEKM) auf Dell PowerEdge-Servern.

ANMERKUNG: Wenn SEKM auf PERC aktiviert ist, wird das CTL136-Protokoll erzeugt. In PERC 12 wird bei der erneuten Schlüsselerstellung jedoch kein CTL136-Protokoll erzeugt. Dies liegt daran, dass der Controller keine Schlüsselanforderung erstellt, da Schlüssel als Teil des Befehls „rekey“ bereitgestellt werden.

Aktivieren oder Deaktivieren der HTTPS-Umleitung

Wenn Sie aufgrund einer Zertifikatwarnung in Bezug auf das standardmäßige iDRAC-Zertifikat oder als temporäre Einstellung für Debugging-Zwecke keine automatische Umleitung von HTTP zu HTTPs wünschen, können Sie iDRAC so konfigurieren, dass die Umleitung vom HTTP-Port (standardmäßig 80) zum HTTPS-Port (standardmäßig 443) deaktiviert ist. Standardmäßig ist dieser aktiviert. Sie müssen sich beim 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, um die HTTPS-Umleitung zu aktivieren oder zu deaktivieren.

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
```

Verwenden des VNC-Client für die Remote-Server-Verwaltung

Sie können einen offenen Standard-VNC-Client zur Remote-Server-Verwaltung mithilfe von Desktop- und mobilen Geräten wie Dell Wyse PocketCloud verwenden. Wenn Server in Rechenzentren nicht mehr funktionieren, sendet iDRAC oder das Betriebssystem eine Warnung an die Konsole der Management Station. Die Konsole sendet dann eine E-Mail oder eine SMS mit den erforderlichen Informationen an ein mobiles Gerät und startet die VNC Viewer-Anwendung auf der Management Station. Der VNC Viewer kann eine Verbindung zum Betriebssystem/zu Hypervisor auf dem Server herstellen und Zugriff auf Tastatur, Video und Maus des Host-Servers bereitstellen, um die erforderliche Fehlerbehebung durchzuführen. Aktivieren Sie vor dem Ausführen des VNC-Client den VNC-Server und konfigurieren Sie in iDRAC die VNC-Servereinstellungen wie Kennwort, VNC-Portnummer, SSL-Verschlüsselung und Zeitüberschreitungswert. Sie können diese Einstellungen über die iDRAC-Webschnittstelle oder RACADM konfigurieren.

ANMERKUNG: Die VNC-Funktion ist lizenziert und ist im Rahmen der iDRAC Enterprise-Lizenz erhältlich.

Sie können zwischen vielen VNC-Anwendungen oder Desktop-Clients beispielsweise von RealVNC oder Dell Wyse PocketCloud auswählen.

Zwei VNC-Clientsitzungen können gleichzeitig aktiviert werden. Die zweite Sitzung befindet sich im schreibgeschützten Modus.

Wenn eine VNC-Sitzung aktiv ist, können Sie den virtuellen Datenträger nur über die Option „Virtuelle Konsole starten“ starten, und nicht über den Viewer der virtuellen Konsole.

Wenn die Videoverschlüsselung deaktiviert ist, beginnt der VNC-Client direkt mit RFB-Handshake, wobei SSL-Handshake nicht erforderlich ist. Ist während des VNC-Client-Handshakes (RFB oder SSL) eine andere VNC-Sitzung aktiv oder eine Sitzung der virtuellen Konsole geöffnet, so wird die neue VNC-Clientsitzung abgelehnt. Nach Abschluss des anfänglichen Handshakes deaktiviert VNC-Server die virtuelle Konsole und lässt lediglich virtuelle Datenträger zu. Nach Beendigung der VNC-Sitzung stellt VNC-Server den ursprünglichen Zustand der virtuellen Konsole (aktiviert oder deaktiviert) wieder her.

ANMERKUNG:

- Wenn sie beim Starten einer VNC-Sitzung einen RFB-Protokollfehler erhalten, ändern Sie die VNC-Clienteinstellungen zu hoher Qualität und starten Sie die Sitzung dann neu.

- Wenn sich die iDRAC-NIC im freigegebenen Modus befindet und das Hostsystem aus- und wieder eingeschaltet wird, geht die Netzwerkverbindung für einige Sekunden verloren. Wenn Sie während dieser Zeit eine Aktion auf dem aktiven VNC-Client ausführen, wird die VNC-Sitzung möglicherweise geschlossen. Sie müssen auf die Zeitüberschreitung warten (der Wert, der für die VNC-Servereinstellungen auf der Seite **Dienste** in der iDRAC-Webschnittstelle konfiguriert ist) und anschließend die VNC-Verbindung neu herstellen.
- Wenn das VNC-Client-Fenster länger als 60 Sekunden minimiert wird, wird das Client-Fenster geschlossen. Sie müssen eine neue VNC-Sitzung öffnen. Wenn Sie das VNC-Client-Fenster innerhalb von 60 Sekunden maximieren, können Sie es weiterhin verwenden.

Konfigurieren von VNC-Server unter Verwendung der iDRAC-Webschnittstelle

So konfigurieren Sie die VNC-Servereinstellungen:

1. Gehen Sie auf der iDRAC-Weboberfläche zu **Konfiguration** > **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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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 so, dass die Verbindung auf `<localhost>:<localport number>` akzeptiert wird. Zum Beispiel: 127.0.0.1:5930.
2. Konfigurieren Sie den SSL-Tunnel für die Verbindung zu `<iDRAC IP address>:<VNC server port Number>`. Zum Beispiel: 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 stellen alle mit Remote Frame Buffer (RFB) kompatiblen VNC Viewer eine Verbindung zum VNC-Server her, indem sie die iDRAC-IP-Adresse und die Portnummer verwenden, die für den VNC-Server konfiguriert sind. Wenn die SSL-Verschlüsselungsoption während der Konfiguration der VNC-Servereinstellungen im iDRAC deaktiviert ist, gehen Sie wie folgt vor, um eine Verbindung zum VNC Viewer herzustellen:

Geben Sie im Dialogfeld **VNC Viewer** die iDRAC-IP-Adresse und die VNC-Schnittstellennummer in das Feld **VNC-Server** ein.

Das Format lautet `<iDRAC IP address:VNC port number>`.

Beispiel: Wenn die iDRAC-IP-Adresse 192.168.0.120 und die VNC-Port-Nummer 5901 lautet, dann geben Sie `192.168.0.120:5901` ein.

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. Nachdem Sie die NTP-Servereinstellungen aktiviert haben, melden Sie sich von allen aktuellen Sitzungen ab und melden sich dann bei iDRAC an.

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

Wenn Sie die NTP-Servereinstellungen aktivieren oder deaktivieren, melden Sie sich von allen aktuellen Sitzungen ab und melden Sie sich dann bei iDRAC an.

So konfigurieren Sie Zeitzone und NTP mithilfe der iDRAC-Web-Schnittstelle:

1. Gehen Sie zu **iDRAC-Einstellungen** > **Einstellungen** > **Zeitzone 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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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 Start oder für alle nachfolgenden Neustarts festlegen. Wenn Sie das Gerät so einstellen, dass es für alle nachfolgenden Startvorgänge verwendet werden soll, verbleibt als erstes Startgerät in der BIOS-Startreihenfolge, bis es erneut entweder über die iDRAC-Webschnittstelle oder über die BIOS-Startsequenz geändert wird.

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
- Lifecycle Controller
- BIOS Boot Manager
- UEFI-Gerätepfad
- UEFI HTTP
- Virtuelle Netzwerkdatei 1
- Virtuelle Netzwerkdatei 2

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. Gehen Sie zu **Konfiguration** > **Systemeinstellungen** > **Hardwareeinstellungen** > **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 beim nächsten Start einmalig vom ausgewählten Gerät zu starten, wählen Sie **Einmalig starten** aus. Danach startet das System vom ersten Startgerät in 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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Einstellen des ersten Startgeräts unter Verwendung der virtuellen Konsole

Sie können das Gerät auswählen, von dem aus gestartet werden soll, während der Server in der virtuellen Konsole angezeigt wird, bevor der Server die Startsequenz durchläuft. Der einmalige Start wird von allen Geräten unterstützt, die in Erstes Startgerät festlegen aufgeführt sind.

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.

Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough

Bei Servern, die Open Compute Project (OCP)-Karten 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 Managen von iDRAC über das Betriebssystem. Weitere Informationen finden Sie im Benutzerhandbuch zu iDRAC-Servicemodul auf der iDRAC Service Module-Seite.

Wenn der Browser durch eine dedizierte NIC aktiviert wurde, kann dieser im Host-Betriebssystem gestartet werden und dann auf die iDRAC-Webschnittstelle zugreifen.

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 (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 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 Type-C-USB-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 Betriebssysteme für USB-NIC

Eine Liste der Betriebssysteme, die für USB-NIC unterstützt werden, finden Sie in den entsprechenden Versionshinweisen unter iDRAC-Versionen und -Versionshinweise.

Für Linux-Betriebssysteme müssen Sie vor dem Aktivieren der USB-NIC die USB-NIC als DHCP auf dem Hostbetriebssystem konfigurieren.

Für vSphere müssen Sie vor dem Aktivieren von USB-NIC die VIB-Datei installieren.

ANMERKUNG:

- Wenn Sie USB-NIC auf dem iDRAC deaktivieren, während iSM im Betriebssystem ausgeführt wird, ändert sich der Status des iSM-Servicemoduls zu „Wird ausgeführt (eingeschränkte Funktionalität)“.
- Wenn Sie iSM im Betriebssystem installieren, während die USB-NIC im iDRAC deaktiviert ist, aktiviert iSM automatisch die USB-NIC im iDRAC, um die Installation abzuschließen. Deaktivieren Sie bei Bedarf USB-NIC, nachdem die Installation abgeschlossen ist.

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 ESXi-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. Geben Sie in der ESXi-Eingabeaufforderung den folgenden Befehl ein: `esxcfg-vmknic -l`.
Die Ausgabe zeigt den usb0-Eintrag.

Aktivieren und Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung von RACADM

Um das Passthrough zwischen Betriebssystem und iDRAC über RACADM zu aktivieren oder zu deaktivieren, verwenden Sie die Objekte in der Gruppe `iDRAC.OS-BMC`.

Weitere Informationen finden Sie in der Attributregistrierung für den Integrated Dell Remote Access Controller auf der Seite iDRAC-Handbücher.

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 IPs sind für den USB-NIC-Anschluss an der Vorderseite, wenn ein Type-C-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 **Fertig stellen** und anschließend auf **Ja**.
   Die Details werden gespeichert.

Aktivieren und Deaktivieren eines Betriebssystems für iDRAC-Passthrough unter Verwendung der Weboberfläche

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

1. Gehen 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 Link zwischen dem iDRAC und dem Hostbetriebssystem für Betriebssystem-zu-iDRAC-PassThrough wird über das LOM oder die OCP hergestellt.
   - **USB-NIC**: Der Link zwischen dem iDRAC und dem Hostbetriebssystem für Betriebssystem-zu-iDRAC-PassThrough wird über den internen USB hergestellt.

   ANMERKUNG: Wenn Sie den Pass-Through-Modus auf LOM einstellen, stellen Sie Folgendes sicher:
   - Das Betriebssystem und der iDRAC befinden sich im selben 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 Hostbetriebssystem nach dem Kaltstart zu starten.
   - Der LOM-Passthrough wird unter Verwendung der Funktion „dedizierter Modus“ 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 IPs sind für den USB-NIC-Anschluss an der Vorderseite, wenn ein Type-C-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.

   ANMERKUNG: Wenn Sie die statische IP-Adresse der USB-NIC ändern, wird der DHCP-Adressbereich automatisch an die neue statische IP angepasst. Wenn Sie beispielsweise die statische IP-Adresse auf 169.254.1.1 festlegen, wird die DHCP-Adresse auf 169.254.1.2 aktualisiert. Diese Änderung ist kompatibel mit dem Netzwerkmanager Wicked, der die neue DHCP-Adresse akzeptiert.
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 Hostbetriebssystem hergestellt ist.

Zertifikate abrufen

In der folgenden Tabelle werden die Zertifikattypen auf der Basis des Anmeldetyps aufgelistet.

Tabelle 15. Zertifikattypen auf der Basis des Anmeldetyps

Anmeldetyp	Zertifikattyp	Abrufmöglichkeit
Einmalige Anmeldung über Active Directory	Vertrauenswürdiges Zertifizierungsstellenzertifikat	Eine Zertifikatsignierungsanforderung (CSR) erstellen und diese von einer Zertifizierungsstelle signieren lassen. **ANMERKUNG:** SHA-2-Zertifikate werden ebenfalls unterstützt.
Smart Card-Anmeldung als lokaler oder Active Directory-Nutzer	• 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. **ANMERKUNG:** SHA-2-Zertifikate werden ebenfalls unterstützt.
Active Directory-Benutzeranmeldung	Vertrauenswürdiges Zertifizierungsstellenzertifikat	Dieses Zertifikat wird durch eine Zertifizierungsstelle ausgegeben. **ANMERKUNG:** SHA-2-Zertifikate werden ebenfalls unterstützt.
Lokale Benutzeranmeldung	SSL-Zertifikat	Zertifikatsignierungsanforderung (CSR) generieren und diese von einer vertrauenswürdigen Zertifizierungsstelle signieren lassen **ANMERKUNG:** Der iDRAC wird mit einem standardmäßigen selbstsignierten SSL-Serverzertifikat ausgeliefert. Der iDRAC-Webserver, die virtuellen Datenträger und die virtuelle Konsole verwenden dieses Zertifikat. **ANMERKUNG:** SHA-2-Zertifikate werden ebenfalls unterstützt.

SSL-Serverzertifikate

iDRAC beinhaltet einen Web-Server, der für die Verwendung des Industriestandard-Sicherheitsprotokolls SSL für die Übertragung von verschlüsselten Daten über ein Netzwerk konfiguriert ist. Eine SSL-Verschlüsselungsoption wird angeboten, um schwache Chiffren zu deaktivieren. 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-Verschlüsselungsstufe des Geräts auf 256 Bit oder höher und 168 Bit oder höher eingestellt ist, erfordern die Kryptografie-Einstellungen für die Umgebung Ihrer virtuellen Maschine (JVM, IcedTea) möglicherweise eine Installation der Richtliniendateien „Unlimited Strength Java Cryptography Extension“, um die Verwendung von iDRAC-Plug-ins wie der vConsole mit dieser höheren Verschlüsselungsebene zuzulassen. Weitere Informationen über das Installieren der Richtliniendateien finden Sie in der Dokumentation für Java.

iDRAC Web Server verfügt standardmäßig über ein selbstsigniertes, eindeutiges digitales SSL-Zertifikat von Dell. Sie können das standardmäßige SSL-Zertifikat durch ein von einer bekannten Zertifizierungsstelle (CA) signiertes Zertifikat ersetzen. Eine

Zertifizierungsstelle ist ein Unternehmen, das in der IT-Branche dafür anerkannt ist, hohe Ansprüche bezüglich der zuverlässigen Hintergrundüberprüfung, Identifizierung und anderer wichtiger Sicherheitskriterien zu erfüllen. Beispiele für Zertifizierungsstellen umfassen Thawte und VeriSign. Um den Vorgang zum Erhalt eines von einer Zertifizierungsstelle signierten Zertifikats zu beginnen, greifen Sie auf die iDRAC-Web-Schnittstelle oder RACADM-Schnittstelle über das Internet zu, um eine Zertifikatsignieranforderung (CSR) mit den Informationen Ihres Unternehmens zu erzeugen. Dann senden Sie die erzeugte CSR an eine Zertifizierungsstelle wie VeriSign oder Thawte. Dabei kann es sich um eine Stamm-Zertifizierungsstelle oder um einen Zertifikatvermittler handeln. Nachdem Sie das von der Zertifizierungsstelle signierte SSL-Zertifikat erhalten haben, laden Sie es auf iDRAC hoch.

Sie können das CA-Zertifikat über die iDRAC-Benutzeroberfläche über **iDRAC-Einstellungen** > **Services** > **Webserver** > **SSL/TLS-Zertifikatsignierungsanforderung** hochladen. Sie können auch Zertifikatdetails über andere Schnittstellen aufrufen.

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 ohne Zertifikat-Warnungen auf iDRAC zugreifen.

Sie können zur Signierung des SSL-Zertifikats auch ein nutzerdefiniertes Signaturzertifikat hochladen, anstatt auf das Standardsignaturzertifikat für diese Funktion zurückzugreifen. Durch Import eines nutzerdefinierten Signaturzertifikats in alle Management Stations wird allen iDRACs, die dieses nutzerdefinierte Signaturzertifikat verwenden, vertraut. Falls ein nutzerdefiniertes Signaturzertifikat hochgeladen wird, wenn bereits ein nutzerdefiniertes SSL-Zertifikat in Verwendung ist, dann wird das nutzerdefinierte SSL-Zertifikat deaktiviert und ein einmaliges, automatisch erzeugtes SSL-Zertifikat verwendet, das mit dem nutzerdefinierten Signaturzertifikat signiert ist. Sie können das nutzerdefinierte Signaturzertifikat herunterladen (ohne den privaten Schlüssel). Sie können auch ein vorhandenes Signaturzertifikat löschen. Nach dem Löschen des nutzerdefinierten Signaturzertifikats setzt iDRAC ein neues, selbst signiertes SSL-Zertifikat zurück und erzeugt es automatisch. Wenn ein selbst signiertes Zertifikat erneut erstellt wird, dann muss das Vertrauen zwischen iDRAC und der Management Workstation wiederhergestellt werden. Automatisch erzeugte SSL-Zertifikate sind selbst signiert und haben ein Ablaufdatum von sieben Jahren und einem Tag; das Startdatum liegt einen Tag zurück (wegen verschiedener Zeitzoneneinstellungen auf den Management Stations und dem iDRAC).

Das iDRAC-Webserver-SSL-Zertifikat unterstützt beim Erstellen einer Zertifikatsignierungsanforderung (CSR) das Sternzeichen (*) als Teil der am weitesten links gelegenen Komponente des allgemeinen Namens. Beispiel: *.qa.com oder *.company.qa.com. Dies wird als Platzhalter-Zertifikat bezeichnet. Wenn eine Platzhalter-CSR außerhalb von iDRAC erstellt wird, können Sie ein einziges signiertes Platzhalter-SSL-Zertifikat für mehrere iDRACs hochladen, wobei die iDRACs für die unterstützten Webbrowser vertrauenswürdig sind. Während der Verbindung zur iDRAC-Webschnittstelle mithilfe eines unterstützten Browsers, der Platzhalter-Zertifikate unterstützt, gilt iDRAC für den Browser als vertrauenswürdig. Beim Starten von Viewern gelten die iDRACs für die Viewer-Clients als vertrauenswürdig.

Sie können die Funktion zur Benachrichtigung über den Ablauf des Zertifikats aktivieren und auch das Benachrichtigungsintervall und die Benachrichtigungshäufigkeit konfigurieren. iDRAC stellt Benachrichtigungen zum Ablauf des Zertifikats bereit.

ANMERKUNG: Die selbstsignierten Standardzertifikate werden beim iDRAC-Neustart automatisch aktualisiert. Daher werden selbstsignierte Zertifikate für den Ablauf des Zertifikats nicht berücksichtigt.

Sie können die Zertifikatablaufbenachrichtigung und das Benachrichtigungsintervall über **iDRAC-Einstellungen** > **Services** > **Webserver** > **Einstellungen** aktivieren. Außerdem wird auf der iDRAC-Anmeldeseite am unteren Rand der Seite zum Ablauf des Zertifikats die Sicherheitswarnung angezeigt.

Neue Zertifikatsignierungsanforderung erstellen

Eine CSR ist eine digitale Anfrage an eine Zertifizierungsstelle (CA) für ein sicheres SSL-Serverzertifikat. SSL-Serverzertifikate ermöglichen es den Clients des Servers, der Identität des Servers zu vertrauen 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.

Nachdem die Zertifizierungsstelle die CSR genehmigt und das SSL-Serverzertifikat ausgestellt hat, kann das Zertifikat in den iDRAC hochgeladen werden. Die Informationen, die zum Erzeugen der CSR verwendet wurden und in der iDRAC-Firmware gespeichert sind, müssen mit den Informationen auf dem SSL-Serverzertifikat übereinstimmen. Das bedeutet, dass das Zertifikat unter Verwendung der durch iDRAC erstellten CSR erzeugt worden sein muss.

CSR über RACADM generieren

Um eine CSR über 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 erzeugen.

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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 der **iDRAC Online-Hilfe**.
3. Klicken Sie auf **Generate**.
   Daraufhin wird eine neue CSR generiert. Speichern Sie sie auf der Management Station.

Automatische Zertifikatregistrierung

Im iDRAC ermöglicht die ACE-Funktion (Automatic Certificate Enrollment) die automatische Installation und Erneuerung der Zertifikate, die vom Webserver verwendet werden. Wenn diese Funktion aktiviert ist, wird das vorhandene Web-Server-Zertifikat durch ein neues Zertifikat ersetzt. Geben Sie die Details der Zertifikatsignieranforderung (CSR, Certificate Signing Request) ein, bevor Sie ACE aktivieren.

ANMERKUNG:

- ACE ist eine lizenzierte Funktion und erfordert eine Datacenter-Lizenz.
- Für die Ausgabe des Serverzertifikats ist eine gültige NDES-Einrichtung (Network Device Enrollment Service) erforderlich.

Die iDRAC-Uhrzeit muss mit dem NDES/der Zertifizierungsstelle synchronisiert werden.

ANMERKUNG: Wenn die Uhrzeit nicht synchronisiert ist, erhält iDRAC während des Registrierungs- und Verlängerungsprozesses möglicherweise ungültige oder abgelaufene Zertifikate.

Nachfolgend sind die ACE-Konfigurationsparameter aufgeführt:

- Aktivieren und Deaktivieren
- SCEP-Server-URL/ACEM (Automatic Certificate Management Environment)
- Anfragekennwort

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

Nachfolgend sind die verfügbaren Status für ACE aufgeführt:

- Registriert – ACE ist aktiviert Das Zertifikat wird überwacht und ein neues Zertifikat kann nach Ablauf der Lizenz ausgestellt werden.
- Registrierung läuft – Zwischenzustand nach der Aktivierung von ACE
- Fehler – Problem mit dem NDES-Server
- Keine – Standardeinstellung

ANMERKUNG: Wenn Sie ACE aktivieren, wird der Web-Server neu gestartet und alle vorhandenen Web-Sitzungen werden abgemeldet.

ANMERKUNG: Die Erfolgs- und Fehlermeldungen können Sie in den Lifecycle-Protokollen einsehen.

Serverzertifikat hochladen

Nach der Generierung einer Zertifikatsignierungsanforderung (CSR) können Sie das signierte SSL-Serverzertifikat auf die iDRAC-Firmware hochladen. iDRAC muss zurückgesetzt werden, um das Zertifikat anzuwenden. iDRAC akzeptiert nur X509- und Base 64-kodierte Webserver-Zertifikate. SHA-2-Zertifikate werden ebenfalls unterstützt.

VORSICHT: Während des Resets ist iDRAC für einige Minuten nicht verfügbar.

Serverzertifikat über RACADM hochladen

Um das SSL-Serverzertifikat hochzuladen, verwenden Sie den Befehl `sslcertupload`. Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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 RACADM-Befehl `racreset` aus, um den 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 über die Web-Schnittstelle hochladen

So laden Sie das SSL-Serverzertifikat hoch:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **iDRAC-Einstellungen** > **Services** > **Web-Server** > **SSL/TLS-Zertifikatsignierungsanforderung**, wählen Sie **Serverzertifikat hochladen** aus und klicken Sie auf **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 Pop-up-Meldung angezeigt, in der Sie aufgefordert werden, iDRAC sofort oder zu einem späteren Zeitpunkt zurückzusetzen. Klicken Sie wie erforderlich auf **iDRAC zurücksetzen** oder **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 ist, bleibt das bestehende Zertifikat aktiv.

Serverzertifikat anzeigen

Sie können das SSL-Serverzertifikat, das derzeit in iDRAC verwendet wird, anzeigen.

Serverzertifikat über RACADM anzeigen

Um das SSL-Serverzertifikat anzuzeigen, verwenden Sie den Befehl `sslcertview`.

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Serverzertifikat über die Web-Schnittstelle anzeigen

Gehen Sie in der iDRAC-Weboberfläche zu **iDRAC Einstellungen** > **Services** > **Webserver** > **SSL-Zertifikat**. Die Seite **SSL** zeigt das SSL-Serverzertifikat an, das derzeit am oberen Rand der Seite verwendet wird.

Hochladen eines nutzerdefinierten Signaturzertifikats

Sie können ein benutzerdefiniertes Signaturzertifikat hochladen, um das SSL-Zertifikat zu signieren. SHA-2-Zertifikate werden ebenfalls unterstützt.

Hochladen von nutzerdefinierten Signaturzertifikaten mithilfe der Web-Schnittstelle

So laden Sie ein benutzerdefiniertes Signaturzertifikat mithilfe der iDRAC-Webschnittstelle hoch:

1. Navigieren Sie zu **iDRAC-Einstellungen** > **Services** > **Webserver** > **Nutzerdefiniertes Signierungszertifikat für SSL/TLS**.
   Die Seite **SSL** wird angezeigt.
2. Klicken Sie unter **Nutzerdefiniertes Signierungszertifikat für SSL/TLS** auf **Signierungszertifikat hochladen**.
   Die Seite **Benutzerdefiniertes SSL-Zeritfikatssignaturzertifikat hochladen** wird angezeigt.
3. Klicken Sie auf **Datei auswählen** und wählen Sie die benutzerspezifische SSL-Signierungszertifikatdatei aus.
   Es werden nur Zertifikate, die mit Public-Key Cryptography Standards #12 (PKCS #12) konform sind, unterstützt.
4. Wenn das Zertifikat kennwortgeschützt ist, geben Sie in das Feld **PKCS#12 Kennwort** das Kennwort ein.
5. Klicken Sie auf **Anwenden**.
   Das Zertifikat wird auf iDRAC hochgeladen.
6. Es wird eine Pop-up-Meldung angezeigt, in der Sie aufgefordert werden, iDRAC sofort oder zu einem späteren Zeitpunkt zurückzusetzen. Klicken Sie wie erforderlich auf **iDRAC zurücksetzen** oder **iDRAC später zurücksetzen**.
   Nach dem Zurücksetzen des iDRAC wird das neue Zertifikat 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.

Hochladen eines nutzerdefinierten SSL-Zeritfikatssignaturzertifikats unter Verwendung von RACADM

Um das benutzerdefinierte SSL-Signaturzertifikat über RACADM hochzuladen, verwenden Sie den Befehl `sslcertupload` und dann den Befehl `racreset`, um den iDRAC zurückzusetzen.

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat herunterladen

Sie können das nutzerdefinierte Signaturzertifikat mithilfe der iDRAC-Webschnittstelle oder RACADM herunterladen.

Herunterladen eines nutzerdefinierten SSL-Zeritfikatssignaturzertifikats unter Verwendung von RACADM

Um das benutzerdefinierte SSL-Signaturzertifikat herunterzuladen, verwenden Sie den Unterbefehl `sslcertdownload`. Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Benutzerdefiniertes Signierungszertifikat herunterladen

So laden Sie Benutzerdefinierte Signierungszertifikate unter Verwendung der iDRAC Webschnittstelle herunter:

1. Navigieren Sie zu **iDRAC-Einstellungen** > **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 nutzerdefinierte Signierungszertifikat an den Speicherort Ihrer Wahl speichern können.

Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat herunterladen

Sie können das nutzerdefinierte Signaturzertifikat mithilfe der iDRAC-Webschnittstelle oder RACADM herunterladen.

Herunterladen eines nutzerdefinierten SSL-Zeritfikatssignaturzertifikats unter Verwendung von RACADM

Um das benutzerdefinierte SSL-Signaturzertifikat herunterzuladen, verwenden Sie den Unterbefehl `sslcertdownload`. Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Benutzerdefiniertes Signierungszertifikat herunterladen

So laden Sie Benutzerdefinierte Signierungszertifikate unter Verwendung der iDRAC Webschnittstelle herunter:

1. Navigieren Sie zu **iDRAC-Einstellungen** > **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 nutzerdefinierte Signierungszertifikat an den Speicherort Ihrer Wahl speichern können.

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 Dell Handbücher-Seite.

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 (aufgeführt nach Gruppenname und Index) und alle Konfigurationseigenschaften für eine/n Nutzerln 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 Nutzer- 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 für das Ändern der iDRAC-Konfigurationseinstellungen über das Dienstprogramm für lokales RACADM oder die iDRAC-Einstellungen deaktivieren. Sie können die Konfigurationseinstellungen jedoch anzeigen. Gehen Sie hierfür folgendermaßen vor:

1. Gehen Sie auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Services** > **Lokale Konfigurationen**.
2. Aktivieren Sie eine oder beide der folgenden Optionen:
   - **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 das IPMITool nicht verwenden, um iDRAC-Konfigurationen durchzuführen. Sie können jedoch IPMI über LAN verwenden.

8

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.

9

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 Nutzersitzungen anzeigen und beenden.

Themen:

- Zustand und Eigenschaften des Managed System anzeigen
- Konfigurieren der Assetnachverfolgung
- System-Bestandsaufnahme anzeigen
- Anzeigen der Systemkomponenten
- Überwachen des Leistungsindex für CPU, Arbeitsspeicher und Eingabe-/Ausgabemodule
- Lesen von Firmware- und Hardwarebeständen
- Durchführen und Überprüfen des System-/Komponentenkonfigurationsstatus
- Durchführen und Überprüfen des Firmwareupdatestatus
- Erkennung eines Servers im Ruhezustand
- GPU-Verwaltung (Beschleuniger)
- Überprüfen der Frischlufttauglichkeit des Systems
- Temperaturverlaufsdaten anzeigen
- Konfigurieren des Warnungsschwellenwerts für die Einlasstemperatur
- Anzeigen der auf dem Host-Betriebssystem verfügbaren Netzwerkschnittstellen
- Anzeigen und Beenden von iDRAC-Sitzungen

Zustand und Eigenschaften des Managed System anzeigen

Wenn Sie sich bei der iDRAC-Weboberfläche 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**.

System-Bestandsaufnahme anzeigen

Sie können Informationen zu den Hard- und Firmwarekomponenten, die auf dem verwalteten System installiert sind, anzeigen. Um den Systembestand auf der iDRAC-Weboberfläche anzuzeigen, gehen Sie zu **System** > **Bestand**. Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der **iDRAC-Online-Hilfe**.

Der Abschnitt **Hardwarebestandsaufnahme** zeigt die Informationen für die folgenden Komponenten an, die auf dem Managed System verfügbar sind:

- iDRAC
- OEM
- RAID-Controller
- Batterien
- CPUs
- GPU
- DIMMs
- HDDs
- Rückwandplatinen
- Netzwerkschnittstellenkarten (integrierte und eingebettete)
- Grafikkarte
- Netzteile
- Lüfter
- Fibre-Channel-HBAs
- USB-Anschluss
- NVMe PCIe SSD-Geräte

ANMERKUNG: Im Hardwarebestand werden für jede GPU nur die Einträge BuildDate, GPUGUID und OEMInfo unterstützt und nur für NVIDIA-Geräte ausgefüllt. OEMInfo-Daten werden nur dann eingetragen, wenn Daten vom NVIDIA-Gerät für dieses Feld angegeben wurden.

In der folgenden Tabelle sind die Attribute und erwarteten Werte auf der Seite **Hardwarebestand** in der iDRAC-UI aufgeführt, wenn die Pensado-DPU-Karte HII nicht unterstützt:

Tabelle 16. Attribute und erwartete Werte

Attribute	Erwartete Werte
CurrentMACAddress	Leer
BusNumber	Zero
DataBusWidth	Leer
PCIDeviceID	Leer
PCISubDeviceID	Leer
PCISubVendorID	Leer
PCIVendorID	Leer
SlotLength	Leer
SlotType	Leer
LastSystemInventoryTime	01.01.1970 00:00:00
LastUpdateTime	01.01.1970 00:00:00
FCoEOffloadMode	Deaktiviert

Tabelle 16. Attribute und erwartete Werte (fortgesetzt)

Attribute	Erwartete Werte
iScsiOffloadMode	Deaktiviert
NicMode	Deaktiviert
MaxBandwidth	0
MinBandwidth	0

ANMERKUNG: Die bereitgestellte Bestandsaufnahme wird erst nach dem Start des Hosts aktualisiert. Bestände wie PCIe-Steckplätze und PCIe-Geräte im Hardwarebestand sind Teil des bereitgestellten Bestands, der während des Hoststarts (nach CSIOR) erzeugt wird. Selbst ein Hot-Plugging/Entfernen der Laufwerke ändert die Bestandsdaten nicht, es sei denn, der Host wird neu gestartet.

In der Benutzeroberfläche sind auf der Seite **Netzwerkgerät** > **Partitionsstatus** die Werte für PCI-Geräte-ID, minimale Bandbreite und maximale Bandbreite leer.

Auf der Seite **Netzwerkgerät** > **Einstellungen und Funktionen** ist der Wert für unterstützte Startprotokolle leer.

Der Abschnitt **Firmwarebestandsaufnahme** zeigt die Firmware-Version für die folgenden Komponenten an:

- BIOS
- Lifecycle Controller
- iDRAC
- Treiberpaket des Betriebssystems
- FPGA
- PERC-Controller
- Physische Laufwerke
- Netzteil
- Netzwerkadapter
- Fibre Channel
- Rückwandplatine
- Gehäuse
- PCIe-SSD-Laufwerke
- TPM-Modul
- iSM

ANMERKUNG: Für Komponenten, die keine Rollback-Funktion über iDRAC haben, wird das Veröffentlichungsdatum nicht im Softwarebestand angezeigt. Wenn eine Komponente vom Hostbetriebssystem aktualisiert wird, werden möglicherweise keine Rollback-Inhalte und Details zum Veröffentlichungsdatum ausgefüllt.

ANMERKUNG: Führen Sie nach dem Durchführen eines In-Band-Updates der Betriebssystemfirmware auf einem externen Gehäuse (JBOD) einen Kaltstart des Servers durch (Aus- und Einschalten), um die Gehäuseinformationen und die Systembestandsaufnahme in iDRAC zu aktualisieren.

ANMERKUNG: Die Firmware-Bestandsaufnahme kann lange dauern oder wird in einigen Fällen nicht angezeigt. Verwenden Sie den RACADM-Befehl `getremoteservicestatus`, bevor Sie die Firmware-Bestandsaufnahme ausführen.

ANMERKUNG:

- Der Softwarebestand zeigt nur die letzten 4 Byte der Firmwareversion und das Veröffentlichungsdatum an. Beispiel: Wenn die Firmware-Version FLVDL06 ist, zeigt die Firmware-Bestandsliste DL06 an.
- Bei SATA-Laufwerken werden für die Firmwareversion immer 4 Zeichen angezeigt. Wenn ein SATA-Laufwerk eine Firmwareversion mit mehr als 4 Zeichen hat, zeigt der Softwarebestand die letzten 4 Zeichen der Firmwareversion an und die Storage-Seite sowie der Hardwarebestand zeigen die vollständige Version an.
- Wenn Sie einen Softwarebestand über die Redfish-Oberfläche anzeigen, werden die Informationen zum Veröffentlichungsdatum nur für Komponenten angezeigt, die Rollbacks unterstützen.

ANMERKUNG:

- Die Firmwareversion des GPU-Bundles wird als 00.00.00.00 angezeigt:
  - bis ein Firmwareupdate über das DUP durchgeführt wurde.

- nachdem die Systemlöschung auf dem System durchgeführt wurde.

- Wenn es zu einem Kommunikationsfehler zwischen der GPU-Basisplatine und iDRAC kommt, wird die GPU-Bundle-Version möglicherweise nicht im Firmwarebestand angezeigt. Um das Kommunikationsproblem zu beheben, schalten Sie das System aus und wieder ein. Die Firmwareversion wird als 00.00.00.00 angezeigt, wenn die Kommunikation wiederhergestellt ist.
- Wenn sich ein Gerät (Beispiel: TPM) im AUS-Zustand befindet, zeigt der Softwarebestand die Version als **Nicht verfügbar** oder **0** an. Wenn die Anwendung nicht installiert ist, wird die Version als **Nicht installiert** angezeigt.
- Das System zeigt auf der Seite **Systembestand** das anfängliche Standard-Systemdatum und die Standard-Systemzeit als **Datum/Uhrzeit der Installation** an, bis eine neue Geräte-Firmwareversion mit dem DUP installiert wird. Außerdem sollten das/die BIOS- und iDRAC-Datum/Uhrzeit für Komponenten synchronisiert werden, deren Bestandsdetails vom BIOS abgerufen werden (Beispiel: BIOS, TPM).
- Das Installationsdatum ändert sich nicht, wenn die aktualisierte Version mit der installierten Version übereinstimmt.
- Manchmal wird im Feld **LastUpdateTime** einer Komponente im iDRAC-Hardwarebestand ein zukünftiges/vergangenes Datum angezeigt. Dies kann passieren, wenn entweder die BIOS- oder die HOST-Zeit auf ein falsches Datum eingestellt ist. Um dieses Problem zu beheben, korrigieren Sie das BIOS- oder HOST-Datum.

Wenn Sie eine Hardware-Komponente ersetzen oder die Firmware-Versionen aktualisieren, aktivieren Sie die Option **Bei Neustart Systeminformationen erfassen** (Collect System Inventory on Reboot, CSIOR) und führen Sie sie aus, um die Systembestandsaufnahme beim Neustart zu erfassen. Melden Sie sich nach einigen Minuten bei iDRAC an und navigieren Sie zur Seite **Systembestandsaufnahme**, um die Details anzuzeigen. Je nach der auf dem Server installierten Hardware kann es bis zu 5 Minuten dauern, bis die Informationen angezeigt werden.

ANMERKUNG: CSIOR-Option ist standardmäßig aktiviert.

ANMERKUNG: Konfigurationsänderungen und Firmware-Aktualisierungen, die innerhalb des Betriebssystems erfolgen, werden möglicherweise erst nach einem Serverneustart richtig in der Bestandsaufnahme angezeigt.

Klicken Sie auf **Exportieren**, um die Hardware-Bestandsaufnahme in ein XML-Format zu exportieren und speichern Sie sie an einen Speicherplatz Ihrer Wahl.

Anzeigen der Systemkomponenten

Die folgenden Komponenten auf der iDRAC-Benutzeroberfläche unterstützen Sie bei der Überwachung des Funktionszustands eines verwalteten Systems:

- **Batterien** – Bietet Informationen zu den Batterien auf dem Hauptplatinen-CMOS und dem Storage-RAID auf der Hauptplatine (ROMB).

  ANMERKUNG: Die Einstellungen für Storage-ROMB-Batterien sind nur verfügbar, wenn das System einen ROMB mit einer Batterie aufweist.

- **CPU** – Zeigt den Funktionszustand und den Status der CPUs im verwalteten System an. Meldet außerdem automatische Prozessordrosselung und vorhergesagte Fehler.
- **Arbeitsspeicher** – Zeigt den Funktionszustand und den Status der im verwalteten System vorhandenen DIMMs (Dual In-line Memory Modules) an.
- **Eingriff** – Zeigt Informationen zum Gehäuse an.
- **Stromversorgung** (nur für Rack- und Tower-Server) – Zeigt Informationen zu den Netzteilen und den Netzteil-Redundanzstatus an.

  ANMERKUNG: Wenn das System nur ein Netzteil aufweist, ist die Netzteilredundanz **deaktiviert**.

- **Spannung** – Zeigt den Status und die Messwerte des Spannungssensors für verschiedene Systemkomponenten an.
- **Kühlung** – Zeigt Details zu Lüftern und Hardwaretemperaturen an. Die vier Lüftertypen sind gebündelter Dual Rotor (Fan1A, Fan1B), gebündelter Single Rotor (Fan1A, Fan1B), nicht gebündelter Dual Rotor (Fan1, Fan2) und nicht gebündelter Single Rotor (Fan1, Fan2).
- **Accelerator** – Zeigt Details zu GPUs und Verarbeitungsbeschleunigern an.
- **PCIe-Steckplätze** – Zeigt Details zu allen PCIe-Geräten, einschließlich PCIe-SSD-Geräten (NVMe) an.
- **Netzwerkgeräte** – Zeigt Details zu allen Netzwerkgeräten, einschließlich DPUs an.

In der folgenden Tabelle sind die Systemkomponenten aufgeführt, die überwacht werden können:

ANMERKUNG: Die Seite **Systemübersicht** zeigt nur Daten für Sensoren an, die auf Ihrem System vorhanden sind.

Tabelle 17. Über die iDRAC-Benutzeroberfläche überwachte Systemkomponenten

Systemkomponenten	Navigationspfad in iDRAC
Batterien	**System** > **Übersicht** > **Batterien**
Kühlung	**System** > **Übersicht** > **Kühlung**
CPU	**System** > **Übersicht** > **CPU**
Arbeitsspeicher	**System** > **Übersicht** > **Arbeitsspeicher**
Eingriff	**System** > **Übersicht** > **Eingriff**
Stromversorgung	**System** > **Übersicht** > **Stromversorgung**
Wechselmedien	**System** > **Übersicht** > **Wechselmedien**
Spannungen	**System** > **Übersicht** > **Spannungen**
Netzwerkgeräte	**System** > **Übersicht** > **Netzwerkgeräte**
Accelerator	**System** > **Übersicht** > **Accelerator**
PCIe-Steckplätze	**System** > **Übersicht** > **PCIe-Steckplätze**

Verwenden Sie den Befehl `racadm getsensorinfo`, um die Details zu jeder dieser Komponenten abzurufen.

ANMERKUNG: Aktuelle Informationen zu den unterstützten Eigenschaften und deren Werten finden Sie in der **iDRAC-Onlinehilfe**.

Überwachen des Leistungsindex für CPU, Arbeitsspeicher und Eingabe-/Ausgabemodule

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 Rechenwerte, Arbeitsspeicher- und I/O-Ressourcenauslastungswerte als CUPS-Index bereitstellt. iDRAC überwacht den CUPS-Index für die Systemauslastung und auch die momentanen Werte des CPU-, Arbeitsspeicher- und I/O-Auslastungsindex.

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 Storage-Controller-Instanzen auftritt. Die Daten von den RMCs werden kombiniert, um den gesamten Speicherdatenverkehr über alle Speicherkanäle im System zu messen. Dies ist ein Maß für die Speicherbandbreitennutzung und nicht für die Speicherauslastung. iDRAC sammelt die Daten eine Minute lang, sodass 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 für CPU-, Storage- und I/O-Module über RACADM

Verwenden Sie den Unterbefehl **SystemPerfStatistics** zur Überwachung des Leistungsindex für CPU, Arbeitsspeicher und I/O-Module. Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Überwachen des Leistungsindex für CPU-, Storage- und I/O-Module über die Weboberfläche

Um den Leistungsindex von CPU, Arbeitsspeicher und I/O-Modulen zu überwachen, gehen Sie auf der iDRAC-Weboberfläche zu **System** > **Leistung**.

- Abschnitt **Systemleistung** – Zeigt den aktuellen Messwert und den Warnungsmesswert für den CPU-, Storage- und I/O-Auslastungsindex sowie den CUPS-Index auf Systemebene in einer grafischen Ansicht an.
- Abschnitt **Historische Daten der Systemleistung**:
  - Dieser Abschnitt enthält die Statistiken zu CPU, Arbeitsspeicher und I/O-Auslastung und den Systemebenen-CUPS-Index. Wenn das Hostsystem ausgeschaltet ist, zeigt das Diagramm die Ausschaltlinie unter 0 % an.
  - Sie können die Spitzenauslastung für einen bestimmten Sensor zurücksetzen. Klicken Sie auf **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 Warnungsschwellenwert für die Auslastung an und ermöglicht die Festlegung des Werts. Sie müssen über die Berechtigung zur Serverkonfiguration verfügen, um die Schwellenwerte festzulegen.

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

Lesen von Firmware- und Hardwarebeständen

ANMERKUNG: Stellen Sie sicher, ein paar Sekunden abzuwarten, während Sie den Befehl `getremoteservicesstatus` mit einem Timeout von 5 Minuten verwenden.

1. Verwenden Sie die Methode/URI/den Befehl `getremoteservicesstatus`, um zu überprüfen, ob der Lifecycle Controller(LC)-Status bereit ist. Stellen Sie sicher, dass das System mindestens einmal **eingeschaltet** ist und **CSIOR (Collect System Inventory On Restart)** mindestens einmal ausgeführt wurde, um die richtigen Details zu erhalten. Basierend auf der Anforderung für einige Komponenten wie Storage und Netzwerk müssen Sie möglicherweise auch überprüfen, ob sich das System im Status **Außerhalb von POST** und **Echtzeit (EZ)** befindet.

2. Das maximale Timeout, damit LC bereit ist, sollte 5 Minuten betragen. Stellen Sie sicher, dass sich das System im folgenden Zustand befindet, damit der LC-Status bereit ist:
   - Außerhalb von POST
   - Job wird noch nicht ausgeführt
   - Nicht in LC-GUI
   - Host steckt in POST fest
3. Sobald der LC-Status bereit ist, verwenden Sie die Methode/URI/den Befehl `getinventory`.

Durchführen und Überprüfen des System-/Komponentenkonfigurationsstatus

ANMERKUNG: Stellen Sie sicher, ein paar Sekunden abzuwarten, während Sie den Befehl `getremoteservicesstatus` mit einem Timeout von 5 Minuten verwenden.

1. Überprüfen Sie die Firmware-Bestandsaufnahme (befolgen Sie das oben genannte Verfahren).
2. Um mögliche Ausfälle später zu vermeiden, stellen Sie sicher, dass die erforderliche Komponente im System vorhanden ist.
3. Verwenden Sie die Methode/URI/den Befehl `getremoteservicesstatus` nach den ersten Prüfungen, um zu überprüfen, ob der LC-Status bereit ist. Basierend auf der Anforderung für einige Komponenten wie Storage und Netzwerk muss möglicherweise ein anderer Status geprüft werden, z. B. ob sich das System im Status **Außerhalb von POST** und **Echtzeit (EZ)** befindet.
4. Sobald LC bereit ist, verwenden Sie die System-/Komponentenkonfigurationen und erstellen Sie den Job.
5. Erstellen Sie einen Neustartjob oder starten Sie den Host neu, wenn die Konfiguration einen Neustart des Hosts erfordert. Bestimmte Konfigurationseinstellungen erfordern möglicherweise einen Kaltstart.
6. Der Aufrufer muss prüfen, ob der Jobstatus abgeschlossen ist: **Erfolg/Fehler**. Rufen Sie die Lebenszyklusprotokollereignisse und den Jobwarteschlangenstatus auf und prüfen Sie die Konfigurationsergebnisse, um weitere Details zu den Fehlern zu erhalten.
7. Erst nachdem **CSIOR (Collect System Inventory On Restart)** auf dem Host bei Bedarf erfolgreich abgeschlossen wurde, wird der Job als abgeschlossen markiert, wenn er nicht fehlgeschlagen ist. Dies gilt, wenn ein Neustart des Hosts erforderlich ist.
8. Wenn der Job abgeschlossen ist, warten Sie 30 Sekunden lang und verwenden Sie dann die Methode/URI/den Befehl `getremoteservicesstatus`, um zu überprüfen, ob der LC-Status bereit ist, mit dem anderen erforderlichen Status, und lesen Sie dann die erwarteten Werte.

Durchführen und Überprüfen des Firmwareupdatestatus

ANMERKUNG: Stellen Sie sicher, ein paar Sekunden abzuwarten, während Sie den Befehl `getremoteservicesstatus` mit einem Timeout von 5 Minuten verwenden.

1. Überprüfen Sie die Firmware-Bestandsaufnahme (befolgen Sie das oben genannte Verfahren).
2. Um mögliche Ausfälle später zu vermeiden, überprüfen Sie, ob die zu aktualisierende Komponente im System vorhanden ist und/oder ob das richtige unterstützte Dell Update Package (DUP) zum Hochladen ausgewählt ist.
3. Verwenden Sie die Methode/URI/den Befehl `getremoteservicesstatus` nach den ersten Prüfungen, um zu überprüfen, ob der LC-Status bereit ist.
4. Sobald LC bereit ist, verwenden Sie die Methode/URI/den Befehl `firmwareupdate` und übergeben Sie das richtige DUP, um das Update zu starten.
5. Wenn für das Update ein Neustart des Hosts erforderlich ist, erstellen Sie einen Neustartjob oder starten Sie den Host neu. Strom-, OSM- und PERC-Updates erfordern einen Kaltneustart.
6. Prüfen Sie, ob der Jobstatus **erfolgreich/fehlgeschlagen** ist. Rufen Sie die Lebenszyklusprotokollereignisse und den Jobwarteschlangenstatus auf und suchen Sie nach den Konfigurationsergebnissen, um weitere Details zu den Fehlern zu erhalten.
7. Erst nachdem **CSIOR (Collect System Inventory On Restart)** auf dem Host bei Bedarf erfolgreich abgeschlossen wurde, wird der Job als abgeschlossen markiert, wenn er nicht fehlgeschlagen ist, selbst bei mehreren oder Katalogupdates. Daher wird empfohlen, dass der Aufrufer kein eigenes Timeout hat oder ein größeres Zeitfenster als dieses Timeout aufweisen sollte
8. Wenn das Update länger als 6 Stunden hängen bleibt (d. h. das Jobmodul erhält vom Updatemodul 6 Stunden lang keinen Status), kann es sein, dass der Job ein Timeout aufweist und fehlschlägt.
9. Die Update-Timeouts basieren auf der Empfehlung des Geräteteams, die zur Laufzeit gelesen wird.
10. Wenn der Job als abgeschlossen markiert ist und der Bestand die neuen Änderungen, die gerade angewendet wurden, nicht meldet, warten Sie auf 30 Sekunden lang und überprüfen Sie den Bestand erneut.

Erkennung eines Servers im Ruhezustand

Der iDRAC bietet einen bandexternen Leistungsüberwachungsindex der Server-Komponenten wie CPU, Storage 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/iDRAC.Embedded.1/Oem/Dell/DellAttributes/
System.Embedded.1
```

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 zu den GPUs überwachen.

Im Folgenden sind die GPU-Eigenschaften und die Lizenzdetails aufgeführt:

Tabelle 18. GPU-Eigenschaften und Lizenzdetails

GPU-Eigenschaften	Lizenz
Bestandsaufnahme	
Platinen-Teilenummer	Alle Lizenzen
OEM-Info	Alle Lizenzen
Seriennummer	Alle Lizenzen
Marketingname	Alle Lizenzen
GPU-Teilenummer	Alle Lizenzen

Tabelle 18. GPU-Eigenschaften und Lizenzdetails (fortgesetzt)

GPU-Eigenschaften	Lizenz
Build-Datum	Alle Lizenzen
Firmware-Version	Alle Lizenzen
GPU-GUID	Alle Lizenzen
PCI-Anbieter-ID	Alle Lizenzen
PCI-Geräte-ID	Alle Lizenzen
PCI-Unteranbieter-ID	Alle Lizenzen
PCI-Untergeräte-ID	Alle Lizenzen
GPU Status	Alle Lizenzen
GPU-Integrität	Alle Lizenzen
Temperaturkennzahlen	
Primäre GPU-Temperatur	Alle Lizenzen
Sekundäre GPU-Temperatur	Alle Lizenzen
Platinentemperatur	Alle Lizenzen
Arbeitsspeichertemperatur	Alle Lizenzen
Min. GPU-HW-Drosselungstemperatur	Enterprise
GPU-Temperatur beim Herunterfahren	Enterprise
Max. Storage-Betriebstemperatur	Enterprise
Max. GPU-Betriebstemperatur	Enterprise
Temperatur-Warnmeldungsstatus	Enterprise
Strombremsstatus	Enterprise
Stromkennzahlen	
Stromverbrauch	Alle Lizenzen
Netzteilstatus	Enterprise
Stromversorgungsstatus der Platine	Enterprise

ANMERKUNG:

- GPU-Eigenschaften werden nicht für integrierte GPU-Karten aufgelistet und der Status wird als **Unbekannt** gekennzeichnet.
- Die Betriebstemperatur kann bei AMD-basierten Systemen anders ausfallen.
- Die Anzahl der GPU-Einträge pro PCIe-Steckplatz, die auf dem Host angezeigt werden, kann sich von der im iDRAC unterscheiden.
- Wenn nach der Durchführung von gebündelten oder Komponenten-Firmwareupdates für GPUs oder PDB-FPGAs ein manuelles Aus- und Einschalten erforderlich ist, wird das SUP0545-Ereignis in LC-Protokollen (Lifecycle) angezeigt. Stellen Sie nach diesem Ereignis sicher, dass Sie ein manuelles Aus- und Einschalten durchführen, um unerwartetes Verhalten im Server zu vermeiden.
- Achten Sie nach einem GPU-Firmwareupdate, das Updates der Komponentenfirmware oder gebündelte Firmwareupdates umfasst, darauf, dass Sie ein virtuelles Aus- und Einschalten durchführen, um das Update abzuschließen. Auf diese Weise wird unerwartetes Verhalten in iDRAC im Zusammenhang mit GPUs vermieden.
- Im persistenten Modus sind die Grenzwerte für die GPU-Strombegrenzung während des Warmstarts möglicherweise nicht korrekt.
- Die GPU-Strombegrenzungsfunktion ist in der Nicht-A2-GPU-Konfiguration nicht verfügbar.

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. Im Folgenden die Integritätsparameter, die vom GPU-Gerät abgerufen werden:

- Stromversorgung
- Temperatur
- Thermische Auslegung

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.

Wenn der Warm-Neustart und der persistente Modus deaktiviert sind, sehen wir das folgende Verhalten:

- Der Stromverbrauch wird als N/A angezeigt.
- Die Stromobergrenze wird mit älteren Bestandsgrenzwerten angezeigt.

Auf dem Hostsystem muss der NVIDIA GPU-Treiber installiert sein und ausgeführt werden, damit verschiedene GPU-Funktionen verfügbar sind. Einige der verfügbaren GPU-Funktionen sind „Stromverbrauch“, „aktueller Grenzwert für die Stromobergrenze“, „GPU-Strombegrenzung und -beschränkung“, „GPU-Zieltemperatur“, „minimale GPU-Drosselungstemperatur“, „GPU-Temperatur beim Herunterfahren“, „maximale Speicher-Betriebstemperatur“ und „maximale GPU-Betriebstemperatur“, „GPU-Auslastung“ usw. Diese Werte werden als **N/A** angezeigt, wenn der NVIDIA GPU-Treiber nicht installiert ist. GPU-Funktionen, die vom geladenen und ausgeführten Treiber abhängen, sind nicht auf diese Liste beschränkt.

