

**Integrated Dell Remote Access Controller 7 (iDRAC7)
Version 1.30.30 Benutzerhandbuch**



Anmerkungen, Vorsichtshinweise und Warnungen

 **ANMERKUNG:** Eine ANMERKUNG liefert wichtige Informationen, mit denen Sie den Computer besser einsetzen können.

 **VORSICHT:** Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.

 **WARNUNG:** Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

© 2012 Dell Inc.

In diesem Text verwendete Marken: Dell™, das Dell Logo, Dell Boom™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ und Vostro™ sind Marken von Dell Inc. Intel®, Pentium®, Xeon®, Core® und Celeron® sind eingetragene Marken der Intel Corporation in den USA und anderen Ländern. AMD® ist eine eingetragene Marke und AMD Opteron™, AMD Phenom™ und AMD Sempron™ sind Marken von Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® und Active Directory® sind Marken oder eingetragene Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Red Hat® und Red Hat® Enterprise Linux® sind eingetragene Marken von Red Hat, Inc. in den USA und/oder anderen Ländern. Novell® und SUSE® sind eingetragene Marken von Novell Inc. in den USA und anderen Ländern. Oracle® ist eine eingetragene Marke von Oracle Corporation und/oder ihren Tochterunternehmen. Citrix®, Xen®, XenServer® und XenMotion® sind eingetragene Marken oder Marken von Citrix Systems, Inc. in den USA und/oder anderen Ländern. VMware®, Virtual SMP®, vMotion®, vCenter® und vSphere® sind eingetragene Marken oder Marken von VMware, Inc. in den USA oder anderen Ländern. IBM® ist eine eingetragene Marke von International Business Machines Corporation.

2012 - 12

Rev. A00

Inhaltsverzeichnis

Anmerkungen, Vorsichtshinweise und Warnungen.....	2
Kapitel 1: Übersicht.....	13
Vorteile der Verwendung von iDRAC7 mit Lifecycle-Controller.....	13
Wichtige Funktionen.....	14
Was ist neu in dieser Version?.....	15
Unterstützte Web-Browser.....	17
Lizenzenverwaltung	17
Lizenztypen.....	17
Lizenzen anfordern.....	17
Lizenzvorgänge.....	18
Lizenzierbare Funktionen in iDRAC7.....	19
Schnittstellen und Protokoll für den Zugriff auf iDRAC7.....	21
iDRAC7-Schnittstelleninformationen.....	24
Weitere nützliche Dokumente.....	25
Kontaktaufnahme mit Dell.....	26
Kapitel 2: Bei iDRAC7 anmelden.....	27
Anmelden als lokaler Benutzer, Active Directory-Benutzer oder LDAP-Benutzer bei iDRAC7.....	27
Anmeldung beim iDRAC7 mit Smart Card.....	28
Bei iDRAC7 über eine Smart Card als lokaler Benutzer anmelden.....	28
Bei iDRAC7 über eine Smart Card als Active Directory-Benutzer anmelden.....	29
Bei iDRAC7 über die einmalige Anmeldung anmelden	30
Bei iDRAC7 SSO über die iDRAC7-Web-Schnittstelle anmelden.....	30
Bei iDRAC7 SSO über die CMC-Web-Schnittstelle anmelden.....	30
Über Remote-RACADM auf iDRAC7 zugreifen.....	30
Zertifizierungsstellenzertifikat für die Verwendung von Remote-RACADM auf Linux validieren.....	31
Über lokalen RACADM auf iDRAC7 zugreifen.....	31
Über Firmware-RACADM auf iDRAC7 zugreifen.....	31
Über SMCLP auf iDRAC7 zugreifen.....	31
Anmeldung beim iDRAC7 mit Authentifizierung mit öffentlichem Schlüssel.....	32
Mehrere iDRAC7-Sitzungen.....	32
Ändern des standardmäßigen Anmeldungskennworts.....	32
Ändern des standardmäßigen Anmeldekennworts unter Verwendung von Web-Schnittstelle.....	33
Ändern eines in den Standardeinstellungen festgelegten Anmeldungskennworts unter Verwendung von RACADM.....	33