Wenn in Linux die Karte nicht verwendet wird, setzt der Treiber die Karte nach unten und wird entladen, um Energie zu sparen. In solchen Fällen sind der Stromverbrauch, die aktuelle Stromobergrenze, GPU-Strombegrenzung und -beschränkung, GPU-Zieltemperatur, minimale GPU-Drosselungstemperatur, GPU-Temperatur beim Herunterfahren, max. Speicher-Betriebstemperatur, max. Speicher-Betriebstemperatur, max. GPU-Betriebstemperatur, GPU-Auslastung und andere Funktionen 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 zu den Telemetriefunktionen finden Sie in Telemetrie-Streaming.

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.

Monitoring von Verarbeitungsbeschleunigern

Beschleunigergeräte mit PCI-Verarbeitungsbeschleunigern benötigen eine Temperatur- und Sensorüberwachung in Echtzeit, da sie bei der Nutzung erhebliche Wärme generieren.

Führen Sie die folgenden Schritte aus, um die Bestandsinformationen der **Verarbeitenden Accelerators** abzurufen:

1. Schalten Sie den Server aus.
2. Installieren Sie die Beschleuniger auf der Riser-Karte.
3. Schalten Sie den Server ein.
4. Warten Sie, bis der POST abgeschlossen ist.
5. Melden Sie sich an der iDRAC-UI an.
6. Navigieren Sie zu **System** > **Übersicht** > **Beschleuniger**. Es werden sowohl der GPU- als auch der Verarbeitungsbeschleuniger-Abschnitt angezeigt.
7. Erweitern Sie den betreffenden Beschleuniger, um die folgenden Sensorinformationen anzuzeigen:
   - Stromverbrauch
   - Temperaturdetails

ANMERKUNG: Logische Temperatursensoren werden in den iDRAC-Schnittstellen nicht angezeigt. Es werden nur physische Temperatursensoren angezeigt.

ANMERKUNG: Sie müssen über die iDRAC-Anmeldeberechtigung verfügen, um auf die Informationen der Beschleuniger zugreifen zu können.

ANMERKUNG: Stromverbrauchssensoren stehen nur für die unterstützten Beschleuniger zur Verfügung und sind nur mit einer Datacenter-Lizenz verfügbar.

ANMERKUNG: iDRAC-Schnittstellen zeigen möglicherweise nicht die Informationen der Strom- und Temperatursensoren an, die vom Hostbetriebssystem (Betriebssystem) abhängen. Installieren Sie in diesem Fall die GPU-Treiber (ROCm-Paket) im Hostbetriebssystem.

ANMERKUNG:

- Es wird empfohlen, das CEC-Firmwareupdate für die A100 GPU vor dem Firmwareupdate der Beschleuniger durchzuführen.
- Führen Sie das CEC- und Beschleuniger-Firmwareupdate der GPU nicht gleichzeitig durch, um ein Fehlschlagen der Updates zu vermeiden. Führen Sie nach dem Fehlschlagen des Firmwareupdates ein Aus- und Einschalten oder ein virtuelles Einschalten durch. Auf diese Weise wird ein weiteres Fehlschlagen eines einzelnen Updates aufgrund eines vorherigen Updatefehlers vermieden.
- Das Firmwareupdate für den HGX A100 8-GPU-Baseboard-FPGA kann zwischen 60 und 90 Minuten dauern.
- DUP-Updates von HGX A100 8-GPU-Baseboard-FPGA und CEC dürfen nicht gleichzeitig gestartet werden. Es wird empfohlen, die folgenden Schritte auszuführen:
  1. Aktualisieren Sie die CEC-Firmware.
  2. Führen Sie einen virtuellen oder manuellen Einschaltzyklus durch.
  3. Aktualisieren Sie die FPGA-Firmware.
  4. Führen Sie einen weiteren virtuellen oder manuellen Einschaltzyklus durch.
- Um das PDB-FPGA vom Betriebssystem aus zu aktualisieren, führen Sie einen Kaltstart durch. Nach dem Update wird ein virtueller Einschaltzyklus durchgeführt.

ANMERKUNG: Gelegentlich senden die FPGA-Geräte „0“-Werte für den Stromverbrauch. Folglich verwendet PLDM auch „0“-Werte und zeigt dies in der Benutzeroberfläche an. Die Werte werden jedoch in nachfolgenden Messwerten automatisch korrigiert.

ANMERKUNG: PCIe-Geräte sind von den Gerätetreibern und der Firmware abhängig, um auf iDRAC-Anfragen zu reagieren. Diese Geräte protokollieren LC-Meldungen HWC9053 (unterbrochene Kommunikation mit dem Gerät), wenn die erforderlichen Treiber und Firmware nicht geladen sind oder wenn der Server das Betriebssystem noch nicht geladen hat (Seite „UEFI-Shell und Lifecycle Controller“).

Überprüfen der Frischlufttauglichkeit des Systems

Bei der Frischluftkühlung wird Außenluft direkt verwendet, um Systeme im Rechenzentrum zu kühlen. Frischlufttaugliche Systeme können über den normalen Umgebungsbetriebsbereich hinaus (Temperaturen bis zu 45 °C (113 °F)) betrieben werden.

ANMERKUNG: Einige Server oder bestimmte Konfigurationen eines Servers sind möglicherweise nicht frischlufttauglich. Weitere Informationen zur Frischlufttauglichkeit finden Sie im jeweiligen Serverhandbuch oder wenden Sie sich für weitere Informationen an Dell.

So prüfen Sie das System auf Frischlufttauglichkeit:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **System** > **Übersicht** > **Kühlung** > **Temperaturübersicht**.
   Die Seite **Temperaturübersicht** wird angezeigt.
2. Im Bereich **Frischluft** wird angezeigt, ob das System frischlufttauglich ist oder nicht.

Temperaturverlaufsdaten anzeigen

Sie können den prozentualen Zeitanteil anzeigen, während dem das System bei Umgebungstemperaturen über dem normalerweise unterstützten Temperaturschwellenwert betrieben wurde. Der Temperatursensor-Messwert 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 vergangenen sieben Jahre nachverfolgen und speichern.

ANMERKUNG: Sie können den Temperaturverlauf auch für Systeme nachverfolgen, die nicht frischlufttauglich sind. Die Schwellenwerte und erzeugten frischluftbezogenen Warnungen basieren jedoch auf den Grenzwerten für frischlufttaugliche Systeme. Die Grenzwerte liegen bei 42 °C für Warnungen und 47 °C für kritische Warnungen. Diese Werte entsprechen den Frischluftgrenzwerten von 40 °C und 45 °C mit einer Genauigkeitsmarge von 2 °C.

Es werden zwei feste Temperaturbereiche erfasst, die mit Grenzwerten für Frischluftkühlung verknüpft sind:

- Warnbereich: Die Zeitdauer, während der ein System oberhalb des Warnungsschwellenwerts des Temperatursensors (42 °C) betrieben wurde. Das System kann innerhalb von 12 Monaten für 10 % der Zeit im Warnbereich betrieben werden.

- Kritischer Bereich: Die Zeitdauer, währen der ein System oberhalb des kritischen Schwellenwerts des Temperatursensors (47 °C) betrieben wurde. Das System kann innerhalb von 12 Monaten für 1 % der Zeit im kritischen Bereich betrieben werden, wodurch auch die Zeit im Warnbereich erhöht wird.

Die erfassten Daten werden in einer Grafik dargestellt, in der die 10-%- und 1-%-Bereiche nachverfolgt werden können. Die protokollierten Temperaturdaten können nur vor dem Versand ab Werk gelöscht werden.

Wenn das System für einen angegebenen Betriebszeitraum weiterhin oberhalb des normalerweise unterstützten Temperaturschwellenwerts betrieben wird, wird ein Ereignis erzeugt. Liegt die Durchschnittstemperatur während des angegebenen Betriebszeitraums auf oder über der Warnungsebene (> = 8 %) oder der kritischen Ebene (> = 0,8 %), wird im Lifecycle-Protokoll ein Ereignis protokolliert und der entsprechende SNMP-Trap erzeugt. Zu den Ereignissen gehören:

- 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 den iDRAC auch so konfigurieren, dass zusätzliche Ereignisse erzeugt werden. Weitere Informationen finden Sie im Abschnitt Alarmwiederholungsereignis einrichten.

Temperaturverlaufsdaten über RACADM anzeigen

Um den Datenverlauf unter Verwendung von RACADM anzuzeigen, verwenden Sie den Befehl `inlettemphistory`.

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

ANMERKUNG: Es kann vorkommen, dass die Einlasstemperaturwerte in der iDRAC-Benutzeroberfläche und in RACADM nicht übereinstimmen. Wenn Sie die Daten zwischen diesen Schnittstellen vergleichen, beachten Sie Folgendes:

- **iDRAC-UI-Optionen** aus der Drop-down-Liste und deren Ausgabe:
  - Letzter Tag: Stündliche Daten, die für die letzten 24 Stunden angezeigt werden.
  - Letzter Monat: Die täglichen Daten werden für die letzten 30 Tage angezeigt.
  - Letztes Jahr: Monatliche Daten, die für die letzten 12 Monate angezeigt wurden.
- **RACADM-Ausgabe**: Zeigt genaue Werte für Stunde, Tag, Monat und Jahr für die jeweiligen RACADM-Befehle an.

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.

Konfigurieren des Warnungsschwellenwerts für die Einlasstemperatur

Sie können die minimalen und maximalen Warnungsschwellenwerte für den Einlasstemperatursensor der Hauptplatine ändern. Wenn ein Zurücksetzen auf die Standardeinstellungen durchgeführt wird, werden die Temperaturschwellenwerte auf die Standardwerte gesetzt. Sie müssen über Berechtigungen zum Konfigurieren verfügen, um den Warnungsschwellenwert für den Einlasstemperatursensor festzulegen.

ANMERKUNG: Der Unterschied zwischen **Oberer Grenzwert – Warnung** und **Messwert** der **Eingangstemperatur auf der Hauptplatine** muss mehr als 2 Grad betragen, um Warnungen zum Funktionszustand zu vermeiden.

ANMERKUNG: Jedes Mal, wenn Sie das System neu starten oder die iDRAC-Firmware aktualisieren, werden LC-Protokolle angezeigt, die Informationen über den für den Einlasstemperatursensor festgelegten Schwellenwert enthalten.

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 nutzerdefinierten 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 der auf dem Hostbetriebssystem verfügbaren Netzwerke über RACADM

Verwenden Sie den Befehl `gethostnetworkinterfaces`, um die Netzwerkschnittstellen auf Hostbetriebssystemen über RACADM anzuzeigen. Weitere Informationen finden Sie im *Referenzhandbuch für iDRAC RACADM CLI*.

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. Gehen Sie zu **System** > **Host-BS** > **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 mit den Gerätedetails kann über den Abschnitt **Hardware** > **Netzwerkgeräte** angezeigt werden. Informationen zu den Eigenschaften finden Sie in der **iDRAC-Online-Hilfe**.
4. Klicken Sie auf das Symbol +, um weitere Details anzuzeigen.

   In ähnlicher Weise können Sie auch die Informationen zur Host-BS-Netzwerkschnittstelle anzeigen, die mit einem Netzwerkgerät verknüpft ist, indem Sie die Seite **Hardware** > **Netzwerkgeräte** aufrufen. Klicken Sie dort auf **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 und Beenden von iDRAC-Sitzungen

Sie können die Anzahl der Nutzer anzeigen, die derzeit bei iDRAC angemeldet sind, und die Benutzersitzungen beenden.

Beenden von iDRAC-Sitzungen über RACADM

Sie benötigen Administratorberechtigungen, um iDRAC-Sitzungen über RACADM beenden zu können.

Verwenden Sie zum Anzeigen der aktuellen Nutzersitzungen den Befehl `getssninfo`.

Verwenden Sie zum Beenden einer Nutzersitzung den Befehl `closessn`.

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Beenden der iDRAC-Sitzungen über die Webschnittstelle

Nutzer 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 auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Nutzer** > **Sitzungen**.
   Auf der Seite **Sitzungen** werden die Sitzungs-ID, der Nutzername, 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.

10

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 Services

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 19. 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 und IPMI	Teil der iDRAC-Firmware und serielles RAC oder serielles IPMI 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-Services [1]	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 Dell Lifecycle Controller* ist verfügbar unter iDRAC-Handbücher..			

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
- Konfigurieren von Linux während des Starts in RHEL für die serielle Konsole
- Konfigurieren des seriellen Terminals in RHEL

- 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: Wenn USB DB9 mit dem System verbunden ist, wird die **Baudrate** (**iDRAC-Einstellungen** > **Konnektivität** > **Seriell**) automatisch festgelegt, je nachdem, ob **RAC Seriell** aktiviert oder deaktiviert ist. Wenn **RAC Seriell** aktiviert ist, wird **RAC Seriell > Baudrate** für USB DB9 festgelegt. Wenn **RAC Seriell** deaktiviert ist (IPMI ist aktiviert), wird **IPMI Seriell > Baudrate** für USB DB9 festgelegt.

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: Ein Aus- und Einschalten des Servers ist bei vConsole oder UI 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 **Fertig stellen** und anschließend 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-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`.

Serielle RAC-Verbindungen über die Weboberfläche aktivieren

So aktivieren Sie die serielle RAC-Verbindung:

1. Navigieren Sie auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Netzwerk** > **Seriell**
   Die Seite **Serial** 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.

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 Weboberfläche 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 auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Konnektivität** > **Seriell**.
2. Legen Sie unter **Serielles IPMI** die Attributwerte fest. 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	Berechtigungsebene
<level> = 2	NutzerIn
<level> = 3	Operator
<level> = 4	AdministratorIn

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 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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Zusätzliche Einstellungen für den seriellen IPMI-Terminalmodus über die Weboberfläche konfigurieren

So legen Sie die Terminalmoduseinstellungen fest:

1. Gehen Sie auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Konnektivität** > **Seriell**.
   Die Seite **Serial** wird angezeigt.
2. Aktivieren Sie „Serielle IPMI-Verbindung“.
3. Klicken Sie auf **Terminalmoduseinstellungen**.
   Daraufhin wird die Seite **Terminalmoduseinstellungen** angezeigt.
4. Geben Sie die folgenden Werte ein:
   - 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.

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 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.:

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 Tastenkombination rufen Sie entweder das `iDRAC Login` (wenn iDRAC auf den seriellen RAC-Modus gesetzt ist) oder den seriellen Verbindungsmodus auf, in dem Terminalbefehle ausgegeben werden können (wenn iDRAC auf den seriellen IPMI-Terminalmodus für Direktverbindung eingestellt ist).

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. Geben Sie die folgenden Werte ein:
   - 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 für das Aufrufen 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 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	Berechtigungsebene
<level> = 2	NutzerIn
<level> = 3	Operator
<level> = 4	AdministratorIn

ANMERKUNG: Um IPMI-SOL zu aktivieren, müssen Sie über die in IPMI-SOL festgelegte Mindestberechtigung verfügen. Weitere Informationen finden Sie in den IPMI-2.0-Spezifikationen.

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 Nutzer 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.

iDRAC für die Verwendung von SOL über die iDRAC-Weboberfläche konfigurieren

Um IPMI Seriell über LAN (SOL) zu konfigurieren:

1. Gehen Sie auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Konnektivität** > **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 helfen dabei, die Leistung zu verbessern.

   Informationen zu den verfügbaren Optionen finden Sie in der **iDRAC-Online-Hilfe**.

Unterstütztes Protokoll aktivieren

Die unterstützten Protokolle sind IPMI und SSH.

Unterstütztes Protokoll über RACADM aktivieren

Um SSH zu aktivieren, führen Sie den folgenden Befehl aus:

SSH

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

Um den SSH-Anschluss zu verändern, führen Sie den folgenden Befehl aus:

```
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

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.

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 das IPMITool von der DVD **Dell Systems Management Tools and Documentation**.
   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 nur SSH-Version 2 mit Kennwortauthentifizierung und ist standardmäßig aktiviert. iDRAC unterstützt bis zu zwei bis vier SSH-Sitzungen gleichzeitig.

ANMERKUNG: Beim Herstellen einer SSH-Verbindung wird die Sicherheitsmeldung `Further Authentication required` angezeigt, obwohl die 2FA deaktiviert 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).

Führen Sie die folgenden Schritte aus, bevor Sie SSH für die Kommunikation mit iDRAC verwenden:

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.

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 com2`
   - `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.

   Aktivieren Sie die serielle Datenerfassung, um den Verlauf der SOL-Schnittstelle anzuzeigen. Sie schreibt alle vom Host empfangenen seriellen Daten in einen iDRAC-Speicher in einem sequenziellen Fenster mit 512 KB. Dafür wird eine Datacenter-Lizenz benötigt.

4. Beenden Sie die SOL-Sitzung, um eine aktive SOL-Sitzung zu schließen.

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 com2` 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.

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 für den iDRAC IPMI-über-LAN konfigurieren, um IPMI-Befehle über LAN-Kanäle an externe Systeme zu aktivieren oder zu deaktivieren. Wenn IPMI-über-LAN nicht konfiguriert ist, können externe Systeme nicht über IPMI-Befehle mit dem iDRAC-Server kommunizieren.

ANMERKUNG: IPMI unterstützt auch das IPv6-Adressprotokoll für Linux-basierte Betriebssysteme.

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 **Fertig stellen** und anschließend 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. Weitere Informationen finden Sie in den IPMI-2.0-Spezifikationen auf **intel.com**.

2. Aktualisieren Sie die IPMI-Kanalberechtigungen.

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

Parameter	Berechtigungsebene
<level> = 2	NutzerIn
<level> = 3	Operator
<level> = 4	AdministratorIn

3. Legen Sie ggf. den IPMI-LAN-Kanalverschlüsselungsschlüssel fest:

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

Parameter	Beschreibung
<key>	20-Zeichen-Verschlüsselungsschlüssel in einem gültigen Hexadezimalformat.

ANMERKUNG: Das iDRAC-IPMI unterstützt das RMCP+-Protokoll. Weitere Informationen finden Sie in den IPMI-2.0-Spezifikationen auf **intel.com**.

IPMI über LAN mithilfe der Weboberfläche konfigurieren

So konfigurieren Sie IPMI über LAN:

1. Gehen Sie auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **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.

Remote-RACADM aktivieren oder deaktivieren

Sie können Remote-RACADM über die iDRAC-Weboberfläche oder RACADM aktivieren oder deaktivieren. Sie können bis zu fünf Remote-RACADM-Sitzungen parallel ausführen.

ANMERKUNG: Remote-RACADM ist standardmäßig aktiviert.

Remote-RACADM über RACADM aktivieren oder deaktivieren

ANMERKUNG: Es wird empfohlen, diese Befehle über lokales RACADM oder Firmware-RACADM auszuführen.

So deaktivieren Sie Remote-RACADM:

- So deaktivieren Sie Remote-RACADM:

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

- So aktivieren Sie Remote-RACADM:

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

Remote-RACADM über die Weboberfläche aktivieren oder deaktivieren

1. Gehen Sie auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **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.

Lokalen RACADM deaktivieren

Das lokale RACADM ist standardmäßig aktiviert. Zur Deaktivierung siehe Zugriff zum Ändern der iDRAC-Konfigurationseinstellungen auf einem Host-System deaktivieren.

Konfigurieren von Linux während des Starts in RHEL für die serielle Konsole

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 eine **/etc/grub.conf**-Beispieldatei, 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/sda1
```

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

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

title Red Hat Linux Advanced Server (2.4.9-e.3smp) root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0
console=ttyS1,115200n8r
initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3) root (hd0,00)
kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
initrd /boot/initrd-2.4.9-e.3.im
```

4. 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

So konfigurieren Sie das serielle Terminal in RHEL:

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 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-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 20. SSH-Verschlüsselungsschemas

Schematyp	Algorithmen
Asymmetrische Verschlüsselung	
Öffentlicher Schlüssel	• curve25519-sha256 • curve25519-sha256@libssh.org • ssh-rsa • ecdsa-sha2-nistp256 • diffie-hellman-group16-sha512 • diffie-hellman-group18-sha512 • diffie-hellman-group14-sha256
Symmetrische Verschlüsselung	
Schlüsselaustausch	• rsa-sha2-512 • rsa-sha2-256 • ssh-rsa • ecdsa-sha2-nistp256 • ssh-ed25519 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 • diffie-hellman-group-exchange-sha256
Verschlüsselung	• chacha20-poly1305@openssh.com • aes128-ctr • aes192-ctr • aes256-ctr • aes128-gcm@openssh.com • aes256-gcm@openssh.com
MAC	• umac-64@openssh.com • umac-128-etm@openssh.com • hmac-sha2-256-etm@openssh.com • hmac-sha2-512-etm@openssh.com • umac-128@openssh.com • hmac-sha2-256 • hmac-sha2-512
Komprimierung	Keine

ANMERKUNG: Wenn Sie OpenSSH 7.0 oder höher aktivieren, ist die Unterstützung für öffentliche DSA-Schlüssel deaktiviert. Um eine bessere Sicherheit für iDRAC zu gewährleisten, empfiehlt Dell, die Unterstützung für öffentliche DSA-Schlüssel nicht zu aktivieren.

Authentifizierung mit öffentlichen Schlüsseln für SSH verwenden

iDRAC unterstützt die Authentifizierung mit öffentlichem Schlüssel (Public Key Authentication, PKA) über SSH. Hierbei handelt es sich um eine lizenzierte Funktion. Wenn PKA über SSH eingerichtet und korrekt verwendet wird, müssen Sie den Nutzernamen eingeben, wenn Sie sich beim iDRAC anmelden. Dies ist für die Einrichtung automatisierter Skripte nützlich, die verschiedene Funktionen ausführen. Die hochgeladenen Schlüssel müssen im RFC 4716- oder OpenSSH-Format vorliegen. Andernfalls müssen Sie die Schlüssel in dieses Format konvertieren.

Auf jeden Fall muss ein Paar privater und öffentlicher Schlüssel auf der Managementstation erzeugt werden. Der öffentliche Schlüssel wird in den lokalen iDRAC-Nutzer hochgeladen und der private Schlüssel wird vom SSH-Client verwendet, um die Vertrauensbeziehung zwischen der Managementstation 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 in der Regel für NutzerInnen reserviert, die Mitglieder der Administrator-Nutzergruppe auf dem iDRAC sind. NutzerInnen in der „nutzerdefinierten“ Nutzergruppe kann diese Berechtigung jedoch zugewiesen werden. Ein Benutzer mit dieser Berechtigung kann die Konfiguration beliebiger Benutzer modifizieren. Hierzu zählen das Erstellen oder Löschen beliebiger Benutzer, die Verwaltung der SSH-Schlüssel für Benutzer, usw. Weisen Sie diese Berechtigung aus diesen Gründen also sorgfältig zu.

VORSICHT: Die Möglichkeit zum Hochladen, Anzeigen und/oder Löschen von SSH-Schlüsseln basiert auf der Berechtigung zum Konfigurieren von NutzerInnen. Diese Berechtigung ermöglicht es NutzerInnen, den SSH-Schlüssel anderer NutzerInnen zu konfigurieren. Sie sollten diese Berechtigung daher mit Bedacht gewähren.

Generieren öffentlicher Schlüssel für Linux

Um die Anwendung **ssh-keygen** für die Erstellung des Basisschlüssels zu verwenden, öffnen Sie ein Terminalfenster und geben Sie bei der Shell-Eingabeaufforderung den Befehl `ssh-keygen -t rsa -b 2048 -C testing` ein,

Wobei:

- `-t` **rsa** ist.
- `-b` die Bit-Verschlüsselungsgröße zwischen 2048 und 4096 angibt.
- `-C` das Ändern des Kommentars des öffentlichen Schlüssels ermöglicht und optional ist.

ANMERKUNG: Bei den Optionen wird zwischen Groß- und Kleinschreibung unterschieden.

Befolgen Sie die Anweisungen. Laden Sie die öffentliche Datei nach der Ausführung des Befehls hoch.

VORSICHT: Schlüssel, die von der Linux Management Station mithilfe von ssh-keygen erstellt werden, sind nicht im 4716-Format. Konvertieren Sie die Schlüssel in das 4716-Format mithilfe von `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub`. Ändern Sie nicht die Berechtigungen der Schlüsseldatei. Die Konvertierung muss mit Standardberechtigungen durchgeführt werden.

ANMERKUNG: iDRAC unterstützt nicht die ssh-agent-Weiterleitung von Schlüsseln.

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 an Bits für den Schlüssel ein. Die Anzahl der Bits muss zwischen 2048 und 4096 Bit liegen.
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.

SSH-Schlüssel hochladen

Sie können bis zu vier öffentliche Schlüssel **pro NutzerIn** für die Verwendung über eine SSH-Schnittstelle hochladen. Bevor Sie die öffentlichen Schlüssel hinzufügen, stellen Sie sicher, dass Sie bereits eingerichtete Schlüssel anzeigen, damit 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. Der iDRAC prüft nicht, ob vorherige Schlüssel gelöscht wurden, bevor neue Schlüssel hinzugefügt werden. Wenn ein neuer Schlüssel hinzugefügt wird, kann er verwendet werden, wenn die SSH-Schnittstelle aktiviert ist.

SSH-Schlüssel über die Weboberfläche hochladen

So laden Sie SSH-Schlüssel hoch:

1. Gehen Sie auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Nutzer** > **Lokale Nutzer**.
   Die Seite **Lokale Nutzer** wird angezeigt.
2. In der Spalte **Nutzer-ID** klicken Sie auf eine Nutzer-ID-Nummer.
   Die Seite **Nutzer-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 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 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`

SSH-Schlüssel über die Weboberfläche löschen

So löschen Sie SSH-Schlüssel:

1. Gehen Sie auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Nutzer**.
   Die Seite **Lokale Nutzer** wird angezeigt.
2. Wählen Sie in der Spalte **Nutzer-ID** eine Nutzer-ID aus und klicken Sie auf **Bearbeiten**.
   Die Seite **Nutzer bearbeiten** wird angezeigt.
3. Wählen Sie unter **SSH-Schlüsselkonfigurationen** einen SSH-Schlüssel aus und klicken Sie dann auf **Bearbeiten**.
   Auf der Seite **SSH-Schlüssel** werden die Details zu **Bearbeiten von** angezeigt.
4. Wählen Sie für den/die zu löschenden Schlüssel die Option **Entfernen** aus und klicken Sie dann auf **Anwenden**.
   Die ausgewählten Schlüssel werden daraufhin gelöscht.

SSH-Schlüssel anzeigen

Sie können die Schlüssel anzeigen, die nach iDRAC hochgeladen wurden.

SSH-Schlüssel über die Weboberfläche anzeigen

So zeigen Sie die SSH-Schlüssel an:

1. Gehen Sie auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Nutzer**.
   Die Seite **Lokale Nutzer** wird angezeigt.
2. In der Spalte **Nutzer-ID** klicken Sie auf eine Nutzer-ID-Nummer.
   Die Seite **Nutzer-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.

11

Nutzerrollen und Nutzerkonten

Sie können Nutzerrollen mit bestimmten Berechtigungen mithilfe von iDRAC erstellen, um Ihr System zu managen und die Systemsicherheit aufrechtzuerhalten. Standardmäßig ist der iDRAC mit einer lokalen Administratorrolle konfiguriert. Der standardmäßige iDRAC-Benutzername und das Standard-iDRAC-Kennwort werden mit der Systemkennzeichnung bereitgestellt. Weitere Informationen finden Sie in der Dokumentation zu Ihrem Server.

Als AdministratorIn können Sie Nutzerrollen mit den zugehörigen Berechtigungen erstellen. Sie können Nutzerkonten erstellen und die neu erstellten Rollen oder die vorhandenen Rollen **Administrator**, **Operator**, **ReadOnly** in iDRAC zuweisen. Sie können lokale NutzerInnen einrichten oder Verzeichnisdienste wie Microsoft Active Directory oder LDAP verwenden, um Nutzerkonten einzurichten. Die Verwendung eines Verzeichnisdiensts stellt einen zentralen Standort für die Verwaltung berechtigter Benutzerkonten bereit.

Themen:

- iDRAC-Benutzerrollen und -Berechtigungen
- Empfohlene Zeichen in Nutzernamen und Kennwörtern
- Erstellen von Benutzerrollen
- Lokale Nutzer konfigurieren
- Konfigurieren von Active Directory-Nutzern
- Generische LDAP-Nutzer konfigurieren
- Einstellungen für LDAP-Verzeichnisdienst testen

iDRAC-Benutzerrollen und -Berechtigungen

Die standardmäßigen iDRAC-Rollen sind **Administrator**, **Operator** und **ReadOnly**. Diese Rollen verfügen über bestimmte Nutzerberechtigungen.

In der folgenden Tabelle sind die Standardnamenamen der iDRAC-Rollen aufgeführt:

Tabelle 21. iDRAC-Rollen

Rollen	Nutzerberechtigungen
AdministratorIn	Am iDRAC anmelden, iDRAC konfigurieren, Nutzer konfigurieren, Protokolle löschen, System konfigurieren, auf virtuelle Konsole zugreifen, auf virtuellen Datenträger zugreifen, Warnungen testen, und Debug-Befehle ausführen.
Operator	Am iDRAC anmelden, iDRAC konfigurieren, Protokolle löschen, System konfigurieren, auf virtuellen Datenträger zugreifen, Warnungen testen, und Debug-Befehle ausführen.
ReadOnly	Melden Sie sich bei iDRAC an.

In der folgenden Tabelle sind die IPMI-Benutzerberechtigungen beschrieben:

Tabelle 22. DRAC/iDRAC-Benutzerberechtigungen

Nutzerberechtigungen	Beschreibung
Melden Sie sich bei iDRAC an.	Ermöglicht den Nutzern, sich am iDRAC anzumelden.
Konfigurieren von iDRAC	Ermöglicht den Nutzern, den iDRAC zu konfigurieren. Mit dieser Berechtigung kann ein Nutzer auch Energiemanagement, virtuelle Konsole, virtuelle Datenträger, Lizenzen, Systemeinstellungen, Storage-Geräte, BIOS-Einstellungen, SCP usw. konfigurieren.
ANMERKUNG: Die Administratorrolle übersteuert alle Privilegien der anderen Komponenten wie z.B. das BIOS-Setup-Kennwort.	
Benutzer konfigurieren.	Ermöglicht den Benutzern die Erstellung von Benutzerkonten.
Protokolle löschen	Ermöglicht den Benutzern, lediglich die Systemereignisprotokolle (SELs) zu löschen.

Tabelle 22. DRAC/iDRAC-Benutzerberechtigungen (fortgesetzt)

Nutzerberechtigungen	Beschreibung
System konfigurieren	Ermöglicht den Benutzern, das Hostsystem aus- und wieder einzuschalten.
Auf die virtuelle Konsole zugreifen	Ermöglicht den Benutzern, die virtuelle Konsole auszuführen.
Auf virtuelle Datenträger zugreifen	Ermöglicht den Benutzern, virtuelle Datenträger auszuführen und zu verwenden.
Testwarnungen	Ermöglicht den Benutzern, E-Mail-Warnmeldungen, SNMP-Traps und andere konfigurierte Warnmeldungsbenachrichtigungen zu testen.
Debug-Befehle ausführen	Ermöglicht den Benutzern, Diagnosebefehle auszuführen.

Empfohlene Zeichen in Nutzernamen und Kennwörtern

Dieser Abschnitt enthält Details zu den empfohlenen Zeichen beim Erstellen und Verwenden von Nutzernamen und Kennwörtern.

ANMERKUNG: Das Kennwort muss einen Großbuchstaben und einen Kleinbuchstaben, eine Zahl und ein Sonderzeichen enthalten.

Verwenden Sie beim Erstellen von Nutzernamen und Kennwörtern die folgenden Zeichen:

Tabelle 23. Empfohlene Zeichen für Nutzernamen

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

Tabelle 24. Empfohlene Zeichen für Kennwörter

Zeichen	iDRAC10-Versionen	Baulänge
• 0-9 • A-Z • a-z • ' - ! " # $ % & ( ) * , . / : ; ? @ [\ ] ^ _ ` { | } ~ + < = >	1.10.17.00 und höher	1 – 127

ANMERKUNG: Sie können möglicherweise Nutzernamen und Kennwörter 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 Zeichen, die in Nutzernamen und Kennwörtern für Netzwerkfreigaben zulässig sind, werden durch den Netzwerkfreigabetyp bestimmt. iDRAC unterstützt zulässige Zeichen in Anmeldeinformationen für die Netzwerkfreigabe dem Freigabetyp, außer < ,> und , (Komma).

ANMERKUNG: Um die Sicherheit zu verbessern, wird empfohlen, komplexe Kennwörter zu verwenden, die acht oder mehr Zeichen umfassen und Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen enthalten. Es wird außerdem empfohlen, die Kennwörter regelmäßig zu ändern (sofern möglich).

Erstellen von Benutzerrollen

Sie können Benutzerrollen mit den erforderlichen Berechtigungen erstellen, damit Sie die Aufgaben effizient an die NutzerInnen delegieren können. Nur NutzerInnen, denen die Rolle eines Administrators zugewiesen ist, können Benutzerrollen erstellen.

1. Gehen Sie zu **iDRAC-Einstellungen** > **Nutzer** > **Lokale Nutzer** > **Benutzerrollen**.
2. Klicken Sie auf **+Add**.
   Das Dialogfeld **Neue Rolle hinzufügen** wird angezeigt.

3. Wählen Sie die **Benutzer-ID** aus.
4. Geben Sie den **Benutzerrollennamen** ein.
5. Wählen Sie die **Nutzerberechtigungen** aus.
6. Klicken Sie auf **Speichern**.
   Die Benutzerrolle wird in der Liste**Benutzerrollen** aufgeführt.

Lokale Nutzer konfigurieren

Sie können in iDRAC bis zu 32 lokale Benutzer mit spezifischen Benutzerrollen 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 Nutzer definieren. Die Benutzernamen und Kennwörter können über die sicheren iDRAC-Schnittstellen (z. B. die Weboberfläche, RACADM oder Redfish) geändert werden.

Erstellen von lokalen Nutzern über die iDRAC UI

Sie können Nutzer hinzufügen und basierend auf den ihnen zugewiesenen Aufgaben bestimmte Rollen zuweisen.

ANMERKUNG: Nur wenn die Ihnen zugewiesene Nutzerrolle über die Berechtigung **Nutzer konfigurieren** verfügt können Sie Nutzer erstellen.

1. Navigieren Sie in der iDRAC UI zu **iDRAC Settings** > **Lokale Benutzer** > **Übersicht**.
   Die lokalen Nutzer werden aufgelistet.
2. Klicken Sie auf **+Add**.
   Das Dialogfeld **Neuer Nutzer hinzufügen** wird angezeigt.
3. Wählen Sie die **ID** aus.
4. Geben Sie die Felder **Nutzername**, **Kennwort** und **Kennwort bestätigen** ein.
5. Wählen Sie die **Nutzerrolle** aus.
   Die entsprechenden **Nutzerberechtigungen** werden angezeigt.
6. Klicken Sie auf **Speichern**.
   Der Benutzername wird in der Liste angezeigt.

Lokale Nutzer über RACADM konfigurieren

ANMERKUNG: Sie müssen als Nutzer **root** angemeldet sein, um RACADM-Befehle auf einem Remote-Linux-System ausführen zu können.

Sie können einen oder mehrere iDRAC-Nutzer über RACADM konfigurieren.

Um mehrere iDRAC-Nutzer mit identischen Konfigurationseinstellungen zu konfigurieren, führen Sie folgende Schritte durch:

- Erstellen Sie mithilfe 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: Nutzer können im Laufe der Zeit aktiviert und deaktiviert werden. Infolgedessen kann ein Nutzer auf jedem iDRAC eine unterschiedliche Indexnummer besitzen.

Um zu überprüfen, ob ein Nutzer 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: Verwenden können Sie

```
racadm get -f <myfile.cfg>
```

und anzeigen oder bearbeiten,

```
myfile.cfg
```

die alle iDRAC-Konfigurationsparameter enthält.

Zur Aktivierung der SNMP v3-Authentifizierung für einen Nutzer verwenden Sie die Objekte **SNMPv3AuthenticationType**, **SNMPv3Enable**, **SNMPv3PrivacyType**. Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Wenn Sie die Serverkonfigurationsprofildatei zur Benutzerkonfiguration verwenden, dann verwenden Sie die Attribute **AuthenticationProtocol, ProtocolEnable,** und **PrivacyProtocol**, um die SNMPv3-Authentifizierung zu aktivieren.

iDRAC-Nutzer 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>	Nutzername

2. Legen Sie das Kennwort fest.

   ```
   racadm set idrac.users.<index>.password <password>
   ```

3. Legen Sie die Nutzerberechtigungen fest.

   Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

4. Aktivieren Sie den Nutzer.

   ```
   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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Aktivieren des iDRAC-Benutzers mit Berechtigungen

Um einen Nutzer 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 Nutzer über keine Berechtigungen verfügt. Eine Liste der gültigen Bitmaskenwerte für bestimmte Benutzerberechtigungen finden Sie unter RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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: StartTLS auf Port 389 wird unterstützt. Standardmäßig ist LDAPS auf Port 636 konfiguriert. Das Verbindungsprotokoll kann mithilfe des Redfish- oder RACADM-Befehls `racadm set iDRAC.ActiveDirectory.Connection StartTLS` auf StartTLS umkonfiguriert werden.

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 wurde in die Active Directory-Infrastruktur integriert. iDRAC verwendet die standardmäßige PKI-Methode (Public Key Infrastructure, Infrastruktur des öffentlichen Schlüssels), um eine sichere Authentifizierung in das Active Directory herzustellen. 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 NutzerInnen mit einem Active Directory Domain Controller authentifiziert, startet er eine SSL-Sitzung mit dem Domain Controller. Zu diesem Zeitpunkt muss der Domain Controller ein von der Zertifizierungsstelle (CA) signiertes Zertifikat veröffentlichen – das Stammzertifikat, das auch in den iDRAC hochgeladen wurde. Damit sich iDRAC bei **einem beliebigen** Domain Controller authentifizieren kann, unabhängig davon, ob es sich um den Stamm- oder den untergeordneten Domain Controller handelt, muss dieser Domain Controller über ein SSL-fähiges Zertifikat verfügen, das von der Zertifizierungsstelle der Domäne 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 **Fertigstellen**. 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 Storage.
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.

- Die **Erweiterte Schemalösung**, die kundenspezifische Active Directory-Objekte verwendet. Alle Zugriffskontrollobjekte werden im Active Directory verwaltet. Dies bietet maximale Flexibilität bei der Konfiguration des Nutzerzugriffs auf verschiedenen iDRACs mit unterschiedlichen Berechtigungsebenen.

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.

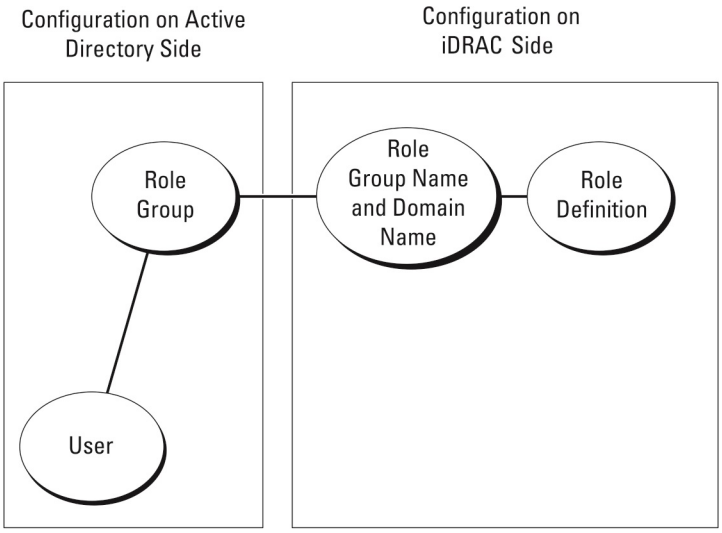


Abbildung 1. Konfiguration von iDRAC mit Active Directory-Standardschema

In Active Directory wird ein Standardgruppenobjekt als Rollengruppe verwendet. Ein Nutzer, der iDRAC-Zugriff hat, ist ein Mitglied der Rollengruppe. Um diesem Nutzer 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 15 Rollengruppen konfigurieren und definieren. Tabellenreferenznummer zeigt die standardmäßigen Rollengruppen-Berechtigungen.

Tabelle 25. Standardeinstellungsberechtigungen der Rollengruppe

Rollengruppen	Standard-Berechtigungsebene	Gewährte Berechtigungen	Bitmaske
Rollengruppe 1	Keine	Am iDRAC anmelden, iDRAC konfigurieren, Nutzer 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, Serversteuerungsbefehle ausführen, auf virtuelle Konsole zugreifen, auf virtuellen Datenträger zugreifen, Warnungen testen, Diagnosebefehle ausführen	0x0000001f3
Rollengruppe 3	Keine	Melden Sie sich bei iDRAC an.	0x00000001
Rollengruppe 4	Keine	Keine zugewiesenen Berechtigungen	0x00000000

Tabelle 25. Standardeinstellungsberechtigungen der Rollengruppe (fortgesetzt)

Rollengruppen	Standard-Berechtigungsebene	Gewährte Berechtigungen	Bitmaske
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 AnmeldenutzerInnen und Rollengruppen sowie die verschachtelten Gruppen in derselben Domäne befinden, müssen lediglich die Adressen der Domain Controller auf dem iDRAC konfiguriert werden. In diesem Szenario mit nur einer Domäne wird jeder Gruppentyp unterstützt.

Wenn sich AnmeldenutzerInnen und Rollengruppen oder eine der verschachtelten Gruppen in mehreren Domänen befinden, müssen die Serveradressen des globalen Katalogs auf dem iDRAC konfiguriert werden. In diesem Szenario mit mehreren Domänen müssen alle Rollengruppen und verschachtelten Gruppen, falls vorhanden, zum universellen Gruppentyp gehören.

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 auf der iDRAC-Weboberfläche 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-Nutzer- und -Computer-Snap-In.
2. Erstellen Sie die iDRAC-Gruppen und -Nutzer.
3. Konfigurieren Sie den Gruppennamen, den Domänennamen und die Rollenberechtigungen auf iDRAC über die iDRAC-Web-Schnittstelle oder RACADM.

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 Domänencontrollers 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 Domain-Controller-Adressen angeben. iDRAC versucht solange, nacheinander mit jeder der konfigurierten Adressen eine Verbindung herzustellen, bis eine Verbindung erfolgreich hergestellt ist. Mit Standardschema sind dies die Adressen der Domänencontroller, 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. Bei mehreren 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 Domänencontrollerservers und den 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.

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 auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Nutzer** > **Verzeichnisdienste**.
   Die Seite **Verzeichnisdienste** wird angezeigt.
2. Wählen Sie die Option **Microsoft Active Directory** und klicken Sie dann auf **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. Hierfür müssen die FQDN der Domain Controller und des globalen Katalogs angegeben werden. Dies geschieht in den nächsten Schritten. Daher sollte der DNS in den Netzwerkeinstellungen ordnungsgemäß konfiguriert werden.
5. Klicken Sie auf **Weiter**.

   Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 2 von 4 wird angezeigt.
6. Aktivieren Sie das Active Directory und geben Sie die Speicherorte der Active Directory-Server und -Nutzerkonten an. Legen Sie außerdem die Zeit fest, die iDRAC während des iDRAC-Anmeldevorgangs auf Antworten vom Active Directory warten soll.

   ANMERKUNG: Wenn die Zertifikatüberprüfung aktiviert ist, geben Sie die Adressen des Domänencontrollerservers und den FQDN des globalen Katalogs an. Stellen Sie sicher, dass der DNS über **iDRAC-Einstellungen** > **Netzwerk** korrekt konfiguriert ist.
7. Klicken Sie auf **Weiter**. Die Seite **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 Nutzer 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.

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, um den iDRAC und Berechtigungen zu integrieren. Auf diese Weise können Sie den iDRAC basierend auf den erteilten Berechtigungen verwenden. Die standardmäßige Zugriffskontrollliste (Access Control List, ACL) der Dell Zuordnungsobjekte ermöglicht es Selbst- und DomänenadministratorInnen, die Berechtigungen und den Umfang von iDRAC-Objekten zu managen.

Standardmäßig erben die Dell Zuordnungsobjekte nicht alle Berechtigungen von den übergeordneten Active Directory-Objekten. Wenn Sie für das Dell Zuordnungsobjekt die Vererbung aktivieren, werden die vererbten Berechtigungen für dieses Zuordnungsobjekt den ausgewählten NutzerInnen und Gruppen gewährt. Dies kann dazu führen, dass unbeabsichtigte Berechtigungen für den iDRAC 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 mit **Attributen** und **Klassen**. Das Active Directory-Schema enthält die Regeln, die den Datentyp bestimmen, der der Datenbank hinzugefügt oder in die Datenbank aufgenommen werden kann. Die Nutzerklasse ist ein Beispiel für eine **Klasse**, die in der Datenbank gespeichert ist. Zu den Attributen der Nutzerklasse zählen beispielsweise der Vor- und Nachname von NutzerInnen, die Telefonnummer usw. Sie können die Active Directory-Datenbank erweitern, indem Sie Ihre eigenen individuellen **Attribute** und **Klassen** für bestimmte Anforderungen hinzufügen. Dell hat das Schema um die erforderlichen Änderungen erweitert, um die Remotemanagement-Authentifizierung und -Autorisierung über Active Directory zu unterstützen.

Jedes **Attribut** und jede **Klasse**, das/die einem vorhandenen Active Directory-Schema hinzugefügt wird, muss über eine eindeutige ID verfügen. Um branchenweit eindeutige IDs zu gewährleisten, führt Microsoft eine Datenbank mit Active Directory-Objektkennungen (OIDs), sodass beim Hinzufügen von Erweiterungen zum Schema sichergestellt werden kann, dass diese eindeutig sind und nicht miteinander in Konflikt stehen. Um das Schema im Microsoft Active Directory zu erweitern, hat Dell eindeutige OIDs, eindeutige Namenserweiterungen und eindeutig verknüpfte Attribut-IDs für die Attribute und Klassen erhalten, die dem Verzeichnisdienst hinzugefügt werden:

- Erweiterung: `dell`
- Basis-OID: `1.2.840.113556.1.8000.1280`
- RAC-LinkID-Bereich: `12070 to 12079`

Übersicht über die iDRAC-Schemaerweiterungen

Dell hat das Schema um die Eigenschaften **Zuordnung**, **Gerät** und **Berechtigung** erweitert. Die Eigenschaft **Zuordnung** wird verwendet, um NutzerInnen oder Gruppen mit einem bestimmten Satz an Berechtigungen für ein oder mehrere iDRAC-Geräte zu verknüpfen. Dieses Modell bietet AdministratorInnen maximale Flexibilität für die verschiedenen Nutzerkombinationen, iDRAC-Berechtigungen und iDRAC-Geräte im Netzwerk ohne große Komplexität.

Erstellen Sie für jedes physische iDRAC-Gerät im Netzwerk, das Sie für die Authentifizierung und Autorisierung in das Active Directory integrieren möchten, mindestens ein Zuordnungsobjekt und ein iDRAC-Geräteobjekt. Sie können mehrere Zuordnungsobjekte erstellen und jedes Zuordnungsobjekt kann mit beliebig vielen NutzerInnen, Nutzergruppen oder iDRAC-Geräteobjekten verknüpft werden. Die NutzerInnen und iDRAC-Nutzergruppen können Mitglieder jeder Domäne im Unternehmen sein.

Jedes Zuordnungsobjekt kann jedoch nur mit einem Berechtigungsobjekt verknüpft werden (oder kann NutzerInnen, Nutzergruppen oder iDRAC-Geräteobjekte verknüpfen). In diesem Beispiel kann ein/e AdministratorIn die Berechtigungen jedes Nutzers/jeder NutzerIn auf spezifischen DRAC-Geräten steuern.

Das iDRAC-Geräteobjekt ist die Verbindung zur iDRAC-Firmware bei der Abfrage des Active Directory für die Authentifizierung und Autorisierung. Wenn ein iDRAC zum Netzwerk hinzugefügt wird, muss der/die AdministratorIn den iDRAC und sein Geräteobjekt mit seinem Active Directory-Namen konfigurieren, damit NutzerInnen eine Authentifizierung und Autorisierung über das Active Directory durchführen können. Darüber hinaus muss der/die AdministratorIn den iDRAC zu mindestens einem Zuordnungsobjekt hinzufügen, damit sich NutzerInnen authentifizieren können.

Die folgende Abbildung zeigt, dass das Zuordnungsobjekt die Verbindung bereitstellt, die für die gesamte Authentifizierung und Genehmigung erforderlich ist.

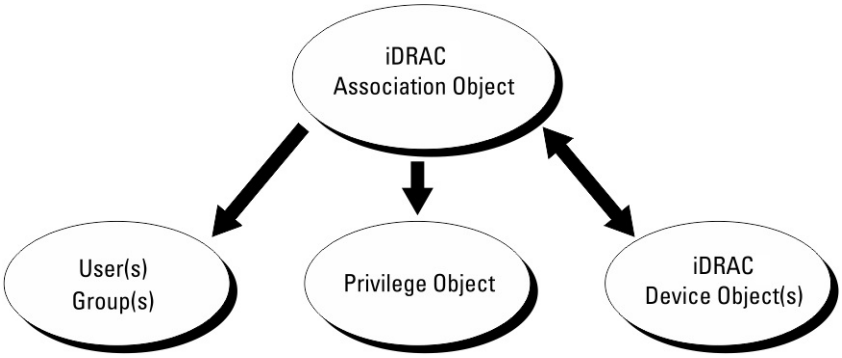


Abbildung 2. Typisches Setup für Active Directory-Objekte

Sie können eine beliebige Anzahl an Zuordnungsobjekten erstellen. Sie müssen jedoch mindestens ein Zuordnungsobjekt erstellen und über ein iDRAC-Geräteobjekt für jeden iDRAC im Netzwerk verfügen, der für die Authentifizierung und Autorisierung über iDRAC mit dem Active Directory integriert werden soll.

Das Zuordnungsobjekt erlaubt eine beliebige Anzahl von NutzerInnen und/oder Gruppen sowie iDRAC-Geräteobjekten. Das Zuordnungsobjekt enthält jedoch nur ein Berechtigungsobjekt pro Zuordnungsobjekt. Das Zuordnungsobjekt verbindet die NutzerInnen, die über Berechtigungen auf iDRAC-Geräten verfügen.

Die Dell Erweiterung zum ADUC-MMC-Snap-in erlaubt nur die Zuordnung von Berechtigungsobjekten und iDRAC-Objekte aus derselben Domäne zum Zuordnungsobjekt. Die Dell Erweiterung lässt nicht zu, dass eine Gruppe oder ein iDRAC-Objekt aus anderen Domänen als Produktmitglied des Zuordnungsobjekts hinzugefügt wird.

Wenn Sie universelle Gruppen aus verschiedenen Domänen hinzufügen, erstellen Sie ein Zuordnungsobjekt mit universellem Umfang. Die vom Schema Extender-Dienstprogramm erstellten Standardzuordnungsobjekte sind lokale Gruppen der Domäne und funktionieren nicht mit universellen Gruppen aus anderen Domänen.

Dem Zuordnungsobjekt können NutzerInnen, Nutzergruppen oder verschachtelte Nutzergruppen aus jeder Domäne hinzugefügt werden. Erweiterte Schemalösungen unterstützen jeden Nutzergruppentyp und jede Nutzergruppe, die über mehrere Domänen hinweg verschachtelt ist, die vom Microsoft Active Directory zulässig sind.

Unter Verwendung des erweiterten Schemas Berechtigungen ansammeln

Der Authentifizierungsmechanismus für das erweiterte Schema unterstützt das Akkumulieren von Berechtigungen für unterschiedliche Berechtigungsobjekte, die über verschiedene Zuordnungsobjekte demselben/derselben NutzerIn zugeordnet sind. Mit anderen Worten sammelt die Authentifizierung des erweiterten Schemas Berechtigungen an, um NutzerInnen einen übergeordneten Satz aller zugewiesenen Berechtigungen zu gewähren, die zu den verschiedenen Berechtigungsobjekten gehören, die dem jeweiligen/der jeweiligen NutzerIn zugeordnet sind.

Die folgende Abbildung enthält ein Beispiel für das Ansammeln von Berechtigungen unter Verwendung des erweiterten Schemas.

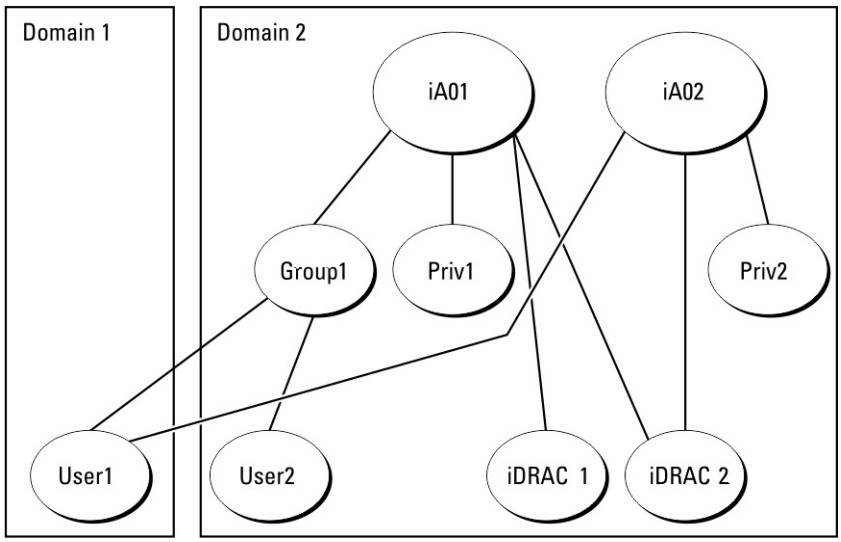


Abbildung 3. Ansammeln von Berechtigungen für einen Nutzer

Die Abbildung zeigt zwei Zuordnungsobjekte: A01 und A02. NutzerIn1 ist über beide Zuordnungsobjekte iDRAC2 zugeordnet.

Die Authentifizierung des erweiterten Schemas sammelt Berechtigungen an, um dem Nutzer den maximalen Satz aller möglichen Berechtigungen zur Verfügung zu stellen, und berücksichtigt dabei die zugewiesenen Berechtigungen der verschiedenen Berechtigungsobjekte für den gleichen Nutzer.

In diesem Beispiel verfügt NutzerIn1 über Priv1- und Priv2-Berechtigungen für iDRAC2. NutzerIn1 verfügt für iDRAC1 nur über Priv1-Berechtigungen. NutzerIn2 verfügt über Priv1-Berechtigungen für iDRAC1 und iDRAC2. Darüber hinaus zeigt diese Abbildung, dass sich NutzerIn1 in einer anderen Domäne befinden und Mitglied einer Gruppe sein 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-Nutzer und Computer-Snap-In erweitern.
3. iDRAC-Nutzer 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

Durch die 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, stellen Sie sicher, dass Sie über Schema-Administratorberechtigungen auf dem Schemamaster-FSMO-Rollenbesitzer der Domänenstruktur verfügen.

ANMERKUNG: Die Schemaerweiterung für dieses Produkt unterscheidet sich von den vorherigen Generationen. Das frühere Schema funktioniert mit diesem Produkt nicht.

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 der 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`
- <DVD-Laufwerk>: `\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender`

Lesen Sie für die 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: Der Dell Schema Extender verwendet die Datei SchemaExtenderOem.ini. Damit das Dienstprogramm Dell Schema Extender richtig funktioniert, dürfen Sie den Namen der Datei nicht verändern.

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. Zur Überprüfung der Schemaerweiterung verwenden Sie MMC und das Active Directory-Schema-Snap-in, um zu überprüfen, ob die Klassen und Attribute vorhanden sind. Weitere Informationen zum Verwenden von MMC und dem Active Directory-Schema-Snap-in finden Sie in der Microsoft Dokumentation.

Klassen und Attribute

Tabelle 26. 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 27. DelliDRACdevice-Klasse

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Beschreibung	Stellt das Dell iDRAC-Gerät dar. iDRAC muss im Active Directory als delliDRACDevice konfiguriert werden. Diese Konfiguration ermöglicht es iDRAC, LDAP-Abfragen (Lightweight Directory Access Protocol) an das Active Directory zu senden.
Klassentyp	Strukturklasse

Tabelle 27. DelliDRACdevice-Klasse (fortgesetzt)

OID	1.2.840.113556.1.8000.1280.1.7.1.1
SuperClasses	dellProduct
Attribute	dellSchemaVersion dellRacType

Tabelle 28. delliDRACAssociationObject Class

OID	1.2.840.113556.1.8000.1280.1.7.1.2
Beschreibung	Stellt das Dell Zuordnungsobjekt dar. Das Zuordnungsobjekt stellt die Verbindung zwischen den NutzerInnen und den Geräten bereit.
Klassentyp	Strukturklasse
SuperClasses	Gruppe
Attribute	dellProductMembers dellPrivilegeMember

Tabelle 29. 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 30. 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.
Klassentyp	Strukturklasse
SuperClasses	Nutzer
Attribute	dellRAC4Privileges

Tabelle 31. 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 32. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden

Attributname/Beschreibung	Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
dellPrivilegeMember – Liste der dellPrivilege-Objekte, 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 – Liste der dellRacDevices- und delliDRACDevice-Objekte, 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 NutzerInnen Anmelderechte auf dem Gerät haben.	• 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 NutzerInnen Kartenkonfigurationsrechte auf dem Gerät haben.	• 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 NutzerInnen Nutzerkonfigurationsrechte auf dem Gerät haben.	• 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 NutzerInnen Protokolllöschrechte auf dem Gerät haben.	• 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
dellIsServerResetUser – TRUE, wenn NutzerInnen Server-Zurücksetzungsrechte auf dem Gerät haben.	• 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 NutzerInnen Rechte für die virtuelle Konsole auf dem Gerät haben.	• 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 NutzerInnen Rechte für virtuelle Datenträger auf dem Gerät haben.	• 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 NutzerInnen Rechte für Warnungstests für Nutzer auf dem Gerät haben.	• 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 NutzerInnen Debug-Befehlsadministratorenrechte auf dem Gerät haben.	• 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 delliDRACDevice-Objekt und die Rückwärtsverbindung zur dellAssociationObjectMembers-Vorwärtsverbindung.	• 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

Tabelle 32. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden (fortgesetzt)

Attributname/Beschreibung	Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
dellAssociationMembers – Liste der dellAssociationObjectMembers, die zu diesem Produkt gehören. Dieses Attribut ist die Rückwärtsverbindung zum zugehörigen 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 Nutzer- und Computer-Snap-In installieren

Wenn Sie das Schema im Active Directory erweitern, müssen Sie auch das Active Directory-Nutzer- und -Computer-Snap-In erweitern, so dass der Administrator iDRAC-Geräte, Nutzer und Benutzergruppen, iDRAC-Zuordnungen und iDRAC-Berechtigungen managen kann.

Wenn Sie die Systems Management Software von der DVD **Dell Systems Management Tools and Documentation** installieren, können Sie das Snap-in erweitern, indem Sie während des Installationsvorgangs die Option **Snap-in von Active Directory-Nutzern und -Computern** auswählen. Weitere Anweisungen zur Installation der Systems Management Software finden Sie im Schnellinstallationshandbuch für die Dell OpenManage Software. Für 64-Bit-Windows-Betriebssysteme befindet sich das Snap-in-Installationsprogramm unter:

<DVD-Laufwerk>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

Weitere Informationen über Active Directory-Nutzer- und -Computer-Snap-In finden Sie in der Microsoft-Dokumentation.

iDRAC-Nutzer und -Berechtigungen zu Active Directory hinzufügen

Mit dem von Dell erweiterten Active Directory-Nutzer- und -Computer-Snap-in können Sie iDRAC-NutzerInnen und -Berechtigungen hinzuzufügen, indem Sie Geräte-, Zuordnungs- und Berechtigungsobjekte erstellen. Um die einzelnen Objekte hinzuzufügen, führen Sie die folgenden Schritte aus:

- 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. Dieser Name muss mit dem iDRAC-Namen identisch sein, den Sie bei der Konfiguration der Active Directory-Eigenschaften über die iDRAC-Weboberfläche 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 Nutzer 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. Gehen Sie zu **Verwaltung** > **ADSI-Bearbeitung**. Das Fenster **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 und klicken Sie auf **Namen überprüfen** und dann auf **OK**. Die authentifizierten NutzerInnen werden der Liste der **Gruppen und Nutzernamen** hinzugefügt.
5. Klicken Sie auf **OK**.

Objekte zu einem Zuordnungsobjekt hinzufügen

Durch die Verwendung des Fensters **Zuordnungsobjekt-Eigenschaften** können Sie Nutzer oder Benutzergruppen, Berechtigungsobjekte und iDRAC-Geräte oder iDRAC-Gerätegruppen zuordnen.

Sie können Benutzergruppen und iDRAC-Geräte hinzufügen.

Berechtigungen hinzufügen

So fügen Sie Berechtigungen hinzu:

Klicken Sie auf die Registerkarte **Berechtigungsobjekt**, um das Berechtigungsobjekt der Zuordnung hinzuzufügen, die die Berechtigungen für die NutzerInnen oder die Nutzergruppe für die Authentifizierung bei einem iDRAC-Gerät festlegt. Einem Zuordnungsobjekt kann nur ein Berechtigungsobjekt hinzugefügt werden.

1. Wählen Sie die Registerkarte **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 **Berechtigungsobjekt**, um das Berechtigungsobjekt der Zuordnung hinzuzufügen, die die Berechtigungen für die NutzerInnen oder die Nutzergruppe für die Authentifizierung bei einem iDRAC-Gerät festlegt. Einem Zuordnungsobjekt kann nur ein Berechtigungsobjekt hinzugefügt werden.

Nutzer oder Benutzergruppen hinzufügen

So fügen Sie Nutzer oder Benutzergruppen hinzu:

1. Klicken Sie mit der rechten Maustaste auf das **Zuordnungsobjekt** und wählen Sie **Eigenschaften** aus.
2. Wählen Sie das Register **Nutzer** und klicken Sie auf **Hinzufügen.**
3. Geben Sie den Namen des Benutzers oder der Benutzergruppe ein und klicken Sie auf **OK**.

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 **Produkte**, um ein iDRAC-Gerät hinzuzufügen, das mit dem Netzwerk verbunden ist, das den angegebenen NutzerInnen oder Nutzergruppen zur Verfügung steht. Sie können einem Zuordnungsobjekt mehrere iDRAC-Geräte hinzufügen.

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 Domänencontrollers 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. iDRAC versucht solange, nacheinander mit jeder der konfigurierten Adressen eine Verbindung herzustellen, bis eine Verbindung erfolgreich hergestellt ist. 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 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. Gehen Sie auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Nutzer** > **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 **Weiter**.
   Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 2 von 4 wird angezeigt.
4. Geben Sie die Standortinformationen der Active Directory-(AD-)Server und -Nutzerkonten an. Legen Sie außerdem die Zeit fest, die iDRAC während des Anmeldevorgangs auf Antworten vom AD warten soll.

   ANMERKUNG:
   - Wenn die Zertifikatvalidierung aktiviert ist, geben Sie die Serveradressen des Domänen-Controllers und den FQDN an. Stellen Sie sicher, dass der DNS über **iDRAC-Einstellungen** > **Netzwerk** korrekt konfiguriert ist.
   - Wenn sich NutzerInnen und iDRAC-Objekte in unterschiedlichen Domänen befinden, wählen Sie nicht die Option **Nutzerdomäne von Anmeldung** aus. Wählen Sie stattdessen die Option **Eine Domäne angeben** aus und geben Sie den Namen der Domäne ein, in der das iDRAC-Objekt verfügbar ist.

5. Klicken Sie auf **Weiter**. Die Seite **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.

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 auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Nutzer** > **Verzeichnisdienste** > **Microsoft Active Directory**, und klicken Sie auf **Testen**.
   Die Seite **Test Active Directory Settings** (Active Directory-Einstellungen testen) wird angezeigt.

2. Klicken Sie auf **Test**.
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.

Generische LDAP-Nutzer konfigurieren

iDRAC bietet eine generische Lösung für den Support der LDAP-basierten Authentifizierung (Lightweight Directory Access Protocol). Diese Funktion erfordert keine Schemaerweiterung für Ihre Verzeichnisservices.

Um die iDRAC-LDAP-Implementierung generisch zu machen, wird die Gemeinsamkeit zwischen verschiedenen Verzeichnisservices genutzt, um Nutzer zu gruppieren und dann die Nutzer-Gruppen-Beziehung zuzuordnen. Die für die Verzeichnisservices spezifische Aktion ist das Schema. Es können beispielsweise unterschiedliche Attributnamen für die Gruppe, den Nutzer und die Verbindung zwischen dem Nutzer und der Gruppe vorliegen. Diese Aktionen können in iDRAC konfiguriert werden.

ANMERKUNG: StartTLS auf Port 389 wird unterstützt. Standardmäßig ist LDAPS auf Port 636 konfiguriert. Das Verbindungsprotokoll kann mithilfe von Redfish oder dem RACADM-Befehl `racadm set iDRAC.LDAP.Connection StartTLS` auf StartTLS umkonfiguriert werden.

ANMERKUNG: Die Smartcard-basierte Zweifaktor-Authentifizierung (TFA) und einfache Anmeldung (SSO) werden nicht für den allgemeinen LDAP-Verzeichnisdienst unterstützt.

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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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-Einstellungen** > **Nutzer** > **Verzeichnisservices** > **Generischer LDAP-Verzeichnisservice** und klicken Sie auf **Bearbeiten**.
   Die Seite **Generisches LDAP - Konfiguration und Management – 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.
3. Klicken Sie auf **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-Einstellungen** > **Netzwerk** korrekt konfiguriert ist.

ANMERKUNG: In dieser Version werden verschachtelte Gruppen nicht unterstützt. Die Firmware sucht nach dem direkten Mitglied der Gruppe, das der Nutzer-DN entspricht. Außerdem wird nur eine einzelne Domain unterstützt. Domainübergreifende Anwendungen werden nicht unterstützt.

5. Klicken Sie auf **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 neuen Rollengruppen-Einstellungen werden gespeichert. Die Seite **Generisches LDAP - Konfiguration und Management – Schritt 3a von 3** zeigt die aktuellen Einstellungen für Rollengruppen an.
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.

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. Navigieren Sie auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Nutzer** > **Verzeichnisdienste** > **Generischer LDAP-Verzeichnisdienst**.
   Die Seite **Generisches LDAP - Konfiguration und Verwaltung** zeigt die aktuellen Einstellungen für das generische LDAP an.
2. Klicken Sie auf **Test**.
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 Nutzer als Verzeichnisbenutzer anzumelden. Schlägt dies fehl, wird die Suche nach lokalen Benutzern aktiviert.

   Die Testergebnisse und das Testprotokoll werden angezeigt.

12

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-I/O-Karten über die Anbieter-Tools.

Der Systemsperrmodus ist nur für Kunden mit Enterprise-Lizenz verfügbar.

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
- Systemkonfigurationsprofil (SCP)
- 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.

ANMERKUNG: Wenn der Sperrmodus aktiviert ist, können Sie keine Warnmeldungen konfigurieren. Sie können jedoch eine Test-E-Mail senden.

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 33. Vom Sperrmodus betroffene Elemente

Deaktiviert	Weiterhin funktionsfähig
• Lizenzen löschen • DUP-Updates • SCP-Import • Auf Standardeinstellung zurücksetzen • IPMI • DRAC/LC • DTK-Dienstprogramm SYSCFG • Redfish • OpenManage Essentials • BIOS (F2-Einstellungen werden schreibgeschützt) • Auswählen von Netzwerkkarten • iLKM/SEKM	• Betriebsvorgänge – Einschalten/Ausschalten, Zurücksetzen • Einstellung der Stromobergrenze • Leistungspriorität • Identifizierung von Geräten (Gehäuse oder PERC) • Teileaustausch, Easy Restore (Einfache Wiederherstellung) und Austausch der Hauptplatine • Diagnosen • Modulare Vorgänge (FlexAddress- oder Remote-zugewiesene Adresse) • Alle Anbieterhilfsprogramme mit direktem Zugriff auf das Gerät (ausgewählte NICs ausgeschlossen) • Lizenzexport

Tabelle 33. 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-N1
	• ISM-Einstellungen (Betriebssystem-BMC-Aktivierung, Watchdog-Ping, Betriebssystemname, Betriebssystemversion)

ANMERKUNG: Wenn der Sperrmodus aktiviert ist, wird die OpenID Connect-Anmeldeoption nicht auf der iDRAC-Anmeldeseite angezeigt.

13

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-Nutzer) und die einmalige Anmeldung (SSO, für Active Directory-Nutzer.) 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 Smartcard-Anmeldung
- iDRAC-SSO-Anmeldung für Active Directory-Nutzer konfigurieren
- Smartcard-Anmeldung aktivieren oder deaktivieren
- Konfigurieren von Smart Card-Anmeldung
- Anmelden mit Smartcard

Voraussetzungen für die einmalige Active Directory-Anmeldung oder die Smartcard-Anmeldung

Die Voraussetzungen für die Active Directory-basierten SSO- oder Smartcard-Anmeldungen lauten wie folgt:

- Die iDRAC-Zeit muss mit der Zeit des Active Directory Domain Controllers synchronisiert werden. Andernfalls schlägt die Kerberos-Authentifizierung auf dem iDRAC fehl. Sie können die Zeitzonen- und NTP-Funktion verwenden, um die Uhrzeit zu synchronisieren. Informationen hierzu finden Sie unter Das Konfigurieren von Zeitzone und NTP.
- Registrieren Sie den iDRAC als Computer in der Active Directory-Root-Domäne.

  ANMERKUNG: iDRAC unterstützt keine PIV- (Personal Identity Verification) oder CAC-Smartcard-Nutzerkonten (Common Access Card) in einer untergeordneten oder Subdomain in einer Gesamtstruktur oder Sammlung von Domains. Um diese Einschränkung zu umgehen, wird empfohlen, alle Smartcard-Nutzerkonten in der Stammdomain und nicht in den untergeordneten Domains innerhalb der Gesamtstruktur bereitzustellen.

- Generieren Sie eine Keytab-Datei über das Ktpass-Tool.
- Um Single Sign-On für das erweiterte Schema zu aktivieren, stellen Sie sicher, dass die Option **Diesem Nutzer für die Delegierung zu einem beliebigen Dienst vertrauen (nur Kerberos)** auf der Registerkarte **Delegierung** für den/die Keytab-Nutzerln 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 Hostname mit der DNS-Rückwärtssuche nicht übereinstimmt, schlägt die Kerberos-Authentifizierung fehl.

- Konfigurieren Sie den Browser für die SSO-Anmeldung. Weitere Informationen finden Sie unter Einmaliges Anmelden.

  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 Nutzer für das Standardschema.

ANMERKUNG: Verwenden Sie die vorhandene AD-Benutzergruppe und den AD-Nutzer.

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-Nutzer (anmeldender Nutzer) zu.
5. Vergeben Sie die Zugriffsberechtigung für den Zugriff auf das erstellte Zuordnungsobjekt an **Authentifizierte Nutzer**.

Anmelden bei Active Directory-SSO

Führen Sie die folgenden Schritte für die Active Directory-SSO-Anmeldung aus:

1. Erstellen Sie einen Kerberos-Schlüssel-Registerkarten-Nutzer, 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-Nutzer 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** finden Sie auf der Microsoft Website: **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 lautet AES256-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 **iDRACname** und **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 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-Nutzer 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-Nutzer 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 auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Nutzer** > **Smart Card**.
   Daraufhin wird die Seite **Smart Card** angezeigt.
2. Wählen Sie in der Drop-down-Liste **Smart Card-Anmeldung konfigurieren** die Option **Aktiviert** aus, um die Smart Card-Anmeldung zu aktivieren, oder wählen Sie **Mit Remote-RACADM aktiviert** aus. Andernfalls wählen Sie **Deaktiviert**.

   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.

Smartcard-Anmeldung über RACADM aktivieren oder deaktivieren

Um die Smartcard-Anmeldung zu aktivieren, verwenden Sie den Befehl `set` mit den Objekten in der Gruppe `iDRAC.SmartCard`.

Weitere Informationen finden Sie im *Benutzerhandbuch für den Integrated Dell Remote Access Controller (RACADM CLI)*.

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 **Aktiviert** aus, um die Smartcard-Anmeldung zu aktivieren. Andernfalls wählen Sie **Deaktiviert**. 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 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-Nutzer konfigurieren

Vor der Konfiguration der iDRAC-Smart-Card-Anmeldung für Active Directory-Nutzer 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 Nutzer konfigurieren

So konfigurieren Sie einen lokalen iDRAC-Nutzer für die Smart Card-Anmeldung:

1. Laden Sie das Smart Card-Nutzerzertifikat 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 konfigurierenAktiviert 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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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 Nutzer über die Smart Card-Zertifikatsregistrierungsstation.
8. Wählen Sie den zu registrierenden Nutzer aus, indem Sie auf die Schaltfläche **Nutzer 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. Gehen Sie auf der iDRAC-Weboberfläche zu **iDRAC-Einstellungen** > **Netzwerk** > **Nutzerauthentifizierung** > **Lokale Nutzer**. Die Seite **Nutzer** wird angezeigt.

2. In der Spalte **Nutzer-ID** klicken Sie auf eine Nutzer-ID-Nummer.
   Die Seite **Nutzer-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 Smartcard über RACADM hochladen

Um ein vertrauenswürdiges Zertifikat einer vertrauenswürdigen Zertifizierungsstelle für die Smartcard-Anmeldung hochzuladen, verwenden Sie das Objekt **usercertupload**. Weitere Informationen finden Sie im *Benutzerhandbuch für den Integrated Dell Remote Access Controller (RACADM CLI)*.

Anmelden mit Smartcard

ANMERKUNG: Smartcard-Anmeldung wird in Edge/Chrome und Firefox unterstützt.

ANMERKUNG: Smartcard-Anmeldung wird nur mit TLS 1.2-Version unterstützt.

So melden Sie sich mit einer Smartcard an:

1. Melden Sie sich von der iDRAC-GUI nach der Aktivierung der Smartcard ab.
2. iDRAC über `http://IP/` oder mit FQDN starten. `http://FQDN/`
3. Klicken Sie nach dem Herunterladen des Smartcard Plug-ins auf **Installieren**.
4. Geben Sie die Smartcard-PIN ein und klicken Sie auf **Senden**.
5. iDRAC meldet sich erfolgreich mit der Smartcard an.

14

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 (E-Mail, SNMP-Trap oder IPMI-Warnung, Remote-System-Protokoll, Redfish-Ereignis oder WS-Ereignis), 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 des Systems), 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.

ANMERKUNG: Für alle Updates, die iDRAC zurücksetzen/neu starten müssen, oder für den Fall, dass iDRAC neu gestartet wird, wird empfohlen, zu überprüfen, ob der iDRAC vollständig bereit ist. Warten Sie hierfür einige Sekunden im Intervall mit einem maximalen Timeout von 5 Minuten, bevor Sie einen anderen Befehl verwenden.

Themen:

- Warnungen aktivieren und deaktivieren
- Ereigniswarnungen einrichten
- Alarmwiederholungsereignis einrichten
- Ereignismaßnahmen festlegen
- Einstellungen für E-Mail-Warnungs-SNMP-Trap oder IPMI-Trap konfigurieren
- Konfigurieren von Redfish-Ereignissen
- Remote-Systemprotokollierung konfigurieren
- IDs für Warnungsmeldung
- CPU- und GPU-Leckerkennung

Warnungen aktivieren und deaktivieren

Zum Senden einer Warnmeldung an konfigurierte Ziele oder zum Durchführen einer Ereignisaktion müssen Sie die globale Warnmeldungsoption aktivieren. Diese Eigenschaft überschreibt einzelne Warnmeldungen oder Ereignisaktionen.

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.
   Alle Warnungen, die konfiguriert sind, werden vollständig unter **Warnungskonfiguration – Zusammenfassung** angezeigt.

ANMERKUNG: Sie müssen mindestens eine Kategorie, einen Schweregrad sowie einen Zieltyp auswählen, um die Konfiguration anzuwenden.

ANMERKUNG: Nachdem die Warnmeldungen über die Registerkarte **Schnellwarnmeldungen** konfiguriert wurden und Sie zur Registerkarte **Warnmeldungskonfiguration** wechseln, sind die konfigurierten Warnmeldungen in den entsprechenden Warnmeldungskategorien nicht aktiviert. So aktivieren Sie die entsprechenden Warnmeldungskategorien:

1. Wählen Sie auf der Seite **Warnmeldungskonfiguration** eine der anderen Kategorieregisterkarten (**Systemintegrität**, **Audit**, **Updates** und **Konfiguration**) aus.
2. Kehren Sie zur Kategorie zurück, die ursprünglich für die Konfiguration der Warnmeldungen verwendet wurde.

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 **Plattformereignisse** die Option **Aktiviert** aus, um die Erzeugung von Warnmeldungen oder Ereignismaßnahmen zu aktivieren. Andernfalls wählen Sie **Deaktiviert**. 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 Warnungseinstellungen sind damit konfiguriert.

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 zu den Ereignis- und Fehlermeldungen, die von der Systemfirmware und den Agents, die die Systemkomponenten überwachen, erzeugt werden, finden Sie im **Referenzhandbuch zu Ereignis- und Fehlermeldungen** auf iDRACmanuals.

Ereigniswarnungen über RACADM einrichten

Verwenden Sie zum Festlegen einer Ereigniswarnung den Befehl **eventfilters**. Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Alarmwiederholungsereignis einrichten

Sie können den iDRAC so konfigurieren, dass in bestimmten Intervallen zusätzliche Ereignisse erzeugt werden, wenn das System weiterhin mit einer Temperatur betrieben wird, die über dem Schwellenwert für die Einlasstemperatur liegt. Das Standardintervall beträgt 30 Tage. Der zulässige Bereich liegt zwischen 0 und 366 Tagen. Ein Wert von 0 zeigt an, dass es keine Ereigniswiederholung gab.

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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Einrichten eines Alarmwiederholungsereignisses über die iDRAC-Weboberfläche

So legen Sie einen Wert für die Alarmwiederholung fest:

1. Gehen Sie auf der iDRAC-Weboberfläche zu **Konfiguration** > **Systemeinstellungen** > **Warnmeldungswiederholung**.
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. Gehen Sie auf der iDRAC-Weboberfläche zu **Konfiguration** > **Systemeinstellungen** > **Warnmeldungs- und Remote-Systemprotokollkonfiguration**.
2. Wählen Sie im Drop-down-Menü **Maßnahmen** für jedes Ereignis eine Maßnahme aus:
   - Neustarten
   - 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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Einstellungen für E-Mail-Warnungs-SNMP-Trap oder IPMI-Trap konfigurieren

Die Managementstation verwendet SNMP- (Simple Network Management Protocol) und IPMI-Traps (Intelligent Platform Management Interface), um Daten vom iDRAC zu empfangen. Bei Systemen mit einer großen Anzahl von Nodes ist es für eine Managementstation möglicherweise nicht effizient, jeden einzelnen iDRAC nach allen möglicherweise auftretenden Bedingungen abzufragen. Beispielsweise können Ereignis-Traps einer Managementstation beim Lastenausgleich zwischen Nodes helfen oder indem sie eine Warnmeldung ausgeben, wenn ein Authentifizierungsfehler auftritt. Die Formate SNMP v1, v2 und v3 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 die SNMP-v3-NutzerInnen festlegen, an die Sie die 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 Das *Dell OpenManage SNMP-Referenzhandbuch* ist verfügbar auf der Seite OpenManage Handbücher..

IP-basierte Warnziele über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die Warnungszieleinstellungen unter Verwendung der Web-Schnittstelle:

1. Gehen Sie auf der iDRAC-Weboberfläche zu **Konfiguration** > **Systemeinstellungen** > **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-Nutzer 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 den Communitystring gibt den Communitystring an, der in einem vom iDRAC gesendeten SNMP-Warnmeldungs-Trap (Simple Network Management Protocol) verwendet werden soll. Stellen Sie sicher, dass der Ziel-Communitystring mit dem iDRAC-Communitystring übereinstimmt. Der Standardwert lautet „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** gilt nur für SNMP-Traps und nicht für IPMI-Traps. IPMI-Traps werden immer im SNMP-v1-Format gesendet und basieren nicht auf dem konfigurierten **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-Nutzer für die Trap-Ziele ein:

  ```
  racadm set idrac.SNMP.Alert.<index>.SNMPv3Username <user_name>
  ```

- Aktivieren Sie SNMPv3 für einen Nutzer:

  ```
  racadm set idrac.users.<index>.SNMPv3Enable Enabled
  ```

5. So testen bei Bedarf Sie den Trap:

   ```
   racadm testtrap -i <index>
   ```

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

IP-basierte Warnziele über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren

Sie können Warnmeldungsziele (IPv4, IPv6 oder FQDN) über das Dienstprogramm 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-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. Navigieren 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
     - **Nutzerdefiniert** – 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 vor Ort 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:
  - Dies ist eine lizenzierte Funktion und nicht im Rahmen einer iDRAC-Core-Lizenz verfügbar.
  - Um diese Funktion zu verwenden, müssen Sie über die Berechtigung zum Konfigurieren des iDRAC verfügen.
- Authentication
- 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 verfügbaren 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 nutzerdefinierte Meldung:

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

Parameter	Beschreibung
index	E-Mail-Zielindex. Zulässige Werte sind 1 bis 4.

Parameter	Beschreibung
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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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. Gehen Sie auf der iDRAC-Weboberfläche zu **Konfiguration** > **Systemeinstellungen** > **Warnmeldungskonfiguration** > **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 Redfish-Ereignissen

Das Redfish-Ereignisauslösungsprotokoll wird für einen Client-Service (Abonnent) verwendet, um das Interesse (Abonnement) an einem Server (Ereignisquelle) für den Empfang von Meldungen zu registrieren, die die Redfish-Ereignisse (Benachrichtigungen oder Ereignismeldungen) enthalten. Clients, die Redfish-Ereignisauslösungsmeldungen empfangen möchten, können iDRAC abonnieren und Lifecycle Controller-Jobereignisse erhalten.

Remote-Systemprotokollierung konfigurieren

Sie können Lebenszyklusprotokolle an ein Remotesystem senden. Dazu müssen folgende Voraussetzungen erfüllt sein:

- iDRAC und das Remote-System sind über eine Netzwerkverbindung verbunden.
- Das Remote-System und iDRAC befinden sich auf dem gleichen Netzwerk.

ANMERKUNG: Diese Funktion ist mit einer iDRAC Enterprise- und Datacenter-Lizenz verfügbar.

Ein Remote Syslog-Identitätszertifikat kann innerhalb der Einrichtung des internen Zertifikatsignierungsservers des Unternehmens erzeugt werden. TLS-basierte Remote Syslog-Server und -Clients verwenden dasselbe CA-Zertifikat in den Konfigurationseinstellungen, das von einem CA-Server abgerufen wird. iDRAC bietet eine Benutzeroberfläche, um dieses CA-Zertifikat hochzuladen und zur Konfigurationsdatei hinzuzufügen und den Remote Sylog-Service neu zu starten.

Remote-Systemprotokollierung über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die Remote-Syslog-Server-Einstellungen:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Systemeinstellungen** > **Warnungskonfiguration** > **Remote Syslog** > **Einstellungen**.
2. Die folgenden Einstellungen sind verfügbar. Wählen Sie die erforderliche Einstellung aus:
   - **Basiseinstellungen**: für Legacy-Lösungen
   - **Sichere Einstellungen**: für neue Implementierung (Verschlüsselung des Remote-Syslog-Datenverkehrs mit TLS) Für
   - **Keine**: zum Deaktivieren von Remote-Syslog-Warnmeldungen

   Informationen zu den Feldwerten dieser Optionen finden Sie in der **iDRAC-Onlinehilfe**.
3. Klicken Sie auf **Anwenden**.
   Die Einstellungen werden gespeichert. Alle in das Lebenszyklusprotokoll geschriebenen Protokolle werden gleichzeitig auf den/die konfigurierten Remote-Server geschrieben.

Remote-Systemanmeldung über RACADM konfigurieren

Um die Einstellungen für die Remote-Systemprotokollierung zu konfigurieren, verwenden Sie den Befehl `set` mit den Objekten in der Gruppe `iDRAC.SysLog`.

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

IDs für Warnungsmeldung

Die folgende Tabelle enthält eine Liste mit Meldungs-IDs, die bei Warnungen angezeigt werden.

Tabelle 34. IDs für Warnungsmeldungen

Meldungs-ID	Beschreibung
AMP	Stromstärke
ASR	Automatische Systemrücksetzung
BAT	Batterieereignis
BIOS	BIOS Management
Boot (Starten)	Boot-Steuerung
CBL	Kabel
CPU	Prozessor
CPUA	Verfahren nicht vorhanden
CTL	Storage-Controller
DH	Zertifikatverwaltung
DIS	Automatische Ermittlung
ENC	Storage-Behälter
LÜFTER	Lüftereereignis
FSD	Debug

Tabelle 34. IDs für Warnungsmeldungen (fortgesetzt)

Meldungs-ID	Beschreibung
HWC	Hardware-Konfiguration
IPA	DRAC-IP-Änderung
ITR	Eingriff
JCP	Jobsteuerung
LC	Lifecycle Controller
LIC	Lizenzierung von
Verbindung	Link-Status
Protokoll	Protokollereignis
MEM	Arbeitsspeicher
NDR	NIC-Betriebssystemtreiber
Netzwerkadapter	NIC-Konfiguration
OSD	BS-Bereitstellung
OSE	OS-Ereignis
PCI	PCI-Gerät
PDR	Physisches Laufwerk
PR	Teileaustausch
PST	BIOS-POST
Stromversorgungseinheit	Netzteil
PSUA	PSU nicht vorhanden
PWR	Stromverbrauch
RAC	RAC-Ereignis
RDU	Redundanz
ROT	FW-Download
RFM	FlexAddress-SD
RSI	Remote-Dienst
SEC	Sicherheitsereignis
Systemereignisprotokoll	System-Ereignisprotokoll
SRD	Software-RAID
SSD	PCIe SSD
STOR	Storage
SUP	FW-Aktualisierungsaufgabe
SWC	Softwarekonfiguration
SWU	Software-Änderung
[SYS]	System Info
tmp	Temperatur
TST	Test-Warnung
UEFI (UEFI-Modus)	UEFI-Ereignis

Tabelle 34. IDs für Warnungsmeldungen (fortgesetzt)

Meldungs-ID	Beschreibung
usr	Benutzerverfolgung
VDR	Virtuelles Laufwerk
VLT	Spannung
VME	Virtueller Datenträger
VRM	Virtuelle Konsole
WRK	Arbeitsanmerkung

CPU- und GPU-Leckerkennung

iDRAC erkennt Kühlflüssigkeitslecks der CPU und GPU und gibt die Meldungen „kritisch“, „Warnung“ und „zur Information“, die von den jeweiligen OEM-IPMI-Sensoren empfangen werden. Die Lecks werden als Systemereignisprotokolle (SELs), LC-Protokolle, WS-Ereignisse, E-Mails und SNMP-Traps basierend auf den konfigurierten Warnmeldungseinstellungen gemeldet. iDRAC führt die entsprechenden Aktionen gemäß den Einstellungen für die Warnmeldungskonfiguration durch.

Standardmäßig ist die Warnmeldung **Standardaktion des Flüssigkühlsystems: Ausschalten** als **ordnungsgemäßes Ausschalten** konfiguriert, wenn ein GPU-Leck im Server vorliegt. Es wird empfohlen, das Ausschalten des Servers zu erzwingen, wenn Sie ein GPU-Leck bemerken, und nicht zu warten, bis der **ordnungsgemäße Ausschaltvorgang** abgeschlossen ist.

Wenn iDRAC beim Zugriff auf die LC-Benutzeroberfläche oder die Pre-Boot-Umgebung (BIOS oder Boot-Manager) oder während des Startvorgangs ein GPU-Leck erkennt, kann der Server ein sofortiges Herunterfahren auslösen.

Konfigurieren der CPU-Leckerkennung

Konfigurieren Sie die Warnmeldungen so, dass die erforderlichen Benachrichtigungen erzeugt werden und bestimmte Aktionen in iDRAC basierend auf dem Schweregrad des CPU-Lecks initiiert werden.

1. Gehen Sie zu **Konfiguration** > **Systemeinstellungen** > **Warnmeldungskonfiguration** > **Warnmeldungen** > **Warnmeldungskonfiguration** > **Flüssigkühlsystem**.
2. Klicken Sie auf **+** und aktivieren Sie dann die Kontrollkästchen **E-Mail**, **SNMP-Trap**, **IPMI-Warnmeldung**, **Remote-Systemprotokoll**, **WS-Ereignis**, **BS-Protokoll** und **Redfish-Ereignis** für kritische, Warn- und Informationswarnmeldungen.
3. Wählen Sie die Maßnahmen (**Neustart, Aus- und Einschalten, Ausschalten)** aus der Liste **Aktionen** für kritische, Warn- und Informationswarnmeldungen aus.

Konfigurieren der GPU-Leckerkennung

Standardmäßig ist die Warnmeldung **Standardaktion des Flüssigkühlsystems: Ausschalten** als **ordnungsgemäßes Ausschalten** konfiguriert, wenn ein GPU-Leck im Server vorliegt. Sie können die Optionen entsprechend Ihren Anforderungen konfigurieren.

1. Navigieren Sie zu **Konfiguration** > **Systemeinstellungen** > **Warnmeldungskonfiguration** > **Warnmeldungskonfiguration** > > **Standardaktion für Flüssigkühlsystem: Ausschalten**.
2. Klicken Sie auf **+**.
   Die Kontrollkästchen **Schweregrad** und **SNMP-Trap** sind aktiviert. In der Liste **Aktionen** ist standardmäßig **Ordnungsgemäßes Ausschalten** ausgewählt.
   ANMERKUNG: Wenn der Server innerhalb von 15 Minuten nicht **ordnungsgemäß heruntergefahren** werden kann, wird ein Herunterfahren erzwungen.

   VORSICHT: Wenn iDRAC neu gestartet und gleichzeitig ein Ordnungsgemäßes Ausschalten durchgeführt wird, benötigt das System mehr als 20 Minuten zum Ausschalten. Es wird empfohlen, das Ausschalten des Servers zu erzwingen und nicht zu warten, bis das ordnungsgemäße Ausschalten abgeschlossen ist.
3. Wenn Sie weitere Benachrichtigungen einschließen möchten, aktivieren Sie die Kontrollkästchen **E-Mail**, **SNMP-Trap**, **IPMI-Warnmeldung**, **Remotesystemprotokoll**, **WS-Ereignis**, **BS-Protokoll** und **Redfish-Ereignis**.
4. Wenn Sie die Standardaktion **Ordnungsgemäßes Ausschalten** ändern möchten, wählen Sie die Aktion **Keine Aktion** oder **Ausschalten** aus.

ANMERKUNG: Wenn **Keine Aktion** ausgewählt ist, schaltet sich das System nicht aus, wenn ein GPU-Flüssigkeitsleck vorliegt.

15

Managen von Protokollen

iDRAC bietet ein Lifecycle-Protokoll, das Ereignisse zum System, zu Speichergeräten, Netzwerkgeräten, Firmware-Aktualisierungen, Konfigurationsänderungen, Lizenzmeldungen usw. enthält. Die Systemereignisse stehen jedoch auch als separates Protokoll mit dem Namen System Event Log (SEL) zur Verfügung. Das Lifecycle-Protokoll ist über die iDRAC-Weboberfläche sowie über RACADM zugänglich.

Wenn die Größe des Lebenszyklusprotokolls 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. Zum Anzeigen von archivierten Protokollen müssen Sie das gesamte Lifecycle-Protokoll auf einen Speicherort auf Ihrem System exportieren.

Themen:

- Systemereignisprotokoll anzeigen
- Lifecycle-Protokoll anzeigen
- Lifecycle-Protokoll über RACADM anzeigen
- Exportieren der Lifecycle Controller-Protokolle
- Verhindern eines Überlaufs von Lebenszyklusprotokollen
- Arbeitsanmerkungen hinzufügen
- Lifecycle-Protokoll anzeigen

Systemereignisprotokoll anzeigen

Wenn ein Systemereignis auf einem Managed System auftritt, wird es im Systemereignisprotokoll (SEL) erfasst. 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 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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Systemereignisprotokoll über die Web-Schnittstelle anzeigen

Um das Systemereignisprotokoll (SEL) anzuzeigen, gehen Sie auf der iDRAC-Weboberfläche zu **Wartung** > **Systemereignisprotokoll**.

Die Seite **Systemereignisprotokoll** enthält eine Systemzustandsanzeige, einen Zeitstempel und eine Beschreibung für jedes protokollierte Ereignis. 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 beim Speichern ein Problem auftritt, laden Sie das kumulative Sicherheitsupdate für Internet Explorer herunter. Sie können es von der Microsoft Supportwebsite über **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.

Nachdem das SEL gelöscht wurde, wird ein Eintrag im Lifecycle Controller-Protokoll protokolliert. Der Protokolleintrag enthält den Nutzernamen und die IP-Adresse, von der aus das SEL gelöscht wurde.

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. Gehen Sie hierfür folgendermaßen vor:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Systemereignisprotokoll**.
   Das **iDRAC- Settings.System Event Log** zeigt die **Gesamtzahl der Einträge** an.
2. Zum Löschen der Einträge wählen Sie **Yes** aus. Wählen Sie andernfalls **Nein** aus.
3. Klicken Sie zum Anzeigen der Systemereignisse auf **Systemereignisprotokoll anzeigen**.
4. Klicken Sie auf **Zurück**, dann auf **Fertig stellen** und anschließend auf **Ja**.

Lifecycle-Protokoll anzeigen

Die Lifecycle Controller-Protokolle enthalten den Änderungsverlauf für die auf einem gemanagten System installierten Komponenten. 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 Nutzer, verwendete Schnittstelle und die IP-Adresse des Systems, von dem aus Sie den Job initiieren.

ANMERKUNG: Wenn ein Ereignis mehrmals auftritt, wird ein einzelnes Ereignisprotokoll in den LC-Protokollen angezeigt. Außerdem wird ein zusätzliches Protokoll (L0G007) angezeigt, das angibt, wie oft dieses Ereignis aufgetreten ist. Standardmäßig sind doppelte Ereignisprotokolle in iDRAC deaktiviert. Wenn Sie möchten, dass alle Ereignisse in den LC-Protokollen angezeigt werden, führen Sie den RACADM-Befehl `set idrac.logging.LCDuplicateEventEnable enabled` aus.

Lifecycle-Protokoll über die Web-Schnittstelle anzeigen

Um die Lifecycle-Protokolle anzuzeigen, klicken Sie auf **Wartung** > **Lifecycle-Protokoll**. Die Seite **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 *Referenzhandbuch für iDRAC RACADM CLI*.

Exportieren der Lifecycle Controller-Protokolle

Sie können das gesamte Lifecycle Controller-Protokoll (aktive und archivierte Einträge) in eine gezippte XML-Datei auf einer Netzwerkfreigabe oder auf dem lokalen System exportieren. Die Erweiterung der komprimierten XML-Datei lautet `.xml.gz`. Die Datei-Einträge sind der Reihe nach sortiert, auf der Basis der Sequenz-Zahlen, von der niedrigsten Folgenummer bis zur die höchsten.

Exportieren von Lifecycle Controller-Protokollen mit RACADM

Verwenden Sie zum Exportieren von Lifecycle Controller-Protokollen den Befehl `lclog export`.

Weitere Informationen finden Sie im *Referenzhandbuch für iDRAC RACADM CLI*.

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 eine beliebige der folgenden Optionen:
   - **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 Nutzername 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.

Verhindern eines Überlaufs von Lebenszyklusprotokollen

IDRAC unterstützt die Möglichkeit, einen Überlauf des Lifecycle-Protokolls von Konsolen aufgrund der hohen Häufigkeit von Anmeldungen von Konsolen zu verhindern.

- Die USR0030/USR0032-Ereignisse werden für jede erfolgreiche Anmeldung/Abmeldung im Lebenszyklusprotokoll erfasst.
- Diese Ereignisse können basierend auf einer Attributeinstellung in einem neuen Protokoll aggregiert werden.
- Ein neues USR0036-Protokoll wird im Lebenszyklusprotokoll erfasst, das eine Aggregation der Anmelde-/Abmelde-Protokollereignisse enthält, die innerhalb einer durch das Attribut `LCLoggingAggregationTimeout` angegebenen Zeit aufgetreten sind.

ANMERKUNG:

- Standardmäßig ist das Funktionsattribut „LCLogAggregation“ deaktiviert.
- Standardmäßig ist die Zeitüberschreitung auf 60 Minuten eingestellt und gilt nur, wenn „LCLogAggregation“ aktiviert ist.

- USR0030 und USR0032 dürfen nicht im Lebenszyklusprotokoll erfasst werden, aber es werden weiterhin einzelne Warnmeldungen gesendet, wenn die entsprechenden Warnmeldungen aktiviert sind (SNMP/E-Mail/Redfish-Ereignis/WS-Ereignis).

Arbeitsanmerkungen hinzufügen

Jede/r NutzerIn, der/die sich beim iDRAC anmeldet, kann Arbeitsanmerkungen hinzufügen, die im Lifecycle-Protokoll als Ereignis gespeichert werden. 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 auf der iDRAC-Weboberfläche zu **Dashboard** > **Anmerkungen** > **Anmerkung hinzufügen**.
   Die Seite **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 **Speichern**.
   Daraufhin wird die Arbeitsanmerkung zum Protokoll hinzugefügt. Weitere Informationen finden Sie in der **iDRAC-Online-Hilfe**.

Lifecycle-Protokoll anzeigen

Die Lifecycle Controller-Protokolle enthalten den Änderungsverlauf für die auf einem gemanagten System installierten Komponenten. 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 Nutzer, verwendete Schnittstelle und die IP-Adresse des Systems, von dem aus Sie den Job initiieren.

ANMERKUNG: Wenn ein Ereignis mehrmals auftritt, wird ein einzelnes Ereignisprotokoll in den LC-Protokollen angezeigt. Außerdem wird ein zusätzliches Protokoll (L0G007) angezeigt, das angibt, wie oft dieses Ereignis aufgetreten ist. Standardmäßig sind doppelte Ereignisprotokolle in iDRAC deaktiviert. Wenn Sie möchten, dass alle Ereignisse in den LC-Protokollen angezeigt werden, führen Sie den RACADM-Befehl `set idrac.logging.LCDuplicateEventEnable enabled` aus.

Lifecycle-Protokoll über die Web-Schnittstelle anzeigen

Um die Lifecycle-Protokolle anzuzeigen, klicken Sie auf **Wartung** > **Lifecycle-Protokoll**. Die Seite **Lifecycle-Protokoll** wird angezeigt. Weitere Informationen zu den verfügbaren Optionen finden Sie in der **iDRAC-Online-Hilfe**.

16

Stromversorgung im iDRAC überwachen und managen

Sie können den iDRAC verwenden, um die Stromanforderungen des verwalteten Systems zu überwachen und zu managen. 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.
- **Optionen für die Netzstromwiederherstellung** – Konfigurieren Sie die Optionen für die Netzstromwiederherstellung, damit das System basierend auf Ihren Anforderungen wiederhergestellt wird.

Themen:

- Stromversorgung überwachen
- Festlegen des Warnungsschwellenwerts für den Stromverbrauch
- Ausführen von Stromsteuerungsvorgängen
- Strombegrenzung
- Netzteiloptionen konfigurieren
- Netzschalter aktivieren oder deaktivieren
- Multi-Vektor-Kühlung
- Konfigurieren der Netzstromwiederherstellung

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: Im reinen HBM-Modus wird die HBM-Speicherleistung als Teil der Paketleistung gezählt, daher wird die Speicherstromtelemetrie für diesen Modus als 0 gemeldet.

ANMERKUNG: Nach der Aktualisierung oder Zurücksetzung der iDRAC-Firmware wird das Diagramm zum Stromverbrauch gelöscht bzw. zurückgesetzt.

Überwachen des Leistungsindex für CPU-, Storage- und I/O-Module über die Weboberfläche

Um den Leistungsindex von CPU, Arbeitsspeicher und I/O-Modulen zu überwachen, gehen Sie auf der iDRAC-Weboberfläche zu **System** > **Leistung**.

- Abschnitt **Systemleistung** – Zeigt den aktuellen Messwert und den Warnungsmesswert für den CPU-, Storage- und I/O-Auslastungsindex sowie den CUPS-Index auf Systemebene in einer grafischen Ansicht an.
- Abschnitt **Historische Daten der Systemleistung**:
  - Dieser Abschnitt enthält die Statistiken zu CPU, Arbeitsspeicher und I/O-Auslastung und den Systemebenen-CUPS-Index. Wenn das Hostsystem ausgeschaltet ist, zeigt das Diagramm die Ausschaltlinie unter 0 % an.
  - Sie können die Spitzenauslastung für einen bestimmten Sensor zurücksetzen. Klicken Sie auf **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 Warnungsschwellenwert für die Auslastung an und ermöglicht die Festlegung des Werts. Sie müssen über die Berechtigung zur Serverkonfiguration verfügen, um die Schwellenwerte festzulegen.

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

Überwachen des Leistungsindex für CPU-, Storage- und I/O-Module über RACADM

Verwenden Sie den Unterbefehl **SystemPerfStatistics** zur Überwachung des Leistungsindex für CPU, Arbeitsspeicher und I/O-Module. Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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.

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 auf der iDRAC-Weboberfläche zu **System** > **Übersicht** > **Aktueller Strommesswert und Schwellenwerte**.
2. Klicken Sie im Abschnitt **Aktueller Strommesswert und Schwellenwerte** auf **Warnungsschwellenwert bearbeiten**. Die Seite **Warnungsschwellenwert bearbeiten** wird angezeigt.
3. Geben Sie in die Spalte **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 **Watt** eingeben, berechnet das System automatisch die **BTU/h**-Werte und zeigt sie an. Wenn Sie BTU/h eingeben, werden die Werte ebenso in **Watt** angezeigt.
4. Klicken Sie auf **Speichern**. Die Werte werden konfiguriert.

Ausführen von Stromsteuerungsvorgängen

iDRAC ermöglicht, im Remote-Zugriff die Maßnahmen Einschalten, Ausschalten, Reset, ordentliches Herunterfahren, (NMI) oder Aus- und Einschalten mithilfe der Webschnittstelle oder RACADM auszuführen.

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.

Ausführen von Stromsteuerungsvorgängen über die Web-Schnittstelle

So führen Sie Stromsteuerungsvorgänge aus:

1. Navigieren Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Energiemanagement** > **Energiesteuerung**. Die Optionen für die **Energiesteuerung** werden angezeigt.
2. Wählen Sie die erforderliche Stromsteuerungsmaßnahme aus:
   - System einschalten
   - System ausschalten
   - 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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Strombegrenzung

Sie können die Stromschwellenwerte (Gleich- und Wechselstromverbrauch) anzeigen, die ein System unter schwerer Belastung dem Rechenzentrum meldet. Hierbei handelt es sich um eine lizenzierte Funktion.

Strombegrenzungsrichtlinie anzeigen und konfigurieren

Wenn die Strombegrenzungsrichtlinie aktiviert ist, werden nutzerdefinierte Strombegrenzungen für das System durchgesetzt. Wenn Strombegrenzung nicht aktiviert ist, wird die standardmäßige Hardware-Stromschutzrichtlinie verwendet. Diese Stromschutzrichtlinie ist unabhängig von der nutzerdefinierten Richtlinie. Die Systemleistung wird dynamisch angepasst, um die Leistungsaufnahme am festgelegten Schwellenwert zu halten.

Der tatsächliche Stromverbrauch hängt von der Workload 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.

ANMERKUNG: Das Festlegen eines Grenzwerts für die Stromobergrenze auf einen Wert unterhalb des empfohlenen Bereichs kann zu einer abweichenden Leistung führen, einschließlich einer verlängerten Startzeit.

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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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 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 **Fertig stellen** und anschließend 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.

ANMERKUNG: Hot Spare- und Power Factor-Korrekturfunktionen sind möglicherweise auf einigen Plattformen/Versionen nicht verfügbar.

Das Hot Spare 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. Navigieren Sie auf der iDRAC-Weboberfläche zu **Konfiguration** > **Energieverwaltung** > **Stromkonfiguration**.
2. Wählen Sie unter **Stromredundanzrichtlinie** die erforderlichen 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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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.
   - Aktiviert oder deaktiviert 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 **Fertig stellen** und anschließend 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 **Fertig stellen** und anschließend auf **Ja**.
Die Einstellungen werden gespeichert.

Multi-Vektor-Kühlung

Die Multi-Vektor-Kühlung nutzt einen mehrschichtigen Ansatz zur thermischen Steuerung auf Dell Serverplattformen. Sie können Multi-Vektor-Kühloptionen über die iDRAC-Webschnittstelle konfigurieren, indem Sie zu **Konfiguration** > **Systemeinstellungen** > **Hardwareeinstellungen** > **Kühlungskonfiguration** 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 Nutzer 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:
  - die maximale LFM-Kapazität jedes Steckplatzes innerhalb des Servers sehen.
  - feststellen, welcher Ansatz für die PCIe-Kühlung für jeden Slot zum Einsatz kommt (luftstromgesteuert, temperaturgesteuert).
  - den Mindest-LFM-Wert jedes Steckplatzes sehen, wenn es sich bei der Karte um eine Drittanbieter-Karte (nutzerdefinierte Karte) handelt.
  - einen nutzerdefinierten Mindest-LFM-Wert für die Drittanbieter-Karte festlegen, der eine genauere Definition des Kühlbedarfs ermöglicht, da der Kunde ein besseres Verständnis der nutzerdefinierten Spezifikation der Karte hat.
- Zeigt dem Nutzer 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 nutzerdefinierte Temperatureinstellungen wie thermische Profile (maximale Leistung im Vgl. zu maximaler Leistung pro Watt, Geräuschobergrenze), nutzerdefinierte Lüfterdrehzahloptionen (minimale Lüfterdrehzahl, Offset für Lüftergeschwindigkeit) und nutzerdefinierte Ablufttemperatureinstellungen.
  - 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.

  - Die nutzerdefinierte Ablufttemperatur-Option begrenzt die Ablufttemperatur auf die vom Kunden gewünschten Einstellungen.

    ANMERKUNG: Bei bestimmten Konfigurationen und Auslastungen ist es möglicherweise physikalisch nicht möglich, die Abluft bis unter einen gewünschten Sollwert zu reduzieren (z. B. nutzerdefinierte Ablufteinstellung von 45 °C mit hoher Einlasstemperatur {z. B. 30 °C} und bestimmter geladener Konfiguration {hoher System-Stromverbrauch, niedriger Luftstrom}).

  - 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.
  - 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.
  - Die durchschnittliche Lebenserwartung eines Serverlüfters variiert je nach Plattformspezifikation.
  - Wenn ein Lüfter während des Betriebs entfernt oder eingesetzt wird, kann es bis zu 90 Sekunden dauern, bis die iDRAC-Schnittstellen die Änderungen auf der Seite **Kühlung** (**System** > **Übersicht** > **Kühlung** > **Lüfter**) anzeigen
- Kundenspezifische Kühlkörper wurden entwickelt, um die Komponentenkühlung für minimalen (erforderlichen) Luftstrom zu optimieren und unterstützen gleichzeitig Hochleistungs-CPUs.

Konfigurieren der Netzstromwiederherstellung

Sie können den erwarteten Stromzustand nach einem Stromausfall und einer Stromwiederherstellung des Servers konfigurieren.

1. Wählen Sie den erwarteten Status des Servers im Feld **AC-Stromversorgung** nach der Stromwiederherstellung aus. Die Standardoption ist **An**.

   ANMERKUNG: Wählen Sie **Letzte** aus, wenn Sie den Server im Zustand vor dem Stromausfall wiederherstellen möchten.

2. Wählen Sie die Option**Verzögerung bei Netzstromwiederherstellung** in Abhängigkeit davon aus, wann Sie den Server einschalten möchten.
3. Wenn Sie unter **Verzögerung bei Netzstromwiederherstellung Benutzerdefiniert** ausgewählt haben, geben Sie unter **User Defined Delay (120 s to 600 s)** die Verzögerung in Sekunden (zwischen 120 und 600 Sekunden) ein.

17

Direkte iDRAC-Updates

iDRAC bietet die Out-of-band-Option, die Firmware verschiedener Komponenten eines PowerEdge-Servers zu aktualisieren. Durch die direkten iDRAC-Updates lassen sich stufenweise Jobs während Updates vermeiden. Nur SEP-Rückwandplatinen (passiv) werden für direkte Updates unterstützt.

iDRAC hatte bisher stufenweise Updates, um die Firmwareupdates der Komponenten zu initiieren. Ab dieser Version gibt es direkte Updates für die PSU und die Rückwandplatine. Mithilfe der direkten Updates kann die Rückwandplatine schneller aktualisiert werden. Für die PSU wird ein Neustart (für die Initialisierung der Updates) vermieden und das Update kann mit einem einzigen Neustart erfolgen.

Mit der direkten Updatefunktion von iDRAC kann der erste Neustart zum Initiieren der Updates vermieden werden. Der zweite Neustart wird vom Gerät selbst gesteuert und iDRAC benachrichtigt den Nutzer anhand des Job-Status, wenn ein separater Reset erforderlich ist.

ANMERKUNG: Für alle Updates, die iDRAC zurücksetzen/neu starten müssen, oder für den Fall, dass iDRAC neu gestartet wird, wird empfohlen, zu überprüfen, ob der iDRAC vollständig bereit ist. Warten Sie hierfür einige Sekunden im Intervall mit einem maximalen Timeout von 5 Minuten, bevor Sie einen anderen Befehl verwenden.

18

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)
- Open Compute Project (OCP)-Karten

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 Storage-Ziele) und Attribute auf Partitionsebene (Beispiel: Bandbreitenzuweisung) löschen. Sie können eine Partition deaktivieren, indem Sie die Attributeinstellung „VirtualizationMode“ auf NPAR ändern oder indem Sie alle Persönlichkeiten auf einer Partition deaktivieren.

Je nach Typ des installierten CNA-Geräts werden die Einstellungen der Partitionsattribute möglicherweise nicht ab dem letzten Zeitpunkt beibehalten, an dem die Partition aktiv war. Legen Sie beim Aktivieren einer Partition alle E/A-Identitätsattribute und partitionsbezogenen Attribute fest. Sie können eine Partition aktivieren, indem Sie entweder die Attributeinstellung „VirtualizationMode“ auf NPAR ändern oder indem Sie eine Persönlichkeit (Beispiel: NicMode) auf der Partition aktivieren.

Themen:

- Bestandsaufnahme und Überwachung von FC-HBA-Geräten
- Bestandsaufnahme für Netzwerkgeräte erstellen und Netzwerkgeräte überwachen
- Bestandsaufnahme und Überwachung von SFP-Transceiver-Geräten
- Telemetrie-Streaming
- Serielle Datenerfassung
- Dynamische Konfiguration von virtuellen Adressen, Initiator- und Speicherziel-Einstellungen
- SSD-Verschleiß-Schwellenwerte
- Konfigurieren der Einstellungen für die Beständigkeitsrichtlinie

Bestandsaufnahme und Überwachung von FC-HBA-Geräten

Sie können den Zustand remote überwachen und die Bestandsaufnahme für die Fibre Channel Hostbusadapter (FC HBA) im Managed System anzeigen. Es werden Emulex- und QLogic-FC HBAs unterstützt. Für jeden FC HBA können Sie die folgenden Informationen zu den Ports abrufen:

- FC-Speicherzielinformationen
- NVMe-Speicherzielinformationen
- Schnittstellen-Eigenschaften
- Empfangs- und Übertragungsstatistiken

ANMERKUNG: Emulex FC8-HBAs werden nicht unterstützt.

Überwachung von FC-HBA-Geräten unter Verwendung von RACADM

Um die FC-HBA-Geräteinformationen über RACADM anzuzeigen, verwenden Sie den Befehl `hwinventory`.

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

FC-HBA-Geräte mit der Webschnittstelle überwachen

Um die FC-HBA-Geräteinformationen auf der Weboberfläche anzuzeigen, gehen Sie zu **System** > **Übersicht** > **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.

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

ANMERKUNG: Im Falle eines integrierten NIC-Geräts wird die BIOS-Darstellung jedes LOM-Ports als einzelnes NIC-Gerät betrachtet, sodass die FQDD-Zeichenfolge als **Integrierte NIC 1 Port 1 Partition 1** und **Integrierte NIC 2 Port 1 Partition 1**angezeigt wird.

Netzwerkgeräte über RACADM überwachen

Um Informationen über Netzwerkgeräte anzuzeigen, verwenden Sie die Befehle `hwinventory` und `nicstatistics`.

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Zusätzliche Eigenschaften werden möglicherweise angezeigt, wenn Sie RACADM neben den auf der iDRAC-Weboberfläche angezeigten Eigenschaften verwenden.

Netzwerkgeräte über die Web-Schnittstelle überwachen

Um die Netzwerkgeräteinformationen über die Webschnittstelle anzuzeigen, gehen Sie zu **System** > **Übersicht** > **Netzwerkgeräte**. Die Seite **Netzwerkgeräte** wird angezeigt. Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der **iDRAC-Online-Hilfe**.

ANMERKUNG: **Wake-on-LAN** Die Porteigenschaft für die Netzwerkgeräte in der iDRAC-UI kann veraltete Daten enthalten, da diese während des CSIOR aktualisiert werden. Die korrekten Daten dieser Eigenschaft finden Sie in der RACADM-Ausgabe.

Verbindungsanzeige

Das manuelle Überprüfen und Troubleshooting der Netzwerkverbindungen der Server ist in einer Rechenzentrumsumgebung nicht zu managen. iDRAC optimiert den Job mit der iDRAC-Verbindungsansicht. 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 Verbindungsansicht in iDRAC bietet Details zur physischen Zuordnung von Switch-Ports zu den Netzwerkanschlüssen des Servers und zu dedizierten iDRAC-Anschlussverbindungen. 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 managen.

Die Verbindungsansicht zeigt Informationen zu den Switch-Ports, die mit den Serveranschlüssen verbunden sind, sowie zum dedizierten Anschluss von iDRAC. Die Server-Netzwerkports beinhalten jene auf PowerEdge LOM-, OCP-, Mezz-Karten, PCIe-Add-In-Karten.

Um die Verbindungsansicht für Netzwerkgeräte anzuzeigen, navigieren Sie zu **System** > **Übersicht** > **Netzwerkgerät** > **Verbindungsansicht**, um die Verbindungsansicht zu sehen.

Sie können die Verbindungsansicht auch mit **iDRAC-Einstellungen** > **Konnektivität** > **Netzwerk** > **Allgemeine Einstellungen** > **Verbindungsansicht** aktivieren oder deaktivieren.

Die Verbindungsansicht kann mit dem RACADM-Befehl `SwitchConnection View` untersucht werden.

Aktiviert	Wählen Sie **Aktiviert** aus, um die Verbindungsansicht zu aktivieren. Standardmäßig ist die Option **Aktiviert** ausgewählt.
Status	Zeigt **Aktiviert** an, wenn Sie in der **Verbindungsansicht** in den iDRAC-Einstellungen die Option „Verbindungsansicht“ 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, wenn die Verbindungsansicht aktiviert und die Verbindung hergestellt ist. Die zugeordnete Netzwerkkarte muss mit der Verbindungsanzeige kompatibel sein. Nur NutzerInnen mit iDRAC-Konfigurationsberechtigung können die Einstellungen für die Verbindungsanzeige ändern.

iDRAC unterstützt das Senden von Standard-LLDP-Paketen an externe Switches. Dies bietet Optionen zum Erkennen von iDRACs im Netzwerk. iDRAC sendet zwei Arten von LLDP-Paketen an das ausgehende Netzwerk:

- **Topologie-LLDP** – Bei dieser Funktion durchläuft das LLDP-Paket alle unterstützten Server-NIC-Anschlüsse, sodass ein externer Switch den Ursprungsserver, den OCP-Anschluss [NIC FQDD], den IOM-Standort im Gehäuse usw. finden kann. Topologie-LLDP ist 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 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-Anschluss (dedizierte NIC oder gemeinsam genutztes LOM), sodass ein benachbarter Switch den iDRAC-Verbindungsanschluss 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 enthält einige Details zum iDRAC, z. B. IP-Adresse, MAC-Adresse, Service-Tag usw. Der Switch kann iDRAC-Geräte, die mit ihm verbunden sind, und einige Daten von iDRAC automatisch ermitteln.

  ANMERKUNG: Wenn die virtuelle MAC-Adresse auf einem Anschluss/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** > **Verbindung** > **Netzwerk** > **Allgemeine Einstellungen** > **Topologie-LLDP**.

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 Switchverbindungs- und Switch-Portverbindungsinformationen für den Server-Netzwerkanschluss oder iDRAC-Netzwerkanschluss verfügt. Wenn die Informationen über die Switchverbindung und die Switch-Portverbindung nicht alle fünf Minuten aktualisiert werden, dann werden die Informationen über die Switchverbindung und die Switch-Portverbindung als veraltete (letzte bekannte gute Daten) Daten für alle Benutzeroberflächen angezeigt.

Mögliche Werte für Verbindungsanzeige

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.

Not Available	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.

Bestandsaufnahme und Überwachung von SFP-Transceiver-Geräten

Sie können den Zustand aus der Ferne überwachen und die Bestandsaufnahme für mit dem System verbundene SFP-Transceiver-Geräte anzeigen: Im Folgenden sind die unterstützten Transceiver aufgeführt:

- SFP
- SFP+
- SFP28
- SFP DD
- QSFP
- QSFP+
- QSFP28
- QSFP DD
- Base-T-Module
- AOC- und DAC-Kabel
- RJ-45 Base-T, verbunden mit Ethernet
- Fiber Channel
- IB-Adapter-Ports

Die nützlichsten Transceiver-Informationen sind Seriennummer und Teilenummer vom Transceiver-EPROM. Diese ermöglichen die Überprüfung der remote installierten Transceiver bei der Fehlerbehebung von Verbindungsproblemen. Für jedes SFP-Transceiver-Gerät können Sie die folgenden Informationen zu den Ports abrufen:

- Herstellername
- Teilenummer
- Version
- Seriennummer
- Gerätekennung
- Schnittstellentyp

SFP-Transceiver-Geräte mit der Webschnittstelle überwachen

Um die SFP-Transceiver-Geräteinformationen über die Webschnittstelle anzuzeigen, gehen Sie zu **System** > **Übersicht** > **Netzwerkgeräte** und klicken Sie auf ein bestimmtes Gerät. Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der **iDRAC-Online-Hilfe**.

Im Seitennamen wird auch die Steckplatznummer angezeigt, die angibt, wo das FC-Transceiver-Gerät verfügbar ist, unter Port-Statistiken.

Die Überwachung von Daten für SFP-Geräte ist nur für aktive SFPs verfügbar. Die folgenden Informationen werden angezeigt:

- Sendeausgangsleistung
- Eingangsruhestrom Sender
- Eingangsleistung Empfänger
- Positive Versorgungsspannung
- Temperatur

SFP-Transceiver-Geräte unter Verwendung von RACADM überwachen

Um die SFP-Transceiver-Geräteinformationen unter Verwendung von RACADM anzuzeigen, verwenden Sie den Befehl `networktransceiverstatistics`.

Weitere Informationen finden Sie im *Benutzerhandbuch für den Integrated Dell Remote Access Controller (RACADM CLI)*.

Telemetrie-Streaming

Die Telemetrie ermöglicht es Nutzern, Gerätekennzahlen, Ereignisse und Datenprotokolle zu sammeln und in Echtzeit von einem PowerEdge-Server zu einer abonnierten externen Client- oder Serveranwendung zu streamen. Mithilfe von Telemetrie kann man den Typ und die Häufigkeit von Berichten festlegen, die generiert werden müssen.

ANMERKUNG: Die Funktion wird auf allen Plattformen unterstützt und erfordert eine iDRAC Datacenter-Lizenz.

Die Telemetrie ist eine 1:n-Lösung zum Erfassen und Streamen von Live-Systemdaten von einem oder mehreren PowerEdge-Server(n) (iDRAC) an einen zentralisierten Service für die Überwachung, Analyse und Warnmeldungsausgabe für Remote-Server. Die Funktion unterstützt auch die On-Demand-Datenerhebung der Daten.

Die Telemetriedaten beinhalten Kennzahlen/Bestände und Protokolle/Ereignisse. Die Daten können vom iDRAC zu oder von Remote-Consumern, wie z. B. Redfish-Client und Remote-Syslog-Server, gestreamt (ausgepusht) oder erfasst (abgerufen) werden. Die Telemetriedaten werden auch dem iDRAC SupportAssist Data Collector nach Bedarf bereitgestellt. Die Datenerhebung und der Bericht basieren auf vordefinierten Redfish-Metriken für die Telemetrie, Auslöser- und Berichtdefinitionen. Die Einstellungen für Telemetrie-Streaming können über die iDRAC-Webschnittstelle, RACADM, Redfish und das Serverkonfigurationsprofil (SCP) konfiguriert werden.

Um die Telemetrie zu aktivieren, gehen Sie zu **Konfiguration** > **Systemeinstellungen** > **Telemetrie-Screening** und wählen Sie **Aktiviert** aus der Liste **Telemetriedaten-Stream** aus. Das Datenstreaming erfolgt automatisch, bis die Telemetrie deaktiviert wird.

In der folgenden Tabelle sind die Metrikberichte aufgeführt, die mithilfe von Telemetrie erzeugt werden können:

Tabelle 35. Metrikbericht

Typ	Metrikgruppe	Bestandsaufnahme	Sensor	Statistics	Konfiguration	Kennzahlen
I/O-Geräte	NICs	Nein	Ja	Ja	Nein	Nein
	FC HBAs	Nein	Ja	Ja	Nein	Nein
Servergeräte	CPUs	Nein	Ja	Nein	Nein	Ja
	Arbeitsspeicher	Nein	Ja	Nein	Nein	Ja
	Lüfter	Nein	Ja	Nein	Nein	Nein
	Stromversorgungseinheiten	Nein	Nein	Nein	Nein	Ja
	Sensoren	Nein	Ja	Nein	Nein	Nein
Umgebungsbedingungen	Thermische Auslegung	Nein	Ja	Nein	Nein	Ja
	Stromversorgung	Nein	Nein	Ja	Nein	Ja
	Performance	Nein	Nein	Ja	Nein	Nein
Accelerator	GPUs	Nein	Nein	Ja	Nein	Ja

Informationen zu den Feldbeschreibungen im Telemetrieabschnitt finden Sie in der **iDRAC-Online-Hilfe**.

ANMERKUNG:

- Wenn die SAS/SATA-Rückwandplatine mit dem integrierten SATA-Controller verbunden ist, wird erwartet, dass die Rückwandplatine möglicherweise nicht als Gehäuse im System und möglicherweise auch nicht im Hardwarebestand angezeigt wird.

- StorageDiskSMARTDATA wird nur auf SSD-Festplatten mit SAS/SATA Bus-Protokoll und hinter dem BOSS-Controller unterstützt.
- StorageSensor-Daten werden nur für die Laufwerke im Bereit/Online/nicht-RAID-Modus und nicht hinter dem BOSS-Controller gemeldet.
- NVMeSMARTData wird nur für SSD-Laufwerke (PCIe-SSD/NVMe Express) mit PCIe-Bus-Protokoll (nicht hinter SWRAID) und hinter dem BOSS-N1-Controller unterstützt.
- GPGPUStatistics-Daten sind nur in spezifischen GPGPU-Modellen verfügbar, die ECC-Speicherkapazität unterstützen.
- PSUMetrics ist auf modularen Plattformen nicht verfügbar.
- Die Lüfterstromversorgungs- und PCIe-Strommetriken können für einige Plattformen als 0 angezeigt werden.
- Der CUPS-Bericht wurde in der Version 4.40.00.00 in SystemUsage umbenannt und wird auf Plattformen mit Intel und AMD unterstützt.

Telemetrie-Workflow:

1. Installieren Sie eine Datacenter-Lizenz, wenn diese nicht bereits installiert ist.
2. Konfigurieren Sie die globalen Telemetrie-Einstellungen, einschließlich der Aktivierung von Telemetrie- und Rsyslog-Server-Netzwerkadresse und -Port mithilfe von RACADM, SCP oder iDRAC UI.
3. Konfigurieren Sie die folgenden Parameter für die Telemetrie-Bericht-Übertragungsparameter im erforderlichen Gerätebericht oder -protokoll unter Verwendung der RACADM- oder Redfish-Oberfläche:
   - EnableTelemetry
   - ReportInterval
   - ReportTriggers

   ANMERKUNG: Aktivieren Sie iDRAC-Warnmeldungen und -Ereignisse für die spezifische Hardware, für die Telemetrie-Berichte benötigt werden.
4. Redfish-KundInnen senden eine Abonnementanfrage an den Redfish EventService auf dem iDRAC.
5. Der iDRAC erzeugt und überträgt die Kennzahlenbericht- oder Protokoll- und Ereignisdaten an den abonnierten Client, wenn die vordefinierten Auslöserbedingungen erfüllt sind.

Funktionseinschränkungen:

1. Aus Sicherheitsgründen unterstützt der iDRAC nur die HTTPS-basierte Kommunikation mit dem Client.
2. Aus Gründen der Stabilität unterstützt der iDRAC bis zu acht Abonnements.
3. Das Löschen von Abonnements ist nur über die Redfish-Schnittstelle möglich, das gilt auch für die manuelle Löschung durch den Administrator.

Verhalten der Telemetrie-Funktion:

- Der iDRAC erzeugt und übermittelt (HTTP POST) die Metrikbericht- oder Protokoll- und Ereignisdaten an alle abonnierten Clients auf dem im Abonnement angegebenen Ziel, wenn die vordefinierten Auslöserbedingungen erfüllt sind. Die Clients erhalten neue Daten nur nach erfolgreicher Abonnementerstellung.
- Die Metrikdaten enthalten den Zeitstempel im ISO-Format mit UTC-Zeit (endet mit Z) zum Zeitpunkt der Datenerhebung von der Quelle.
- Clients können ein Abonnement beenden, indem Sie über die Redfish-Schnittstelle eine HTTP-Löschmeldung an die URI der Abonnementressource senden.
- Wenn das Abonnement entweder vom iDRAC oder vom Client gelöscht wird, sendet der iDRAC keine Berichte (HTTP POST). Wenn die Anzahl der Lieferfehler vordefinierte Schwellenwerte überschreitet, kann der iDRAC ein Abonnement löschen.
- Wenn ein Nutzer über Administratorberechtigungen verfügt, kann er die Abonnements löschen, jedoch nur über die Redfish-Schnittstelle.
- Der Client wird über die Beendigung eines Abonnements vom iDRAC benachrichtigt, indem das Ereignis „Abonnement beendet“ als letzte Nachricht gesendet wird.
- Abonnements sind persistent und können auch nach dem Neustart des iDRAC aktiv bleiben. Sie können die Abonnements jedoch löschen, indem Sie die Vorgänge `racadm systemerase idrac` oder `racresetcfg` ausführen.
- Auf Nutzeroberflächen wie RACADM, Redfish, SCP und iDRAC wird der aktuelle Status der Client-Abonnements angezeigt.
- Die Bereitschaft des TelemetryService kann mithilfe eines neuen Attributs `TelemetryServiceStatus` überprüft werden, das unter dem `GetRemoteServiceAPIStatus`-API-Aufruf hinzugefügt wurde. Dieses Attribut wird der vorhandenen Liste mit LTStatus, RTStatus, ServerStatus und Status hinzugefügt.

Metrische Berichtsdefinition

Eine Metrikberichtsdefinition bietet eine Möglichkeit, die Metriken zu definieren, die in einem Telemetriebericht enthalten sein müssen, und wie der Bericht erzeugt und gestreamt werden muss.

Das iDRAC-Telemetrie-Streaming bietet Metriken, die Daten zum Serverstatus ohne Leistungsbeeinträchtigung des Hauptservers bereitstellen können. Diese Metriken umfassen verschiedene Systemparameter wie CPU-Auslastung, Speicherauslastung, Stromverbrauch, Temperaturmesswerte, Lüftergeschwindigkeit und mehr.

Importieren und Bearbeiten der Metrikberichtsdefinition

Wenn Sie eine Metrikberichtsdefinition an Ihre spezifischen Anforderungen anpassen möchten, importieren Sie die Metrikberichtsdefinition und bearbeiten Sie die Eigenschaften.

1. Gehen Sie zu **Konfiguration** > **Systemeinstellungen** > **Telemetriekonfiguration** > **Metrikberichtsdefinition**.
2. Wählen Sie den **Standorttyp** aus.
3. Klicken Sie auf **Datei auswählen** und wählen Sie eine Datei aus.
4. Klicken Sie auf **Importieren**.
   Die Datei mit dem Metrikbericht wird importiert. Der Bericht wird in der Liste **Telemetrieberichte** angezeigt.
5. Wenn Sie einen bestimmten Metrikbericht bearbeiten möchten, klicken Sie für diesen bestimmten Bericht auf **Aktionen** > **Berichtseigenschaften bearbeiten**.
   Das Dialogfeld **Berichtseinstellungen** wird angezeigt.
6. Ändern Sie die Berichtseinstellungen und klicken Sie auf **Speichern**.

Metrikberichtsdefinition exportieren

Exportieren Sie die Definition des Metrikberichts, wenn Sie die Performance von Servern vergleichen oder den Metrikbericht als Vorlage für andere Server verwenden möchten.

1. Gehen Sie zu **Konfiguration** > **Systemeinstellungen** > **Telemetriekonfiguration** > **Metrikberichtsdefinition**.
2. Wählen Sie den **Standorttyp** aus.
3. Wählen Sie die **Metrikberichtsdefinition** aus.
4. Klicken Sie auf **Speichern**.
   Die Metrikberichtsdatei wird gespeichert.

Auslöser

Telemetrieauslöser definieren eine Reihe von Bedingungen. Basierend auf diesen Bedingungen werden die zugehörigen Metrikberichte erzeugt und gestreamt. Die Bedingungen können ein Systemereignis oder eine nutzerdefinierte Bedingung umfassen, z. B. wenn ein Metrikwert einen Schwellenwert überschreitet oder einen konkreten Wert erreicht.

Trigger können so konfiguriert werden, dass sie eine Vielzahl von Bedingungen überwachen, z. B. Hardwarefehler, Änderungen in der Systemleistung oder andere wichtige Ereignisse. iDRAC sendet den zugehörigen Kennzahlenbericht mithilfe einer der konfigurierten Streaming-Methoden. Bei diesen Methoden handelt es sich um vom Server gesendete Ereignisse (SSE) oder „Post to Subscription“.

Trigger exportieren

Exportieren Sie Trigger, wenn Sie die Trigger von Servern vergleichen oder als Vorlage für andere Server verwenden möchten.

1. Navigieren Sie zu **Konfiguration** > **Systemeinstellungen** > **Telemetriekonfiguration** > **Trigger**.
2. Wählen Sie den **Standorttyp** aus.
3. Wählen Sie den Trigger aus der Liste **Dateiname** aus.
4. Klicken Sie auf **Exportieren**.
   Die Triggerdatei wird in der Liste **Trigger** angezeigt.

Importtrigger

Wenn Sie einen Trigger an Ihre spezifischen Anforderungen anpassen möchten, importieren Sie ihn.

1. Navigieren Sie zu **Konfiguration** > **Systemeinstellungen** > **Telemetriekonfiguration** > **Trigger**
2. Wählen Sie den **Standorttyp** aus.
3. Klicken Sie auf **Datei auswählen** und wählen Sie eine Datei aus.
4. Klicken Sie auf **Importieren**.
   Die Triggerdatei wird importiert. Die Trigger werden in der Liste **Trigger** angezeigt.

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 die Kunden sie später zu Debugging-Zwecken abrufen können.

Sie können eine serielle Datenerhebung mit den Schnittstellen RACADM, Redfish und iDRAC aktivieren oder deaktivieren. Wenn dieses Attribut aktiviert ist, erfasst der iDRAC den seriellen Datenverkehr, der auf den seriellem Host-Gerät2 empfangen wird, unabhängig von den Einstellungen des seriellen MUX-Modus.

Um die serielle Datenerhebung mit der iDRAC-UI 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/die NutzerIn die serielle Erfassung deaktiviert und erneut aktiviert, beginnt der iDRAC den Anhängevorgang ab dem letzten Update.

Die serielle Datenerhebung des Systems beginnt, wenn der/die NutzerIn 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 Storage mit einer Begrenzung von 512 KB. Dieser Puffer ist zirkulär.

ANMERKUNG:
- Um diese Funktion zu nutzen, muss man über die Berechtigung zur Anmeldung und Systemsteuerung verfügen.
- Für diese Funktion wird eine iDRAC Datacenter-Lizenz benötigt.

Dynamische Konfiguration von virtuellen Adressen, Initiator- und Speicherziel-Einstellungen

Sie können die Einstellungen für die virtuelle Adresse, den Initiator und das Storage-Ziel dynamisch anzeigen und konfigurieren sowie eine Persistenzrichtlinie anwenden. Dies ermöglicht es der Anwendung, die Einstellungen basierend auf Änderungen des Energiestatus (d. h. Neustart des Betriebssystems, Warmstart, Kaltstart oder Ein-/Ausschalten) sowie basierend auf der Persistenzrichtlinieneinstellung für diesen Energiestatus anzuwenden. Dies bietet mehr Flexibilität für Bereitstellungen, die eine schnelle Neukonfiguration von System-Workloads auf einem anderen System erfordern.

Die virtuellen Adressen sind:

- Virtuelle MAC-Adresse
- Virtuelle iSCSI MAC-Adresse
- Virtuelle FIP-MAC-Adresse
- Virtuelles 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 Storage-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 den Initiator und die Storage-Ziele ändern sich möglicherweise je nachdem, wie die Hauptstromversorgung beim System-Reset erfolgt und ob das NIC-, CNA- oder FC-HBA-Gerät mit Hilfsstrom versorgt wird. Die Persistenz der E/A-Identitätseinstellungen kann basierend auf der über den iDRAC festgelegten Richtlinieneinstellung erreicht werden.

Nur wenn die E/A-Identitätsfunktion aktiviert ist, werden die Persistenzrichtlinien wirksam. Jedes Mal, wenn das System zurückgesetzt oder eingeschaltet wird, werden die Werte basierend auf den Richtlinieneinstellungen beibehalten oder gelöscht.

ANMERKUNG: Nachdem die Werte gelöscht wurden, können sie erst wieder angewendet werden, nachdem der Konfigurationsjob ausgeführt wurde.

Anzeigen der Unterstützung für die I/O-Identitätsoptimierung auf der Weboberfläche

Wird unter **Port-Eigenschaften** der spezifischen NIC-Karte (**System** > **Netzwerkgeräte**) **Persistenz-Richtlinienfähigkeit Möglich** angezeigt, unterstützt diese Karte die I/O-Identitätsoptimierung.

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 36. 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	Persistenzrichtlinie löschen – Virtuelle Adresse
Remote-zugewiesene Adresse aktiviert	RemoteAssignedAddress-Modus	Aktiviert	Virtuelle Adressverwaltung (VAM) ist konfiguriert.	Konfigurierte VAM besteht weiterhin	Auf Remote-zugewiesene Adresse eingestellt
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	RemoteAssignedAddress-Modus	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	RemoteAssignedAddress-Modus	Deaktiviert	VAM nicht konfiguriert	Auf Remote-zugewiesene Adresse eingestellt	Auf Remote-zugewiesene Adresse eingestellt
Remote-zugewiesene Adresse deaktiviert	RemoteAssignedAddress-Modus	Aktiviert	VAM konfiguriert	Konfigurierte VAM besteht weiterhin	Nur Persistenz – Löschen ist nicht möglich
Remote-zugewiesene Adresse deaktiviert	RemoteAssignedAddress-Modus	Aktiviert	VAM nicht konfiguriert	Auf Hardware-MAC-Adresse eingestellt	Persistenz wird nicht unterstützt.

Tabelle 36. 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	Persistenzrichtlinie löschen – Virtuelle Adresse
					Abhängig vom Kartenverhalten
Remote-zugewiesene Adresse deaktiviert	RemoteAssignedAddress-Modus	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	RemoteAssignedAddress-Modus	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

ANMERKUNG:

- Die Teileaustauschkonfiguration für partitionsfähige Karten funktioniert einwandfrei, wenn VirtualizationMode (das Attribut zum Aktivieren der Anzahl von Partitionen) mit der ausgetauschten Karte und der im Server vorhandenen NIC-Karte identisch ist.
- Die Teileaustauschkonfiguration wird nicht ausgelöst, wenn der VirtualizationMode (Anzahl der Partitionen) der ersetzten Karte nicht mit der im Server vorhandenen NIC-Karte übereinstimmt.
- Im Fenster „Teileaustausch“ vor CSIOR stellt der Lifecycle Controller die NIC-Konfiguration wieder her. Dies beinhaltet einen Kaltstart gefolgt von einem Warmstart. Nach beiden Neustarts verfügt die NIC über dieselbe Firmware; diese wird während des Wiederherstellungsvorgangs installiert.
- Die Persistenzrichtlinie gilt für jeden Neustart basierend auf der Policy. Beim Kaltstart werden virtuelle Identitäten nicht angewendet, da die Firmware-Version nicht übereinstimmt und Persistenzdaten gelöscht werden.
- Die Persistenz-Policy-Funktion prüft die PCI-IDs und die Firmwareversion der aktuellen und vorherigen NIC desselben Anbieters, der ersetzt wird. Falls diese Felder nicht übereinstimmen, werden virtuelle Identitäten nicht angewendet und Persistenzdaten (virtuelle Identitäten) werden ebenfalls von iDRAC gelöscht.
- Für den Austausch von Teilen muss der Anbieter die gleichen PCI-IDs und die gleiche Firmwareversion beibehalten oder Sie müssen eine VAM-Job-/Vorlagenbereitstellung durchführen.

Systemverhalten für FlexAddress und E/A-Identität

Tabelle 37. 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 Device-Konfiguration 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.

ANMERKUNG: E/A-Identitätsattribute sollten nur mithilfe von SCP festgelegt werden, damit sie über Neustarts hinweg bestehen bleiben. Werden andere Methoden verwendet, um sie festzulegen, bleiben die Attribute nicht bestehen.

Eine Liste der E/A-Identitätsoptimierungsattribute, die Sie in der SCP-Datei ändern können, finden Sie im Dokument **NIC-Profil** auf Dell Supportseite.

ANMERKUNG: Ändern Sie keine Attribute außerhalb der E/A-Identitätsoptimierung.

Aktivieren oder Deaktivieren der E/A-Identitätsoptimierung über die Weboberfläche

So aktivieren oder deaktivieren Sie die E/A-Identitätsoptimierung:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Systemeinstellungen** > **Hardwareeinstellungen** > **E/A-Identitätsoptimierung**.
   Die Seite **E/A-Identitätsoptimierung** wird angezeigt.
2. Klicken Sie auf die Registerkarte **E/A-Identitätsoptimierung** und wählen Sie die Option **Aktivieren** aus, um diese Funktion zu aktivieren. Wählen Sie die Option zum Deaktivieren der Funktion ab.
3. Klicken Sie auf **Anwenden,** um die Einstellung zu übernehmen.

Aktivieren oder Deaktivieren der I/O-Identitätsoptimierung über RACADM

Verwenden Sie zum Aktivieren der I/O-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 I/O-Identitätsoptimierung den folgenden Befehl:

```
racadm set idrac.ioidopt.IOIDOptEnable Disabled
```

Verwenden Sie zum Anzeigen der Einstellungen für die I/O-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 **Beständigkeitsrichtlinie** kann möglicherweise nicht ausgeführt werden, wenn das Attribut **VirtualAddressManagement** in iDRAC auf **FlexAddress-**Modus eingestellt ist. Stellen Sie sicher, dass Sie das Attribut **VirtualAddressManagement** in iDRAC auf den **Konsole**-Modus einstellen.

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- oder E-Mail-Benachrichtigungen aktiviert. Protokolle sind ebenfalls in den Remote-Syslogs enthalten.

Standardwerte für die Beständigkeitsrichtlinie

Tabelle 38. Standardwerte für die Beständigkeitsrichtlinie

Beständigkeitsrichtlinie	Stromausfall	Hardwarestart	Softwareneustart
Virtuelle Adresse: Auxiliär-betriebene Geräte	Nicht markiert	Ausgewählt	Ausgewählt
Virtuelle Adresse: Nicht-auxiliär-betriebene Geräte	Nicht markiert	Nicht markiert	Ausgewählt
Initiator	Ausgewählt	Ausgewählt	Ausgewählt

Tabelle 38. Standardwerte für die Beständigkeitsrichtlinie (fortgesetzt)

Beständigkeitsrichtlinie	Stromausfall	Hardwarestart	Softwareneustart
Storage Target	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 Storage-Ziele gemäß der Definition in Standardwerte für iSCSI-Initiator und Storage-Ziel 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 Adressen die Objekte **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyAuxPwrd** und **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyNonAuxPwrd**.
- Verwenden Sie für Initiatoren das Objekt **iDRAC.IOIDOPT.InitiatorPersistencePolicy**.
- Verwenden Sie für Storage-Ziele das Objekt **iDRAC.IOIDOpt.StorageTargetPersistencePolicy**.

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 39. 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

Tabelle 39. iSCSI-Initiator – Standardwerte (fortgesetzt)

iSCSI-Initiator	Standardeinstellungen im IPv4-Modus	Standardeinstellungen im IPv6-Modus
IscsiInitiatorGateway	0.0.0.0	::
IscsiInitiatorIpv4Gateway	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Gateway	::	::
IscsiInitiatorPrimDns	0.0.0.0	::
IscsiInitiatorIpv4PrimDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6PrimDns	::	::
IscsiInitiatorSecDns	0.0.0.0	::
IscsiInitiatorIpv4SecDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6SecDns	::	::
iscsiInitiatorName	Wert wurde gelöscht	Wert wurde gelöscht
IscsiInitiatorChapId	Wert wurde gelöscht	Wert wurde gelöscht
IscsiInitiatorChapPwd	Wert wurde gelöscht	Wert wurde gelöscht
IPVer	Ipv4	Ipv6

Tabelle 40. 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	-

19

Managen von Storage-Geräten

iDRAC unterstützt PERC 12- und BOSS N1-Controller.

ANMERKUNG: Das Löschen des Hardwarecaches schlägt auf einem konfigurierten externen PERC12-Controller fehl. Führen Sie den Konfigurationsvorgang zum Zurücksetzen aus, bevor Sie den Hardware-Cache löschen.

ANMERKUNG:

- BOSS-Controller unterstützen nur RAID 0 und RAID 1.
- Alle fremden virtuellen Laufwerke, die hinter BOSS-Controllern erkannt werden, sollten entweder aus dem BIOS HII oder mithilfe des Vorgangs zum Controller-Reset gelöscht werden.
- Bei BOSS-Controllern sind die vollständigen Informationen des virtuellen Laufwerks möglicherweise nicht verfügbar, wenn beide physischen Laufwerke ausgesteckt und wieder eingesteckt werden.
- Für alle Updates, die iDRAC zurücksetzen/neu starten müssen, oder für den Fall, dass iDRAC neu gestartet wird, wird empfohlen, zu überprüfen, ob der iDRAC vollständig bereit ist. Warten Sie hierfür einige Sekunden im Intervall mit einem maximalen Timeout von 5 Minuten, bevor Sie einen anderen Befehl verwenden.
- Für PERC12 ist die Online-Kapazitätserweiterung (OCE) durch Hinzufügen eines Laufwerks nur auf einem virtuellen Laufwerk mit voller Größe möglich. OCE durch Hinzufügen eines Laufwerks wird nicht für virtuelle Laufwerke mit Slice unterstützt.
- Um unvorhersehbare Fehler zu vermeiden, wird empfohlen, während ein Storage-Job ausgeführt wird, keine Storage-bezogenen Vorgänge durchzuführen.

iDRAC erweitert seine Managementfunktionen ohne Agent um die direkte Konfiguration der PERC-Controller. Damit können Sie die an Ihr System angeschlossenen Storage-Komponenten während der Laufzeit remote konfigurieren. Zu diesen Komponenten gehören RAID- und Nicht-RAID-Controller sowie die damit verbundenen Kanäle, Anschlüsse, Gehäuse und Festplatten.

Die Erkennung, Topologie, Zustandsüberwachung und Konfiguration des gesamten Speichersubsystems erfolgt im CEM-Framework (Comprehensive Embedded Management), indem durch das MCTP-Protokoll über die I2C-Schnittstelle eine Verbindung zwischen den internen und externen PERC-Controllern hergestellt wird.

ANMERKUNG: Der Software-RAID (SWRAID) wird von CEM nicht unterstützt und somit auch nicht in der iDRAC-UI. SWRAID kann mithilfe von RACADM oder Redfish verwaltet werden.

Unter Verwendung von iDRAC können Sie die meisten der in OpenManage Storage Management verfügbaren Funktionen ausführen, einschließlich der Echtzeitkonfigurationsbefehle (ohne Neustart) (beispielsweise die Befehle zum Erstellen virtueller Laufwerke). Sie können RAID vollständig konfigurieren, bevor Sie das Betriebssystem installieren.

Sie können die Controller-Funktionen ohne Zugriff auf das BIOS konfigurieren und managen. Diese Funktionen umfassen das Konfigurieren von virtuellen Laufwerken und das Anwenden von RAID-Stufen und Hot Spares für den Schutz von Daten. Sie können zahlreiche weitere Controller-Funktionen initiieren, wie z. B. Wiederherstellungen und Troubleshooting. Sie können Ihre Daten schützen, indem Sie Datenredundanz konfigurieren oder Hot Spares zuweisen.

ANMERKUNG: Wenn die BIOS-Einstellung für Volume Management Device (VMD) (mit ID-Modul-Unterstützung) auf einem PowerEdge-Server aktiviert ist, vermeiden Sie die Konfiguration von an die CPU angebundenen NVMe-Laufwerken, um unvorhersehbares Verhalten zu verhindern.

Zu den Storage-Geräten gehören:

- Controller – Die meisten Betriebssysteme lesen und schreiben Daten nicht direkt von den/auf die Festplatten, sondern senden stattdessen Lese- und Schreibanweisungen an einen Controller. Der Controller ist die Hardware in Ihrem System, die direkt mit den Festplatten kommuniziert, damit Daten geschrieben und abgerufen werden. Ein Controller besitzt Konnektoren (Kanäle oder Schnittstellen), die mit einem oder mehreren physischen Laufwerken oder mit einem Gehäuse verbunden sind, das physische Laufwerke enthält. RAID-Controller können sich über die Grenzen von Festplatten erstrecken, um einen erweiterten Speicherplatz (oder ein virtuelles Laufwerk) zu erzeugen, der/das die Kapazität von mehr als einer Festplatte verwendet. Controller führen auch andere Aufgaben aus, wie z. B. das Starten von Neuerstellungen, Initialisieren von Festplatten usw. Um diese Aufgaben auszuführen, benötigen Controller spezielle Software, die Firmware und Treiber genannt wird. Damit der Controller ordnungsgemäß funktioniert, muss darauf die erforderliche Mindestversion der Firmware und Treiber installiert sein. Unterschiedliche Controller besitzen verschiedene Eigenschaften, was das Lesen und Schreiben von Daten sowie das Ausführen von Aufgaben angeht. Voraussetzung für eine möglichst effiziente Verwaltung des Speichers ist, diese Merkmale zu kennen.

- Physische Laufwerke oder physische Geräte – Befinden sich in einem Gehäuse oder sind mit dem Controller verbunden. Bei einem RAID-Controller werden die physischen Laufwerke oder Geräte für die Erstellung von virtuellen Laufwerken verwendet.
- Virtuelles Laufwerk – Hierbei handelt es sich um Storage, der unter Verwendung eines oder mehrerer Laufwerke durch einen RAID-Controller erstellt wird. Obwohl ein virtuelles Laufwerk aus mehreren physischen Laufwerken bestehen kann, wird sie vom Betriebssystem als ein einzelnes Laufwerk betrachtet. Bei einem Laufwerkausfall oder bei bestimmten Leistungsmerkmalen können je nach der verwendeten RAID-Stufe redundante Daten bei einem virtuellen Laufwerk erhalten bleiben. Virtuelle Laufwerke können nur auf einem RAID-Controller erstellt werden.
- Gehäuse – Es wird extern mit dem System verbunden, während die Rückwandplatine und deren physische Laufwerke integriert sind. Wenn die Gehäuse in einer Multipath-Konfiguration verbunden sind, stellen Sie sicher, dass die folgenden Portkombinationen für die Verbindung mit den Controllern verwendet werden:
  - Port 0 und Port 2
  - Port 1 und Port 3
- Rückwandplatine – Sie ähnelt einem Gehäuse. Bei einer Rückwandplatine sind der Controller-Konnektor und die physischen Laufwerke mit dem Gehäuse verbunden. Sie verfügt jedoch nicht über die Managementfunktionen (Temperatursonden, Alarme usw.), die mit externen Gehäusen assoziiert werden. Physische Laufwerke können sich in einem Gehäuse befinden oder an die Rückwandplatine eines Systems angeschlossen sein.

ANMERKUNG: Bei der Maximalkonfiguration mit ca. 192 physischen Laufwerken nimmt das Abschließen der Bestandsaufnahme mindestens 30 Minuten in Anspruch.

ANMERKUNG: Wenn ein System über ein umfangreiches Array an Storage-Komponenten verfügt, z. B. 240 virtuelle Laufwerke und 60 Laufwerke, wird davon ausgegangen, dass bestimmte ausstehende Storage-Vorgänge oder die Vorgänge „Ausstehende verwerfen“ zu Fehlern in Kombination mit dem Fehler RAC0508 führen.

ANMERKUNG: Wenn eine oder mehrere Rückwandplatinen mit einem Expander verbunden sind, wird die Gehäuseposition als **Unbekannt** angezeigt.

ANMERKUNG: Auf einigen Plattformen wird das Entfernen/Einsetzen von SLED bei laufendem Betrieb nicht unterstützt und es treten möglicherweise unerwartete Fehler auf. Vor dem Entfernen/Einsetzen muss das Gerät ausgeschaltet werden.

Es können nicht nur die im Gehäuse enthaltenen physischen Laufwerke verwaltet werden, sondern Sie können auch den Status der Lüfter, Netzteile und Temperatursonden des Gehäuses überwachen. Sie können Gehäuse per Hotplugging anschließen. Hotplugging ist das Hinzufügen einer Komponente zu einem System, während das Betriebssystem ausgeführt wird.

ANMERKUNG: Der Status der Laufwerke, die im laufenden Betrieb entfernt werden, wird als **Entfernt** angezeigt und die Laufwerksinformationen sind in den Hardware- und Firmwarebeständen bis zum nächsten Neustart des Hosts abrufbar.

Die physischen Geräte, die mit dem Controller verbunden sind, müssen über die neueste Firmware verfügen. Die neueste unterstützte Firmware erhalten Sie von Ihrem Serviceanbieter.

ANMERKUNG: Wenn Sie ein Update der Laufwerksfirmware auf Hot-Plug-fähigen Laufwerken durchführen, fehlt das PR36-Protokoll möglicherweise in den Lifecycle-Protokollen, obwohl das Update erfolgreich war. Um dies zu vermeiden, führen Sie vor dem Firmwareupdate einen Neustart des Hosts durch.

ANMERKUNG: PR36 wird nach Firmwareupdates für Batteriebackupeinheiten (Battery Backup Units, BBUs) und Datenverarbeitungseinheiten (Data Processing Units, DPUs) nicht protokolliert.

Speicherereignisse vom PERC werden gegebenenfalls SNMP-Traps zugeordnet. Alle Änderungen an den Speicherkonfigurationen werden im Lifecycle-Protokoll erfasst.

ANMERKUNG: Nach einem Serverneustart meldet iDRAC möglicherweise das PDR8 LC-Protokoll für Laufwerke, die hinter PERC-Controllern angeschlossen sind.

ANMERKUNG: In iDRAC können Sie die Rückwandplatine/das Gehäuse sehen, die/das mit dem PERC-Controller Ihres Systems verknüpft ist. Dieses Gehäuse meldet 16 Steckplätze (auch wenn Ihr System nicht so viele Laufwerke unterstützt).

In Systemen, in denen Laufwerke direkt mit dem RAID-Controller verkabelt sind, wird ein Eintrag für jede mögliche Laufwerksverbindung zu PERC erstellt. PERC unterstützt bis zu 16 kabelgebundene Laufwerke, sodass Ihnen 16 Steckplätze gemeldet werden.

Tabelle 41. PERC-Fähigkeit

PERC-Fähigkeit	CEM-konfigurationsfähiger Controller
Echtzeit	Bei ausstehenden oder geplanten Jobs für jegliche Controller müssen die Jobs gelöscht werden, oder Sie müssen warten, bis die Jobs abgeschlossen sind, bevor Sie die Konfiguration zur Laufzeit

Tabelle 41. PERC-Fähigkeit (fortgesetzt)

PERC-Fähigkeit	CEM-konfigurationsfähiger Controller
	anwenden. Ein Neustart ist für Laufzeit- oder Echtzeitjobs nicht erforderlich.
Durchgeführt	k. A.

Themen:

- Zum Verständnis von RAID-Konzepten
- Unterstützte Controller
- Unterstützte Gehäuse
- Übersicht über die unterstützten Funktionen für Speichergeräte
- Bestandsaufnahme für Storage-Geräte erstellen und Storage-Geräte überwachen
- Anzeigen der Speichergerätetopologie
- Managen von physischen Festplatten
- Konvertieren einer physischen Festplatte in den RAID- und Nicht-RAID-Modus
- Löschen physischer Laufwerke
- Löschen von SED/ISE-Gerätedaten
- Physisches Laufwerk neu erstellen
- Verwalten von virtuellen Festplatten
- RAID-Konfigurationsfunktionen
- Managen von PCIe-SSDs
- Managen von Gehäusen oder Rückwandplatinen
- Storage-Geräte – Szenarien des Anwenden-Vorgangs
- Blinken oder Beenden des Blinkens der Komponenten-LEDs
- Softwareneustart

Zum Verständnis von RAID-Konzepten

Storage Management verwendet RAID-Technologie (Redundantes Array unabhängiger Festplatten), um Speicherverwaltungsfunktionalität bereitzustellen. Kenntnisse von Storage Management setzen ein Verständnis von RAID-Konzepten voraus, sowie eine gewisse Vertrautheit mit der Art und Weise, wie die RAID-Controller Ihres Systems und das Betriebssystem mit Festplattenspeicherplatz umgehen.

Was bedeutet RAID?

RAID ist eine Technologie zur Verwaltung von Storage auf den physischen Laufwerken, die sich in einem System befinden oder mit ihm verbunden sind. Ein wichtiger Aspekt von RAID ist die Fähigkeit, mehrere physische Laufwerke zusammenzufassen, sodass ihre kombinierte Storage-Kapazität als einzelner, erweiterter Speicherplatz behandelt werden kann. Ein weiterer wichtiger Aspekt von RAID ist die Möglichkeit, redundante Daten zu managen und bei einem Festplattenausfall zu verwenden, um Daten wiederherzustellen. RAID verwendet verschiedene Techniken wie Striping, Spiegelung und Parität, um Daten zu speichern und zu rekonstruieren. Es gibt verschiedene RAID-Level, die unterschiedliche Methoden zum Speichern und Rekonstruieren von Daten verwenden. Die RAID-Level weisen unterschiedliche Merkmale in Bezug auf Lese-/Schreibleistung, Data Protection und Storage-Kapazität auf. Nicht alle RAID-Level umfassen Datenredundanz, was bedeutet, dass verlorene Daten für einige RAID-Level nicht wiederhergestellt werden können. Der gewählte RAID-Level hängt davon ab, ob Ihre Priorität auf Performance, Schutz oder Storage-Kapazität liegt.

ANMERKUNG: Das RAID Advisory Board (RAB) definiert die Spezifikationen für die Implementierung von RAID. Obwohl GPU die RAID-Level definiert, kann die kommerzielle Implementierung von RAID-Leveln durch verschiedene Anbieter von den tatsächlichen RAID-Spezifikationen abweichen. Eine Implementierung eines bestimmten Anbieters kann sich auf die Lese- und Schreibleistung und den Grad der Datenredundanz auswirken.

Hardware- und Software-RAID

RAID kann über Hardware oder Software implementiert werden. Ein System, das Hardware-RAID verwendet, verfügt über einen RAID-Controller, der die RAID-Level implementiert und Datenlese- und Schreibvorgänge auf die physischen Laufwerke verarbeitet. Bei

Verwendung von Software-RAID, das vom Betriebssystem bereitgestellt wird, implementiert das Betriebssystem die RAID-Level. Aus diesem Grund kann die Verwendung von Software-RAID allein die Systemleistung verlangsamen. Sie können jedoch Software-RAID zusammen mit Hardware-RAID-Volumes verwenden, um eine bessere Leistung und Vielfalt bei der Konfiguration von RAID-Volumes zu erhalten. Beispielsweise können Sie ein Paar Hardware-RAID-5-Volumes auf zwei RAID-Controller spiegeln, um RAID-Controller-Redundanz bereitzustellen.

RAID-Konzepte

RAID verwendet bestimmte Techniken zum Schreiben von Daten auf Festplatten. Diese Techniken ermöglichen es RAID, Datenredundanz oder eine bessere Leistung bereitzustellen. Diese Techniken umfassen:

- Spiegelung – Duplizieren von Daten von einem physischen Laufwerk auf ein anderes physisches Laufwerk. Spiegelung bietet Datenredundanz, indem zwei Kopien derselben Daten auf verschiedenen physischen Laufwerken aufbewahrt werden. Wenn eine der Festplatten in der Spiegelung ausfällt, kann das System weiterhin mit der nicht betroffenen Festplatte betrieben werden. Beide Seiten der Spiegelung enthalten immer dieselben Daten. Beide Seiten der Spiegelung können als operative Seite fungieren. Eine gespiegelte RAID-Laufwerksgruppe ist bei Lesevorgängen mit einer RAID-5-Laufwerksgruppe vergleichbar, bei Schreibvorgängen jedoch schneller.
- Striping – Disk Striping schreibt Daten auf alle physischen Laufwerke in einem virtuellen Laufwerk. 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 einem einzelnen physikalischen Festplatten befindet, ist ein Stripe-Element. Mit Striping allein erhält man keine Datenredundanz. Wenn Striping jedoch mit Parität kombiniert wird, lässt sich Datenredundanz erzielen.
- Stripe-Größe: Der gesamte Speicherplatz, der von einem Stripe verbraucht wird, ohne Paritätsfestplatte. Beispielsweise beträgt bei einem Stripe, der 64 KB Speicherplatz enthält und 16 KB Daten auf jedem Laufwerk im Stripe aufweist, die Stripe-Größe 64 KB und die Stripe-Elementgröße 16 KB.
- Stripe-Element – Ein Stripe-Element ist ein Teil eines Stripes, welcher sich auf einer einzigen physischen Festplatte befindet.
- Stripe-Elementgröße: Die Speicherplatzmenge, die von einem Stripe-Element verbraucht wird. Beispielsweise beträgt bei einem Stripe, der 64 KB Speicherplatz enthält und 16 KB Daten auf jedem Laufwerk im Stripe aufweist, die Stripe-Elementgröße 16 KB und die Stripe-Größe 64 KB.
- Parität – Parität bezieht sich auf redundante Daten, die mithilfe eines Algorithmus in Kombination mit Striping verwaltet werden. Wenn eine der Striping-Festplatten ausfällt, können die Daten mithilfe des Algorithmus aus den Paritätsinformationen rekonstruiert werden.
- Bereich – Ein Bereich ist eine RAID-Technik, mit der Speicherplatz von Gruppen physischer Laufwerke in einem virtuellen RAID 10, 50, oder 60 Laufwerk kombiniert wird.

RAID-Level

Jede RAID-Stufe verwendet eine Kombination von Datenspiegelung, Striping und Parität, um Datenredundanz oder eine verbesserte Lese- und Schreibleistung bereitzustellen. Details zu den einzelnen RAID-Leveln finden Sie in Auswählen des RAID-Levels.

Datenspeicher-Organisation zur erhöhten Verfügbarkeit und Leistung

RAID bietet verschiedene Methoden oder RAID-Level für die Organisation des Festplattenspeichers. Einige RAID-Level behalten redundante Daten bei, sodass Sie Daten nach einem Festplattenausfall wiederherstellen können. Verschiedene RAID-Level bedeuten auch eine Steigerung oder Verringerung der I/O-Leistung (Lese- und Schreibvorgänge) eines Systems.

Die Wartung redundanter Daten erfordert die Verwendung zusätzlicher physischer Laufwerke. Die Wahrscheinlichkeit eines Festplattenausfalls steigt mit einer Erhöhung der Anzahl der Festplatten. Da die Unterschiede bei der I/O-Leistung und Redundanz variieren, ist ein RAID-Level je nach Den Anwendungen in der Betriebsumgebung und der Art der gespeicherten Daten möglicherweise besser geeignet als ein anderes.

Wenn eine RAID-Stufe ausgewählt wird, treffen die folgenden Leistungs- und Kostenerwägungen zu:

- **Verfügbarkeit oder Fehlertoleranz** – Verfügbarkeit oder Fehlertoleranz bezieht sich auf die Fähigkeit eines Systems, den Betrieb aufrechtzuerhalten und den Zugriff auf Daten sicherzustellen, selbst wenn eine seiner Komponenten ausgefallen ist. In RAID-Volumes wird Verfügbarkeit oder Fehlertoleranz durch die Aufrechterhaltung redundanter Daten erreicht. Redundante Daten umfassen Spiegelungen (doppelte Daten) und Paritätsinformationen (Rekonstruieren von Daten mithilfe eines Algorithmus).
- **Leistung** – Die Lese- und Schreibleistung kann je nach dem ausgewählten RAID-Level erhöht oder verringert werden. Einige RAID-Level sind möglicherweise für bestimmte Anwendungen besser geeignet.
- **Kosteneffizienz** – Die Beibehaltung redundanter Daten oder Paritätsinformationen im Zusammenhang mit RAID-Volumes erfordert zusätzlichen Speicherplatz. In Situationen, in denen die Daten temporär, einfach reproduziert oder nicht wesentlich sind, sind die erhöhten Kosten für Datenredundanz möglicherweise nicht gerechtfertigt.

- **Mean Time Between Failure (MTBF)** – Die Verwendung zusätzlicher Festplatten zur Beibehaltung redundanter Daten erhöht auch die Wahrscheinlichkeit eines Festplattenausfalls zu einem beliebigen Zeitpunkt. Diese Option kann zwar in Situationen, in denen redundante Daten erforderlich sind, nicht vermieden werden, hat jedoch Auswirkungen auf die Arbeitslast der Systemsupportmitarbeiter in Ihrem Unternehmen.
- **Volume** – Volume bezieht sich auf ein einzelnes virtuelles nicht-RAID-Laufwerk. Sie können Volumes mit externen Dienstprogrammen wie dem O-ROM-<Ctrl> <r> erstellen. Storage Management bietet keine Unterstützung für die Erstellung von Volumes. Sie können jedoch Volumes anzeigen und Laufwerke von diesen Volumes für die Erstellung neuer virtueller Laufwerke oder für die Online-Kapazitätserweiterung (OCE) vorhandener virtueller Laufwerke verwenden, sofern freier Speicherplatz verfügbar ist.

Auswählen der RAID-Stufen

Sie können RAID zur Steuerung des Daten-Storage auf mehreren Festplatten verwenden. Jede RAID-Stufe oder -Verkettung besitzt unterschiedliche Leistungs- und Datenschutz-Eigenschaften.

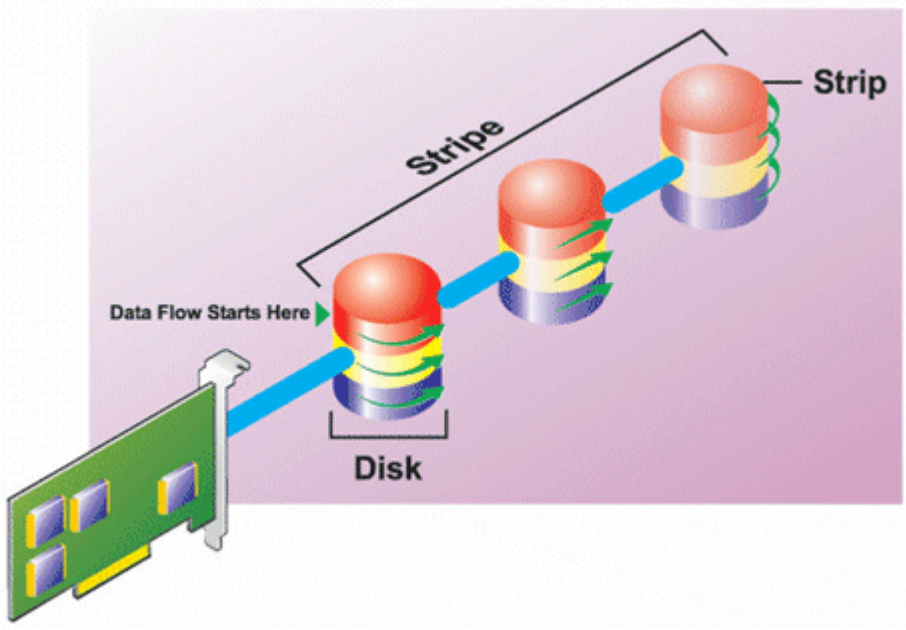
ANMERKUNG: Die H3xx-PERC-Controller bieten keine Unterstützung für die RAID-Stufen 6 und 60.

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 Laufwerke geschrieben werden. RAID 0 bietet keine Datenredundanz.

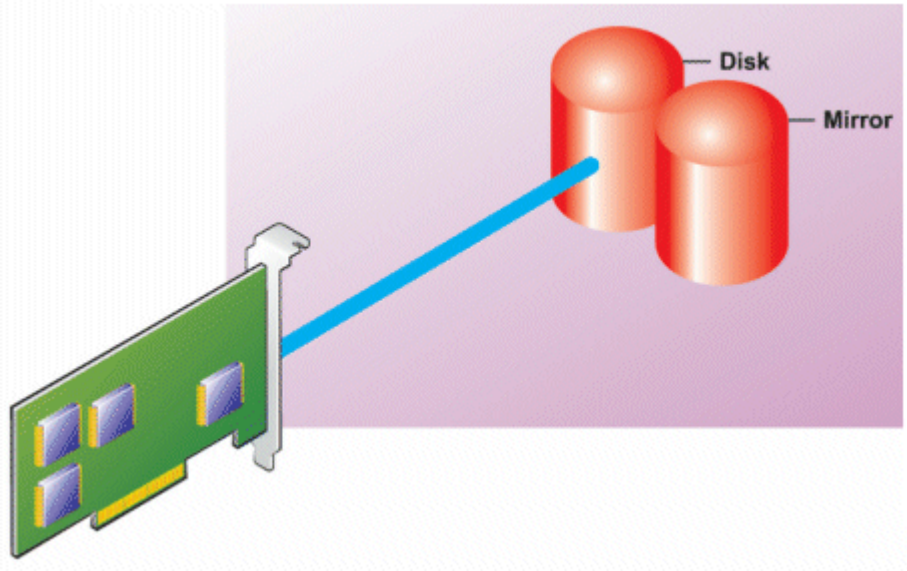


RAID 0-Eigenschaften:

- 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 das große virtuelle Laufwerk aus – ohne eine Möglichkeit zur Neuerstellung der Daten.
- Bessere Lese- und Schreibleistung.

RAID-Stufe 1 (Datenspiegelung)

RAID 1 ist die einfachste Form der Aufrechterhaltung redundanter Daten. In RAID 1 werden Daten auf einem oder mehreren physischen Laufwerken gespiegelt oder dupliziert. Wenn ein physisches Laufwerk ausfällt, können die Daten unter Verwendung der Daten der anderen Seite der Spiegelung wieder aufgebaut werden.

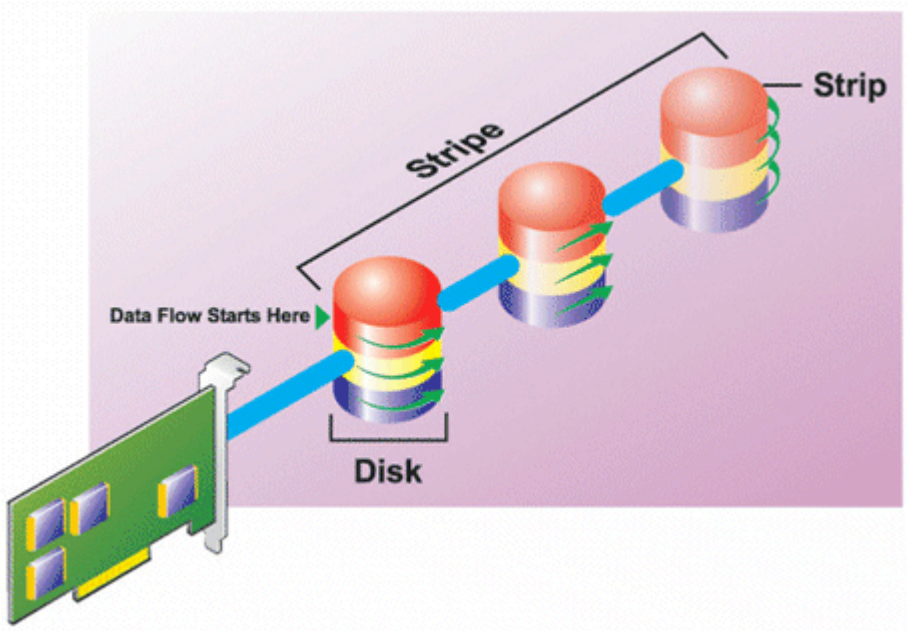


RAID 1-Eigenschaften:

- Gruppiert **n**+**n**-Festplatten zu einem großen virtuellen Laufwerk mit einer Kapazität von **n**-Festplatten. Die Controller, die derzeit von Storage Management unterstützt werden, ermöglichen die Auswahl von zwei Laufwerken bei der Erstellung eines RAID 1. Da diese Laufwerke gespiegelt werden, entspricht die Gesamtspeicherkapazität einem Laufwerk.
- Die Daten werden auf den beiden Laufwerken repliziert.
- Wenn ein Laufwerk ausfällt, funktioniert das virtuelle Laufwerk weiterhin. Die Daten werden von der Spiegelung des ausgefallenen Laufwerks gelesen.
- Bessere Leseleistung, aber etwas langsamere Schreibleistung.
- Redundanz zum Schutz der Daten.
- RAID 1 ist in Bezug auf Laufwerksspeicherplatz teurer, da die doppelte Anzahl von Laufwerken verwendet wird, die zum Speichern der Daten ohne Redundanz erforderlich wären.

RAID-Level-5 oder Striping mit verteilter Parität

RAID 5 bietet Datenredundanz durch Die Verwendung von Daten-Striping in Kombination mit Paritätsinformationen. Anstatt ein physisches Laufwerk der Parität zu dedizieren, werden die Paritätsinformationen auf alle physischen Laufwerke in der Laufwerksgruppe verteilt.

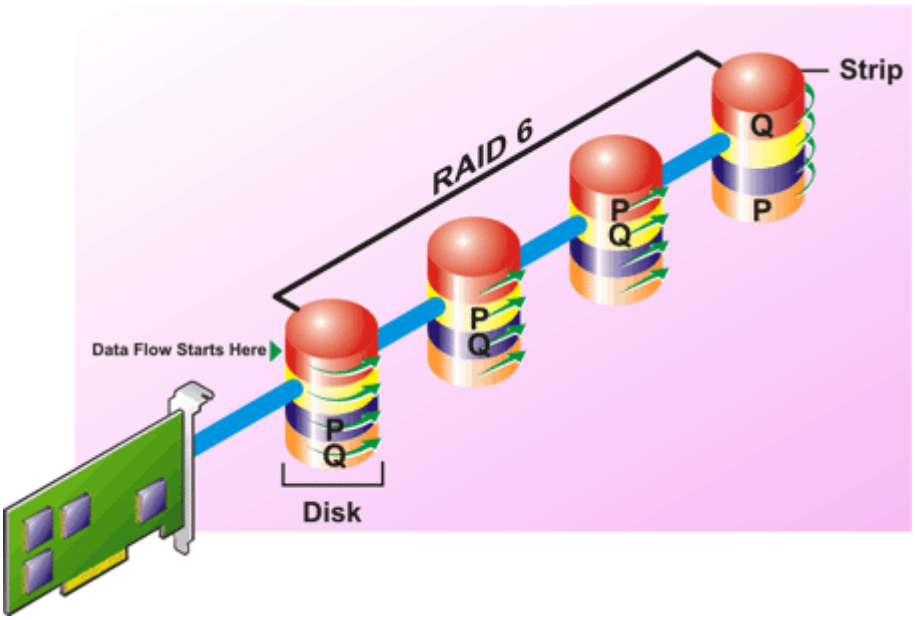


RAID 5-Eigenschaften:

- Gruppiert **n** Laufwerke als ein großes virtuelles Laufwerk mit einer Kapazität von (**n**-1) Laufwerken.
- Redundante Informationen (Parität) werden abwechselnd auf allen Laufwerken gespeichert.
- Wenn ein Laufwerk fehlerhaft wird, funktioniert das virtuelle Laufwerk weiterhin, aber es wird in einem herabgesetzten Zustand betrieben. Die Daten werden von den verbleibenden Laufwerken rekonstruiert. Die Daten werden von den verbleibenden Laufwerken rekonstruiert.
- Bessere Leseleistung, aber langsamere Schreibleistung.
- Redundanz zum Schutz der Daten.

RAID-Level-6-Striping mit zusätzlicher verteilter Parität

RAID 6 bietet Datenredundanz durch Die Verwendung von Daten-Striping in Kombination mit Paritätsinformationen. Ähnlich wie bei RAID 5 wird die Parität in jedem Stripe verteilt. RAID 6 verwendet jedoch ein zusätzliches physisches Laufwerk, um die Parität aufrechtzuerhalten, sodass jeder Stripe in der Laufwerksgruppe zwei Festplattenblöcke mit Paritätsinformationen verwaltet. Die zusätzliche Parität bietet Data Protection bei zwei Festplattenausfällen. In der folgenden Abbildung werden die beiden Sätze von Paritätsinformationen als **P** und **Q** identifiziert.



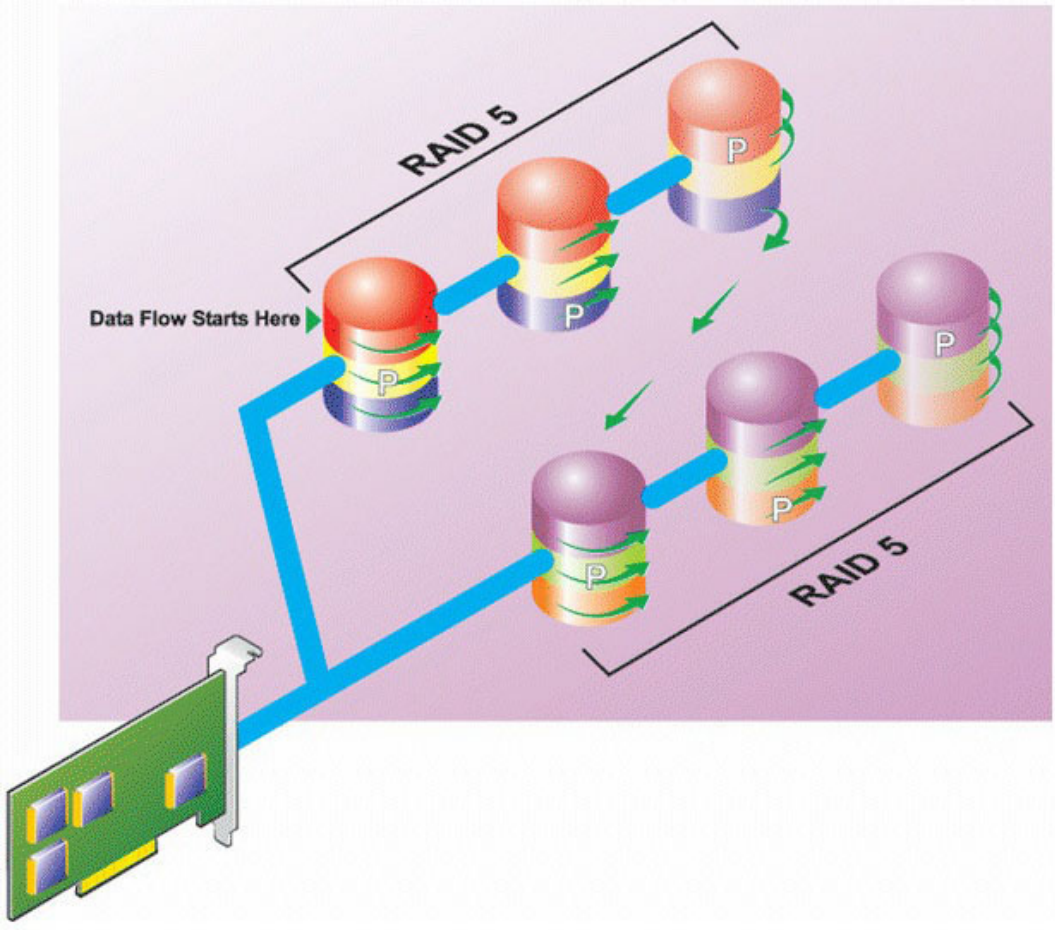
RAID 6-Eigenschaften:

- Gruppiert **n** Laufwerke als ein großes virtuelles Laufwerk mit einer Kapazität von (**n**-2) Laufwerken.
- Redundante Informationen (Parität) werden abwechselnd auf allen Laufwerken gespeichert.
- Das virtuelle Laufwerk funktioniert auch bei bis zu zwei ausgefallenen Laufwerken weiterhin. Die Daten werden von den verbleibenden Laufwerken rekonstruiert.
- Bessere Leseleistung, aber langsamere Schreibleistung.
- Erhöhte Redundanz zum Schutz der Daten.
- Für die Parität sind zwei Laufwerke pro Bereich erforderlich. RAID 6 ist in Bezug auf Festplattenspeicher teurer.

RAID-Stufe 50 (Striping über RAID 5-Sets)

Wählen Sie RAID 50 aus, um Striping über mehr als einen Bereich physischer Laufwerke zu implementieren. Bei RAID 50 erstreckt sich Striping über mehr als einen Bereich physischer Laufwerke. Eine RAID 5-Festplattengruppe, die mit drei physischen Laufwerken implementiert ist und dann mit einer Festplattengruppe von drei weiteren physischen Laufwerken fortfährt, wäre beispielsweise ein RAID 50.

Es ist möglich, RAID 50 zu implementieren, auch wenn die Hardware sie nicht direkt unterstützt. In diesem Fall können Sie mehr als ein virtuelles RAID-5-Laufwerk implementieren und dann die RAID 5-Laufwerke in dynamische Laufwerke konvertieren. Sie können dann ein dynamisches Volume erstellen, das sich über alle virtuellen RAID-5-Laufwerke erstreckt.

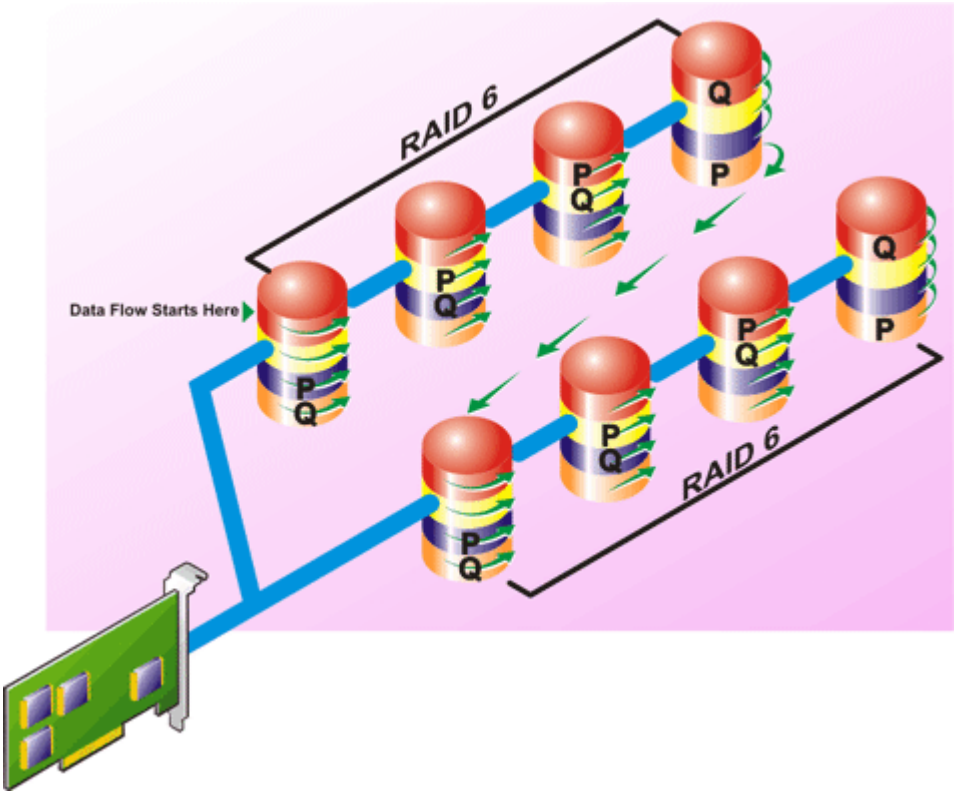


RAID 50-Eigenschaften:

- Gruppiert **n*****s** Laufwerke als ein großes virtuelles Laufwerk mit einer Kapazität von **s***(**n**-1) Laufwerken, wobei **s** die Anzahl von Bereichen und **n** die Anzahl von Laufwerken innerhalb jeden Bereiches darstellt.
- Redundante Informationen (Parität) werden abwechselnd auf allen Laufwerken jedes RAID 5-Bereiches gespeichert.
- Bessere Leseleistung, aber langsamere Schreibleistung.
- Erfordert die gleiche Menge an Paritätsinformationen wie RAID 5.
- Die Daten werden kontinuierlich auf alle Festplatten verteilt. RAID 50 ist in Bezug auf Festplattenspeicher teurer.

RAID-Stufe 60 (Striping über RAID 6-Sets)

RAID 60 verteilt sich über mehr als einen Bereich physischer Laufwerke, die als RAID 6 konfiguriert sind. Beispiel: Eine RAID-6-Laufwerksgruppe, die mit vier physischen Laufwerken implementiert wird und dann mit einer Laufwerksgruppe von vier weiteren physischen Laufwerken fortgesetzt wird, wäre ein RAID 60.

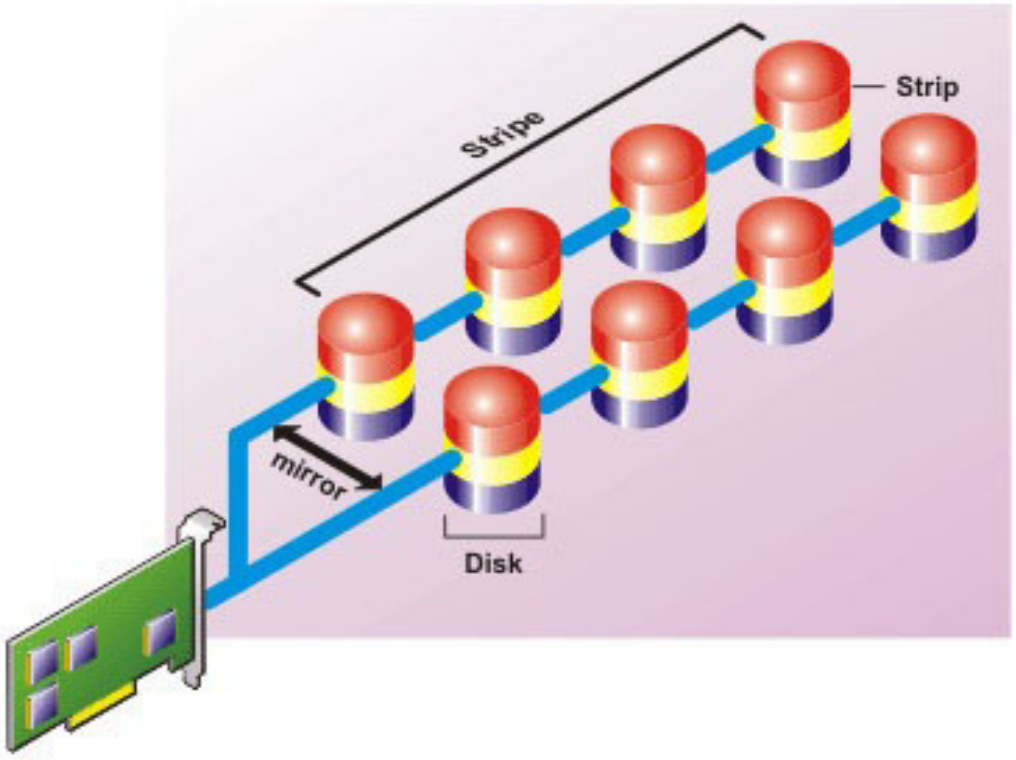


RAID 60-Eigenschaften:

- Gruppiert **n*****s** Laufwerke als ein großes virtuelles Laufwerk mit einer Kapazität von **s***(**n**-2) Laufwerken, wobei **s** die Anzahl von Bereichen und **n** die Anzahl von Laufwerken innerhalb jeden Bereiches darstellt.
- Redundante Informationen (Parität) werden abwechselnd auf allen Laufwerken 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 die Parität sind zwei Laufwerke pro Bereich erforderlich. RAID 60 ist in Bezug auf Festplattenspeicher teurer.

RAID-Level 10 – Striping mit Spiegelungen

Die HÖCHSTMAß betrachtet RAID-Level 10 als eine Implementierung von RAID-Level 1. RAID 10 kombiniert gespiegelte physische Laufwerke (RAID 1) mit Daten-Striping (RAID 0). Bei RAID 10 werden Daten über mehrere physische Laufwerke verteilt. Die Striping-Laufwerksgruppe wird dann auf einen anderen Satz physischer Laufwerke gespiegelt. RAID 10 kann als **Spiegelung von Stripes** betrachtet werden.



RAID 10-Eigenschaften:

- Gruppiert **n** Laufwerke als ein großes virtuelles Laufwerk mit einer Kapazität von (**n**/2) Laufwerken, wobei **n** für eine gerade Ganzzahl steht.
- Spiegelungsbilder der Daten werden über Sätze physischer Laufwerke verteilt. Diese Stufe bietet Redundanz durch Spiegelung.
- Wenn ein Laufwerk ausfällt, funktioniert das virtuelle Laufwerk weiterhin. Die Daten werden von dem überlebenden gespiegelten Laufwerkspaar 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 42. 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	2N (N = 1)	Kleine Datenbanken, Datenbank-Protokolle und kritische Informationen
RAID 5	Gut	Sequenzielles Lesen: Gut.	Mittelmäßig, es sei denn Rückschreiben in	Moderat	N + 1 (N = wenigstens zwei Festplatten)	Datenbanken und andere lese-

Tabelle 42. 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	Moderat	Gut	2N x X	Daten-intensive Umgebungen (große Datensätze)
RAID 50	Gut	Sehr gut	Moderat	Moderat	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)	Wichtige Informationen. Datenbanken und andere lese-intensive direkte Verwendungen
RAID 60	Ausgezeichnet	Sehr gut	Moderat	Schlecht	N + 2 (N = wenigstens 2)	Wichtige Informationen. Mittelgroße direkte oder Daten-intensive Verwendungen
N = Anzahl der physischen Laufwerke und X = Anzahl der RAID-Sets						

Unterstützte Controller

Unterstützte RAID-Controller

Die iDRAC-Schnittstellen unterstützen die folgenden PERC12-Controller:

- PERC H965i Front
- PERC H965e

Die iDRAC-Schnittstellen unterstützen die folgenden BOSS-Controller:

- BOSS-N1

Unterstützte Gehäuse

iDRAC unterstützt MD1400- und MD1420-Gehäuse.

Übersicht über die unterstützten Funktionen für Speichergeräte

Die folgenden Tabellen enthalten die Funktionen, die über iDRAC durch die Speichergeräte unterstützt werden.

Tabelle 43. Unterstützte Funktionen für Storage-Controller – PERC 12

Funktionen	H965i-Front und H965i-Adapter	H965e Adapter	H465i Adapter
Physisches Laufwerk als einen globalen Hot Spare zuweisen oder die Zuweisung rückgängig machen	Echtzeit	Echtzeit	Nicht zutreffend
In RAID konvertieren	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Zu RAID/Nicht-RAID konvertieren,	Echtzeit (wandelt das Laufwerk in ein Nicht-RAID-Volume um)	Echtzeit (wandelt das Laufwerk in ein Nicht-RAID-Volume um)	Echtzeit
Neu erstellen	Echtzeit	Echtzeit	Nicht zutreffend
Erneutes Aufbauen abbrechen	Echtzeit	Echtzeit	Nicht zutreffend
Virtuelle Laufwerke erstellen	Echtzeit	Echtzeit	Nicht zutreffend
Virtuelle Laufwerke umbenennen	Echtzeit	Echtzeit	Nicht zutreffend
Cache-Richtlinien für virtuelle Laufwerke bearbeiten	Echtzeit	Echtzeit	Nicht zutreffend
Konsistenz der virtuellen Laufwerke überprüfen	Echtzeit	Echtzeit	Nicht zutreffend
Konsistenzüberprüfung abbrechen	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Virtuelle Laufwerke initialisieren	Echtzeit	Echtzeit	Nicht zutreffend
Initialisierung abbrechen	Echtzeit	Echtzeit	Nicht zutreffend
Virtuelle Laufwerke verschlüsseln	Echtzeit	Echtzeit	Nicht zutreffend
Dedizierten Hot Spare zuweisen und Zuweisung rückgängig machen	Echtzeit	Echtzeit	Nicht zutreffend
Virtuelle Laufwerke löschen	Echtzeit	Echtzeit	Nicht zutreffend
Hintergrundinitialisierung abbrechen	Echtzeit	Echtzeit	Nicht zutreffend
Online-Kapazitätserweiterung	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
RAID-Level-Migration	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Verwerfen des beibehaltenen Cache	Echtzeit	Echtzeit	Echtzeit
Patrol Read-Modus einstellen	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Manueller Patrol Read-Modus	Echtzeit	Echtzeit	Nicht zutreffend
Patrol Read – Nicht konfigurierte Bereiche	Echtzeit	Echtzeit	Nicht zutreffend
Konsistenzüberprüfungsmodus	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Copyback-Modus	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Lastausgleichsmodus	Nicht zutreffend	Nicht zutreffend	Echtzeit
Konsistenzüberprüfungsrate	Echtzeit	Echtzeit	Nicht zutreffend

Tabelle 43. Unterstützte Funktionen für Storage-Controller – PERC 12 (fortgesetzt)

Funktionen	H965i-Front und H965i-Adapter	H965e Adapter	H465i Adapter
Boot VD	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
PD-Status ändern	Nicht zutreffend	Nicht zutreffend	Echtzeit
Erneute Aufbaurate	Echtzeit	Echtzeit	Nicht zutreffend
Hintergrundinitialisierungsrate	Echtzeit	Echtzeit	Nicht zutreffend
Rekonstruktionsrate	Echtzeit	Echtzeit	Nicht zutreffend
Fremdkonfiguration importieren	Echtzeit	Echtzeit	Nicht zutreffend
Fremdkonfiguration automatisch importieren	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Fremdkonfiguration löschen	Echtzeit	Echtzeit	Nicht zutreffend
Controller-Konfiguration zurücksetzen	Echtzeit	Echtzeit	Nicht zutreffend
Sicherheitsschlüssel erstellen oder ändern	Echtzeit	Echtzeit	Echtzeit
Secure Enterprise Key Manager	Echtzeit	Echtzeit	Echtzeit
Bestandsaufnahme und die Remote-Überwachung des Status von PCIe SSD-Geräte	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Entfernen der PCIe SSD vorbereiten	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Daten von PCIe-SSD sicher löschen	Nicht zutreffend	Nicht zutreffend	Echtzeit
Rückwandplatinen-Modus konfigurieren (geteilt/vereint)	Echtzeit	Echtzeit	Nicht zutreffend
Komponenten-LEDs blinken oder Blinken beenden	Echtzeit	Echtzeit	Echtzeit
Controller-Modus ändern	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
T10PI-Unterstützung für virtuelle Laufwerke	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend

Tabelle 44. Unterstützte Funktionen für Speichergeräte

Funktion	BOSS-N1
Virtuelle Laufwerke erstellen	Durchgeführt
Controller-Konfiguration zurücksetzen	Durchgeführt
Schnellinitialisierung	Durchgeführt
Virtuelle Laufwerke löschen	Durchgeführt
Vollinitialisierung	Nicht zutreffend
Bestandsaufnahme und die Remote-Überwachung des Status von PCIe SSD-Geräte	Nicht zutreffend
Entfernen der PCIe SSD vorbereiten	Nicht zutreffend
Daten von PCIe-SSD sicher löschen	Nicht zutreffend

Tabelle 44. Unterstützte Funktionen für Speichergeräte (fortgesetzt)

Funktion	BOSS-N1
Komponenten-LEDs blinken oder Blinken beenden	Echtzeit
Hotplugging von Laufwerken	Echtzeit
SEKM	Durchgeführt
Unterstützte RAID-Level	RAID 0, RAID 1

Bestandsaufnahme für Storage-Geräte erstellen und Storage-Geräte überwachen

Sie können den Zustand remote überwachen und die Bestandsliste für die folgenden Comprehensive Embedded Management (CEM)-aktivierten Storage-Geräte 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

ANMERKUNG:

- Auf einem System mit mehr virtuellen Laufwerken zeigt die Hardware-Bestandsaufnahme möglicherweise leere physische Laufwerksdaten für einige der virtuellen Laufwerke an.
- Für Speicherereignisse werden Warnungen und SNMP-Traps angezeigt. Die Ereignisse werden im Lifecycle-Protokoll aufgezeichnet.
- Wenn Sie versuchen, abgeschlossene Jobs aus der Jobwarteschlange zu löschen, wenn ein Job ausgeführt wird, schlägt der gerade ausgeführte Job möglicherweise fehl. Daher wird empfohlen, zu warten, bis der laufende Job abgeschlossen ist, bevor Sie den Job löschen.
- 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.
- Physische Laufwerke in einem System mit mehreren Rückwandplatinen werden möglicherweise unter einer anderen Rückwandplatine aufgelistet. Verwenden Sie die Blinkfunktion, um die Laufwerke zu identifizieren.
- FQDD bestimmter Rückwandplatinen ist möglicherweise nicht identisch mit der Software- und Hardware-Bestandsaufnahme.
- Das 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.
- Beim Hot-Removal des M.2-Laufwerks für BOSS N1-Controller wird der Integritätsstatus des iDRAC-Dashboards gelb, aber die LED für die Vorder-/Rückseite des Servers bleibt blau.

ANMERKUNG: Der SRV015-Fehler tritt in zwei Fällen auf: wenn das Gerät die TSR-Erfassung nicht unterstützt, wie bei AHCI-Controllern, oder wenn das Gerät die TSR-Erfassung unterstützt, aber noch nicht auf Seitenband inventarisiert wurde.

Netzwerkgeräte über die Weboberfläche überwachen

So zeigen Sie die Storage-Geräteinformationen 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.

ANMERKUNG: Wenn der Server über eine ungerade Anzahl von Steckplätzen verfügt, wird eine leere Steckplatzreihe in der Liste **Zusammenfassung der Steckplätze** auf der Seite **Gehäuse** hinzugefügt.

ANMERKUNG: Aktuelle Informationen zu den unterstützten Eigenschaften und deren Werten finden Sie in der **iDRAC-Onlinehilfe**.

Sie können Filter verwenden, um spezifische Geräteinformationen anzuzeigen.

ANMERKUNG:

- Die Storage-Hardwareliste wird nicht angezeigt, wenn das System nicht über Storage-Geräte 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:

Tabelle 45. Unterstützung für grafische Benutzeroberflächen und andere Schnittstellen

Typ	Web-GUI-Unterstützung	Unterstützung für andere Schnittstellen
SATA	Nicht verfügbar	Bestandsaufnahme und RAID-Konfiguration
NVMe	Nur Bestandsaufnahme der physischen Laufwerke	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 Informationen zum Storage-Gerät anzuzeigen, verwenden Sie den Befehl `storage`.

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Überwachen der Verwendung der Rückwandplatine über das Dienstprogramm für iDRAC-Einstellungen

Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Systemzusammenfassung**. Daraufhin wird die Seite **iDRAC-Einstellungen – Systemzusammenfassung** angezeigt. Im Abschnitt **Rückwandplatinenbestand** werden Informationen zur Rückwandplatine 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 zeigt eine hierarchische Ansicht der physischen Aufbewahrung der wichtigsten Storage-Komponenten, d. h. es werden die Controller, die an den Controller angeschlossenen Gehäuse sowie eine Verbindung zum physischen Laufwerk in jedem Gehäuse aufgelistet. Zudem werden die physischen Laufwerke angezeigt, die direkt mit dem Controller verbunden sind.

Um die Topologie des Storage-Geräts anzuzeigen, gehen Sie zu **Storage** > **Übersicht**. Die Seite **Übersicht** zeigt die hierarchische Darstellung der Storage-Komponenten im System an. Folgende Optionen stehen zur Verfügung:

- Controller
- Physische Laufwerke
- Virtuelle Laufwerke
- Gehäuse

Klicken Sie für die Ansicht der jeweiligen Komponentendetails auf die zugehörigen Links.

Managen 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.
- Physisches Laufwerk neu erstellen
- Neuerstellung des physischen Laufwerks abbrechen
- Kryptografischer Löschvorgang

ANMERKUNG: Wenn eines der SEKM-gesicherten Laufwerke, die direkt an den Server oder hinter einem Controller angeschlossen sind, vom Betriebssystem nicht erkannt wird oder nicht zugänglich ist, wird empfohlen, die Lifecycle-Protokolle zu überprüfen und sicherzustellen, dass alle gesicherten Laufwerke entsperrt sind. Andernfalls ergreifen Sie die empfohlenen Maßnahmen, die in Lifecycle-Protokollen erwähnt werden.

Zuweisen oder Aufheben der Zuweisung von dezidierten Hotspares

Ein dedizierter Hot Spare ist eine nicht verwendete Backup-Festplatte, die einem virtuellen Laufwerk zugewiesen ist. Wenn ein physisches Laufwerk in dem virtuellen Laufwerk versagt, wird der Hot Spare aktiviert, um das fehlerhafte physische Laufwerk ohne Unterbrechung des Systems oder erforderlichen Nutzereingriff 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 ein physisches Laufwerk als dedizierten Hot Spare im Modus „Zu ausstehenden Vorgängen hinzufügen“ zugewiesen haben, wird der ausstehende Vorgang, jedoch kein Job erstellt. Wenn Sie dann versuchen, die Zuweisung dieses Laufwerks als dedizierter Hot Spare aufzuheben, wird der ausstehende Vorgang „Dedizierten Hot Spare zuweisen“ gelöscht.

Wenn Sie die Zuweisung eines physischen Laufwerks als dedizierter Hot Spare im Modus „Zu ausstehenden Vorgängen hinzufügen“ aufgehoben haben, wird der ausstehende Vorgang, jedoch kein Job erstellt. Wenn Sie dann versuchen, den dedizierten Hot Spare zuzuweisen, wird der ausstehende Vorgang „Zuweisung des dedizierten Hot Spare aufheben“ gelöscht.

ANMERKUNG: Während der Protokollexportvorgang ausgeführt wird, werden keine Informationen zu den dedizierten Hot Spares auf der Seite **Virtuelle Laufwerke managen** angezeigt. Laden Sie nach Abschluss des Protokollexportvorgangs die Seite **Virtuelle Laufwerke managen** neu, um die Informationen anzuzeigen.

Zuweisen oder Aufheben der Zuweisung von globalen Hot Spares über die Webschnittstelle

So weisen Sie ein globalen Hot Spares einem physischen Laufwerk zu oder heben die Zuweisung auf:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Storage** > **Übersicht** > **Physisches Laufwerk**.
2. Alle physischen Laufwerke werden angezeigt.
3. 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 Laufwerke aus.
4. 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 Laufwerke aus.
5. Klicken Sie auf **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 Hot Spares über RACADM

Verwenden Sie den Befehl `storage` und legen Sie den Typ als globalen Hot Spare fest.

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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 „Good“ (Gut) für das Betriebssystem freigegeben und in einem direkten Passthrough-Modus verwendet.

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 oder Redfish.
- 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 und Redfish 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.

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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller

Löschen physischer Laufwerke

Mit der Systemlöschfunktion können Sie den Inhalt der physischen Laufwerke löschen. Diese Funktion ist über RACADM oder die LC-UI zugänglich. Physische Laufwerke auf dem Server werden in zwei Kategorien unterteilt.

- Sicheres Löschen von Laufwerken – Enthält Laufwerke, die kryptografisches Löschen ermöglichen, wie ISE-, SED-SAS- und SATA-Laufwerke sowie PCIe-SSDs.

  ANMERKUNG: ISE-Laufwerke folgen dem NIST SP 800-88r1-Standard und sind NIST-löschkonform. Das bedeutet, dass alle **alten Daten** nach der Löschung unwiederbringlich entfernt wurden.

- Laufwerke durch Überschreiben löschen – Umfasst alle Laufwerke, die das kryptografische Löschen nicht unterstützen.

ANMERKUNG: Die Option zum Löschen des Systems gilt nur für Laufwerke innerhalb des Servers. 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 Methode `SystemErase` durchgeführt werden und wird von der LC-Benutzeroberfläche 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-UI oder RACADM gelöscht werden. Weitere Informationen finden Sie in den Abschnitten Löschen von PCIe-SSD-Gerätedaten und Löschen von SED-Gerätedaten über Benutzeroberfläche.

Informationen zur Systemlöschfunktion innerhalb der Lifecycle Controller-Benutzeroberfläche finden Sie unter *Benutzerhandbuch für den Dell Lifecycle Controller* ist verfügbar unter iDRAC-Handbücher..

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.
- Ein kryptografischer Löschvorgang kann auch mithilfe von PSID durchgeführt werden.

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>
```

Durchführen des kryptografischen Löschvorgangs:

```
<SED FQDD> -psid<PSID>
```

Weitere Informationen finden Sie im *Benutzerhandbuch für den Integrated Dell Remote Access Controller (RACADM CLI)*.

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.

Physisches Laufwerk neu erstellen

Mit der Option „Physisches Laufwerk neu erstellen“ können Sie die Inhalte eines fehlerhaften Laufwerks wiederherstellen. Diese Option ist nur aktiviert, wenn die Option zur automatischen Neuerstellung auf „false“ eingestellt ist. Wenn ein redundantes virtuelles Laufwerk vorhanden ist, kann der Wiederherstellungsvorgang den Inhalt eines fehlerhaften physischen Laufwerks wiederherstellen. Eine Neuerstellung kann während des Normalbetriebs stattfinden, wobei jedoch die Systemleistung herabgesetzt wird.

Die Option „Neuerstellung abbrechen“ kann verwendet werden, um eine laufende Neuerstellung abzubrechen. Wenn Sie eine Neuerstellung abbrechen, verbleibt das virtuelle Laufwerk in einem heruntergestuften Zustand. Der Ausfall eines zusätzlichen physischen Laufwerks kann dazu führen, dass das virtuelle Laufwerk ausfällt und zu Datenverlust führen kann. Es wird empfohlen, so schnell wie möglich eine Neuerstellung auf dem fehlerhaften physischen Laufwerk durchzuführen.

Wenn Sie die Neuerstellung eines physischen Laufwerks abbrechen, das als Hot Spare zugewiesen ist, starten Sie die Neuerstellung auf demselben physischen Laufwerk erneut, um die Daten wiederherzustellen. Das Abbrechen der Neuerstellung eines physischen Laufwerks und dann das Zuweisen eines anderen physischen Laufwerks als Hot Spare führt nicht dazu, dass das neu zugewiesene Hot spare die Daten neu erstellt.

Verwalten von virtuellen Festplatten

Sie können die folgenden Vorgänge für die virtuellen Festplatten ausführen:

- Erstellen
- Löschen
- Richtlinien bearbeiten
- Initialisieren
- Konsistenzüberprüfung
- Konsistenzüberprüfung abbrechen
- Virtuelle Laufwerke 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 Laufwerke über die iDRAC-Schnittstelle managen und überwachen. Um virtuelle Geräte zu erstellen, verwenden Sie entweder das Geräte-Setup (F2) oder das PERCCLI-Befehlszeilentool.

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 ein virtuelles Laufwerk erstellen, sollten Sie sich mit den Informationen unter Erwägungen vor der Erstellung von virtuellen Laufwerken vertraut machen.

Sie können ein virtuelles Laufwerk mithilfe der 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 von einer Laufwerksgruppe unterstützte Höchstzahl virtueller Festplatten wurde erstellt. Sie müssen ein virtuelles Laufwerk aus der ausgewählten Gruppe löschen und dann ein neues virtuelles Laufwerk erstellen.

- Auf dem ausgewählten Controller wird 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 Queue“ (Job-Warteschlange) anzeigen und managen.
- Das physische Laufwerk befindet sich im Nicht-RAID-Modus. Es muss unter Verwendung der iDRAC-Schnittstellen, wie z. B. iDRAC-Webschnittstelle, RACADM und Redfish, oder mit <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: 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 und Redfish sollte die Größe des virtuellen Laufwerks nicht angegeben werden.

ANMERKUNG: Das Erstellen virtueller Laufwerke auf bereits gesicherten Laufwerken ist nicht zulässig.

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 die Controller einige Stripes und Bereiche (Methoden zur Kombination des Storage 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 und RAID 0 werden 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.

ANMERKUNG: Einige Aktionen können dazu führen, dass die Startziel-ID nicht auf ffff zurückgesetzt wird, wenn kein VD oder EPD-PT konfiguriert ist.

Erstellen von virtuellen Festplatten über RACADM

Verwenden Sie den Befehl `racadm storage createvd`.

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

ANMERKUNG: Das Aufteilen von Festplatten oder das Konfigurieren von Teil-VDs wird auf den von S140-Controller verwalteten Laufwerken nicht mit RACADM unterstützt.

Erstellen von virtuellen Laufwerken über die Webschnittstelle

So erstellen Sie ein virtuelles Laufwerk:

1. Gehen Sie auf der iDRAC-Webschnittstelle zu **Storage** > **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 das virtuelle Laufwerk erstellen möchten.
   b. Wählen Sie die RAID-Stufe für das virtuelle Laufwerk 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 Laufwerke.
   c. Wählen Sie den **Medientyp**, die **Stripe Size**, 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 Laufwerke aktualisiert wird.
   e. Das Feld für die **Span-Anzahl** wird basierend auf den ausgewählten physischen Laufwerken angezeigt (Schritt 3). Sie können diesen Wert nicht festlegen. Er wird automatisch berechnet, nachdem Sie Laufwerke 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 Laufwerken für die Erstellung von RAID verwendet wird. Es kann geändert werden, wenn mehr Laufwerke verwendet werden.
3. Wählen Sie im Abschnitt **Physische Laufwerke auswählen** die Anzahl der physischen Laufwerke 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 **Virtuelles Laufwerk erstellen**.
   Basierend auf der Option **Betriebsmodus wählen** werden die Einstellungen angewendet.
   ANMERKUNG: Sie können alphanumerische Zeichen, Bindestriche und Unterstriche im Laufwerksnamen verwenden.

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-und 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 beiden letzten Leseanforderungen ein Zugriff auf sequenzielle Sektoren der Festplatte erfolgte. Wenn durch die nachfolgenden Leseanforderungen ein Zugriff auf wahlfreie Sektoren der Festplatte erfolgt, kehrt die Steuerung zur Kein Vorauslesen-Richtlinie zurück. Der Controller prüft weiterhin, ob Leseanforderungen auf sequenzielle Sektoren der Festplatte zugreifen, und leitet das Vorauslesen bei Bedarf ein.
- **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 der virtuellen Festplatte geschrieben werden.
- **Kein Vorauslesen** – Das Auswählen der Richtlinie „Kein Vorauslesen“ gibt an, dass der Controller die Richtlinie „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. Das Durchschreiben im Cache bietet eine bessere Datensicherheit als das Rückschreiben im Cache, da das System annimmt, dass die Daten erst verfügbar sind, nachdem sie auf das Laufwerk 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. Ein Rückschreiben im Cache kann die Systemleistung verbessern, da bei nachfolgenden Leseaufforderungen die Daten schneller aus dem Cache als vom Laufwerk abgerufen werden können. Es kann jedoch im Falle eines Festplattenausfalls zu Datenverlust kommen, da ein Systemausfall das Schreiben der Daten auf die Festplatte verhindert. Bei anderen Anwendungen können ebenfalls Probleme auftreten, wenn Aktionen die Verfügbarkeit der Daten auf der Festplatte voraussetzen.
- **Rückschreiben erzwingen** – Der Schreib-Cache wird unabhängig davon aktiviert, ob der Controller über eine Batterie verfügt. 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 einem bestimmten virtuellen Laufwerk. 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 eines virtuellen Laufwerks löscht alle Informationen, einschließlich Dateisysteme und Volumes auf dem virtuellen Laufwerk, und entfernt das virtuelle Laufwerk aus der Controller-Konfiguration. Wenn virtuelle Laufwerke gelöscht werden, ist es möglich, dass die Zuweisung für alle zugewiesenen globalen Hot Spares rückgängig gemacht wird, wenn das letzte virtuelle Laufwerk, das mit dem Controller verknüpft ist, gelöscht wird. Wenn das letzte virtuelle Laufwerk einer Laufwerksgruppe gelöscht wird, werden alle zugewiesenen dedizierten Hot Spares automatisch globale Hot Spares.

Wenn Sie alle VDs für ein globales Hot Spare löschen, wird das globale Hot Spare 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. Dies erfolgt über das Seitenband und unabhängig vom Betriebssystem. Entsprechend wird eine Warnmeldung angezeigt, bevor Sie das virtuelle Laufwerk löschen.

Wenn eine virtuelle Festplatte gelöscht wird und sofort eine neue virtuelle Festplatte mit den gleichen Eigenschaften wie die gelöschte virtuelle Festplatte neu erstellt wird, erkennt der Controller die Daten, als ob die erste virtuelle Festplatte nie gelöscht worden wäre. Wenn Sie in diesem Fall die alten Daten nach der Neuerstellung einer neuen virtuellen Festplatte nicht behalten möchten, initialisieren Sie das virtuelle Laufwerk erneut.

ANMERKUNG: Vorgänge zum Zurücksetzen der Konfiguration und zum Löschen virtueller Laufwerke können nicht gestapelt werden, das Maximum beträgt 240 Vorgänge zur Erstellung virtueller Laufwerke. Dies führte zum Fehlschlagen des Vorgang. Diese beiden Vorgänge können als separate Jobs im Abstand von mindestens 2 Minuten ausgeführt werden.

Überprüfen der Übereinstimmung der virtuellen Festplatte

Dieser Vorgang überprüft die Richtigkeit der redundanten (Paritäts-)Informationen. Diese Aufgabe bezieht sich nur auf redundante, virtuelle Festplatten. 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 Laufwerke werden alle Daten auf der Festplatte gelöscht, die Konfiguration des virtuellen Laufwerks wird jedoch nicht geändert. Sie müssen ein konfiguriertes virtuelles Laufwerk initialisieren, bevor Sie es verwenden.

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 Initialisierung ist ein Echtzeitvorgang. Sie können die Initialisierung nur über die iDRAC-Weboberfläche und nicht über RACADM abbrechen.

Schnellinitialisierung

Der Vorgang der Schnellinitialisierung initialisiert alle physischen Laufwerke, die im virtuellen Laufwerk enthalten sind. Dabei werden die Metadaten auf den physischen Laufwerken aktualisiert, sodass der gesamte Speicherplatz für künftige Schreibvorgänge verfügbar ist. Die Initialisierungsaufgabe kann schnell abgeschlossen werden, da vorhandene Informationen auf den physischen Laufwerken nicht gelöscht werden. Bei zukünftigen Schreibvorgängen werden jedoch alle Informationen überschreiben, die auf den physischen Laufwerken vorhanden sind.

Bei der Schnellinitialisierung werden nur die Startsektor- und Stripe-Informationen gelöscht. Führen Sie eine Schnellinitialisierung nur dann durch, wenn Zeitdruck vorliegt oder die Festplatten neu sind bzw. noch nicht verwendet wurden. Die Schnellinitialisierung nimmt weniger Zeit in Anspruch (normalerweise 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 Laufwerken, Da die Schnellinitialisierung keinen Schreibvorgang ausführt, verursacht sie eine geringere Herabsetzung der Festplatte.

Eine Schnellinitialisierung auf einer virtuellen Festplatte überschreibt die ersten und letzten 8 MB der virtuellen Festplatte und löscht alle Startdaten oder Partitionsinformationen. Der Vorgang dauert nur 2 bis 3 Sekunden und wird empfohlen, wenn Sie virtuelle Laufwerke neu erstellen.

Eine Hintergrundinitialisierung beginnt fünf Minuten nach Abschluss der Schnellinitialisierung.

Vollständige oder langsame Initialisierung

Der Vorgang der vollständigen Initialisierung (auch langsame Initialisierung genannt) initialisiert alle physischen Laufwerke, die im virtuellen Laufwerk enthalten sind. Dabei werden die Metadaten auf den physischen Laufwerken aktualisiert und alle vorhandenen Daten und Dateisysteme gelöscht. Sie können eine vollständige Initialisierung nach der Erstellung des virtuellen Laufwerks durchführen. Anstelle der Schnellinitialisierung wird empfohlen, eine vollständige Initialisierung durchzuführen, wenn bei einem physischen Laufwerk Probleme aufgetreten sind oder beschädigte Festplattenblöcke vermutet werden. Bei der vollständigen Initialisierung werden beschädigte Blöcke neu zugewiesen und Nullen in alle Festplattenblöcke geschrieben.

Wenn die vollständige Initialisierung eines virtuellen Laufwerks durchgeführt wird, ist keine Hintergrundinitialisierung erforderlich. Bei der vollständigen Initialisierung kann der Host nicht auf das virtuelle Laufwerk zugreifen. Wenn das System während der vollständigen Initialisierung neu gestartet wird, wird der Vorgang abgebrochen und auf dem virtuellen Laufwerk wird eine Hintergrundinitialisierung durchgeführt.

Es wird immer empfohlen, auf Laufwerken, die zuvor Daten enthielten, eine vollständige Initialisierung durchzuführen. Die vollständige Initialisierung kann 1 bis 2 Minuten pro GB dauern. Die Geschwindigkeit der Initialisierung hängt vom Controller-Modell, der Geschwindigkeit der Festplatten und der Firmwareversion ab.

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 die Verschlüsselung auf einem Controller deaktiviert ist (d. h. der Sicherheitsschlüssel wurde gelöscht), aktivieren Sie die Verschlüsselung für virtuelle Laufwerke, die mithilfe von SED-Laufwerken erstellt wurden, manuell. Wenn das virtuelle Laufwerk erstellt wird, nachdem die Verschlüsselung auf einem Controller aktiviert wurde, wird das virtuelle Laufwerk automatisch verschlüsselt. Es wird automatisch als verschlüsseltes virtuelles Laufwerk konfiguriert, es sei denn, die aktivierte Verschlüsselungsoption wird während der Erstellung des virtuellen Laufwerks deaktiviert.

Sie müssen über die Berechtigung zur Anmeldung und zur Server-Steuerung zur Verwaltung der Schlüssel für die Verschlüsselung verfügen.

ANMERKUNG: Obwohl die Verschlüsselung auf den Controllern aktiviert ist, müssen NutzerInnen die Verschlüsselung auf dem virtuellen Laufwerk manuell aktivieren, wenn das virtuelle Laufwerk über den iDRAC erstellt wird.

Zuweisen oder Aufheben der Zuweisung von dezidierten Hotspares

Ein dedizierter Hot Spare ist eine nicht verwendete Backup-Festplatte, die einem virtuellen Laufwerk zugewiesen ist. Wenn ein physisches Laufwerk in dem virtuellen Laufwerk versagt, wird der Hot Spare aktiviert, um das fehlerhafte physische Laufwerk ohne Unterbrechung des Systems oder erforderlichen Nutzereingriff 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 ein physisches Laufwerk als dedizierten Hot Spare im Modus „Zu ausstehenden Vorgängen hinzufügen“ zugewiesen haben, wird der ausstehende Vorgang, jedoch kein Job erstellt. Wenn Sie dann versuchen, die Zuweisung dieses Laufwerks als dedizierter Hot Spare aufzuheben, wird der ausstehende Vorgang „Dedizierten Hot Spare zuweisen“ gelöscht.

Wenn Sie die Zuweisung eines physischen Laufwerks als dedizierter Hot Spare im Modus „Zu ausstehenden Vorgängen hinzufügen“ aufgehoben haben, wird der ausstehende Vorgang, jedoch kein Job erstellt. Wenn Sie dann versuchen, den dedizierten Hot Spare zuzuweisen, wird der ausstehende Vorgang „Zuweisung des dedizierten Hot Spare aufheben“ gelöscht.

ANMERKUNG: Während der Protokollexportvorgang ausgeführt wird, werden keine Informationen zu den dedizierten Hot Spares auf der Seite **Virtuelle Laufwerke managen** angezeigt. Laden Sie nach Abschluss des Protokollexportvorgangs die Seite **Virtuelle Laufwerke managen** neu, um die Informationen anzuzeigen.

VD umbenennen

Um den Namen eines virtuellen Laufwerks zu ändern, muss die/der NutzerIn über Systemsteuerungsberechtigungen verfügen. Der Name des virtuellen Laufwerks darf nur alphanumerische Zeichen, Bindestriche und Unterstriche enthalten. Die maximale Länge des Namens hängt vom jeweiligen Controller ab. In den meisten Fällen beträgt die maximale Länge 15 Zeichen. Jedes Mal, wenn ein virtuelles Laufwerk umbenannt wird, wird ein LC-Protokoll erstellt.

Bearbeiten der Festplattenkapazität

Mit der Online-Kapazitätserweiterung (OCE) können Sie die Storage-Kapazität ausgewählter RAID-Level erhöhen, während das System online bleibt. Der Controller verteilt die Daten auf dem Array neu (als Neukonfiguration bezeichnet) und stellt dadurch neuen Speicherplatz am Ende jedes RAID-Arrays zur Verfügung.

Die Online-Kapazitätserweiterung (OCE) kann auf zwei Arten erfolgen:

- Wenn freier Speicherplatz auf dem kleinsten physischen Laufwerk in der virtuellen Festplattengruppe nach dem Start der Adressierung logischer Blöcke von virtuellen Laufwerken zur Verfügung steht, kann die Kapazität des virtuellen Laufwerks innerhalb des freien Speicherplatzes erweitert werden. Diese Option ermöglicht Ihnen die Eingabe einer neuen größeren virtuellen Festplattengröße. Wenn eine Festplattengruppe in einer virtuellen Festplatte nur über Speicherplatz vor dem Start der Adressierung logischer Blöcke verfügt, dann ist Festplattenkapazität bearbeiten in derselben Festplattengruppe nicht zulässig, auch wenn es verfügbaren Speicherplatz auf einem physischen Laufwerk gibt.
- Die Kapazität eines virtuellen Laufwerks kann ebenfalls erweitert werden, wenn zusätzliche kompatible physische Laufwerke zu der bestehenden virtuellen Festplattengruppe hinzugefügt werden. Diese Option erlaubt es Ihnen nicht, die neue größere Größe der virtuellen Festplatte einzugeben. Die neue erhöhte Größe der virtuellen Festplatte wird berechnet und dem Nutzer basierend auf dem genutzten Speicherplatz der vorhandenen physischen Festplattengruppe auf einem bestimmten virtuellen Laufwerk, bereits vorhandener RAID-Level der virtuellen Festplatte und der Anzahl neuer Laufwerke, die zur virtuellen Festplatte hinzugefügt wurden, angezeigt.

Mit der Kapazitätserweiterung können NutzerInnen die endgültige Größe des virtuellen Laufwerks festlegen. Die endgültige interne Größe des virtuellen Laufwerks wird in Prozent an den PERC übermittelt (dieser Prozentsatz ist der Speicherplatz, den NutzerInnen vom leeren Speicherplatz im Array für die Erweiterung der lokalen Festplatte verwenden möchten). Aufgrund dieser Prozentlogik kann sich die endgültige Größe des virtuellen Laufwerks nach Abschluss der Neukonfiguration von der vom Nutzer eingegebenen Größe unterscheiden, wenn NutzerInnen nicht die maximal mögliche Größe des virtuellen Laufwerks als endgültige Größe des virtuellen Laufwerks eingegeben haben (der Prozentsatz ergibt weniger als 100 %). NutzerInnen sehen nach der Neukonfiguration keinen Unterschied zwischen der eingegebenen Größe des virtuellen Laufwerks und der endgültigen Größe des virtuellen Laufwerks, wenn sie die maximal mögliche Größe des virtuellen Laufwerks eingegeben haben.

RAID-Level-Migration

Das Ändern des RAID-Levels eines virtuellen Laufwerks wird als RAID-Level-Migration (RLM) bezeichnet. iDRAC bietet eine Option, um das virtuelle Laufwerk mithilfe von RLM zu vergrößern. RLM erlaubt gewissermaßen die Migration des RAID-Levels eines virtuellen Laufwerks, was wiederum die Größe virtueller Laufwerke 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 46. Mögliche Layouts 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
R5	R0/R6	R0
R6	R0/R5	R0/R5

Zulässige Operationen während OCE oder RLM

Die folgenden Vorgänge sind während OCE/RLM zulässig:

Tabelle 47. 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	k. A.	In eine Nicht-RAID-Festplatte konvertieren	Rename
Controller-Eigenschaften ändern	k. A.	k. A.	Policy ändern
Strom der physischen Festplatte managen	k. A.	k. A.	Langsam initialisieren
In RAID-fähige Festplatten konvertieren	k. A.	k. A.	Schnell initialisieren
In Nicht-RAID-Festplatten konvertieren	k. A.	k. A.	Mitgliedfestplatte ersetzen
Controller-Modus ändern	k. A.	k. A.	k. A.

Initialisierung abbrechen

Diese Option bietet die Möglichkeit, die Hintergrundinitialisierung auf einem virtuellen Laufwerk abzubrechen. Auf PERC-Controllern beginnt die Hintergrundinitialisierung redundanter virtueller Laufwerke automatisch nach der Erstellung eines virtuellen Laufwerks. Die Hintergrundinitialisierung redundanter virtueller Laufwerke bereitet das virtuelle Laufwerk für Paritätsinformationen vor und verbessert die Schreibleistung. Andere Prozesse, wie das Erstellen eines virtuellen Laufwerks, können jedoch nicht ausgeführt werden, während

die Hintergrundinitialisierung läuft. Die Option „Initialisierung abbrechen“ bietet die Möglichkeit, die Hintergrundinitialisierung manuell abzubrechen. Im Falle eines Abbruchs startet die Hintergrundinitialisierung automatisch innerhalb von 0 bis 5 Minuten erneut.

ANMERKUNG: Die Hintergrundinitialisierung kann nicht auf virtuellen RAID-0-Laufwerken ausgeführt werden.

OCE- und RLM-Einschränkungen

Im Folgenden sind die allgemeinen Einschränkungen in Bezug auf OCE und RLM aufgeführt:

- OCE/RLM ist auf Szenarien beschränkt, bei denen die Laufwerksgruppe nur ein virtuelles Laufwerk enthält.
- OCE wird für RAID50 und RAID60 nicht unterstützt. RLM wird für RAID10, RAID50 und RAID60 nicht 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 Schreibcache-Richtlinie aller virtuellen Laufwerke auf denen RLM/OCE ausgeführt wird, auf „Durchschreiben“ bis der Vorgang abgeschlossen ist.
- Die Neukonfiguration virtueller Laufwerke verursacht bis zum Abschluss des Vorgangs üblicherweise einen gewissen Leistungsverlust.
- Eine Festplattengruppe darf nicht mehr als 32 physikalische Festplatten enthalten.
- Wenn bereits ein Hintergrundvorgang (z. B. Hintergrundinitialisierung/Neuaufbau/Rückkopieren/Patrol Read) auf dem entsprechenden virtuellen/physischen Laufwerk ausgeführt wird, ist eine Neukonfiguration (OCE/RLM) zu diesem Zeitpunkt nicht zulässig.
- Jede Art von Festplattenmigration während der Neukonfiguration (OCE/RLM) von Laufwerken, die einem virtuellen Laufwerk zugeordnet sind, führt dazu, dass die Neukonfiguration fehlschlägt.
- Jedes neue Laufwerk, das für OCE/RLM hinzugefügt wird, wird nach Abschluss der Rekonstruktion Teil des virtuellen Laufwerks. Der Status für diese neuen Laufwerke wird jedoch direkt nach dem Start der Rekonstruktion auf „Online“ geändert.

Managen von virtuellen Festplatten über RACADM

Verwenden Sie die folgenden RACADM-Befehle, um virtuelle Festplatten zu managen:

- 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 Hot Spares zu oder machen die Zuweisung rückgängig:

  ```
  racadm storage hotspare:<Physical Disk FQDD> -assign <option> -type dhs -vdkey: <FQDD of
  VD>
  ```

  <option>=yes

  Hot Spare zuweisen

  <Option>=no

  Zuweisung von Hotspare aufheben

Managen von virtuellen Laufwerken über die Webschnittstelle

1. Gehen Sie auf der iDRAC-Webschnittstelle zu **Storage** > **Übersicht** > **Virtuelle Laufwerke**.

2. Wählen Sie aus dem Drop-Down-Menü **Virtuelles Laufwerk** den Controller aus, für den Sie die virtuellen Laufwerke managen 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.
   - **Rename**
   - **Delete**
   - **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-Storage 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 Schreibcache-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-Storage abgelegt werden, wird Schreibcache 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 Schreibcache verwendet. Für SATA-Laufwerke lautete dieser „aktiviert“ und für SAS-Laufwerke „deaktiviert“.
       - **Aktiviert** – Zeigt an, dass der Schreibcache der Festplatte aktiviert ist. Dies erhöht die Leistung und die Wahrscheinlichkeit eines Datenverlusts bei einem Stromausfall.
       - **Deaktiviert** – Zeigt an, dass der Schreibcache 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 Nutzer 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.

   - **Konsistenzüberprüfung** - Zum Überprüfen der Übereinstimmung eines virtuellen Laufwerks wählen Sie **Konsistenzüberprüfung** 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 **iDRAC 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.

RAID-Konfigurationsfunktionen

Die folgende Tabelle zeigt einige der RAID-Konfigurationsfunktionen, die in RACADM verfügbar sind:

VORSICHT: Wenn ein physisches Laufwerk dazu gezwungen wird, online oder offline zu gehen, kann dies zu Datenverlusten führen.

Tabelle 48. 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, 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>`	Diese Funktion wird verwendet, um gesperrte Laufwerke zu authentifizieren, die eine andere Quellcontrollerverschlüsselung aufweisen als das Ziel. Sobald die

Tabelle 48. RAID-Konfigurationsfunktionen (fortgesetzt)

Funktion	RACADM-Befehl	Beschreibung
	`-key <Key id> -passwd <passphrase>`	Konfiguration entsperrt ist, kann das Laufwerk erfolgreich von einem Controller zu einem anderen migriert werden.

Managen 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
- Verwerfen des beibehaltenen Cache

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
- Konsistenzüberprüfungsmodus
- Copyback-Modus
- Lastausgleichsmodus
- Konsistenzüberprüfungsrate
- Erneute Aufbaurate
- Hintergrundinitialisierungsrate
- 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 Konsistenzüberprüfung

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.

Hintergrundinitialisierungsrate

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 eines virtuellen RAID 5-Laufwerks abgeschlossen wurde, wurden beispielsweise die Paritätsinformationen initialisiert. Nachdem die Hintergrundinitialisierung eines virtuellen RAID 1-Laufwerks 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 Konsistenzüberprüfung. 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.

Konsistenzüberprüfung

Anhand der Aufgabe Check Consistency (Übereinstimmungsüberprüfung) wird die Richtigkeit der redundanten (Paritäts-)Informationen geprüft. Diese Aufgabe bezieht sich nur auf redundante, virtuelle Festplatten. Bei Bedarf können über die Aufgabe Check Consistency (Übereinstimmungsüberprüfung) redundante Daten neu erstellt werden. Falls das virtuelle Laufwerk den Zustand „Fehlerhafte Redundanz“ aufweist, kann dieser Zustand möglicherweise durch das Durchführen einer Konsistenzüberprüfung in den Zustand „Bereit“ geändert werden.

Die Konsistenzüberprüfungsrate, konfigurierbar zwischen 0 und 100 %, ist der Prozentsatz der Systemressourcen für die Konsistenzüberprüfung. Bei 0 % hat die Konsistenzüberprüfung die niedrigste Priorität für den Controller, dauert am längsten und hat die geringste Auswirkung auf die Systemleistung. Eine Konsistenzüberprüfungsrate von 0 % bedeutet nicht, dass die Konsistenzüberprüfung angehalten oder unterbrochen wird. Bei 100 % hat die Konsistenzüberprüfung die höchste Priorität für den Controller. Die Konsistenzüberprüfungszeit wird minimiert und diese Einstellung hat die größte Auswirkung auf die Systemleistung.

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 Laufwerke auf dem Controller verfügbar sind. Sie können jedoch die Vorgänge erfolgreich mit der iDRAC-Schnittstelle aufrufen. Die Vorgänge schlagen fehl, wenn der verknüpfte Job gestartet wird.

ANMERKUNG: Die Storage-Attribute PatrolReadMode und PersistHotspare, die HBA12- und PERC12-Controllern zugewiesen sind, sind unveränderlich. Wenn Sie versuchen, diese Attribute zu ändern, können Fehler auftreten. Obwohl der Job erstellt und ausgeführt wird, bleiben die ursprünglichen Werte unverändert.

- 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 Lastenausgleichsmodus 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 eines fehlerhaften Laufwerks abgestellt wurden, verwenden Sie das Objekt **Storage.Controller.RebuildRate**.
- Um den Prozentsatz der Controller-Ressourcen festzulegen, der für die Hintergrundinitialisierung (BGI) eines virtuellen Laufwerks nach deren Erstellung bereitgestellt werden soll, verwenden Sie das Objekt **Storage.Controller.BackgroundInitializationRate**.
- Um den Prozentsatz der Controller-Ressourcen festzulegen, der für die Neuerstellung einer Laufwerksgruppe nach dem Hinzufügen eines physischen Laufwerks oder der Änderungen der RAID-Ebene eines virtuellen Laufwerks in einer Laufwerksgruppe 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>
```

Konfigurieren der Controller-Eigenschaften über die Webschnittstelle

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Speicher** > **Übersicht** > **Controller**.
   Daraufhin wird die Seite **Controller-Setup** angezeigt.
2. Wählen Sie im Abschnitt **Controller** den Controller aus, der konfiguriert werden soll.
3. Geben Sie die erforderlichen Informationen für die verschiedenen Eigenschaften an.

   Die Spalte **Aktueller Wert** zeigt die bestehenden Werte für jede Eigenschaft. Sie können diese Werte ändern, indem Sie für die einzelnen Eigenschaften die entsprechende Option aus dem Drop-Down-Menü **Maßnahme** wählen.

   Weitere Informationen zu den Feldern finden Sie in der **iDRAC Online-Hilfe**.
4. Wählen Sie unter **Betriebsmodus anwenden** aus, wann Sie die Einstellungen anwenden möchten.
5. Klicken Sie auf **Anwenden**.

   Basierend auf dem ausgewählten Betriebsmodus werden die Einstellungen angewendet.

SPDM (Security Protocol and Data Model)

Das SPDM-Protokoll wird verwendet, um die Sicherheitsfunktionen und die Echtheit zwischen Hardwarekomponenten festzulegen. SPDM ermöglicht den Nachrichtenaustausch zwischen iDRAC und Endgeräten wie Storage-Controllern, (PERC12), FC und CPU. Dies umfasst Hardwareidentitätszertifikate. Sie können SPDM mithilfe von Redfish oder RACADM aktivieren.

Tabelle 49. SPDM-Funktionslizenzierung

Funktion	Lizenz
Bestand: Erkennen von SPDM-fähigen Geräten	Unlizenziert
Erfassen der Hardwareidentität von Geräten	Enterprise
Erfassung von Messwerten von Geräten	Enterprise
Einrichten der Vertrauensstellung auf dem Gerätezertifikat mit SCV	SCV-Lizenz

Tabelle 49. SPDM-Funktionslizenzierung (fortgesetzt)

Funktion	Lizenz
Verschlüsselter Kommunikationskanal	SEKM-Lizenz

Wenn ein Gerät SPDM-fähig ist, enthalten die erfassten SCV-Daten zusätzlich zu den vorhandenen Feldern SPDM-Hardwareidentitätszertifikate. Firmware-Identitätszertifikate sind nicht im SCV-Zertifikat enthalten.

ANMERKUNG: Möglicherweise stellen Sie fest, dass die NIC-Portnummer im heruntergeladenen SPDM-HW-Zertifikatsdateinamen fehlt.

ANMERKUNG: Ein Jobfehler kann beim Exportieren des SPDM-Zertifikats in der Jobwarteschlange auftreten, wenn Sie häufige Neustarts durchführen.

SPDM über RACADM aktivieren

Mit der SPDM-Funktion in iDRAC können Sie den Sicherheitsstatus verschiedener Komponenten managen und überwachen.

1. Führen Sie zum Aktivieren von SPDM den folgenden Befehl aus:
   ```
   racadm set idrac.SPDM.enable enabled
   ```
2. Führen Sie die folgenden Befehle aus, um sicherzustellen, dass die Änderungen übernommen werden:
   ```
   racadm racreset
   racadm get idrac.SPDM
   ```

SPDM über Redfish aktivieren

Mit der SPDM-Funktion in iDRAC können Sie den Sicherheitsstatus verschiedener Komponenten managen und überwachen.

1. Führen Sie eine PATCH-Anforderung für die folgenden URI durch, indem Sie die Payload `{"Attributes":{"SPDM.1.Enable":"Enabled"}}` verwenden:
   ```
   /redfish/v1/Managers/iDRAC.Embedded.1/Oem/Dell/DellAttributes/iDRAC.Embedded.1
   ```
2. Führen Sie `racreset` aus, um sicherzustellen, dass die Änderungen übernommen werden.

Importieren oder automatisches Importieren von Fremdkonfigurationen

Eine Fremdkonfiguration sind Daten, die sich auf physischen Laufwerken befinden, die von einem Controller zu einem anderen verschoben wurden. Virtuelle Laufwerke, die sich auf umgesetzten physischen Laufwerken befinden, werden als Fremdkonfiguration betrachtet.

Sie können Fremdkonfigurationen importieren, damit virtuelle Laufwerke nach dem Umsetzen der physischen Laufwerke nicht verloren gehen. Eine Fremdkonfiguration kann nur importiert werden, wenn sie ein virtuelles Laufwerk im Status „Bereit“ oder „Herabgesetzt“ enthält, oder einen Hot Spare, der für ein virtuelles Laufwerk dediziert ist und importiert werden kann oder bereits vorhanden ist.

Alle Daten des virtuellen Laufwerks müssen vorhanden sein. Wenn das virtuelle Laufwerk jedoch ein redundantes RAID-Level verwendet, sind die zusätzlichen redundanten Daten nicht erforderlich.

Wenn zum Beispiel die Fremdkonfiguration nur eine Seite einer Spiegelung auf einem virtuellen RAID 1-Laufwerk enthält, weist das virtuelle Laufwerk den Status „Heruntergestuft“ auf und kann importiert werden. Wenn die Fremdkonfiguration nur ein physisches Laufwerk enthält, das ursprünglich als RAID 5 mit drei physischen Laufwerken konfiguriert wurde, gilt für das virtuelle RAID 5-Laufwerk der Status „Fehlgeschlagen“ und es kann nicht importiert werden.

Eine Fremdkonfiguration kann neben virtuellen Laufwerken auch ein physisches Laufwerk enthalten, das auf einem Controller als Hot Spare zugewiesen war und dann auf einen anderen Controller umgesetzt wurde. Die Aufgabe „Fremdkonfiguration importieren“ importiert das neue physische Laufwerk als Hot Spare. Wenn das physische Laufwerk auf dem vorhergehenden Controller ein dedizierter Hot Spare war, aber das virtuelle Laufwerk, zu dem der Hot Spare zugewiesen war, nicht mehr in der Fremdkonfiguration enthalten ist, wird das physische Laufwerk als globaler Hot Spare importiert.

Die Aufgabe „Fremdkonfiguration importieren“ wird nur angezeigt, wenn der Controller eine Fremdkonfiguration erkannt hat. Durch Überprüfung des Zustands des physischen Laufwerks können Sie auch feststellen, ob ein physisches Laufwerk eine Fremdkonfiguration (virtuelles Laufwerk oder Hot Spare) enthält. Wenn der Zustand des physischen Laufwerks Fremd ist, dann enthält das physische Laufwerk sämtliche oder einige Teile eines virtuellen Laufwerks oder verfügt über eine Hot Spare-Zuweisung.

ANMERKUNG: Wenn eine Konfiguration im Rahmen des Fremdkonfigurationsimports unvollständig ist, wird sie nicht importiert. Der Job schlägt jedoch nicht fehl. Der Jobstatus wird als **Erfolgreich abgeschlossen** angezeigt. Sie müssen den PD-Status überprüfen, um zu wissen, ob das virtuelle Laufwerk importiert wurde oder nicht.

ANMERKUNG: Beim Importieren der Fremdkonfiguration werden alle virtuellen Laufwerke importiert, die sich auf physischen Laufwerken befinden, die dem Controller hinzugefügt wurden. Wenn mehr als ein fremdes virtuelles Laufwerk vorhanden ist, werden alle Fremdkonfigurationen importiert.

Der PERC9-Controller bietet Unterstützung für den automatischen Import von Fremdkonfigurationen, ohne dass Nutzerinteraktionen erforderlich sind. Der automatische Import kann aktiviert oder deaktiviert werden. Wenn diese Option aktiviert ist, kann der PERC-Controller alle erkannten Fremdkonfigurationen automatisch ohne manuelle Intervention importieren. Wenn diese Option deaktiviert ist, importiert PERC keine Fremdkonfiguration automatisch.

Sie müssen über die Berechtigung zur Anmeldung und Serversteuerung für den Import von Fremdkonfigurationen verfügen.

Diese Aufgabe 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 des Kabels könnte zu einer Fremdkonfiguration führen, wenn die Verbindung wiederhergestellt wird.

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 Laufwerksstatus eines physischen Laufwerks kann sich von dem Zeitpunkt, zu dem die Fremdkonfiguration gescannt wird, bis zum Zeitpunkt des tatsächlichen Imports ändern. Der Fremdimport erfolgt nur auf Laufwerken, die sich im Status „Nicht konfiguriert funktionsfähig“ befinden.
- Festplatten, die fehlerhaft oder offline sind, können nicht importiert werden.
- Die Firmware lässt das Importieren oder Löschen von Fremdkonfigurationen nicht zu, wenn mehr als acht fremde Laufwerke vorhanden sind.

Importieren von Fremdkonfigurationen über RACADM

So importieren Sie die Fremdkonfiguration:

```
racadm storage importconfig:<Controller FQDD>
```

Weitere Informationen finden Sie im **RACADM-Befehlszeilen-Referenzhandbuch für iDRAC** unter **dell.com/idracmanuals**.

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. Gehen Sie auf der iDRAC-Weboberfläche zu **Storage** > **Übersicht** > **Controller**.
2. Wählen Sie in den **Controller**-Optionen den Controller aus, in den Sie die Fremdkonfiguration importieren möchten.
3. Klicken Sie unter **Fremdkonfiguration** auf **Import** und anschließend auf **Übernehmen**.

Fremdkonfiguration löschen

Nach dem Umsetzen eines physischen Laufwerks von einem Controller zu einem anderen ist es möglich, dass das physische Laufwerk ein gesamtes virtuelles Laufwerk oder einen Teil eines virtuellen Laufwerks enthält (Fremdkonfiguration). Durch Überprüfung des Zustands des physischen Laufwerks können Sie feststellen, ob ein vorher verwendetes physisches Laufwerk eine Fremdkonfiguration (virtuelles Laufwerk) enthält. Wenn der Zustand des physischen Laufwerks Fremd ist, dann enthält das physische Laufwerk sämtliche oder einige Teile eines virtuellen Laufwerks. Sie können die Informationen des virtuellen Laufwerks von den neu angeschlossenen physischen Laufwerken löschen bzw. entfernen.

Mit dem Vorgang „Fremdkonfiguration löschen“ werden alle Daten auf den physischen Laufwerken, die dem Controller hinzugefügt wurden, unwiderruflich gelöscht. Wenn mehr als ein fremdes virtuelle Laufwerk vorhanden ist, werden alle Konfigurationen gelöscht. Es ist daher möglicherweise besser, das virtuelle Laufwerk zu importieren als die Daten zu zerstören. Zum Entfernen der Fremddaten muss eine Initialisierung durchgeführt 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 Laufwerken zu löschen.

Löschen von Fremdkonfigurationen über die Webschnittstelle

So löschen Sie eine Fremdkonfiguration:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Speicher** > **Übersicht** > **Controller**.
   Die Seite **Controller-Konfiguration** wird angezeigt.
2. Wählen Sie aus den Optionen **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 **Apply** (Übernehmen).
   Basierend auf dem ausgewählten Betriebsmodus werden die virtuellen Laufwerke, die sich auf dem physischen Laufwerk befinden, gelöscht.

Löschen von Fremdkonfigurationen über RACADM

So löschen Sie eine Fremdkonfiguration:

```
racadm storage clearconfig:<Controller FQDD>
```

Weitere Informationen finden Sie im **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 Laufwerke und hebt die Zuweisung aller Hotspares auf dem Controller auf. Es werden keine anderen Daten gelöscht als das Entfernen der Festplatten aus der Konfiguration. Das Zurücksetzen der Konfiguration entfernt keine Fremdkonfigurationen. Zurücksetzen der Konfiguration löscht keine Daten. Sie können die exakt gleiche Konfiguration neu erstellen, ohne einen Initialisierungsvorgang, der dazu führen kann, dass die Daten wiederhergestellt werden. Sie müssen Serversteuerungsberechtigungen haben.

ANMERKUNG: Durch das Zurücksetzen der Controller-Konfiguration wird keine Fremdkonfiguration entfernt. Um eine Fremdkonfiguration zu entfernen, führen Sie den Vorgang zum Löschen der Konfiguration durch.

Zurücksetzen der Controller-Konfiguration über die Webschnittstelle

Um einen Konfigurations-Reset durchzuführen:

1. Gehen Sie auf der iDRAC-Weboberfläche zu **Storage** > **Übersicht** > **Controller**.
2. Wählen Sie unter **Aktionen** die Option **Konfiguration zurücksetzen** 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 **RACADM-Befehlszeilen-Referenzhandbuch für iDRAC** unter **dell.com/idracmanuals**.

Wechseln des Controller-Modus

Sie können 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.

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 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.

Ausnahmen beim Wechseln des Controller-Modus

Die folgende Liste enthält die Ausnahmen beim Festlegen des Controller-Modus über die iDRAC-Schnittstellen, wie z. B. die Weboberfläche und RACADM:

- 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 dann versuchen, das BGI-Attribut zu setzen, wird der ausstehende Wert nicht initialisiert.
- Wenn Sie den PERC-Controller vom RAID- auf den HBA-Modus umschalten, bleiben die Festplatten im Nicht-RAID-Zustand und werden nicht automatisch in den Status „Ready“ (Bereit) gesetzt. Darüber hinaus wird das **RAIDEnhancedAutoImportForeignConfig**-Attribut automatisch auf **Aktiviert** gesetzt.

Die folgende Liste enthält die Ausnahmen beim Festlegen des Controller-Modus über die Serverkonfigurationsprofil-Funktion bei Verwendung der RACADM-Schnittstelle:

- Die Serverkonfigurationsprofil-Funktion ermöglicht Ihnen neben der Einstellung des Controller-Modus die Konfiguration mehrerer RAID-Vorgänge. Befindet sich der PERC-Controller beispielsweise im HBA-Modus können Sie die Export-Serverkonfigurationsprofil-Datei bearbeiten, um den Controller-Modus auf RAID zu ändern, Laufwerke in den „Bereit“-Status zu versetzen und virtuelle Laufwerke zu erstellen.
- Beim Ändern des Modus von RAID auf HBA wird das **RAIDaction Pseudo**-Attribut auf „update“ gesetzt ist (das 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 das RAIDaction-Attribut in der SCP-Datei auskommentieren.

- Wenn sich der PERC-Controller im HBA-Modus befindet und Sie auf die Export-Serverkonfigurationsprofil-Datei, in der Sie den Controller-Modus auf RAID geändert haben, die Import-Vorschau anwenden und versuchen ein virtuelles Laufwerk zu erstellen, schlägt die Erstellung des virtuellen Laufwerks fehl. Die Import-Vorschau 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-CLI-Referenzhandbuch** auf **dell.com/idracmanuals**.

HBA-Adaptervorgänge

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.

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 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 Hot-Plug
- Blinken der LEDs oder Beenden des Blinkens

ANMERKUNG:

- 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.

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 vorausschauende Fehleranalyse auf jedem Laufwerk durch und sendet Warnmeldungen, wenn ein Festplattenausfall prognostiziert wird. Die Controller prüfen die physischen Laufwerke auf Fehlerprognosen und leiten diese Informationen, sofern gefunden, an iDRAC weiter. iDRAC protokolliert sofort eine Warnmeldung.

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
  - Konsistenzüberprüfungsmodus
  - Patrol Read-Modus
  - Copyback-Modus
  - Controller-Startmodus
  - Erweiterter automatischer Fremdkonfigurationsimport
  - Erneute Aufbaurate
  - Konsistenzüberprüfungsrate
  - Rekonstruktionsrate
  - Hintergrundinitialisierungsrate
  - 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 Storage-Controllern

Während der Ausführung von Vorgängen auf mehr als zwei Storage-Controllern über eine beliebige unterstützte iDRAC-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.

Beibehaltenen Cache managen

Die Funktion „Beibehaltenen Cache managen“ ist eine Controller-Option, die NutzerInnen die Möglichkeit gibt, Controller-Cache-Daten zu verwerfen. In der Rückschreib-Policy werden Daten in den Cache geschrieben, bevor sie auf das physische Laufwerk geschrieben werden. Wenn das virtuelle Laufwerk offline geht oder aus irgendeinem Grund gelöscht wird, gehen die Daten im Cache verloren.

Der PERC-Controller behält die in den beibehaltenen oder fehlerhaften Cache geschriebenen Daten bei einem Stromausfall oder einer Kabeltrennung bei, bis Sie das virtuelle Laufwerk wiederherstellen oder den Cache löschen.

Der Status des Controllers wird durch den beibehaltenen Cache beeinflusst. Der Controllerstatus wird als „Herabgesetzt“ angezeigt, wenn der Controller einen beibehaltenen Cache hat. Das Verwerfen des beibehaltenen Caches ist nur möglich, wenn alle der folgenden Bedingungen erfüllt sind:

- Der Controller hat keine Fremdkonfiguration.
- Der Controller hat keine offline genommenen oder fehlenden virtuellen Laufwerke.
- Kabelverbindungen zu einem virtuellen Laufwerk sind nicht unterbrochen.

Managen von PCIe-SSDs

Peripheral Component Interconnect Express (PCIe) Solid State Device (SSD) ist ein Hochleistungs-Speichergerät, das für Lösungen konzipiert wurde, die eine niedrige Latenzzeit, hohe Eingabe-/Ausgabevorgänge pro Sekunde (IOPS) und Speicherzuverlässigkeit und Dienstbarkeit der Unternehmensklasse erfordern. Die PCIe-SSD basiert auf der Single-Level Cell (SLC) und Multi-Level Cell (MLC) NAND-Flash-Technologie mit einer PCIe-2.0-, PCIe-3.0- oder PCIe-4.0-konformen Hochgeschwindigkeitsschnittstelle.

Über die iDRAC-Schnittstellen können Sie NVMe-PCIe-SSDs anzeigen und konfigurieren.

Es folgen die Hauptfunktionen des PCIe SSD:

- Hot-Plug-Fähigkeit
- Hochleistungsgerät

Sie können die folgenden Vorgänge für PCIe-SSDs ausführen:

- Bestandsaufnahme und die Remote-Überwachung des Status von PCIe-SSDs im Server
- Auf das Entfernen von PCIe SSD vorbereiten
- Daten sicher löschen
- Blinken oder Beenden des Blinkens der Geräte-LED (Identifizieren des Geräts)

Sie können die folgenden Vorgänge für HHHL SSDs ausführen:

- Bestandsaufnahme und Echtzeitüberwachung des HHHL SSD auf dem Server
- Fehlgeschlagener Kartenbericht und fehlgeschlagene Anmeldung bei iDRAC und OMSS
- Sicheres Löschen der Daten und Entfernen der Karte
- TTY Protokollberichte

Sie können die folgenden Vorgänge für SSDs ausführen:

- Laufwerkstatusbericht, wie z. B. Online, Fehlgeschlagen und Offline

ANMERKUNG: Funktionen wie Hotplug, das Vorbereiten auf das Entfernen und das Aufleuchten oder Erlöschen der Geräte-LED gelten nicht für HHHL PCIe SSD-Geräte.

ANMERKUNG: Wenn NVMe-Geräte hinter SW-RAID gesteuert werden, werden die Vorgänge „Zum Entfernen vorbereiten“ und „Kryptografisches Löschen“ nicht unterstützt. Blinken und Beenden des Blinkens werden unterstützt.

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

ANMERKUNG: 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

Um PCIe-SSD-Geräte zu inventarisieren und zu überwachen, gehen Sie auf der iDRAC-Weboberfläche zu **Storage** > **Übersicht** > **Physische Laufwerke**. Die Seite **Eigenschaften** wird angezeigt. Für PCIe-SSDs wird in der Spalte **Name PCIe-SSD** angezeigt. Erweitern Sie den Eintrag, um die Eigenschaften anzuzeigen.

Bestandsaufnahme und Überwachung von PCIe-SSDs mithilfe von RACADM

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 **Befehlszeilen-Referenzhandbuch für iDRAC RACADM CLI** 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.

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 auf der iDRAC-Weboberfläche zu **Storage** > **Übersicht** > **Physische Laufwerke**.
   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 das iSM installiert ist und ausgeführt wird, und führen Sie den Vorgang `preparetoremove` aus.

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** verfügbar. Dieser Vorgang wird im Modus „Bereitgestellt“ nicht unterstützt.

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.

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 Zieljob 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 *Referenzhandbuch für RACADM CLI*.

Löschen von PCIe-SSD-Gerätedaten

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 **Storage** > **Übersicht** > **Physische Festplatten**.
   Daraufhin wird die Seite **Physische Festplatten** 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:
   - **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 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 erhalten Sie im *Befehlszeilen-Referenzhandbuch für iDRAC RACADM*.

Managen 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
- Ressourcenname

Konfigurieren des Rückwandplatinen-Modus

PowerEdge-Server unterstützen eine neue interne Speichertopologie, bei der zwei Storage-Controller (PERCs) über einen einzigen Expander mit internen Laufwerken 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 Storage-Controllern auf. In diesem Modus zeigt die Erstellung der virtuellen Laufwerke 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.
- 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.

ANMERKUNG: Wenn zwei oder mehr Rückwandplatinen mit einem einzigen PERC-Controller verbunden sind, kombiniert der Controller sie und zeigt sie als einzelnes Gehäuse an. Daher wird erwartet, dass eine einzelne Rückwandplatine auf der Seite „Hardwarebestand“ oder „Storage“ angezeigt wird. Die Firmware-Bestandsaufnahme zeigt die tatsächliche Anzahl der im System vorhandenen Rückwandplatinen an.

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.
- Wenn die Rückwandplatine mit dem Wert **0** für das Attribut **Physische Steckplätze** konfiguriert ist, zeigt der iDRAC HII keine Details zur Rückwandplatine an.
- 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 Laufwerke verloren.

Gehäuse über RACADM konfigurieren

Um das Gehäuse oder die Rückwandplatine zu konfigurieren, verwenden Sie den Befehl `set` mit den Objekten in **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 sich 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` die in Schritt 6 erstellte Job-ID ist.

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 Attributwerts `backplanerequestedmode` 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 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.

Konfigurieren des Rückwandplatinen-Modus über die Webschnittstelle

So konfigurieren Sie den Rückwandplatinen-Modus über die iDRAC-Webschnittstelle:

1. Gehen Sie in der iDRAC-Webschnittstelle zu **Storage** > **Übersicht** > **Gehäuse**.
2. Wählen Sie in der Option **Gehäuse** das zu konfigurierende Gehäuse aus.
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: Diese Optionen sind:
   - Unified-Betrieb
   - Split-Betrieb
   - Split-Betrieb 4:20
   - Split-Betrieb 8:16
   - Split-Betrieb 16:8
   - Split-Betrieb 20:4
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 Einstellungen wirksam werden.

ANMERKUNG: Um Bestandsprobleme zu vermeiden, müssen bei Änderungen der Rückwandplatinenkabelverbindung zusätzlich iDRAC neu gestartet und der Host aus- und eingeschaltet werden.

Einrichten des SGPIO-Modus

Der Storage-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 die Option auf Deaktiviert gesetzt ist, ist der I2C-Modus festgelegt. Ist die Option aktiviert, so ist der SGPIO-Modus festgelegt.

Weitere Informationen erhalten Sie im **iDRAC RACADM Command Line Interface Reference Guide (RACADM-Referenzhandbuch für Befehlszeilenschnittstellen für iDRAC)** unter **dell.com/idracmanuals**.

Gehäusebestandsnamen festlegen

„Gehäusebestandsnamen festlegen“ ermöglicht es NutzerInnen, den Bestandsnamen eines Storage-Gehäuses zu konfigurieren.

NutzerInnen können die Eigenschaft „Bestandsname“ des Gehäuses ändern, um Gehäuse einfach zu identifizieren. Diese Felder werden auf ungültige Werte geprüft und bei Eingabe eines ungültigen Werts wird ein Fehler angezeigt. Diese Felder sind Teil der Gehäusefirmware. Die anfänglich angezeigten Daten sind die in der Firmware gespeicherten Werte.

ANMERKUNG: Der Bestandsname hat eine Zeichenbegrenzung von 32, einschließlich Nullzeichen.

ANMERKUNG: Diese Vorgänge werden auf internen Gehäusen nicht unterstützt.

Gehäuse-Bestands-Tag festlegen

Mit der Option „Gehäuse-Bestands-Tag festlegen“ können Sie das Bestands-Tag eines Storage-Gehäuses konfigurieren.

NutzerInnen können die Eigenschaft „Bestands-Tag“ 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 Gehäusefirmware. Die anfänglich angezeigten Daten sind die in der Firmware gespeicherten Werte.

ANMERKUNG: Das Bestands-Tag hat eine Zeichenbegrenzung von 10, einschließlich Nullzeichen.

ANMERKUNG: Diese Vorgänge werden auf internen Gehäusen nicht unterstützt.

Auswählen des Betriebsmodus zum Anwenden von Einstellungen

Beim Erstellen und Managen virtueller Laufwerke, beim Einrichten der physischen Laufwerke, Controller und Gehäuse oder beim Zurücksetzen von Controllern und bevor Sie die verschiedenen Einstellungen anwenden, müssen Sie den Betriebsmodus auswählen. Das heißt, Sie müssen angeben, 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** > **Physische Datenträger** .
   - **Storage** > **Virtuelle Datenträger**
   - **Storage** > **Controller**
   - **Storage** > **Gehäuse**
2. Wählen Sie eine der folgenden Optionen aus dem Drop-Down-Menü **Betriebsmodus anwenden** aus:
   - **Beim nächsten Neustart**: Wählen Sie diese Option aus, um die Einstellungen beim nächsten Systemneustart anzuwenden.
   - **Zu einer geplanten Zeit** – Wählen Sie diese Option aus, um die Einstellungen 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 Einstellungen werden 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)
   - **Zu offenen Vorgängen hinzufügen**: Wählen Sie diese Option aus, um einen ausstehenden Vorgang für die Einstellung zu erstellen. Sie können alle offenen Vorgänge für einen Controller auf der Seite **Storage** > **Übersicht** > **Ausstehende Vorgänge** anzeigen.

   ANMERKUNG:
   - Die Option **Zu ausstehenden Vorgängen hinzufügen** ist für die Seite **Ausstehende Vorgänge** und für PCIe-SSDs auf der Seite **Physische Datenträger** > **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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Anzeigen und Anwenden von ausstehenden Vorgängen

Auf dieser Seite können Sie alle ausstehenden Vorgänge für den Storage Controller anzeigen und anwenden. 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 dem 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** > **Übersicht** > **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/Löschen von Fremdkonfigurationen, Vorgänge von Sicherheitsschlüsseln und das Verschlüsseln virtueller Laufwerke erzeugt. Sie werden jedoch weder auf der Seite **Ausstehenden Vorgänge** noch in der Pop-up-Meldung für ausstehende Vorgänge 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:
   - **Beim nächsten Neustart**: Wählen Sie diese Option, um die Vorgänge beim nächsten Systemneustart anzuwenden.
   - **Zu einer geplanten Zeit**: Wählen Sie diese Option, um die Vorgänge 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. Wenn der Job nicht erfolgreich erstellt wurde, wird eine Meldung angezeigt, die besagt, dass der Job nicht erfolgreich erstellt wurde. Die Meldungs-ID und die empfohlene Antwortmaßnahme werden ebenfalls angezeigt.
6. 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 sich die Vorgänge „Fremdkonfiguration löschen“, „Fremdkonfiguration importieren“, „Sicherheitsschlüsselvorgänge“ oder „Virtuelles Laufwerk verschlüsseln“ im Status „Ausstehend“ befinden und dies die einzigen ausstehenden Vorgänge sind, können Sie keinen Job auf der Seite **Ausstehende Vorgänge** erstellen. Sie müssen alle anderen Storage-Konfigurationsvorgänge durchführen oder RACADM verwenden, um den erforderlichen Konfigurationsjob auf dem erforderlichen Controller zu erstellen.

   Ausstehende Vorgänge für PCIe-SSDs können auf der Seite **Ausstehende Vorgänge** nicht angezeigt oder gelöscht werden. Verwenden Sie den Befehl racadm, um die ausstehenden Vorgänge für PCIe-SSDs 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-CLI-Referenzhandbuch** unter **dell.com/idracmanuals**.

Storage-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 Storage-Konfigurationsvorgang erstellt.

- Wenn der ausstehende Vorgang erfolgreich ist und keine früheren ausstehenden Vorgänge vorhanden sind, wird der Job erstellt. Ist der Job erfolgreich erstellt, wird eine Meldung angezeigt, die besagt, dass die Job-ID für das ausgewählte Gerät erstellt wurde. Klicken Sie auf **Job-Warteschlange**, um den Fortschritt des Auftrags auf der Seite **Job-Warteschlange** anzuzeigen. 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 Antwortmaßnahme werden ebenfalls 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 Storage-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 **Job erstellen**, um einen Job für das ausgewählte Gerät zu erstellen. Ist der Job erfolgreich erstellt, wird eine Meldung angezeigt, die besagt, dass die Job-ID für das ausgewählte Gerät erstellt wurde. Klicken Sie auf **Job-Warteschlange**, um den Fortschritt des Auftrags auf der Seite **Job-Warteschlange** anzuzeigen. 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.
  - Klicken Sie auf **Abbrechen**, um den Job nicht zu erstellen und auf der Seite zu bleiben und weitere Storage-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 **Job für erfolgreiche Vorgänge erstellen**, um einen Job für die vorhandenen ausstehenden Vorgänge zu erstellen. Ist der Job erfolgreich erstellt, wird eine Meldung angezeigt, die besagt, dass die Job-ID für das ausgewählte Gerät erstellt wurde. Klicken Sie auf **Job-Warteschlange**, um den Fortschritt des Auftrags auf der Seite **Job-Warteschlange** anzuzeigen. 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 Antwortmaßnahme werden ebenfalls angezeigt.
  - Klicken Sie auf **Abbrechen**, um den Job nicht zu erstellen und auf der Seite zu bleiben und weitere Storage-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 Storage-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 Storage-Konfigurationsvorgänge auszuführen.
  - Klicken Sie auf **Ausstehende Vorgänge**, um die ausstehenden Vorgänge für das Gerät anzuzeigen. Bis der Job auf dem ausgewählten Controller erstellt wurde, werden die 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 Storage-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 Storage-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 Storage-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 Storage-Konfigurationsseite zu irgendeinem Zeitpunkt nicht angezeigt, gehen Sie zu der Seite **Storage-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 SSD. Sie können die ausstehenden Vorgänge für PCIe SSD-Laufwerke nicht anzeigen und daher ist die Option **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 ein physisches Laufwerk, ein virtuelles Laufwerk und PCIe-SSDs innerhalb eines Gehäuses durch das Blinken einer der Leuchtdioden (LEDs) auf dem Laufwerk finden.

Sie müssen Berechtigungen zum Anmelden sowie zur Steuerung und Konfiguration des Systems haben, um eine LED blinken zu lassen oder das Blinken zu beenden.

Der Controller muss in Echtzeit konfiguriert werden können. Die Echtzeitunterstützung dieser Funktion ist nur mit der Firmware PERC 9.1 und höher verfügbar.

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** > **Übersicht** > **Physische Laufwerke** > **Status** – Zeigt die Seite der identifizierten physischen Laufwerke an, auf der Sie die physischen Laufwerke und PCIe-SSDs blinken und das Blinken beenden können.
   - **Storage** > **Übersicht** > **Virtuelle Laufwerke** > **Status** – Zeigt die Seite der identifizierten virtuellen Laufwerke an, auf der Sie die virtuellen Laufwerke blinken oder das Blinken beenden können.
2. Bei Auswahl des physischen Laufwerks:
   - Auswählen/Abwählen aller Komponenten-LEDs – Wählen Sie die Option **Alle auswählen/abwählen** und klicken Sie auf **Blinken**, um das Blinken der Komponenten-LEDs zu starten. Klicken Sie auf **Blinken beenden**, um das Blinken der Komponenten-LEDs zu stoppen.
   - Auswählen/Abwählen einzelner Komponenten-LEDs – Wählen Sie eine oder mehrere Komponente(n) aus und klicken Sie auf **Blinken**, um das Blinken der Komponenten-LED(s) zu starten. Klicken Sie auf **Blinken beenden**, um das Blinken der Komponenten-LEDs zu stoppen.
3. Bei Auswahl des virtuellen Laufwerks:
   - Auswählen oder Abwählen aller physischen Festplattenlaufwerke oder PCIe-SSDs – Wählen Sie die Option **Alle auswählen/abwählen** und klicken Sie auf **Blinken**, um das Blinken der LEDs für die physischen Festplattenlaufwerke und PCIe-SSDs zu starten. Klicken Sie auf **Blinken beenden**, um das Blinken der LEDs zu stoppen.
   - Aktivieren oder deaktivieren Sie einzelne physische Festplattenlaufwerke und PCIe-SSDs – Wählen Sie eine oder mehrere physischen Festplattenlaufwerke und PCIe-SSDs aus und klicken Sie auf **Blinken**, um das Blinken der LEDs für die physischen Festplattenlaufwerke und PCIe-SSDs zu beginnen. Klicken Sie auf **Blinken beenden**, um das Blinken der LEDs zu stoppen.
4. Wenn Sie sich auf der Seite **Virtuelle Festplatte identifizieren** befinden:
   - Aktivieren oder deaktivieren Sie alle virtuellen Festplatten – Wählen Sie die Option **Alle auswählen/abwählen** aus und klicken Sie auf **Blinken**, um das Blinken der LEDs für die virtuellen Festplatten zu starten. Klicken Sie auf **Blinken beenden**, um das Blinken der LEDs zu stoppen.
   - Aktivieren oder deaktivieren Sie einzelne virtuelle Festplatten – Wählen Sie eine oder mehrere virtuelle Festplatten aus und klicken Sie auf **Blinken**, um das Blinken der LEDs für die virtuellen Festplatten zu beginnen. Klicken Sie auf **Blinken beenden**, um das Blinken der LEDs zu stoppen.

   Wenn die Vorgänge „Blinken“ oder „Blinken beenden“ nicht erfolgreich sind, wird eine Fehlermeldung angezeigt.

Blinken der Komponenten-LEDs über RACADM ein- oder ausschalten

Um das Blinken der Komponenten-LEDs ein- oder auszuschalten, verwenden Sie 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 **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.

ANMERKUNG: Nach dem Durchführen eines Server-Softwareneustarts gibt iDRAC möglicherweise die Meldung `Disk Inserted` in LC-Protokollen für Laufwerke aus, die sich hinter dem HBA befinden. Ignorieren Sie diesen Protokolleintrag.

20

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 Nutzer eine Konfigurationsgruppe erweitert, werden die Attribute in alphabetischer Reihenfolge angezeigt.

ANMERKUNG: Hilfeinhalt auf Merkmalsebene wird dynamisch generiert.

Anwenden

Die Schaltfläche **Anwenden** bleibt so lange ausgegraut, bis eines der Attribute geändert wird. Nachdem Sie ein Attribut geändert haben, klicken Sie auf **Übernehmen**. Das Attribut wird mit den erforderlichen Änderungen modifiziert. Kann die Anforderung das BIOS-Attribut nicht festlegen, wird eine Fehlermeldung angezeigt. Weitere Informationen finden Sie auf der Dell Support-Website im *Referenzhandbuch zu Dell Technologies 17G-, 16G-, 15G-, 14G- und 13G-PowerEdge-Servern mit Fehlermeldungen und Ereignismeldungen*.

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 neuesten Änderungen verworfen und die vorherigen oder ursprünglichen Werte werden wiederhergestellt.

Anwenden und neu starten

Wenn NutzerInnen den Wert eines Attributs oder einer Startreihenfolge ändern, werden ihnen zwei Optionen angezeigt, um die Konfiguration anzuwenden. **Anwenden und neu starten** oder **Beim nächsten Neustart anwenden**. In beiden Anwendungsoptionen werden NutzerInnen auf die Seite der Jobwarteschlange umgeleitet, um den Fortschritt dieses bestimmten Jobs zu überwachen.

NutzerInnen können 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. Kann die Anforderung die BIOS-Attribute nicht festlegen, wird eine Fehlermeldung angezeigt.

Beim nächsten Neustart anwenden

Wenn NutzerInnen den Wert eines Attributs oder einer Startreihenfolge ändern, werden ihnen zwei Optionen angezeigt, um die Konfiguration anzuwenden. **Anwenden und neu starten** oder **Beim nächsten Neustart anwenden**. In beiden Anwendungsoptionen werden NutzerInnen auf die Seite der Jobwarteschlange umgeleitet, um den Fortschritt dieses bestimmten Jobs zu überwachen.

NutzerInnen können 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. Kann die Anforderung die BIOS-Attribute nicht festlegen, wird eine Fehlermeldung 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 NutzerInnen die Konfigurationsänderungen nicht übernehmen möchten, können sie auf die

Schaltfläche **Alle ausstehenden Werte löschen** klicken, um alle Änderungen zu verwerfen. Kann die Anforderung die BIOS-Attribute nicht entfernen, wird eine Fehlermeldung 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 UI 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 Ergebnisse 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/Recovery-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. **ROM-Update des primären BIOS** – Der 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 Nutzer 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: Beim Einschalten des Servers aus dem **Aus**-Zustand kann es 20 bis 30 Sekunden dauern, bis iDRAC den Stromzustand als **Ein** meldet.

21

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 managen, 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 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
- Videoverschlüsselung – aktiviert/deaktiviert
- Lokales Servervideo – aktiviert/deaktiviert
- 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.

  ANMERKUNG:
  - Jede Änderung in der Web-Serverkonfiguration führt zum Beenden der vorhandenen Sitzung der virtuellen Konsole.
  - Selbst wenn die Videoverschlüsselungsoption in der GUI deaktiviert ist, können Sie die Funktion weiterhin über andere Schnittstellen konfigurieren, die Videoverschlüsselung ist standardmäßig aktiviert.
  - Der Link zur virtuellen Konsole kann während der Ausführung des Video-Belastungstests in Internet Explorer unterbrochen werden.

- 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.
- Sie können bis zu 6 Sitzungen der virtuellen Konsole von der Verwaltungsstation auf dem verwalteten Server öffnen.
- Wenn ein zweiter Nutzer eine Virtuelle Konsole-Sitzung anfordert, wird der erste Nutzer benachrichtigt und erhält die Option, den Zugriff abzulehnen, den schreibgeschützten Zugriff zu erlauben oder vollständig freigegebenen Zugriff zu erlauben. Der zweite Nutzer wird benachrichtigt, dass ein anderer Nutzer die Steuerung übernommen hat. Wenn der erste Nutzer nicht innerhalb von 30 Sekunden antwortet, wird dem zweiten Nutzer je nach Standardeinstellung ein Zugriff gewährt. Wenn weder der erste noch der zweite Nutzer über Administratorberechtigungen verfügt, wird die Sitzung des zweiten Nutzers automatisch beendet, wenn der erste Nutzer seine aktive Sitzung beendet.
- Start- und Absturzprotokolle werden als Videoprotokolle im MPEG1-Format erfasst.
- Der Absturzbildschirm wird als JPEG-Datei erfasst.

.

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.

Themen:

- Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen
- Konfigurieren einer virtuellen Konsole

- Virtuelle Konsole starten
- Anzeige der virtuellen 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 50. 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
1920x1200	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.

Konfigurieren einer virtuellen Konsole

Vor dem Konfigurieren 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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Vorschau der virtuellen Konsole

Bevor Sie die virtuelle Konsole starten, können Sie eine Vorschau des Status der virtuellen Konsole auf der Seite **System** > **Eigenschaften** > **Systemzusammenfassung** anzeigen. Im Abschnitt **Vorschau der virtuellen Konsole** wird ein Bild mit dem Status der virtuellen Konsole angezeigt. Das Bild wird automatisch 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.
- Die Mindestnetzwerkbandbreite von 1 MB/s ist verfügbar.

ANMERKUNG: Wenn der nutzerdefinierte HTTP-Port oder der Standardport in iDRAC konfiguriert ist, müssen Sie zuerst den Browser-Cache löschen und dann iDRAC mit HTTPS starten und die Zertifikate akzeptieren. Melden Sie sich anschließend bei iDRAC an und starten Sie die virtuelle Konsole.

ANMERKUNG: Wenn der integrierte Videocontroller im BIOS deaktiviert ist und Sie die virtuelle Konsole starten, ist der Viewer der virtuellen Konsole leer.

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. **Leistung**: Ändert die Videoqualität und -geschwindigkeit.
4. **Nutzerliste**: Zeigt die Liste der NutzerInnen an, 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.

ANMERKUNG: Wenn in iDRAC-Version 5.10.00.00 die RFS-Sitzung aktiv ist, wird die Sitzung des virtuellen Datenträgers blockiert. Wenn Sie also ein Upgrade von Version 4.40.00.00 auf Version 5.10.00.00 mit aktivierter RFS-Sitzung durchführen, wird RFS erneut eingehängt, wenn iDRAC aktiv ist. Wenn Sie in diesem Fall versuchen, die Sitzung für virtuelle Datenträger zu starten, schlägt dies mit der Fehlermeldung `Virtual media already in use` fehl.

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 eine 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 lokale, Active Directory-, LDAP-, Smartcard-(SC-) und Single Sign-On-(SSO-)Anmeldungen. 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.

Anzeige der virtuellen 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 Virtual Console Viewer zeigt den DNS-Namen oder die IP-Adresse des iDRAC an, mit dem Sie über die Verwaltungsstation verbunden sind. Wenn iDRAC keinen DNS-Namen hat, wird die IP-Adresse angezeigt. Das Format lautet:

- Für Rack- und Tower-Server: `<DNS name / IPv6 address / IPv4 address>, <Model>, User: <username>, <fps>`

Manchmal zeigt der Virtual Console Viewer Videos mit niedriger Qualität an. Dies ist auf eine langsame Netzwerkverbindung zurückzuführen, die zum Verlust von einem oder zwei Video-Frames führt, wenn Sie die Sitzung der virtuellen Konsole starten. Um alle Video-Frames zu übertragen und die nachfolgende Videoqualität zu verbessern, führen Sie einen der folgenden Schritte aus:

- 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**.

Verwenden der virtuellen Konsole

ANMERKUNG: Standardmäßig ist der Typ der virtuellen Konsole auf eHTML5 eingestellt.

Sie können die virtuelle Konsole mithilfe einer der folgenden Methoden als Pop-up-Fenster starten:

- Klicken Sie auf der iDRAC-Startseite auf den Link **Virtuelle Konsole starten**, der in der Konsolenvorschau angezeigt wird.
- Klicken Sie auf der iDRAC-Seite „Virtuelle Konsole“ auf den Link **Virtuelle Konsole starten**.
- Geben Sie auf der iDRAC-Anmeldeseite **https//<iDRAC-IP-Adresse>/console** ein. Diese Methode wird als direktes Starten bezeichnet.

In der virtuellen eHTML5-Konsole sind die folgenden Menüoptionen verfügbar:

- Stromversorgung
- Starten
- Chat
- Tastatur
- Bildschirmerfassung
- Aktualisieren
- Vollbild
- Verbindung zum Anzeigeprogramm trennen.
- Konsolensteuerung
- Virtueller Datenträger

Die Option **Alle Tastenanschläge an den Server senden** wird in der virtuellen eHTML5-Konsole nicht unterstützt. Verwenden Sie Tastatur und Tastaturmakros für alle Funktionstasten.

- **Allgemein**:
  - **Konsolensteuerung**: Dieses Element bietet die folgenden Konfigurationsoptionen:
    - Tastaturmakros: Diese werden in der virtuellen eHTML5-Konsole unterstützt und als folgende Drop-down-Optionen aufgeführt. Klicken Sie auf **Anwenden**, um die ausgewählte Tastenkombination auf dem Server anzuwenden.
      - Strg+Alt+Entf
      - Strg+Alt+F1
      - Strg+Alt+F2
      - Strg+Alt+F3
      - Strg+Alt+F4
      - Strg+Alt+F5
      - Strg+Alt+F6
      - Strg+Alt+F7
      - Strg+Alt+F8
      - Strg+Alt+F9
      - Strg+Alt+F10
      - Strg+Alt+F11
      - Strg+Alt+F12
      - Alt+Tab
      - Alt+Esc
      - Strg+Esc
      - Alt+Leertaste
      - Alt+Eingabe
      - Alt+Bindestrich
      - Alt+F1
      - Alt+F2
      - Alt+F3
      - Alt+F4

- Alt+F5
- Alt+F6
- Alt+F7
- Alt+F8
- Alt+F9
- Alt+F10
- Alt+F11
- Alt+F12
- Druck
- Alt+Druck
- F1
- Pause
- Registerkarte
- Strg+Eingabe
- SysRq
- Alt+SysRq
- Win-P

  - Seitenverhältnis: In der virtuellen eHTML5-Konsole wird die Größe des Videobilds automatisch angepasst, damit das Bild angezeigt werden kann. Es werden folgende Konfigurationsoptionen in der Drop-Down-Liste angezeigt:
    - Wartung
    - Nicht warten.

    Klicken Sie auf **Anwenden**, um die ausgewählten Einstellungen auf den Server anzuwenden.
  - Touch-Modus: Die virtuelle eHTML5-Konsole unterstützt die Touch-Funktion. Es werden folgende Konfigurationsoptionen in der Drop-Down-Liste angezeigt:
    - Direkt
    - Relativ

    Klicken Sie auf **Anwenden**, um die ausgewählten Einstellungen auf den Server anzuwenden.

- **Virtuelle Zwischenablage**: Die virtuelle Zwischenablage ermöglicht das Ausschneiden/Kopieren/Einfügen von Textpuffern von der virtuellen Konsole auf den iDRAC-Host-Server. Der Host-Server könnte BIOS, UEFI oder in der Betriebssystem-Eingabeaufforderung sein. Dabei handelt es sich um eine unidirektionale Maßnahme vom Client-System zum Host-Server des iDRAC. Gehen Sie wie folgt vor, um die virtuelle Zwischenablage zu verwenden:
  - Platzieren Sie den Mauszeiger oder den Tastaturfokus auf dem gewünschten Fenster des Host-Server-Desktops.
  - Wählen Sie das Menü **Konsolensteuerungen** von vConsole aus.
  - Kopieren Sie den Zwischenspeicher aus der Zwischenablage des Betriebssystems je nach Client-Betriebssystem mithilfe der Tastaturschnelltasten, der Maus oder des Touchpads. Alternativ können Sie den Text manuell in das Textfeld eingeben.
  - Klicken Sie auf **Zwischenablage an Host senden**.
  - Der Text wird im aktiven Fenster des Host-Servers angezeigt.

  ANMERKUNG:
  - Diese Funktion ist mit einer Enterprise- und Datacenter-Lizenz verfügbar.
  - Diese Funktion unterstützt nur ASCII-Text.
  - Diese Funktion unterstützt nur die Tastatur in englischer Sprache.
  - Steuerungszeichen werden nicht unterstützt.
  - Zeichen wie **Neue Zeile** und **Tabulator** sind zulässig.
  - Die Textpuffergröße ist auf 4000 Zeichen begrenzt.
  - Wenn mehr als ein maximaler Puffer eingefügt wird, kürzt das Bearbeitungsfeld in der iDRAC GUI dies auf die maximale Puffergröße.

- **KVM** – Dieses Menü enthält eine Liste der folgenden schreibgeschützten Komponenten:
  - Bildfrequenz
  - Bandbreite
  - Komprimierung
  - Paketrate
- **Leistung** – Sie können mit dem Schieberegler **Maximale Videoqualität** und **Maximale Videogeschwindigkeit** einstellen.
- **Benutzerliste** – Zeigen Sie die Liste der NutzerInnen an, die bei der virtuellen Konsole angemeldet sind.
- **Tastatur** – Der Unterschied zwischen der physischen und der virtuellen Tastatur besteht darin, dass die virtuelle Tastatur ihr Layout entsprechend der Browsersprache ändert.

ANMERKUNG: Achten Sie darauf, dass die vKeyboard-Sprache und die Hostbetriebssystem-Sprache identisch sind.

- **Virtueller Datenträger** – Klicken Sie auf die Option **Virtuellen Datenträger verbinden**, um die virtuelle Datenträgersitzung zu starten.
  - **Virtuellen Datenträger verbinden** – Dieses Menü enthält die Optionen für das Zuordnen von CD/DVD, das Zuordnen von Wechseldatenträgern, das Zuordnen von externen Geräten und das Zurücksetzen von USB.
  - **Statistik für virtuelle Datenträger** – Dieses Menü zeigt die Übertragungsrate (schreibgeschützt) an. Außerdem werden die Details für CD/DVD und Wechseldatenträger angezeigt, wie z. B. Zuordnungsdetails, Status (schreibgeschützt oder nicht), Dauer und Lesen/Schreiben von Bytes.
  - **Image erstellen** – Mit diesem Menü können Sie einen lokalen Ordner auswählen und eine FolderName.img-Datei mit Inhalten des lokalen Ordners erzeugen.

ANMERKUNG: Aus Sicherheitsgründen ist der Lese-/Schreibzugriff während des Zugriffs auf die virtuelle Konsole in eHTML5 deaktiviert.

Unterstützte Browser

Die virtuelle eHTML5-Konsole wird auf folgenden Browsern unterstützt:

- Microsoft EDGE
- Safari 16.6
- Safari 17.x
- Mozilla Firefox 128
- Mozilla Firefox 129
- Mozilla Firefox 130
- Google Chrome 137
- Google Chrome 138

ANMERKUNG: Es wird empfohlen, die Mac OS Betriebssystemversion 10.10.2 (oder höher) auf dem System zu verwenden.

ANMERKUNG: Wenn Sie den Chrome-/Edge-Browser verwenden, wird möglicherweise die Meldung „Anmeldung verweigert“ angezeigt.

Weitere Informationen zu den unterstützten Browsern und Versionen finden Sie unter Die *Versionshinweise zum Benutzerhandbuch für Integrated Dell Remote Access Controller* sind verfügbar auf der Seite iDRAC-Handbücher..

22

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, Redfish und RACADM. 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:

- Sie können das iDRAC Service Module nur dann verwenden, wenn Sie die iDRAC Express- oder iDRAC Enterprise/Datacenter-Lizenz installiert haben.
- iSM-Versionen, die älter als 4.2 sind, unterstützen TLS 1.3 nicht.
- Wenn das HOST-Netzwerk nicht ordnungsgemäß konfiguriert ist, meldet die iDRAC-SupportAssist-Seite das LC-Protokoll, was darauf hinweist, dass ein Problem beim Herstellen der Verbindung mit dem iSM aufgetreten ist.
- Wenn Sie während der Erstellung von SupportAssist-Erfassungen eine SRV042-Warnung im iDRAC-LC erhalten, führen Sie einen Kaltstart des iDRAC durch, um diese Warnung im iDRAC-LC aufzulösen.

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 Service Moduls aktivieren und deaktivieren können.
- Deaktivieren Sie nicht die Option **iDRAC-Konfiguration über lokale RACADM-Schnittstelle**.
- Der Passthrough-Kanal zwischen Betriebssystem und iDRAC wurde über den internen USB-Bus im 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 der Passthrough-Kanal zwischen Betriebssystem und iDRAC im iDRAC standardmäßig 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 im 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 Service Module von **dell.com/support** herunterladen. Sie müssen über die Administratorberechtigung für das Betriebssystem des Servers verfügen, um das iDRAC Service Module zu installieren. Weitere Informationen zur Installation finden Sie im Benutzerhandbuch zu iDRAC Service Module auf der iDRAC Service Module-Seite.

ANMERKUNG: Wenn USB-NIC auf dem iDRAC deaktiviert ist, aktiviert das iSM-Installationsprogramm automatisch USB-NIC. Sobald die Installation abgeschlossen ist, deaktivieren Sie bei Bedarf USB-NIC.

Installieren des iDRAC Service Module von iDRAC Core

Klicken Sie auf der Einrichtungsseite für das **iDRAC Service Module** auf **Service Module installieren**.

1. Das Installationsprogramm für das Service Module steht dem Hostbetriebssystem zur Verfügung und es wird ein Job im iDRAC erstellt. Melden Sie sich bei Microsoft Windows- oder Linux-Betriebssystemen entweder remote oder lokal beim Server an.
2. Machen Sie in der Geräteliste das gemountete Volume mit der Bezeichnung **SMINST** ausfindig und führen Sie das entsprechende Skript aus:
   - Öffnen Sie unter Windows die Eingabeaufforderung und führen Sie die Batchdatei **ISM-Win.bat** aus.
   - Öffnen Sie unter Linux die Shell-Eingabeaufforderung und führen Sie die Skriptdatei **ISM-Lx.sh** aus.
3. Nachdem die Installation abgeschlossen ist, zeigt iDRAC das Service Module als **installiert** an und gibt das Installationsdatum an.

   ANMERKUNG: Das Installationsprogramm steht dem Hostbetriebssystem 30 Minuten lang zur Verfügung. Wenn Sie die Installation nicht innerhalb von 30 Minuten starten, müssen Sie mit der Servicemodul-Installation von vorne beginnen.

Installieren des iDRAC Service Module von iDRAC Enterprise

1. Navigieren Sie auf der iDRAC-Benutzeroberfläche zu **iDRAC-Einstellungen** > **Einstellungen** > **iDRAC-Service Module-Setup**.
2. Klicken Sie auf der Seite **Einrichten des iDRAC Service Module** auf **Service Module installieren**.
3. Klicken Sie auf **Virtuelle Konsole starten** und klicken Sie dann im Dialogfeld mit der Sicherheitswarnung auf **Weiter**.
4. Sie können die Installationsdatei für das iSM ausfindig machen, indem Sie sich entweder remote oder lokal beim Server anmelden.

   ANMERKUNG: Das Installationsprogramm steht dem Hostbetriebssystem 30 Minuten lang zur Verfügung. Wenn Sie die Installation nicht innerhalb von 30 Minuten starten, müssen Sie mit der Installation von vorne beginnen.

5. Machen Sie in der Geräteliste das gemountete Volume mit der Bezeichnung **SMINST** ausfindig und führen Sie das entsprechende Skript aus:
   - Öffnen Sie unter Windows die Eingabeaufforderung und führen Sie die Batchdatei **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 **Einrichten des iDRAC Service Module** wird die Schaltfläche **Service Module installieren** deaktiviert, nachdem die Installation abgeschlossen ist, und der Status des Service Module wird als **Wird ausgeführt** angezeigt.

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 auf der iDRAC Service Module-Seite verfügbar ist.

Überwachungsfunktionen des iDRAC-Servicemoduls

Das iDRAC Service Module (iSM) bietet die folgenden Überwachungsfunktionen:

Tabelle 51. Vom iSM unterstützte Funktionen

Wird ausgeführt	Wird ausgeführt (eingeschränkte Funktionalität)
Unterstützung des Redfish-Profils für Netzwerkattribute	Dienst auf Host-BS
Remote-iDRAC-Hardware-Reset	Betriebssystem-Informationen
iDRAC-Zugriff über das Hostbetriebssystem (experimentelle Funktion)	Automatische Systemwiederherstellung
Bandinterne iDRAC-SNMP-Warnungen	Service Module ermöglichen, iDRAC-Kaltstart durchzuführen
Anzeigen von Informationen zum Betriebssystem	k. A.

Tabelle 51. Vom iSM unterstützte Funktionen (fortgesetzt)

Wird ausgeführt	Wird ausgeführt (eingeschränkte Funktionalität)
Replizieren von Lifecycle Controller-Protokollen zu den Betriebssystemprotokollen	k. A.
Automatische Systemwiederherstellung ausführen	k. A.
WMI (Windows Management Instrumentation)-Management-Provider bestücken	k. A.
Integration mit SupportAssist-Sammlung. **ANMERKUNG:** Dies gilt nur, wenn das iDRAC Service-Modul Version 2.0 oder höher installiert ist.	k. A.
Bereiten Sie das Entfernen der NVMe-PCIe-SSD vor. **ANMERKUNG:** Weitere Informationen finden Sie auf der Seite Unterstützung für Dell iDRAC Service Module.	k. A.
Aus- und Einschalten des Servers (Remote)	k. A.

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“.

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 der entsprechenden RACADM-Schnittstelle), 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: 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.

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).

Diese Funktion ist standardmäßig 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.

- **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**

  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-BandSNMPAlerts**, das auf der Dell Support-Seite verfügbar ist.

iDRAC-Zugriff über Host-BS

Mit dieser Funktion können Sie die Hardwareparameter über die iDRAC-Weboberfläche 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 durchführen.

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-Anschlussnummer. Diese wird als Verbindungsportnummer bezeichnet, an die alle eingehenden Verbindungen auf der Überwachungsportnummer umgeleitet werden. Sie können die Portnummer über die iDRAC-Weboberfläche 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:

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

Disable

`<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

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 Service Moduls.
   - 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):
     - **Neustart**
     - **System ausschalten**
     - **System aus- und einschalten**

     Diese Option ist deaktiviert, wenn OpenManage Server Administrator auf dem System installiert ist.

ANMERKUNG: Wenn sich iSM im vollständigen oder eingeschränkten Modus befindet und der iDRAC auf die Werkseinstellungen zurückgesetzt wird, gibt es keine Möglichkeit für iDRAC, den Funktionszustand „eingeschränkter Modus“ als iSM-Status festzulegen.

Verwenden des iDRAC Servicemodul von RACADM

Zur Verwendung des iDRAC Service Module über RACADM verwenden Sie die Objekte in der Gruppe `ServiceModule`.

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

23

Verwenden des Typ-C-USB-Dual-Mode-Ports für das Servermanagement

Bei Servern der 17. Generation ist ein dedizierter Typ-C-USB-Dual-Mode-Port im Bedienfeld verfügbar, das sich auf der Vorderseite des Servers befindet. Standardmäßig befindet sich der Port im Betriebssystemmodus. Auf dem Bedienfeld befindet sich eine System-ID-Taste (¡). Um den Port in den iDRAC-Modus zu wechseln, halten Sie die Taste ¡ 5 bis 10 Sekunden lang gedrückt, bis die Schraubenschlüssel-LED aufleuchtet. Um den Port wieder in den Betriebssystemmodus zu wechseln, halten Sie die Taste ¡ erneut 5 bis 10 Sekunden lang gedrückt, bis die Schraubenschlüssel-LED erlischt.

SCP-Importvorgänge (Server Configuration Profiles) über USB werden nur mit der Enterprise- oder Datacenter-Lizenz unterstützt.

Sie können die folgenden Funktionen über den Typ-C-USB-Dual-Mode-Port ausführen, wenn sich der Port im iDRAC-Modus befindet:

- 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 Typ-C-USB-Dual-Mode-Port zu managen 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 angeschlossen wird, wird eine Warnmeldung generiert.

Themen:

- Konfigurieren von iDRAC über das Server-Konfigurationsprofil auf dem USB-Gerät

Konfigurieren von iDRAC über das Server-Konfigurationsprofil auf dem USB-Gerät

Mit dem Type-C-USB-Dual-Mode-Anschluss im iDRAC-Modus können Sie iDRAC auf dem Server konfigurieren. Konfigurieren Sie die Einstellungen des Type-C-USB-Dual-Mode-Anschlusses in iDRAC, setzen Sie das USB-Gerät mit dem Server-Konfigurationsprofil ein und importieren Sie dann das Server-Konfigurationsprofil vom USB-Gerät auf iDRAC.

Konfigurieren der Type-C-USB-Dual-Mode-Porteinstellungen über die iDRAC-UI

So konfigurieren Sie den Type-C-USB-Dual-Mode-Anschluss:

1. Aktivieren Sie den Type-C-USB-Dual-Mode-Anschluss des Servers in iDRAC (**Konfiguration** > **BIOS-Einstellungen** > **Integrierte Geräte**. Sorgen Sie dafür, dass **Alle Schnittstellen ein** oder **Alle Schnittstellen aus (dynamisch)** als **Vom Nutzer zugreifbare USB-Anschlüsse** ausgewählt ist. Wenn **Alle Schnittstellen aus (dynamisch)** ausgewählt ist, stellen Sie sicher, dass **Nur Frontschnittstellen aktiviert** ist.
2. Halten Sie die System-ID-Taste auf dem Bedienfeld etwa 5 bis 10 Sekunden lang gedrückt, bis die Schraubenschlüssel-LED aufleuchtet.
   Die USB-LED leuchtet stetig grün und der Port ist als iDRAC-Port konfiguriert.
3. Navigieren Sie in der iDRAC-Webschnittstelle zu **iDRAC-Einstellungen** > **Einstellungen** > **Verwaltungs-USB-Einstellungen**. Die **USB-Verwaltungsschnittstelle** wird **aktiviert**.
4. Wählen Sie unter **Über iDRAC verwaltet: USB-SCP** eine der aktivierten Optionen aus:
   - **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: iDRAC10 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.

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

Zugriff auf die iDRAC-Schnittstelle über eine direkte USB-Verbindung

Mit der iDRAC-Direct-Funktion können Sie Ihren Laptop direkt an den iDRAC-USB-Anschluss anschließen. Diese Funktion erlaubt die direkte Interaktion mit den iDRAC-Schnittstellen wie Webschnittstelle, RACADM und Redfish zur erweiterten Serververwaltung und -wartung.

Eine Liste der unterstützten Browser und Betriebssysteme finden Sie unter Die *Versionshinweise zum Benutzerhandbuch für Integrated Dell Remote Access Controller* sind verfügbar auf der Seite iDRAC-Handbücher..

ANMERKUNG: Wenn Sie ein Windows-Betriebssystem verwenden, installieren Sie einen RNDIS-Treiber, um diese Funktion nutzen zu können.

Zum Zugriff auf die iDRAC-Schnittstelle über den USB-Anschluss:

1. Schalten Sie alle Wireless-Netzwerke aus und trennen Sie jedes andere kabelgebundene Netzwerk. Stellen Sie sicher, dass keines der externen oder internen Netzwerke oder Einstellungen die Kommunikation beeinträchtigt.
2. Stellen Sie sicher, dass sich der USB-Anschluss im iDRAC-Modus befindet.
3. Warten Sie einige Sekunden, bis der Laptop die IP-Adresse 169.254.0.4 erhält. Der iDRAC ruft die IP-Adresse 169.254.0.3 ab.
4. Beginnen Sie mit der Verwendung von iDRAC-Netzwerkschnittstellen, z. B. Webschnittstelle, RACADM und Redfish.
   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, blinkt die LED und zeigt so Aktivität an. Dabei leuchtet die LED einmal in zwei Sekunden auf.
6. Trennen Sie das USB-Kabel nach Abschluss der erforderlichen Aktionen vom System.
   Die LED leuchtet wieder stetig grün.

Importieren des Serverkonfigurationsprofils von einem USB-Gerät

Ertellen Sie im Stammverzeichnis des USB-Geräts ein Verzeichnis mit dem Namen `System_Configuration_XML`, in dem sowohl die Konfigurations- als auch die Steuerungsdateien enthalten sind:

- Das Serverkonfigurationsprofil (SCP) befindet sich im Unterverzeichnis `System_Configuration_XML` des Stammverzeichnisses 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` lauten.
- 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 einer `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-Management-Port-Modus** auf **iDRAC**.
   - Stellen Sie **iDRAC-Verwaltet: USB SCP** auf **Aktiviert mit Standard-Anmeldeinformationen** oder „Aktiviert“ ein.
2. Setzen Sie den USB-Stick (der die Dateien `configuration.xml` und `control.xml` enthält) in den iDRAC-USB-Anschluss ein.

   ANMERKUNG: Bei Dateiname und Dateityp wird bei XML-Dateien zwischen Groß- und Kleinschreibung unterschieden. Stellen Sie sicher, dass beide in Kleinbuchstaben geschrieben sind.

   ANMERKUNG: Das USB-Laufwerk darf nur über das unterstützte FAT32-Dateisystem verfügen.

3. Das Serverkonfigurationsprofil wird auf dem USB-Gerät im Unterverzeichnis `System_Configuration_XML` des Stammverzeichnisses 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 SCP-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. , 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, 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 LED an, dass der Job abgeschlossen ist.
8. Wenn das USB-Gerät weiterhin mit dem Server verbunden bleibt, wird das Ergebnis des Importvorgangs in der Datei `results.xml` des USB-Geräts aufgezeichnet.

LC-Protokolle und Fehlermeldungen während USB-bezogener Vorgänge

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 iDRAC-Modus befindet und das USB-Gerät angeschlossen oder entfernt wird

- der USB-Verwaltungsanschlussmodus geändert wird
- Das Gerät manuell vom iDRAC in den Betriebssystemmodus umgeschaltet wird
- Das Gerät aus dem iDRAC entfernt wurde

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 und Remote-Syslog
- Maßnahmen: Keine

Eine Fehlermeldung wird angezeigt, und im Lifecycle Controller-Protokoll protokolliert wenn:

- Wenn Eingabedateien für das Serverkonfigurationsprofil (SCP) falsch sind.
- Wenn das USB-Laufwerk Hardwarefehler oder nicht unterstützte Dateisysteme aufweist.

LED-Funktionsweise

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.

- Aus: Der Type-C-USB-Dual-Mode-Anschluss befindet sich im Betriebssystemmodus.
- Stetig grün: Der USB-Anschluss ist mit iDRAC verbunden oder der SCP-Importjob wurde erfolgreich abgeschlossen.
- Grün blinkend: Der SCP-Importjob wird ausgeführt oder I/O wird ausgeführt.
- Stetig gelb: Der SCP-Importjob ist fehlgeschlagen.
- Gelb blinkend: Die USB-Hardware weist Fehler auf.

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 im 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.

24

Verwendung von Quick Sync 2

Mit Dell OpenManage Mobile auf einem Android- oder iOS-Mobilgerät können Sie problemlos direkt oder über OpenManage Essentials oder die OpenManage Enterprise (OME)-Konsole auf den Server zugreifen. Es ermöglicht Ihnen, Serverdetails und Bestand zu überprüfen, LC- und Systemereignisprotokolle anzuzeigen, automatische Benachrichtigungen auf mobilen Geräten von einer OME-Konsole aus zu empfangen, IP-Adressen zuzuweisen und das iDRAC-Passwort zu ändern, wichtige BIOS-Attribute zu konfigurieren und Korrekturmaßnahmen wie erforderlich durchzuführen. Sie können auch einen Server aus- und wieder einschalten, auf die Systemkonsole zugreifen oder auf 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 mobilen Gerät installieren (unterstützt mobile Geräte mit Android ab Version 5.0 und iOS ab Version 9.0), um den Server über die iDRAC Quick Sync 2-Schnittstelle zu managen.

ANMERKUNG: Dieser Abschnitt wird nur auf den Servern angezeigt, auf denen sich das Quick Sync 2-Modul im linken Rackwinkel befindet.

ANMERKUNG: Diese Funktion wird derzeit auf mobilen Geräten mit Android- oder iOS-Betriebssystem unterstützt.

Aktivieren Sie nach der Konfiguration der Schnellkonfiguration die Taste Quick Sync 2 auf dem linken Bedienfeld. Stellen Sie sicher, dass die Quick Sync 2-LED leuchtet. Greifen Sie auf die Quick Sync 2-Informationen über ein mobiles Gerät zu (Android 5.0 bzw. iOS 9.0 oder höher, OMM 2.0 oder höher).

Mit dem OpenManage Mobile können Sie:

- Bestandsaufnahme-Informationen anzeigen
- Überwachungsinformationen anzeigen
- Die grundlegende iDRAC-Netzwerkeinstellungen konfigurieren

Weitere Informationen zu OpenManage Mobile finden Sie unter Das *Benutzerhandbuch für Dell OpenManage Mobile* ist verfügbar auf der Seite OpenManage-Handbücher..

Themen:

- Konfigurieren von iDRAC Quick Sync 2
- Verwenden vom Mobilgerät zum Anzeigen von iDRAC-Informationen

Konfigurieren von iDRAC Quick Sync 2

Mithilfe der iDRAC-Webschnittstelle RACADM 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 die Option Minuten ausgewählt. Der Standardwert ist 2 Minuten. Der Bereich liegt zwischen 2 und 60 Minuten.
  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 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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Konfigurieren von iDRAC Quick Sync 2-Einstellungen über die Weboberfläche

Konfigurieren von iDRAC Quick Sync 2:

1. Gehen Sie auf der iDRAC-Weboberfläche zu **Konfiguration** > **Systemeinstellungen** > **Hardwareeinstellungen** > **iDRAC Quick Sync**.
2. Wählen Sie im Abschnitt **iDRAC Quick Sync** im Menü **Zugriff** eine der folgenden Optionen für den Zugriff auf das mobile Android- oder iOS-Gerät aus:
   - Lesen/Schreiben
   - Schreibgeschützt
   - Deaktiviert
3. Aktivieren Sie den Zeitgeber.
4. Legen Sie den Timeout-Wert fest.

   Weitere Informationen zu den Feldern finden Sie in der **iDRAC Online-Hilfe**.
5. Klicken Sie auf **Anwenden**, um die Einstellungen zu übernehmen.

Konfigurieren der iDRAC Quick Sync 2-Einstellungen über das Dienstprogramm für die iDRAC-Einstellungen

Konfigurieren von iDRAC Quick Sync 2:

1. Gehen Sie auf der iDRAC-Benutzeroberfläche zu **Konfiguration** > **Systemeinstellungen** > **Hardwareeinstellungen** > **iDRAC Quick Sync**.
2. Im **iDRAC Quick Sync-**Abschnitt:
   - Geben Sie die Zugriffsebene an.
   - Aktivieren Sie Timeout.
   - Legen Sie den benutzerdefinierten Timeout-Wert (120 Sekunden bis 3600 Sekunden) fest.

   Weitere Informationen zu den Feldern finden Sie in der **iDRAC Online-Hilfe**.
3. Klicken Sie auf **Zurück**, dann auf **Fertig stellen** und anschließend auf **Ja**.
   Die Einstellungen werden angewendet.

Verwenden vom Mobilgerät zum Anzeigen von iDRAC-Informationen

Eine Anleitung zum Anzeigen von iDRAC-Informationen auf dem Mobilgerät finden Sie unter Das *Benutzerhandbuch für Dell OpenManage Mobile* ist verfügbar auf der Seite OpenManage-Handbücher..

25

Virtuelle Datenträger managen

iDRAC bietet virtuelle Datenträger mit einem HTML5-basierten Client mit lokaler ISO- und IMG-Datei und Unterstützung für Remote-ISO- und IMG-Dateien. Mit virtuellen Medien kann der gemanagte Server auf Mediengeräte auf der Managementstation oder auf ISO-CD/DVD-Images auf einer Netzwerkfreigabe zugreifen, als wären es Geräte auf dem gemanagten Server. Sie benötigen die Berechtigung zur iDRAC-Konfiguration, um die Konfiguration zu ändern.

Nachfolgend sind die konfigurierbaren Attribute aufgeführt:

- Angeschlossene Datenträger aktiviert – aktiviert oder deaktiviert
- Verbindungsmodus – automatisch verbinden, verbunden und getrennt
- Max. Sitzungen – 1
- Aktive Sitzungen – 1
- Virtuelle Datenträgerverschlüsselung – aktiviert (standardmäßig)
- Diskettenemulation – deaktiviert (standardmäßig)
- Einmaliges Starten – aktiviert oder deaktiviert
- Verbindungsstatus – verbunden oder getrennt

Über die Funktion für den virtuellen Datenträger können Sie die folgenden Schritte ausführen:

- Fernzugriff auf Medien zu erhalten, die über das Netzwerk mit einem entfernten System verbunden sind
- Anwendungen zu installieren
- Treiber zu aktualisieren
- Ein Betriebssystem auf dem gemanagten System zu installieren

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.

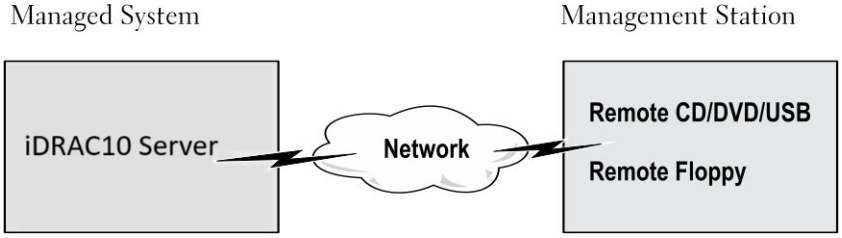


Abbildung 4. Setup für den virtuellen Datenträger

Themen:

- Unterstützte Laufwerke und Geräte
- Virtuellen Datenträger konfigurieren
- Auf virtuellen Datenträger zugreifen
- Einmalstart für virtuelle Datenträger aktivieren
- Remote-Dateifreigabe
- Startreihenfolge über das BIOS festlegen
- Zugriff auf Treiber

Unterstützte Laufwerke und Geräte

Die folgende Tabelle listet die Laufwerke auf, die durch den virtuellen Datenträger unterstützt werden.

Tabelle 52. Unterstützte Laufwerke und Geräte

Laufwerk	Unterstützte Speichermedien
Virtuelle optische Laufwerke	• ISO-Imagedatei • IMG-Imagedatei
USB-Flash-Festplatten	• USB-Schlüssel-Image im ISO9660-Format

Virtuellen Datenträger 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 Sie eine Sitzung mit einem virtuellen Datenträger ausführen. Andernfalls kann es zu unerwünschten Ergebnissen wie z. B. Datenverlust kommen.

1. Gehen Sie auf der iDRAC-Weboberfläche zu **Konfiguration** > **Virtuelle Datenträger** > **Verbundene Datenträger**.
2. Geben Sie die erforderlichen Einstellungen ein. 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` mit den Objekten in der Gruppe **iDRAC.VirtualMedia group**.

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

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. Gehen Sie hierfür folgendermaßen vor:

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 Abschnitt **Virtuelle Datenträger** je nach Anforderung **Trennen**, **Verbinden** oder **Automatisch verbinden** aus.
   Weitere Informationen zu den Optionen finden Sie in der **Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen**.
3. Klicken Sie auf **Zurück**, dann auf **Fertig stellen** und anschließend 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 53. Status des verbundenen Datenträgers und Systemantwort

Status des verbundenen Datenträgers	Systemreaktion
Trennen	Image konnte dem System nicht zugeordnet werden.
Beifügen	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 auf der Managementstation konfigurieren, damit leere Laufwerke angezeigt 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 Computerordner ausblenden** und klicken Sie auf **OK**.

Auf virtuellen Datenträger zugreifen

Sie können mit oder ohne Verwendung der virtuellen Konsole auf virtuelle Datenträger zugreifen. Bevor Sie auf virtuelle Datenträger zugreifen, stellen Sie sicher, dass Sie Ihre(n) Webbrowser konfigurieren.

Virtuelle Datenträger und RFS schließen sich gegenseitig aus. Wenn die RFS-Verbindung aktiv ist und Sie versuchen, den virtuellen Datenträger-Client zu starten, wird die folgende Fehlermeldung angezeigt: **Der virtuelle Datenträger steht derzeit nicht zur Verfügung. Eine virtuelle Datenträger- oder Remote-Dateifreigabe-Sitzung wird gerade ausgeführt.**

Virtuelle Datenträger und RFS schließen sich gegenseitig aus. Wenn die RFS-Verbindung aktiv ist und Sie versuchen, den virtuellen Datenträger-Client zu starten, wird die folgende Fehlermeldung angezeigt: `Virtual Media is currently unavailable. A Virtual Media or Remote File Share session is in use. If virtual media connected first then user can able to connect RFS1 also.`

Wenn die RFS-Verbindung nicht aktiv ist und Sie versuchen, den virtuellen Datenträger-Client zu starten, wird der Client erfolgreich gestartet. Sie können dann den virtuellen Datenträger-Client dazu verwenden, Geräte und Dateien den virtuellen Datenträgern zuzuweisen.

Eine .img-Datei, die über **virtuelle Konsole** > **virtuelle Datenträger oder eigenständige virtuelle Datenträger** zugeordnet ist, unterstützt keine Schreibvorgänge im Host-Betriebssystem.

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. Navigieren Sie in der iDRAC-Webschnittstelle zu **Konfiguration** > **Virtuelle Konsole**.
   Daraufhin wird die Seite **Virtuelle Konsole** angezeigt.
2. Klicken Sie auf **Virtuelle Konsole starten**.
   Der **Virtuelle Konsole-Viewer** wird gestartet.
3. Klicken Sie auf **Virtueller Datenträger** > **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 USB-angeschlossenes Gerät im Serverbetriebssystem mounten. So fügen Sie Images virtueller Datenträger hinzu:

1. Klicken Sie auf **Virtueller Datenträger** > **Abbild erstellen...**.
2. Klicken Sie im Feld **Quellordner** auf **Durchsuchen** und navigieren Sie zu der Datei oder dem Verzeichnis, die/das als Quelle für die Imagedatei verwendet werden soll. Die Imagedatei befindet sich auf der Managementstation oder auf Laufwerk C: des verwalteten Systems.
3. Der Standardpfad zur Speicherung der erstellen Imagedateien (normalerweise das Desktop-Verzeichnis) wird im Feld **Imagedateiname** angezeigt. Um diesen Speicherort zu ändern, klicken Sie auf **Durchsuchen** und navigieren Sie zum Speicherort.
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 Managementstation erstellt, auf der diese Funktion verwendet wird. Wenn diese **.img**-Datei verschoben oder gelöscht wird, funktioniert der entsprechende Eintrag für diesen Ordner im Menü **Virtuelle Datenträger** nicht. Es wird daher empfohlen, die **.img**-Datei nicht zu verschieben oder zu löschen während das **Image** verwendet wird. Die **.img**-Datei kann jedoch entfernt werden, nachdem die Auswahl des entsprechenden Eintrags aufgehoben und der Eintrag dann über **Image entfernen** entfernt wurde.

Details zum virtuellen Gerät anzeigen

Um die Details des virtuellen Geräts anzuzeigen, klicken Sie im Viewer der virtuellen Konsole auf **Tools** > **Statistik**. Im Fenster **Statistik** werden im Abschnitt **Virtuelle Datenträger** die zugeordneten virtuellen Geräte und die Lese-/Schreibaktivitäten für jedes Gerät

angezeigt. Wenn ein virtueller Datenträger angeschlossen ist, werden diese Informationen angezeigt. Wenn kein virtueller Datenträger angeschlossen ist, wird die Meldung „Virtueller Datenträger ist nicht angeschlossen“ angezeigt.

Wenn der virtuelle Datenträger ohne die virtuelle Konsole gestartet wird, dann wird der Abschnitt **Virtuelle Datenträger** als Dialogfeld angezeigt, das Informationen zu den zugeordneten Geräten anzeigt.

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 Nutzer 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 **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 virtuellen Datenträgern müssen Sie über Administratorrechte verfügen, um eine Betriebssystem-DVD oder eine USB-Flash-Festplatte (die 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
   - Externes Gerät zuordnen

   Die Option **DVD/CD zuordnen** kann für ISO-Dateien verwendet werden und die Option **Wechseldatenträger zuordnen** kann für Images mit eHTML5-basierten virtuellen Datenträgern verwendet werden. Die Option **Externes Gerät zuordnen** kann für die Zuordnung von physischen USB-Laufwerken 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 Nutzers). 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 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. Gehen Sie hierfür folgendermaßen vor:

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.

Leeren des Java-Cache

Im Falle unerwarteter Fehler bei der Verwendung von USB leeren Sie bitte den Java-Cache. Führen Sie die folgenden Schritte aus, um den Java-Cache zu leeren:

1. Klicken Sie im Java-Bedienfeld auf der Registerkarte **Allgemein** im Abschnitt **Temporäre Internetdateien** auf **Einstellungen**. Das Dialogfeld **Einstellungen für temporäre Dateien** wird angezeigt.
2. Klicken Sie im Dialogfeld „Einstellungen für temporäre Dateien“ auf **Dateien löschen**.

   Das Dialogfeld **Dateien und Anwendungen löschen** wird angezeigt.
3. Klicken Sie im Dialogfeld **Dateien und Anwendungen löschen** auf **OK**. Dadurch werden alle heruntergeladenen Anwendungen und Applets aus dem Cache gelöscht.
4. Klicken Sie im Dialogfeld **Einstellungen für temporäre Dateien** auf **OK**. Wenn Sie eine bestimmte Anwendung und ein bestimmtes Applet aus dem Cache löschen möchten, klicken Sie auf die Optionen „Anwendung anzeigen“ bzw. „Applet anzeigen“.

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 **Ja**.
   Das Häkchen für das Menüelement wird nicht angezeigt, was bedeutet, dass es dem Host-Server nicht zugeordnet ist.

ANMERKUNG: Nach dem Aufheben der Zuordnung eines an vKVM angeschlossenen USB-Geräts von einem Client-System mit Macintosh-Betriebssystem aus steht das nicht zugeordnete Gerät auf dem Client eventuell nicht zur Verfügung. Starten Sie das System neu oder mounten Sie das Gerät manuell auf dem Client-System, um das Gerät anzuzeigen.

ANMERKUNG: Um die Zuordnung eines virtuellen DVD-Laufwerks auf einem Linux-Betriebssystem aufzuheben, unmounten Sie das Laufwerk und werfen Sie es aus.

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 **Nutzer 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.

Remote-Dateifreigabe

Diese Funktion ist nur mit einer iDRAC Enterprise- oder Datacenter-Lizenz verfügbar.

RFS-Mounts können Schreibattributänderungen lesen und werden nur von racadm/redfish unterstützt.

ANMERKUNG: Stellen Sie vor der Verwendung von RFS sicher, dass Sie über eine minimale Netzwerkbandbreite von 1 MB/s verfügen.

Remote-Dateifreigabe 1 (RFS1)

Die Funktion Remote-Dateifreigabe 1 (RFS1) verwendet die Implementierung virtueller Medien in iDRAC.

Wenn eine Abbilddatei unter Verwendung der RFS1-Funktion bereitgestellt wird, sind beide virtuellen Laufwerke der virtuellen Datenträger für das Hostbetriebssystem sichtbar. Wenn eine **.img**-Datei zugeordnet ist, wird das virtuelle Disketten-/Festplattenlaufwerk verwendet, um die Abbilddatei dem Betriebssystem vorzulegen. Wenn eine **.iso**-Datei zugeordnet ist, wird das virtuelle CD/DVD-Laufwerk verwendet, um die Abbilddatei dem Betriebssystem vorzulegen. Das nicht verwendete virtuelle Laufwerk erscheint für das Betriebssystem als leeres Laufwerk. Der Client für virtuelle Datenträger kann Abbilder oder Festplatten beiden virtuellen Laufwerken zuordnen, aber RFS kann nur eines auf einmal verwenden. RFS und Funktionen des virtuellen Datenträgers schließen sich gegenseitig aus.

ANMERKUNG:

- RFS1 erscheint je nach verbundenem Bild als virtuelles optisches Laufwerk oder Diskettenlaufwerk, wenn keine aktive virtuelle Datenträger-Sitzung vorhanden ist.
- RFS1 erscheint als virtuelle Netzwerkdatei 1, wenn eine aktive virtuelle Datenträger-Sitzung vorhanden ist, da das virtuelle optische Laufwerk und die virtuellen Diskettenlaufwerke mit virtuellen Datenträgern aufgebraucht werden.

Alle erforderlichen Informationen eingeben und auf **Verbinden** klicken, um die Remote-Dateifreigabe 1 anzuschließen. Für die Trennung von der Remote-Dateifreigabe 1 auf **Trennen** klicken. Weitere Informationen zu den erforderlichen Feldinformationen finden Sie in der **Online-Hilfe** in der iDRAC-UI.

ANMERKUNG:

- Das iDRAC-Timeout für RFS-Verbindung beträgt 55 Sekunden. Wenn die Verbindung länger als 55 Sekunden dauert, wird der Timeout-Fehler angezeigt.
- Grundlegende Authentifizierung und Digest-Authentifizierung für HTTP/HTTPS-Freigaben werden unterstützt.

- **Verbinden** ist deaktiviert, wenn die RFS-Funktion nicht lizenziert ist. Die Option **Trennen** ist unabhängig vom Lizenzstatus immer verfügbar. Klicken Sie auf **Trennen**, um eine bestehende RFS-Verbindung zu trennen.

Szenarien

- Falls der virtuelle Datenträger-Client nicht gestartet wurde und Sie versuchen, eine RFS-Verbindung herzustellen, wird die Verbindung hergestellt, und das Remote-Abbild steht dem Hostbetriebssystem zur Verfügung.
- Falls die RFS-Verbindung nicht aktiv ist und Sie versuchen, den virtuellen Datenträger-Client zu starten, wird der Client erfolgreich gestartet. Sie können dann den virtuellen Datenträger-Client dazu verwenden, Geräte und Dateien den virtuellen Datenträgern zuzuweisen.
- Wenn die RFS1-Sitzung aktiv ist und Sie versuchen, eine vMedia-Verbindung herzustellen, wird die vMedia-Verbindung verweigert.
- Wenn der Client des virtuellen Datenträgers aktiv ist und Sie versuchen, eine RFS-Verbindung herzustellen, ist es möglich, dass das virtuelle optische Laufwerk/virtuelle Diskettenlaufwerk, das virtuellen Datenträgern und der virtuellen Netzwerkdatei1 zugewiesen ist, RFS zugewiesen wird.

Remote-Dateifreigabe 2 (RFS2)

Die Remote-Dateifreigabe 2 (RFS2) ist unabhängig von der RFS1 und virtuellen Datenträgern. Die RFS2 verfügt über eine eigene Kopie von Attributen unabhängig von der RFS1. Die RFS2 Image-Option verhält sich wie die vorhandene RFS1 auf allen iDRAC-Schnittstellen. Beide können unabhängig voneinander verbunden/getrennt werden. RFS2 wird über die Attribute „Aktiviert/Deaktiviert“ und „Verbindungsmodus RFS2“ gesteuert.

Um mit der virtuellen Netzwerkdatei 2 (RFS2) zu starten, wählen Sie **Virtuelle Netzwerkdatei 2** aus den Startoptionen aus. Der einmalige Start des virtuellen Datenträgers hat keine Auswirkungen auf die RFS2, wenn diese Option aktiviert ist.

Geben Sie die erforderlichen Informationen ein und klicken Sie auf **Verbinden**, um eine Verbindung zu RFS2 herzustellen, und klicken Sie auf **Trennen**, um die Verbindung zu RFS2 zu trennen.

Wenn Sie ein HTTPS-Zertifikat in RFS1 hochladen/löschen, wird das Zertifikat auch in RFS2 hochgeladen/gelöscht. Da dieses Zertifikat für die iDRAC-Identität bestimmt ist und für mehrere RFS- oder freigegebene Verbindungen gleich bleibt.

Der Verbindungsstatus für RFS ist im iDRAC-Protokoll verfügbar. Wenn eine Verbindung hergestellt wurde, wird ein über RFS bereitgestelltes virtuelles Laufwerke nicht getrennt, selbst wenn Sie sich beim iDRAC abmelden. Die RFS-Verbindung wird beendet, wenn der iDRAC zurückgesetzt wird oder die Verbindung zum Netzwerk abbricht.

Wenn Sie die iDRAC-Firmware während einer aktiven RFS-Verbindung aktualisieren und gleichzeitig der Virtual Media-Attach-Modus auf **Anhängen** oder **Automatisch anhängen** gesetzt ist, versucht iDRAC, die RFS-Verbindung erneut herzustellen, nachdem das Firmwareupdate abgeschlossen ist und iDRAC neu gestartet wird.

Wenn Sie die iDRAC-Firmware während einer aktiven RFS-Verbindung aktualisieren und gleichzeitig der Virtual Media-Attach-Modus auf **Entfernen** gesetzt ist, versucht iDRAC nicht, die RFS-Verbindung erneut herzustellen, nachdem das Firmwareupdate abgeschlossen ist und iDRAC neu gestartet wird.

ANMERKUNG:

- CIFS und NFS unterstützen IPv4- und IPv6-Adressen.
- Beim Herstellen einer Verbindung zu einer Remote-Dateifreigabe unter Verwendung von IPv6 durch die Angabe eines FQDN, muss IPv4 auf dem HTTPS-Server deaktiviert sein.
- Wenn der iDRAC sowohl mit IPv4 als auch mit IPv6 konfiguriert ist, kann der DNS-Server Datensätze enthalten, die den iDRAC-Hostnamen beiden Adressen zuordnen. Wenn die IPv4-Option in iDRAC deaktiviert ist, kann iDRAC möglicherweise nicht auf die externe IPv6-Freigabe zugreifen. Dies liegt daran, dass der DNS-Server eventuell noch IPv4-Einträge enthält und die DNS-Namensauflösung die IPv4-Adresse zurückgeben kann. In solchen Fällen wird empfohlen, die IPv4-DNS-Einträge vom DNS-Server zu löschen, wenn die IPv4-Option in iDRAC deaktiviert wird.
- Wenn Sie CIFS verwenden und Teil einer Active Directory-Domäne sind, geben Sie den Domänennamen mit der IP-Adresse im Imagedatei-Pfad ein.
- Wenn Sie von einer NFS-Freigabe auf eine Datei zugreifen, konfigurieren Sie die folgenden Freigabeberechtigungen. Diese Berechtigungen sind erforderlich, da iDRAC-Schnittstellen im Nicht-Root-Modus ausgeführt werden.
  - Linux: Stellen Sie sicher, dass die Freigabeberechtigungen mindestens auf **Lesen** für das Konto **Andere** festgelegt wurden.
  - Windows: Gehen Sie zur Registerkarte **Sicherheit** der Freigabeeigenschaften und fügen Sie **Jeder** zum Feld **Gruppen oder Nutzernamen** mit der Berechtigung **Lesen und ausführen** hinzu.
- Wenn ESXi auf dem verwalteten System ausgeführt wird und Sie ein Floppy-Abbild (**.img**) über die Remote-Dateifreigabe bereitstellen, ist das verbundene Floppy-Abbild auf dem ESXi-Betriebssystem nicht verfügbar.
- Nur englische ASCII-Zeichen werden in den Dateipfaden der Netzwerkfreigabe unterstützt.
- Die Funktion zum Auswerfen des Betriebssystems wird nicht unterstützt, wenn virtuelle Medien über RFS angeschlossen werden.

- RFS wird möglicherweise getrennt, wenn die iDRAC-IP-Adresse länger als 1 Minute nicht erreichbar ist. Versuchen Sie, erneut zu mounten, sobald das Netzwerk aktiv ist.
- Beim Angeben der Netzwerkfreigabe-Einstellungen wird empfohlen, für Nutzername und Kennwort Sonderzeichen zu vermeiden oder diese mit Prozentzeichen zu kodieren.
- Die folgenden Zeichen werden für die Felder **Nutzername**, **Kennwort** und **Image-Dateipfad** unterstützt:
  - A-Z
  - a-z
  - 0-9
  - Sonderzeichen: . _ - ? < > / \ :* | @
  - Leerzeichen
- Für HTTP verwenden Sie nicht die folgenden Zeichen: ! @ # % ^. Diese Zeichen werden mit anderen Freigabetypen unterstützt. Verwenden Sie jedoch zur Bewahrung der Kompatibilität die empfohlenen Zeichen.

Ordner mounten über RFS

iDRAC unterstützt das direkte Mount von Ordnern über RFS. Mit dieser Funktion können Sie Ordner direkt ohne Konvertierung an eine ISO/IMG-Datei anhängen.

ANMERKUNG:
- Diese Funktion ist mit der iDRAC Enterprise- oder Datacenter-Lizenz verfügbar.
- Die Ordneranbindung ist nur über NFS- und CIFS-Freigabe möglich. HTTP/HTTPS-Freigaben werden nicht unterstützt.
- Die Größe des anzuhängenden NFS-/CIFS-Ordners ist auf 1 GB und die maximale Anzahl der Unterordner auf 1.000 begrenzt.
- Es ist nicht möglich, einen leeren Ordner zuzuordnen.

In den folgenden Szenarien wird erläutert, wie RFS1 und RFS2 in der BIOS-Startreihenfolge aufgeführt werden:

Szenario 1:

Wenn virtuelle Datenträger bereits über die virtuelle Konsole angeschlossen sind, meldet die BIOS-Startreihenfolge Geräte je nach Image-Typ als **virtuelles optisches** oder **virtuelles Diskettenlaufwerk**. Wenn ein RFS 1-Gerät angeschlossen ist, wird es in der BIOS-Startreihenfolge als **virtuelle Netzwerkdatei 1** gemeldet. Für RFS 2-Geräte meldet die BIOS-Startreihenfolge dies als **virtuelle Netzwerkdatei 2**.

Szenario 2:

Wenn kein virtueller Datenträger angeschlossen ist und Sie ein RFS 1-Gerät anschließen, meldet die BIOS-Startreihenfolge es je nach Image-Typ als **Virtuelles optisches** oder **Virtuelles Diskettenlaufwerk**. Wenn Sie ein RFS 2-Gerät anschließen, wird es in der BIOS-Startreihenfolge als **Virtuelle Netzwerkdatei 2** gemeldet.

Szenario 3

Wenn kein virtueller Datenträger verbunden ist und RFS1 verbunden ist:

- Virtuelles optisches Laufwerk für ISO-Image
- Virtuelles Diskettenlaufwerk für IMG-Image

Virtuelle Datenträgersitzung ist blockiert, wenn die RFS1-Sitzung aktiv ist.

Wenn ein virtueller Datenträger verbunden ist und RFS1 verbunden ist, wird RFS1 als virtuelle Netzwerkdatei 1 für ISO/IMG-Image aufgeführt. Damit soll die Kompatibilität mit vorhandenen vMedia und RFS aufrechterhalten werden, was jeweils nur eine Option zulässt. RFS2 wird unabhängig von virtuellen Medien und RFS1 als **virtuelle Netzwerkdatei 2** aufgeführt.

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-Einstellungen** > **Starteinstellungen** > **BIOS-Starteinstellungen** > **Startsequenz**.

Im Pop-up-Fenster werden die virtuellen optischen Laufwerke, virtuellen Diskettenlaufwerke, virtuelle Netzwerkdatei 1 und virtuelle Netzwerkdatei 2 mit den Standardstartgeräten aufgeführt.

4. Stellen Sie sicher, dass das virtuelle Laufwerk aktiviert und als erstes Gerät mit startfähigen Datenträgern aufgeführt ist. Befolgen Sie bei Bedarf die Anweisungen auf dem Bildschirm, um die Startreihenfolge zu ändern.
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 verbunden ist und ein startfähiger Datenträger vorhanden ist, startet das System mit dem virtuellen Gerät. Andernfalls übersieht das System das Gerät – ähnlich wie ein physisches Gerät ohne startfähige Datenträger.

Zugriff auf Treiber

Dell Power Edge-Server verfügen im in den System integrierten Flash-Storage 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 Dell Supportseite herunterladen und installieren.

26

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

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 **Nutzer konfigurieren** und **Zugriff auf virtuelle Datenträger** sind für den Nutzer aktiviert.
- Die Netzwerkfreigabe enthält Treiber und eine startfähige Imagedatei für das Betriebssystem in einem branchenüblichen Standardformat, wie z. B. **.img**, **.iso** oder **Ordnerpfad**.

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.
2. Gehen Sie zu **Konfiguration** > **Systemeinstellungen** > **Hardwareeinstellungen** > **Erstes Startgerät**.
3. Legen Sie die Startreihenfolge in der Liste **Erstes Startgerät** fest, um einen virtuellen Datenträger wie Floppy, CD, DVD, ISO, virtuelle Netzwerkdatei 1 und virtuelle Netzwerkdatei 2 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.

Managen der Remote-Dateifreigaben

Mit der RFS-Funktion (Remote-Dateifreigabe) können Sie eine ISO- oder IMG-Image-Datei auf einer Netzwerkfreigabe festlegen, und diese dem Betriebssystem des verwalteten Servers als virtuelles Laufwerk zur Verfügung stellen, indem sie mithilfe von NFS, CIFS, HTTP oder HTTPS als CD oder DVD geladen wird. Die RFS-Funktion ist lizenziert.

Die Remote-Dateifreigabe unterstützt nur die Imagedatei-Formate **.img** und **.iso**. Eine **.img**-Datei wird als virtuelle Diskette und eine **.iso**-Datei als virtuelle CDROM umgeleitet.

Sie müssen über Virtuelle Datenträger-Berechtigungen verfügen, um RFS-Mounting durchführen zu können.

Diese Funktion ist nur mit einer iDRAC Enterprise- oder Datacenter-Lizenz verfügbar.

Remote-Dateifreigabe über die Web-Schnittstelle konfigurieren

So aktivieren Sie die Remote-Dateifreigabe:

1. Gehen Sie auf der iDRAC-Weboberfläche zu **Konfiguration** > **Virtuelle Datenträger** > **Verbundener Datenträger**.

Daraufhin wird die Seite **Verbundener Datenträger** angezeigt.

2. Wählen Sie unter **Verbundener Datenträger** die Option **Verbinden** oder **Automatisch Verbinden**aus.
3. Legen Sie unter **Remote-Dateifreigabe** den Dateipfad für das Image, den Domänennamen, Benutzernamen und das Kennwort fest. 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.

   ANMERKUNG: Die Zeichen, die in Benutzernamen und Kennwörtern für Netzwerkfreigaben zulässig sind, werden durch den Netzwerkfreigabetyp bestimmt. iDRAC unterstützt zulässige Zeichen in Anmeldeinformationen für die Netzwerkfreigabe, die vom Freigabetyp definiert sind, 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 beim Betrieb mit runlevel init 3 einen Befehl zum manuellen Bereitstellen erfordern. 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 **.iso-**Gerät) `/dev/scd0` und das Diskettengerät (virtuelles **.img**-Gerät) `/dev/sdc`.

   Für SLES ist das CD-Gerät `/dev/sr0` und das Diskettengerät /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
   ```

   Dadurch wird der Text zur Identifizierung des Geräts angezeigt (z. B. SCSI device sdc). Dieses Verfahren gilt auch für virtuelle Datenträger, wenn Sie Linux-Distributionen in runlevel init 3 verwenden. 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 zu Image herstellen

`-d`: Verbindung zu Image abbrechen

`-u` <Nutzername>: Nutzername für den Zugriff auf den freigegebenen Ordner

`-p` <Kennwort>: Kennwort für den Zugriff auf den freigegebenen Ordner

`-l` <Image_Speicherort>: Image-Speicherort auf der Netzwerkfreigabe; doppelte Anführungszeichen um den Speicherort setzen Beispiele für Image-Dateipfade finden Sie im Abschnitt „Konfigurieren der Remote-Dateifreigabe über die Webschnittstelle“.

`-s` : aktuellen Remote-Image-Status anzeigen

Anwendungsbeispiele

- CIFS-basierte RFS:

```
racadm remoteimage -c -u "user" -p "pass" -l //shrloc/foo.iso
```

- NFS-basierte RFS:

```
racadm remoteimage -c -u "user" -p "pass" -l <nfs ip>:/shrloc/foo.iso
```

- HTTP/HTTPS-basierte RFS:

```
racadm remoteimage -c -u "user" -p "pass" -l http://url/shrloc/foo.iso
```

```
racadm remoteimage -c -l https://url/shareloc/foo.iso
```

- Trennen Sie die Verbindung zum Remote-Image:

```
racadm remoteimage -d
```

- Anzeigen des aktuellen Remote-Image-Status:

```
racadm remoteimage -s
```

ANMERKUNG: Dieser Befehl unterstützt IPV4- und IPV6-Formate. IPV6 gilt für CIFS- und NFS-Remote-Freigaben.

ANMERKUNG: Die Optionen -u und -p sind obligatorisch, wenn der Freigabetyp cifs ist.

ANMERKUNG: Alle Zeichen einschließlich alphanumerischer Zeichen und Sonderzeichen sind als Teil des Nutzernamens, 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.

Um Hilfe beim Anzeigen der Eigenschaften einer Gruppe zu erhalten, führen Sie den Befehl – `racadm help get` aus.

Um Hilfe bei der Konfiguration der Eigenschaften einer Gruppe zu finden, führen Sie den Befehl – `racadm help set` aus.

`racadm>>help remoteimage2`

ANMERKUNG: remoteimage2 -- Macht ein Remote-ISO-Image auf dem Server verfügbar. Er erfordert eine Remote-Dateifreigabelizenz.

Verwendung

```
racadm remoteimage2 -c -u <user> -p <pass> -l <image_location>
racadm remoteimage2 -d
racadm remoteimage2 -s
```

Die Optionen sind:

`-c`: Verbindung zu Image herstellen

`-d`: Verbindung zu Image abbrechen

`-u` <Nutzername>: Nutzername für den Zugriff auf den freigegebenen Ordner

`-p` <Kennwort>: Kennwort für den Zugriff auf den freigegebenen Ordner

`-l` <Image_Speicherort>: Image-Speicherort auf der Netzwerkfreigabe; doppelte Anführungszeichen um den Speicherort setzen Beispiele für Image-Dateipfade finden Sie im Abschnitt „Konfigurieren der Remote-Dateifreigabe über die Webschnittstelle“.

`-s` : aktuellen Remote-Image-Status anzeigen

Anwendungsbeispiele

- CIFS-basierte RFS:

```
racadm remoteimage2 -c -u "user" -p "pass" -l //shrloc/foo.iso
```

- NFS-basierte RFS:

```
racadm remoteimage2 -c -u "user" -p "pass" -l <nfs ip>:/shrloc/foo.iso
```

- HTTP/HTTPS-basierte RFS:

```
racadm remoteimage2 -c -u "user" -p "pass" -l http://url/shrloc/foo.iso
```

```
racadm remoteimage2 -c -l https://url/shareloc/foo.iso
```

- Trennen Sie die Verbindung zum Remote-Image:

```
racadm remoteimage2 -d
```

- Anzeigen des aktuellen Remote-Image-Status:

```
racadm remoteimage2 -s
```

ANMERKUNG: Dieser Befehl unterstützt IPV4- und IPV6-Formate. IPV6 gilt für CIFS- und NFS-Remote-Freigaben.

ANMERKUNG: Die Optionen -u und -p sind obligatorisch, wenn der Freigabetyp cifs ist.

Um Hilfe beim Anzeigen der Eigenschaften einer Gruppe zu erhalten, führen Sie den Befehl – `racadm help get` aus.

Um Hilfe bei der Konfiguration der Eigenschaften einer Gruppe zu finden, führen Sie den Befehl – `racadm help set` aus.

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. 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-BIOS-Einstellungen** fest, indem Sie während des Startvorgangs auf <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.

27

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
- Systemintegrität

Themen:

- Diagnosekonsole verwenden
- POST-Codes anzeigen
- Videos zum Startvorgang und zur Absturzerfassung anzeigen
- Protokolle anzeigen
- Bildschirm „Letzter Systemabsturz“ anzeigen
- Anzeigen des Systemstatus
- Anzeigen für Hardwareprobleme
- Systemzustand anzeigen
- iDRAC-Neustart
- Löschen von System- und Nutzerdaten
- Zurücksetzen des iDRAC auf die Standardeinstellungen

Diagnosekonsole verwenden

iDRAC bietet einen Standardsatz an Netzwerkdiagnosetools, die den Tools ähneln, die in Microsoft Windows- oder Linux-basierten Systemen enthalten sind. Über die iDRAC-Weboberfläche können Sie auf die Netzwerk-Debugging-Tools zugreifen.

So rufen Sie die Diagnosekonsole auf:

1. Gehen Sie in der iDRAC-Weboberfläche zu **Wartung** > **Diagnose**.
   Daraufhin wird die Seite **Diagnosekonsolenbefehl** angezeigt.
2. Geben Sie im Textfeld **Befehl** einen Befehl ein, und klicken Sie auf **Senden**. 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. Alle Einstellungen verwerfen und Nutzernamen und Kennwort zurücksetzen

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-Storage gespeichert. Sie können die Ergebnisse dann mit dem racadm-Befehl `diagnostics export` in eine NFS-, CIFS-, HTTP- oder HTTP-Netzwerkfreigabe exportieren.

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 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 der automatisierten Remote-Diagnose und Exportieren der Ergebnisse über 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>
```

- Um die Diagnoseergebnisse zu exportieren, stellen Sie sicher, dass sich der Server im Status **Außerhalb von POST** und der LC im Status **Bereit** befindet. Um den Status des LC und Servers zu überprüfen, führen Sie den folgenden Befehl aus:

```
racadm getremoteservicesstatus
```

- 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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

POST-Codes anzeigen

POST-Codes zeigen den Fortschritt des System-BIOS an, indem sie die verschiedenen Phasen der Startreihenfolge von Power-on-Reset anzeigen, und ermöglichen, Fehler beim Systemstart zu diagnostizieren. Die Seite **POST-Codes** zeigt den letzten POST-Code des Systems vor dem Start des Betriebssystems an.

Gehen Sie zum Anzeigen der POST-Codes zu **Wartung** > **Troubleshooting** > **POST-Code**.

Die Seite **POST-Code** blendet die Systemzustandsanzeige, einen Hexadezimalcode sowie eine Beschreibung des Codes ein.

Videos zum Startvorgang und zur Absturzerfassung anzeigen

Sie können die folgenden Videoaufzeichnungen anzeigen:

- **Letzte drei Startzyklen** – Ein Startzyklusvideo protokolliert die Sequenz der Ereignisse für einen Startzyklus. Bei den Videos zum Startzyklus wird das jeweils neueste Video zuerst angezeigt.
- **Video zum letzten Absturz** – Ein Video zum letzten Absturz protokolliert die Sequenz der Ereignisse, die zum Ausfall geführt haben.

ANMERKUNG: Die Funktion „Video zum letzten Absturz“ ist standardmäßig aktiviert. Sie können diese Funktion je nach Bedarf aktivieren oder deaktivieren.

Hierbei handelt es sich um eine lizenzierte Funktion.

Der iDRAC zeichnet 50 Frames während der Startzeit auf. Die Wiedergabe der Startbildschirme erfolgt mit einer Geschwindigkeit von 1 Frame pro Sekunde. Wenn der iDRAC zurückgesetzt wird, ist das Starterfassungsvideo nicht verfügbar, da es im RAM gespeichert und gelöscht wird.

ANMERKUNG:

- Sie müssen über Berechtigungen für den Zugriff auf die virtuelle Konsole oder über Administratorberechtigungen verfügen, um die Videos zum Startvorgang und zu Abstürzen abzuspielen.
- Die Videoerfassungszeit, die im iDRAC-GUI-Videoplayer angezeigt wird, kann von der Videoerfassungszeit abweichen, die in anderen Videoplayern angezeigt wird Der iDRAC GUI Videoplayer zeigt die Uhrzeit in der iDRAC-Zeitzone an, während alle anderen Videoplayer die Uhrzeit in den jeweiligen Betriebssystem-Zeitzonen anzeigen.

ANMERKUNG:

- Der Grund für die Verzögerung bei der Verfügbarkeit der Starterfassungsdatei ist, dass der Starterfassungspuffer nach dem Start des Hosts nicht voll ist.
- Standardmäßige /inbox SLES/RHEL Video-Player unterstützen den MPEG-1-Video-Decoder nicht. Sie müssen einen Video-Player mit Unterstützung für den MPEG-Decoder installieren und die Dateien abspielen.
- Videos im MPEG-1-Format werden im integrierten Player von Mac OS nicht unterstützt.

Um den Bildschirm **Systemstartprotokoll** anzuzeigen, klicken Sie auf **Wartung** > **Troubleshooting** > **Videoerfassung**.

Auf dem Bildschirm **Videoerfassung** werden die Videoaufzeichnungen angezeigt. Weitere Informationen finden Sie in der **iDRAC-Online-Hilfe**.

ANMERKUNG: Wenn der integrierte Videocontroller deaktiviert ist und der Server über Add-on-Videocontroller verfügt, ist eine gewisse Latenz in Bezug auf die Starterfassung zu erwarten. Daher werden die Ende des POST-Nachrichten eines Videos in der nächsten Erfassung aufgezeichnet.

Konfigurieren der Videoerfassungs-Einstellungen

So konfigurieren Sie die Videoerfassungs-Einstellungen:

1. Gehen Sie auf der iDRAC-Weboberfläche zu **Wartung** > **Troubleshooting** > **Videoaufnahme**.
   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 in Anzeigen des Systemereignisprotokolls und Anzeigen des Lifecycle-Protokolls.

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 zeigt den Status der folgenden Komponenten im System an:

- Zusammenfassung
- Batterien
- Kühlung
- CPUs
- Frontblende
- Eingriff
- Speicher
- Netzwerkgeräte
- Netzteile
- Spannungen

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).
- Stetig 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`.

ANMERKUNG: Beim Hot-Removal des M.2-Laufwerks für BOSS N-1-Controller wird der Integritätsstatus des iDRAC-Dashboards gelb, aber die LED für die Vorder-/Rückseite des Servers bleibt blau.

Weitere Informationen finden Sie im RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

Anzeigen für Hardwareprobleme

Die Hardware-bezogenen Probleme lauten:

- Gerät kann nicht hochgefahren werden
- Laute Lüfter
- Verlust der Netzwerkkonnektivität
- Festplattenfehler
- Fehler des USB-Datenträgers
- Physische Beschädigung

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.
- Tauschen Sie die Festplatten oder die USB-Flash-Laufwerke aus.
- Schließen Sie die Strom- und Netzwerkkabel erneut an, oder tauschen Sie sie aus

Wenn das Problem weiterhin besteht, finden Sie im *Installations- und Service-Handbuch* auf der Seite Handbücher für PowerEdge konkrete Informationen zum Hardwaregerät.

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 der folgenden Komponenten in iDRAC anzeigen:

- Batterien
- CPUs
- Kühlung
- Eingriff
- Speicher
- Netzteile
- Wechselbarer Flash-Datenträger
- Spannungen
- Sonstiges

Klicken Sie einen beliebigen Komponentennamen im Abschnitt **Server-Zustand**, um die Details zu den jeweiligen Komponenten anzuzeigen.

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.

Zurücksetzen des iDRAC über RACADM

Verwenden Sie zum Neustarten von iDRAC den Befehl **racreset**.

Zum Zurücksetzen auf Standardbetrieb verwenden Sie die folgenden Befehle:

- Datei mit nutzerdefinierten 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`

Zurücksetzen des iDRAC über die iDRAC-Webschnittstelle

Führen Sie zum Zurücksetzen von iDRAC einen der folgenden Schritte über die iDRAC-Weboberfläche aus:

- Datei mit nutzerdefinierten 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 nutzerdefinierten Standardeinstellungen wird erstellt.
- Auf die Standardeinstellungen zurücksetzen:
  - Wenn der Job zum Hochladen der nutzerdefinierten 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 nutzerdefinierte Voreinstellungen zurückzusetzen.

Löschen von System- und Nutzerdaten

ANMERKUNG: Löschen von System- und Nutzerdaten wird von iDRAC-GUI nicht unterstützt.

Sie können Systemkomponenten und die Nutzerdaten für die folgenden Komponenten löschen:

- Zurücksetzen des BIOS auf die Standardeinstellungen
- Integrierte Diagnosefunktionen
- Integriertes Treiberpaket des Betriebssystems
- Lifecycle-Controller-Daten
- Zurücksetzen des iDRAC auf die Standardeinstellungen
- Überschreiben von Festplattenlaufwerken, die keine Unterstützung für Instant Secure Erase (ISE) bieten
- Controller-Cache zurücksetzen
- Löschen von Festplatten, SSDs und NVMes mit Unterstützung von ISE
- Löschen Sie alle 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 Standardeinstellung zurückgesetzt
- diag – Integrierte Diagnosefunktionen
- drvpack – Integriertes BS-Treiberpaket
- lcdata – Löscht die Lifecycle Controller-Daten
- idrac – iDRAC wird auf Standardeinstellung zurückgesetzt
- overwritepd – Überschreiben von Festplattenlaufwerken, die keine Unterstützung für Instant Secure Erase (ISE) bieten
- percnvcache – Controller-Cache wird zurückgesetzt
- secureerasepd – Löschen von Festplatten, SSDs und NVMes mit Unterstützung von ISE
- allapps – Löscht alle Betriebssystemanwendungen

ANMERKUNG: Beim sicheren Löschen wird die **iDRAC-Rollback-Firmware** nicht von der Partition gelöscht, wenn der Befehl `racadm systemerase lcdata` verwendet wird.

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 RACADM-CLI-Handbuch für Integrated Dell Remote Access Controller.

ANMERKUNG: Der Dell Tech Center-Link wird in der iDRAC-UI auf Systemen der Marke Dell angezeigt.

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.

ANMERKUNG: In den neuesten iDRAC-Versionen ist der Befehl `LCWipe` veraltet. Um den Systemlöschvorgang durchzuführen, führen Sie den Befehl `systemerase` aus.

Zurücksetzen des iDRAC auf die Standardeinstellungen

Sie können iDRAC mithilfe des Dienstprogramms für die iDRAC-Einstellungen oder der iDRAC-Weboberfläche 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 **Wartung** > **Diagnosen**.
   Daraufhin wird die Seite **Diagnoseprogramm Konsole** angezeigt.
2. Klicken Sie auf **iDRAC auf Standardeinstellungen zurücksetzen**.
   Der Fertigstellungsstatus wird in Prozent angezeigt. iDRAC wird neu gestartet und auf die Werkseinstellungen zurückgesetzt. Die iDRAC-IP-Adresse wird zurückgesetzt und ist nicht zugänglich. Sie können die IP-Adresse über die Frontblende oder das 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 **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.

28

Integration von SupportAssist im iDRAC

Mit SupportAssist können Sie SupportAssist-Erfassungen erstellen und andere SupportAssist-Funktionen zur Überwachung Ihres Systems und Rechenzentrums verwenden. iDRAC bietet einen Anwendungsschnittstelle für die Sammlung von Plattforminformationen, die es Support Services ermöglicht, Plattform- und Serverprobleme zu beheben. iDRAC hilft Ihnen, eine SupportAssist Erfassung des Servers zu erstellen und die Erfassung anschließend an einen Speicherort auf der Management Station (lokal) oder an einem freigegebenen Speicherort im Netzwerk wie FTP, Trivial File Transfer Protocol (TFTP), HTTP, HTTPS, Common Internet File System (CIFS) zu exportieren. Die Erfassung wird im Standard-ZIP-Format erstellt. Sie können diese Erfassung zur Fehlersuche oder Inventarsammlung an den technischen Support senden.

Themen:

- SupportAssist
- SupportAssist
- Erfassungsprotokoll
- Generieren der SupportAssist-Erfassung
- Erfassungsprotokoll

SupportAssist

ANMERKUNG: IDRAC10 unterstützt keine SupportAssist-Registrierung. Sie können OpenManage Enterprise oder Secure Connect Gateway für denselben Zweck verwenden.

Sie können eine Sammlung lokal oder in einem Netzwerk erzeugen und speichern.

SupportAssist

Sobald SupportAssist konfiguriert ist, können Sie das **Erfassungsprotokoll** über das SupportAssist-Dashboard aufrufen. Eine Registrierung ist nicht erforderlich, um das Erfassungsprotokoll einzusehen oder zu versenden.

Erfassungsprotokoll

Das **Erfassungsprotokoll** zeigt die Details von **Erfassungsdatum und -Uhrzeit, Erfassungstyp** (Manuell), **Erfasste Daten** (nutzerdefinierte Auswahl, alle Daten), **Erfassungsstatus** (abgeschlossen mit Fehlern, Abgeschlossen) und **Job-ID** an. Sie können die zuletzt in iDRAC gespeicherte Erfassung 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.

Generieren der SupportAssist-Erfassung

Zum Generieren der BS- und Anwendungsprotokolle muss das iDRAC-Servicemodul installiert sein und im Hostbetriebssystem ausgeführt werden.

ANMERKUNG: Die SupportAssist-Erfassung dauert mehr als 10 Minuten, wenn sie vom OS/iDRAC aus durchgeführt wird, während OMSA 10.1.0.0 damit ausgeführt wird.

Wenn Sie zusammen mit dem technischen Support ein Problem mit einem Server beheben müssen, Ihre Sicherheitsrichtlinien aber keine direkte Internetverbindung zulassen, können Sie dem technischen Support die notwendigen Daten zur Behebung des Problems zukommen lassen, ohne Software installieren oder Hilfsprogramme von Dell herunterladen zu müssen und ohne über Zugang zum Internet über das Betriebssystem oder iDRAC zu verfügen.

Sie können einen Zustandsbericht des Servers erstellen und dann das Protokoll der Sammlung exportieren:

- An einen Speicherort der Management Station (lokal).
- In eine Netzwerkfreigabe wie CIFS (Common Internet File System) oder NFS (Network File Share). Für den Export in eine Netzwerkfreigabe, wie z. B. CIFS oder NFS, ist eine direkte Netzwerkverbindung zum freigegebenen oder dedizierten iDRAC-Netzwerkport erforderlich.
- An Dell.

Die SupportAssist-Erfassung wird im Standard-ZIP-Format erstellt. Die Sammlung kann die folgenden Informationen enthalten:

- Hardwarebestand für alle Komponenten (umfasst Systemkomponentenkonfiguration und Firmware-Details, Hauptplatinen-Systemereignisprotokolle, iDRAC-Statusinformationen und Lifecycle Controller-Protokolle)
- Betriebssystem- und Anwendungsinformationen
- Speicher-Controller-Protokolle.
- iDRAC-Debug-Protokolle.
- Es enthält einen HTML5-Viewer, auf den zugegriffen werden kann, sobald die Sammlung abgeschlossen ist.
- Die Sammlung bietet eine große Menge an detaillierten Systeminformationen und Protokollen in einem nutzerfreundlichen Format, das geöffnet werden kann, ohne dass die Sammlung auf der Technischer-Support-Website hochgeladen werden muss.

Nachdem die Daten erstellt wurden, können Sie die Daten anzeigen, die mehrere XML-Dateien und Log-Dateien enthalten.

Jedes Mal, wenn eine Datenerfassung durchgeführt wird, wird ein Ereignis im Lifecycle Controller-Protokoll aufgezeichnet. Das Ereignis enthält Informationen wie der Nutzer, der den Bericht initiiert hat, die verwendete Schnittstelle sowie das Datum und die Uhrzeit des Exports.

Wenn WMI unter Windows deaktiviert ist, hält die OS Collector-Erfassung mit einer Fehlermeldung an.

Überprüfen Sie die entsprechenden Berechtigungsebenen und stellen Sie sicher, dass keine Firewall- oder Sicherheitseinstellungen verhindern, dass die Registrierungs- oder Softwaredaten erfasst werden.

Stellen Sie vor dem Generieren eines Funktionszustandreports Folgendes sicher:

- Lifecycle Controller ist aktiviert.
- Die Funktion Systembestandsaufnahme beim Neustart erfassen (CSIOR) ist aktiviert.
- Sie verfügen über Anmelde- und Serversteuerungsberechtigungen.

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 **Wartung** > **SupportAssist**.
2. Klicken Sie auf **Erfassung starten**.
3. Wählen Sie die Datensätze aus, die in die Sammlung aufgenommen werden müssen.
4. Sie können festlegen, die Sammlung nach personenbezogenen Daten (PII) zu filtern.
5. Wählen Sie das Ziel, in der die Erfassung gespeichert werden soll.
   a. Mit der Option **Lokal speichern** können Sie die generierte Erfassung auf dem lokalen System speichern.
   b. Mit der Option **Im Netzwerk speichern** wird die generierte Erfassung in einer benutzerdefinierten CIFS- oder NFS-Netzwerkfreigabe gespeichert.

      ANMERKUNG: Wenn **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 **Im Netzwerk speichern** ausgewählt ist, werden die vom Benutzer bereitgestellten Netzwerkdetails als Standardwerte (falls keine Netzwerkfreigabe zuvor gespeichert wurde) für künftige Erfassungen gespeichert.
6. Klicken Sie auf **Erfassen**, um mit der Erfassung fortzufahren.
7. Wenn Sie dazu aufgefordert werden, akzeptieren Sie die **Endnutzer-Lizenzvertrag (EULA)**, 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.

Erfassungsprotokoll

Das **Erfassungsprotokoll** zeigt die Details von **Erfassungsdatum und -Uhrzeit, Erfassungstyp** (Manuell), **Erfasste Daten** (nutzerdefinierte Auswahl, alle Daten), **Erfassungsstatus** (abgeschlossen mit Fehlern, Abgeschlossen) und **Job-ID** an. Sie können die zuletzt in iDRAC gespeicherte Erfassung 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.

29

Häufig gestellte Fragen

In diesem Abschnitt werden häufig gestellte Fragen zu den folgenden Themen aufgelistet:

- Systemereignisprotokoll
- Netzwerksicherheit
- Active Directory
- Einfache Anmeldung
- Smartcard-Anmeldung
- Virtuelle Konsole
- Virtueller Datenträger
- SNMP-Authentifizierung
- Storage-Geräte
- iDRAC Service Module
- RACADM
- Sonstiges

Themen:

- Betriebssystem
- Active Directory
- iDRAC Service Module
- Netzwerksicherheit
- RACADM
- Benutzerdefinierte Absender-E-Mail-Konfiguration für iDRAC-Warnmeldungen
- Smartcard-Anmeldung
- SNMP-Authentifizierung
- Single Sign-On
- Speichergeräte
- System-Ereignisprotokoll
- Virtuelle Konsole
- Virtueller Datenträger
- Sonstiges
- Proxyservereinstellungen
- Standardkennwort dauerhaft auf „calvin“ setzen

Betriebssystem

Anleitung zum Installieren des Betriebssystems mithilfe der iDRAC10-Erstversionen (1.10.17.00, 1.20.05.00)

Die Lifecycle Controller-Benutzeroberfläche wird auf iDRAC10 nicht unterstützt. Sie können das Betriebssystem mithilfe der iDRAC10 Core-Lizenz installieren.

Im Folgenden sind die Schritte zum Installieren des Betriebssystems aufgeführt:

1. Erstellen einer virtuellen Festplatte auf einem Dell RAID-Controller:
   a. Drücken Sie während des Systemstartvorgangs **F2** und rufen Sie das **System-Setup** auf.
   b. Klicken Sie auf **Geräteeinstellungen** und dann auf den RAID-Controller.
   c. Klicken Sie auf **Hauptmenü** > **Konfigurationsmanagement**.
   d. Klicken Sie auf **Virtuelles Laufwerk erstellen**.
   e. Wählen Sie die entsprechenden Optionen aus, um die Parameter des virtuellen Laufwerks zu definieren.

f. Klicken Sie auf **Physikalisches Laufwerk auswählen** und wählen Sie die entsprechenden Laufwerke aus.
g. Klicken Sie auf **Änderungen anwenden** und dann auf **OK**.
h. Klicken Sie auf **Virtuelles Laufwerk erstellen**.
i. Klicken Sie auf **Bestätigen** und anschließend auf **Ja**. Das virtuelle Laufwerk wird erstellt.

2. Installieren Sie das Betriebssystem von der DVD:
   a. Legen Sie die Installations-DVD des Betriebssystems ein.
   b. Starten Sie von der DVD, um den Installationsvorgang des Betriebssystems zu starten.
3. Laden Sie die fehlenden Laufwerke herunter und installieren Sie das Betriebssystem:
   a. Laden Sie die erforderlichen Treiber für das Betriebssystem von der Dell Support-Website herunter.
   b. Kopieren Sie die heruntergeladene Datei auf ein USB-Laufwerk.
   c. Wenn Sie während der Installation des Betriebssystems zur Eingabe von Treibern aufgefordert werden, schließen Sie das USB-Laufwerk an und laden Sie die Treiber davon.

Active Directory

Die Active Directory-Anmeldung ist fehlgeschlagen. Wie kann dieses Problem behoben werden?

Um das Problem zu diagnostizieren, klicken Sie auf der Seite **Active Directory-Konfiguration und -Verwaltung** auf **Einstellungen testen**. Überprüfen Sie die Testergebnisse und beheben Sie das Problem. Ändern Sie die Konfiguration und führen Sie den Test solange durch, bis der Testnutzer den Autorisierungsschritt erfolgreich abschließt.

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-Nutzerkonto verfügen, melden Sie sich mit den lokalen Zugangsdaten beim iDRAC 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 Nutzer und das iDRAC-Objekt in unterschiedlichen Domänen befinden, wählen Sie nicht die Option **Nutzerdomäne von Anmeldung** aus. Wählen Sie stattdessen die Option **Eine Domäne angeben** aus und geben Sie den Namen der Domäne ein, in der das iDRAC-Objekt verfügbar ist.
- Überprüfen Sie die SSL-Zertifikate des Domänen-Controllers, um sicherzustellen, dass die iDRAC-Zeit innerhalb der Gültigkeitsdauer des Zertifikats liegt.

Die Active Directory-Anmeldung schlägt fehl, auch wenn die Zertifikatsüberprüfung aktiviert ist. Die Testergebnisse zeigen die folgende Fehlermeldung an. Warum tritt dieses Verhalten auf und wie kann es behoben 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 Zertifikatsüberprüfung aktiviert ist und iDRAC die SSL-Verbindung mit dem Verzeichnisserver herstellt, 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 der Gültigkeitsdauer des Serverzertifikats oder Zertifizierungsstellenzertifikats. Überprüfen Sie die iDRAC-Zeit und die Gültigkeitsdauer Ihres Zertifikats.
- Die in iDRAC konfigurierten Domain Controller-Adressen stimmen nicht mit dem Antragstellernamen oder alternativen Antragstellernamen des Verzeichnisserverzertifikats überein. Wenn Sie eine IP-Adresse verwenden, gehen Sie zur nächsten Frage. Wenn Sie einen FQDN verwenden, stellen Sie sicher, dass Sie den FQDN des Domain Controllers und nicht der Domäne verwenden. Beispiel: **servername.example.com** anstatt **example.com**.

Die Zertifikatsüberprüfung schlägt fehl, auch wenn als Domain Controller-Adresse die IP-Adresse verwendet wird. Wie kann dieses Problem behoben werden?

Überprüfen Sie das Feld „Antragstellername“ oder „Alternativer Antragstellername“ in Ihrem Domain Controller-Zertifikat. Normalerweise verwendet Active Directory den Hostnamen und nicht die IP-Adresse des Domain Controllers im Feld „Antragstellername“ oder „Alternativer Antragstellername“ des Domain Controller-Zertifikats. Gehen Sie folgendermaßen vor, um das Problem zu beheben:

- Konfigurieren Sie als **Adresse(n) des Domain Controllers** den Hostnamen (FQDN) des Domain Controllers auf dem iDRAC, damit er mit dem Antragstellernamen bzw. dem alternativen Antragstellernamen des Serverzertifikats 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 NutzerInnen und Rollengruppen verschiedenen Domänen angehören, sind Adressen des globalen Katalogs erforderlich. In diesem Fall können Sie nur die universelle Gruppe verwenden.

Wenn Sie das Standardschema verwenden und alle Nutzer 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 zuerst eine Verbindung zu den konfigurierten Domain Controller-Adressen her. Wenn sich die NutzerInnen und Rollengruppen in dieser Domäne befinden, werden die Berechtigungen gespeichert.

Wenn globale Controller-Adressen konfiguriert sind, fragt iDRAC weiterhin den globalen Katalog ab. Wenn zusätzliche Berechtigungen aus dem globalen Katalog abgerufen werden, werden diese Berechtigungen akkumuliert.

Verwendet iDRAC immer LDAP über SSL?

Ja. Der gesamte Datentransfer erfolgt über den sicheren Port 636 und/oder 3269. Beim Testen der Einstellungen 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 setzt hohe Sicherheitsstandards durch, um die korrekte Identität des Domain Controllers zu gewährleisten, mit dem iDRAC eine Verbindung herstellt. Ohne eine Zertifikatsüberprüfung können HackerInnen einen Domain Controller fälschen und die SSL-Verbindung kapern. Wenn Sie sich dafür entscheiden, allen Domain Controllern innerhalb Ihrer Sicherheitszone ohne Zertifikatsüberprüfung zu vertrauen, können Sie die Funktion über die Weboberfläche 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.

Das Active Directory ist für eine Domäne konfiguriert, die im Windows Server 2008-Active Directory vorhanden ist. Für die Domäne ist eine untergeordnete Domäne vorhanden, der Nutzer und die Gruppe befinden sich in dieser untergeordneten Domäne und der Nutzer ist Mitglied dieser Gruppe. Beim Versuch, sich mit dem in der untergeordneten Domäne vorhandenen Nutzer beim iDRAC anzumelden, schlägt die Single Sign-On-Anmeldung beim Active Directory fehl.

Dies kann an einem falschen Gruppentyp liegen. Es gibt zwei Gruppentypen im Active Directory-Server:

- Sicherheit – Sicherheitsgruppen ermöglichen Ihnen, den Nutzer- und Computerzugriff auf freigegebene Ressourcen zu managen und Gruppenrichtlinieneinstellungen zu filtern.
- Verteilung – Verteilungsgruppen sind nur als E-Mail-Verteilerlisten vorgesehen.

Stellen Sie immer sicher, dass der Gruppentyp „Sicherheit“ lautet. Sie können keine Verteilungsgruppen verwenden, um Berechtigungen für ein Objekt zuzuweisen. Sie können sie jedoch für das Filtern der Gruppenrichtlinieneinstellungen verwenden.

iDRAC Service Module

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.

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 Windows-Systemen: Öffnen Sie die **Systemsteuerung** und überprüfen Sie, ob das iDRAC Service Module in der Liste der installierten Programme angezeigt wird.
- Auf Linux-Systemen: 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 Service Module 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 Benutzer mindestens haben, um das iDRAC Service Module installieren zu können?

Zum Installieren des iDRAC Service Module müssen Sie über Administratorrechte verfügen.

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 54. 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	U	0	0	0 em1
Link-lokal	0.0.0.0	255.255.255.0	U	0	0	0 em1
Link-lokal	0.0.0.0	255.255.255.0	U	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.

Wo befindet sich das replizierte Lifecycle-Protokoll im Betriebssystem?

So zeigen Sie die replizierten Lifecycle-Protokolle an:

Tabelle 55. Speicherort für Lifecycle-Protokolle

Betriebssystem	Position
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 Das *iDRAC-Servicemodul-Benutzerhandbuch* ist verfügbar auf der Seite iDRAC-Handbücher..

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 auf 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.

RACADM

Wenn nach dem Zurücksetzen eines iDRAC (über den Befehl „racadm racreset“) ein Befehl eingegeben wird, wird die folgende Meldung angezeigt. Worauf weist dies hin?

```
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 die offiziellen openssl- und libopenssl-Versionen installiert sind. Führen Sie für die Installation der RPM-Pakete den folgenden Befehl aus:

```
rpm -ivh --force < filename >
```

wobei `filename` die openssl- oder libopenssl-rpm-Paketdatei ist.

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 sie über `racadm set -f <config file>` geändert wird.
- 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 tritt auf, weil der Vorgang zum Erstellen einer Partition ausgeführt wird. Die Partition wird jedoch nach einiger Zeit gelöscht und es wird eine Meldung angezeigt, dass die Partition gelöscht wurde. Wenn nicht, warten Sie, bis der Vorgang zum Erstellen der Partition abgeschlossen ist, und löschen Sie dann die Partition.

Benutzerdefinierte Absender-E-Mail-Konfiguration für iDRAC-Warnmeldungen

Die generierte E-Mail-Benachrichtigung ist nicht von der nutzerdefinierten Absender-E-Mail auf dem cloudbasierten E-Mail-Service.

Sie müssen Ihre Cloud-E-Mail über diesen Prozess registrieren: Support.google.com.

Smartcard-Anmeldung

Bei Verwendung der Active Directory Smart-Card-Anmeldung dauert es bis zu vier Minuten, um sich am iDRAC anzumelden.

Die normale Active Directory-Smartcard-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. iDRAC meldet Sie unter Verwendung des alternativen DNS-Servers an.

Falsche Smartcard-PIN

Überprüfen Sie, ob die Smartcard aufgrund zu vieler Versuche mit einer falschen PIN gesperrt ist. Wenden Sie sich in solchen Fällen an den Kartenaussteller im Unternehmen, um eine neue Smartcard zu erhalten.

SNMP-Authentifizierung

Warum wird die Meldung „Remote-Zugriff: SNMP-Authentifizierungsfehler“ angezeigt?

Im Rahmen der Ermittlung versucht der IT Assistant, die Community-Namen „get“ und „set“ des Geräts zu überprüfen. Im IT Assistant ist der „get“-Community-Name = „öffentlich“ und der „set“-Community-Name = „privat“. Standardmäßig ist der Community-Name des SNMP-Agent für den iDRAC-Agent „öffentlich“. Wenn der IT Assistant eine „set“-Anfrage sendet, erzeugt der iDRAC-Agent diesen SNMP-Authentifizierungsfehler, da Anfragen nur von Community = „öffentlich“ akzeptiert werden.

Um zu verhindern, dass SNMP-Authentifizierungsfehler erzeugt werden, müssen Sie Community-Namen eingeben, die vom Agent akzeptiert werden. Da der iDRAC nur einen Community-Namen zulässt, müssen Sie denselben „get“- und „set“-Community-Namen für die Einrichtung der IT Assistant-Ermittlung verwenden.

Single Sign-On

Die SSO-Anmeldung schlägt auf Windows Server 2008 R2 x64 fehl. Welche Einstellungen sind zum Lösen dieses Problems erforderlich?

1. Führen Sie **technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** für den Domain Controller und die Domänenrichtlinie aus.
2. Konfigurieren Sie die Computer zur Verwendung der DES-CBC-MD5-Cipher-Suite.

   ANMERKUNG: Diese Einstellungen können sich auf die Kompatibilität mit Client-Computern oder Services und Anwendungen in Ihrer Umgebung auswirken. Die zulässigen Verschlüsselungskonfigurationstypen für die Kerberos-Richtlinieneinstellung sind unter **Computerkonfiguration** > **Sicherheitseinstellungen** > **Lokale Richtlinien** > **Sicherheitsoptionen** zu finden.

3. Stellen Sie sicher, dass die Domänen-Clients über das aktualisierte 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 Nutzer mit Administratorrechten an.
2. Navigieren Sie zu **Start** und führen Sie **gpedit.msc** aus. Das Fenster **Editor für lokale Gruppenrichtlinien** wird angezeigt.
3. Gehen Sie zu **Lokale Computereinstellungen** > **Windows-Einstellungen** > **Sicherheitseinstellungen** > **Lokale Richtlinien** > **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 **Editor für lokale Gruppenrichtlinien** zu **Lokale Computereinstellungen** > **Windows-Einstellungen** > **Sicherheitseinstellungen** > **Lokale Richtlinien** > **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. Navigieren Sie zu **Start** und führen Sie cmd aus. Das Eingabeaufforderungsfenster wird angezeigt.
5. Führen Sie den folgenden Befehl aus: `gpupdate /force`. Die Gruppenrichtlinien werden aktualisiert. Schließen Sie das Eingabeaufforderungsfenster.
6. Navigieren Sie zu **Start** und führen Sie regedit aus. Das Fenster **Registrierungseditor** wird angezeigt.
7. Navigieren Sie zu **HKEY_LOCAL_MACHINE** > **System** > **CurrentControlSet** > **Control** > **LSA**.
8. Klicken Sie mit der rechten Maustaste in den rechten Fensterbereich und wählen Sie **Neu** > **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 **Wert** die Zahl **1** ein und klicken Sie auf **OK**.
12. Schließen Sie das Fenster **Registry Editor**. Sie können sich jetzt unter Verwendung der SSO am iDRAC anmelden.

Wenn Sie SSO für iDRAC aktiviert haben und Internet Explorer zur Anmeldung beim iDRAC verwenden, schlägt SSO fehl und Sie werden aufgefordert, Ihren Nutzernamen und Ihr Kennwort einzugeben. Wie kann dieses Problem behoben werden?

Stellen Sie sicher, dass die iDRAC-IP-Adresse unter **Extras** > **Internetoptionen** > **Sicherheit** > **Vertrauenswürdige Websites** aufgeführt ist. Wenn sie nicht aufgeführt ist, schlägt SSO fehl und Sie werden aufgefordert, Ihren Nutzernamen und Ihr Kennwort einzugeben. Klicken Sie auf **Abbrechen** und fahren Sie fort.

Speichergeräte

OpenManage Storage Management zeigt mehr Storage-Geräte als der iDRAC an. Warum?

iDRAC zeigt Informationen nur für die von CEM (Comprehensive Embedded Management) unterstützten Geräte an.

Für externe JBODs/Einblicke hinter dem HBA wird eine EEMI-Meldung für die Entfernung des SAS-Anschlusses/IOM mit der EEMI-Meldungs-ID ENC42 erzeugt. Die EEMI-Meldungen ENC41 und ENC1 für die Wiederherstellung des SAS-Anschlusses/IOM werden jedoch nicht erzeugt.

So überprüfen Sie die Wiederherstellung des IOM auf der iDRAC-Weboberfläche:

1. Gehen Sie zu **Storage** > **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.

Warum unterscheidet sich die Seriennummer, die auf dem PCIe-Gerät aufgedruckt ist, von der in der iDRAC-GUI?

Geräte, die auf der PCIe-Basisklasse basieren, können unterschiedliche Typen und Formfaktoren aufweisen. In diesen Szenarien unterscheiden sich die Seriennummern der Geräteform möglicherweise von denen eines PCIe-Basisgeräts. Zum Beispiel können NVMe-Laufwerke, NIC-Karten usw. abgeleitete Formen von PCIe-Geräten sein.

System-Ereignisprotokoll

Warum verwendet SEL während der Verwendung der iDRAC-Webschnittstelle über den Internet Explorer nicht die Option „Speichern unter“?

Dies liegt an einer Browser-Einstellung. So können Sie das Problem lösen:

1. Gehen Sie im Internet Explorer zu **Tools** > **Internetoptionen** > **Sicherheit** und wählen Sie die Zone aus, in die Sie versuchen herunterzuladen. Wenn sich das iDRAC-Gerät beispielsweise im lokalen Intranet befindet, wählen Sie **Lokales Intranet** aus und klicken Sie auf **Benutzerdefiniertes Level...**.
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.

Virtuelle Konsole

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 Nutzer 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 Nutzer das Video aus- oder einschalten?

Wenn die lokale Konsole deaktiviert ist, kann der lokale Nutzer das Video nicht aus- oder einschalten.

Werden beim Ausschalten des lokalen Videos auch die lokale Tastatur und Maus ausgeschaltet?

Anzahl

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-Nutzer erforderlich, um das lokale Server-Video ein- oder auszuschalten?

Sämtliche Nutzer 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:

- Gehen Sie zur Registerkarte**Extras** > **Sitzungsoptionen** > **Maus**. Wählen Sie unter **Mausbeschleunigung Linux** 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 Nutzer 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 Nutzer auf den Managed Server zugreift, wird dem ersten Nutzer eine Warnmeldung angezeigt?

Nein. Wenn ein/e lokale/r NutzerIn 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 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.

Warum kann der Linux S-Abf-Schlüssel nicht mit Internet Explorer verwendet werden?

Das Verhalten der Linux 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.

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 oder virtuelle Diskette 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 werden als Composite-USB-Gerät mit dem Host-USB-Bus verbunden und nutzen einen gemeinsamen USB-Anschluss. Immer, wenn ein virtueller Datenträger mit dem Host-USB-Bus verbunden oder vom Host getrennt wird, werden alle virtuellen Datenträger kurzzeitig vom Host-USB-Bus getrennt und dann erneut verbunden. Verbinden oder trennen Sie keine virtuellen Datenträger, 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.

Sonstiges

Für HBM-CPUs (High Bandwidth Memory) im HBM-Modus wird der MemoryRollupStatus als „Unbekannt“ angezeigt.

Für den reinen HBM-Modus sind arbeitsspeicherbezogene Daten, die im HW-Bestand, Sensoren, Telemetrie usw. gemeldet werden, nicht verfügbar. Sie sollten dies nicht als fehlerhafte Konfiguration betrachten. Für Schnittstellen, die alle einzelnen DIMM-Steckplatzsensoren melden, werden sie mit dem Status „Unbekannt“ gemeldet. Auf ähnliche Weise kann der max. DIMM-Temperatursensor auch weiterhin mit unbekanntem Status gemeldet werden.

Beim Versuch, den iDRAC mit einem anderen Netzwerk zu verbinden, erhält der iDRAC keine andere IP-Adresse aus dem neuen Subnetz.

Stellen Sie sicher, dass das Netzwerkkabel mindestens fünf Sekunden lang vom iDRAC getrennt ist.

Nach dem Zurücksetzen von iDRAC werden in der iDRAC UI 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 nicht automatisch angezeigt oder geändert.

Es gibt zwei Szenarien:

- Szenario 1: iDRAC zeigt nach der Installation eines Betriebssystems nicht den aktuellen Hostnamen an. Sie müssen OMSA oder iSM zusammen mit iDRAC installieren, damit der aktuelle Hostname abgerufen wird.
- Szenario 2: iDRAC hatte einen Hostnamen für ein bestimmtes Betriebssystem, dann wurde ein anderes Betriebssystem installiert und es erscheint weiterhin der alte Hostname. Der Grund hierfür ist, dass der Hostname vom Betriebssystem kommt, der iDRAC speichert diese Informationen nur. Nach der Installation eines neuen Betriebssystems setzt der iDRAC den Wert des Hostnamens nicht zurück. Neuere Betriebssystemversionen können jedoch den Hostnamen in iDRAC beim ersten Betriebssystemstart aktualisieren.

Die iDRAC-Netzwerkverbindung funktioniert nicht.

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 den 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, ist das gemeinsame LOM möglicherweise funktionsfähig, 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.

Wie können ein iDRAC-Administrator-Nutzername und das zugehörige Kennwort abgerufen werden?

Sie müssen die Standardeinstellungen des iDRAC wiederherstellen. Weitere Informationen finden Sie unter iDRAC auf die Werkseinstellungen zurücksetzen.

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 unzugänglich.
- Die Video-Riser-Karte fehlt oder ist falsch eingesteckt.

Weitere Informationen finden Sie, wenn Sie über die iDRAC-Webschnittstelle 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 in den 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 für eingebettete Netzwerkadapter nicht 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.

Proxyservereinstellungen

Konfigurieren von Proxyservereinstellungen in der RACADM-CLI und der Redfish API

In RACADM müssen die folgenden LC-Attribute festgelegt werden, um den Proxyserver zu konfigurieren:

- LifeCycleController.LCAttributes.UserProxyPassword
- LifeCycleController.LCAttributes.UserProxyPort
- LifeCycleController.LCAttributes.UserProxyServer
- LifeCycleController.LCAttributes.UserProxyType

- LifeCycleController.LCAttributes.UserProxyUserName

Weitere Informationen zum Ausführen dieser Befehle finden Sie im **CLI-Handbuch zum Integrated Dell Remote Access Controller**.

Bei Verwendung von HTTP mit einem Proxy ist die Verbindung zwischen dem iDRAC und dem Proxy nicht so sicher wie die Verbindung zwischen dem iDRAC und dem HTTPS-Server. Der `UserProxyServer` ist ein wichtiges Attribut. Wenn es nicht festgelegt ist, können die anderen Attribute nicht verwendet werden. Der Vorteil der Verwendung von RACADM und der Redfish API besteht darin, dass Sie nicht jedes Mal das Kennwort eingeben müssen, wenn Sie den Proxyserver verwenden.

Führen Sie in der Redfish API einen Patch-Vorgang mit dem URI `/redfish/v1/Managers/<Manager-ID>/Oem/Dell/DellAttributes/<Dell-attributes-ID>` durch, um den Proxyserver zu konfigurieren.

Konfigurieren von Proxyservereinstellungen in der iDRAC-Benutzeroberfläche

In der iDRAC-Benutzeroberfläche können Sie die Proxy-Einstellungen auf allen Seiten aktualisieren, auf denen der Proxy-Server erforderlich ist. Selbst wenn Sie die Proxy-Einstellungen über RACADM und die Redfish API eingerichtet haben, können Sie die Proxy-Einstellungen in der iDRAC-Benutzeroberfläche aktualisieren. So konfigurieren Sie die Proxy-Einstellungen auf der Seite **Systemupdate**:

1. Klicken Sie auf **Wartung** > **Systemupdate** > **Manuelles Update**.
2. Wählen Sie unter **Manuelles UpdateHTTPS** unter **Speicherorttyp** aus.
3. Wählen Sie unter **Proxyserver aktivieren** die Option **Aktiviert** aus.
4. Geben Sie **Server**, **Port**, **Nutzername** und **Kennwort** ein.
5. Wählen Sie **Typ** aus und klicken Sie auf **Proxyeinstellungen als Standard speichern**.

ANMERKUNG: Sie können Proxy-Einstellungen auf jeder beliebigen Seite konfigurieren, z. B. **Lifecycle-Protokoll exportieren**, **Automatisches Update**, **SupportAssist-Erfassungseinstellungen**, **Serverkonfigurationsprofil-Import** und **Serverkonfigurationsprofil-Export**.

ANMERKUNG: Standardmäßig ist **Proxy-Einstellungen aktivieren** in der iDRAC-Benutzeroberfläche deaktiviert. Dies wird nach jeder Verwendung auf „deaktiviert“ zurückgesetzt. Weitere Informationen finden Sie in der **Onlinehilfe zum Integrated Dell Remote Access Controller (iDRAC)**.

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 die dauerhafte Änderung der Jumper-Einstellungen wird das Standardkennwort auf 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 Dell Supportseite.

30

Anwendungsfallszenarien

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 Systemereignisprotokolls und Lifecycle-Protokolls
- Schnittstellen zum Aktualisieren der iDRAC-Firmware
- Ordnungsgemäßes Herunterfahren
- Neues Administratorbenutzerkonto erstellen
- Starten der Server-Remote-Konsole und Mounten eines USB-Laufwerks
- Bare Metal-Betriebssystem über verbundenen virtuellen Datenträger und Remote-Dateifreigabe installieren
- Rack-Dichte managen
- Neue elektronische Lizenz installieren
- Anwenden der E/A-Identitätskonfigurationseinstellungen für mehrere Netzwerkkarten über Einzel-Host-Systemneustart

Fehler auf einem Managed System beheben, auf das nicht zugegriffen werden kann

Nach dem Empfang von Warnmeldungen von OpenManage Essentials, der Dell Management Console oder einem lokalen Trap-Collector sind fünf Server in einem Rechenzentrum aufgrund von Problemen wie einem nicht mehr reagierenden Betriebssystem oder Server nicht mehr zugänglich. Daher ist es erforderlich, die Ursache zu ermitteln, um den Fehler zu beheben und den Server über 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:

- Server-LED-Status – Blinkt gelb oder leuchtet dauerhaft gelb.
- Das Betriebssystem-Image wird in der virtuellen Konsole angezeigt. Wenn das Image angezeigt wird, setzen Sie das System zurück (Warmstart) und melden Sie sich erneut an. Wenn Sie sich anmelden können, ist das Problem behoben.
- Bildschirm „Letzter Absturz“
- Capture-Video beim Startvorgang
- Absturzvideo-Capture
- Serverzustand – Rote **x**-Symbole für die Systemkomponenten, bei denen Fehler vorliegen.
- Storage-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 auf der iDRAC-Weboberfläche zu **Übersicht** > **Zusammenfassung**, um die Systeminformationen anzuzeigen, und verwenden Sie die Links auf dieser Seite, um den Systemzustand zu überprüfen.
- 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 Systemereignisprotokolls und Lifecycle-Protokolls

So zeigen Sie das Lifecycle-Protokoll und das Systemereignisprotokoll (SEL) an und exportieren diese:

1. Gehen Sie auf der iDRAC-Weboberfläche zu **Wartung** > **Systemereignisprotokoll**, um das SEL anzuzeigen, und zu **Lifecycle-Protokoll**, um das Lifecycle-Protokoll anzuzeigen.

   ANMERKUNG: Das SEL wird auch im Lifecycle-Protokoll aufgezeichnet. Verwenden Sie die Filteroptionen, um das SEL anzuzeigen.

2. Exportieren Sie das SEL oder das Lifecycle-Protokoll im XML-Format an einen externen Speicherort (Managementstation, USB, Netzwerkfreigabe usw.). Alternativ können Sie die Remote-Systemprotokollierung aktivieren, sodass alle Protokolle, die in das Lifecycle-Protokoll geschrieben werden, gleichzeitig auch auf die konfigurierten Remoteserver geschrieben werden.
3. Wenn Sie das iDRAC Service Module 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
- Dell Update Package (DUP)
- Lifecycle Controller
- Dell Remote Access Configuration Tool (DRACT)

Ordnungsgemäßes Herunterfahren

Die Software leitet ein ordnungsgemäßes Herunterfahren ein, indem der Server ausgeschaltet wird, sodass das Betriebssystem Prozesse sicher stoppen kann. Außerdem werden die PCIe-Steckplätze ausgeschaltet. Daher reagieren die Adapter in PCIe-Steckplätzen nicht auf NC-SI-Steuerbefehle.

Wenn auf die Befehle nicht reagiert wird, behandelt das NIC-CEM-Modul die Adapter als nicht reagierend und protokolliert HWC8607 in den LCLOGs (Lifecycle Controller Logs), um anzuzeigen, dass die Kommunikation mit den Adaptern verloren ging.

Um ein ordnungsgemäßes Herunterfahren durchzuführen, gehen Sie in der iDRAC-Weboberfläche zu einem der folgenden Standorte:

- Wählen Sie im **Dashboard Ordnungsgemäß herunterfahren** aus und klicken Sie auf **Anwenden**.

ANMERKUNG: Sobald die Anforderung an den Host gesendet wurde, muss der Host diese Anforderung berücksichtigen und ausführen. Der Erfolg des ordnungsgemäßen Herunterfahrens hängt vom Status des Hosts ab.

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

Neues Administratorbenutzerkonto erstellen

Sie können das standardmäßige lokale Administratornutzerkonto ändern oder ein neues Administratornutzerkonto erstellen. Informationen zum Ändern des lokalen Administratornutzerkontos finden Sie in Ändern der Einstellungen des lokalen Administratorkontos.

Weitere Informationen zum Erstellen eines neuen Administratorkontos finden Sie in den folgenden Abschnitten:

- Lokale Nutzer konfigurieren
- Konfigurieren von Active Directory-Benutzern
- Generische LDAP-Nutzer konfigurieren

Starten der 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 mit einer der folgenden Methoden über die iDRAC-Weboberfläche:
   - Gehen Sie zu **Dashboard** > **Virtuelle Konsole** und klicken Sie auf **Virtuelle Konsole starten**.

   Daraufhin wird der **Viewer für die virtuelle Konsole** angezeigt.
3. Klicken Sie über das Menü **Datei** auf **Virtueller Datenträger** > **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

Weitere Informationen finden Sie im Abschnitt Betriebssystem über Remote-Dateifreigabe bereitstellen.

Rack-Dichte managen

Bevor Sie zusätzliche Server in einem Rack installieren, müssen Sie die verbleibende Kapazität im Rack bestimmen.

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.

Anwenden der E/A-Identitätskonfigurationseinstellungen für mehrere Netzwerkkarten über Einzel-Host-Systemneustart

Wenn Sie über mehrere Netzwerkkarten in einem Server verfügen, der Teil einer SAN-Umgebung (Storage Area Network) ist, und Sie verschiedene virtuelle Adressen sowie Initiator- und Zielkonfigurationseinstellungen auf diese Karten anwenden möchten, verwenden Sie die Funktion zur E/A-Identitätsoptimierung, um den Zeitaufwand für die Konfiguration dieser Einstellungen zu reduzieren. Gehen Sie hierfür folgendermaßen vor:

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 Serverkonfigurationsprofil-Datei (SCP) aus dem iDRAC.
4. Bearbeiten Sie die E/A-Identitätsoptimierungseinstellungen in der SCP-Datei.
5. Importieren Sie die SCP-Datei in den iDRAC.

Index

I

Installieren eines Plug-ins in iDRAC 87, 88

M

Metrikdefinition 206