Ändern des standardmäßigen Anmeldekennworts unter Verwendung des Dienstprogramms für iDRAC-Einstellungen	33
Aktivieren oder Deaktivieren der standardmäßigen Kennwortwarnungsmeldung	34
Aktivieren oder Deaktivieren einer standardmäßigen Kennwortwarnungsmeldung unter Verwendung der Web-Schnittstelle.....	34
Aktivieren oder Deaktivieren der Warnungsmeldung zum Ändern des standardmäßigen Anmeldungskennworts unter Verwendung von RACADM.....	34

Kapitel 3: Managed System und Management Station einrichten.....35

iDRAC7-IP-Adresse einrichten.....	35
iDRAC-IP-Adresse über das Dienstprogramm für die iDRAC-Einstellungen einrichten.....	36
iDRAC7-IP-Adresse über die CMC-Web-Schnittstelle einrichten.....	39
Auto-Ermittlung aktivieren.....	39
Management Station einrichten.....	40
Per Remote auf iDRAC7 zugreifen.....	41
Managed System einrichten.....	41
Einstellungen für lokales Administratorkonto ändern.....	41
Standort für das Managed System einrichten.....	42
Systemleistung und Stromverbrauch optimieren.....	42
Konfigurieren von unterstützten Webbrowsern.....	42
iDRAC7 zur Liste vertrauenswürdiger Domänen hinzufügen.....	45
Weiße Liste-Funktion in Firefox deaktivieren.....	45
Lokalisierte Versionen der Webschnittstelle anzeigen.....	45
Aktualisieren der Gerätefirmware.....	46
Herunterladen der Gerätefirmware.....	47
Aktualisieren der Gerätefirmware über die iDRAC7-Web-Schnittstelle.....	47
Aktualisieren der Gerätefirmware über RACADM.....	48
Firmware über die CMC-Web-Schnittstelle aktualisieren.....	48
Firmware über DUP aktualisieren.....	48
Firmware über Remote-RACADM aktualisieren.....	48
Firmware über die Lifecycle-Controller-Remote-Dienste aktualisieren.....	49
Anzeigen und Verwalten von gestuften Aktualisierungen.....	49
Anzeigen und Verwalten gestufter Aktualisierungen unter Verwendung der iDRAC7 Web-Schnittstelle.....	49
Anzeigen und Verwalten gestufter Aktualisierungen unter Verwendung von RACADM.....	50
Rollback der iDRAC7-Firmware durchführen.....	50
Rollback für die Firmware über die iDRAC7-Web-Schnittstelle durchführen.....	50
Rollback der Firmware über die CMC-Web-Schnittstelle durchführen.....	51
Rollback der Firmware über RACADM durchführen.....	51
Rollback der Firmware über Lifecycle-Controller durchführen.....	51
Rollback der Firmware über die Remote-Dienste für den Lifecycle Controller durchführen.....	51
iDRAC7 wiederherstellen.....	51
TFTP-Server verwenden.....	51

Sichern und Wiederherstellen eines Serverprofils.....	52
Sichern des Serverprofils unter Verwendung der iDRAC7-Web-Schnittstelle.....	52
Sichern des Serverprofils unter Verwendung von RACADM.....	53
Sichern des Serverprofils unter Verwendung der iDRAC7-Web-Schnittstelle.....	53
Wiederherstellen des Serverprofils unter Verwendung von RACADM.....	53
Sequenz für den Wiederherstellungsvorgang.....	53
iDRAC7 über andere Systemverwaltungs-Tools überwachen.....	54

Kapitel 4: iDRAC7 konfigurieren.....55

iDRAC7-Informationen anzeigen.....	56
iDRAC7-Informationen über die Web-Schnittstelle anzeigen.....	56
iDRAC7-Informationen über RACADM anzeigen.....	56
Netzwerkeinstellungen ändern.....	57
Netzwerkeinstellungen über die Web-Schnittstelle ändern.....	57
Netzwerkeinstellungen über einen lokalen RACADM ändern.....	57
IP-Filterung und IP-Blockierung konfigurieren.....	58
Dienste konfigurieren.....	60
Services unter Verwendung der Webschnittstelle konfigurieren.....	61
Dienste über RACADM konfigurieren.....	61
Anzeige auf der Frontblende konfigurieren.....	62
LCD-Einstellung konfigurieren.....	62
LED-Einstellung für die System-ID konfigurieren.....	63
Das Konfigurieren von Zeitzone und NTP.....	64
Konfigurieren von Zeitzone und NTP unter Verwendung der iDRAC- Web-Schnittstelle.....	64
Konfigurieren von Zeitzone und NTP unter Verwendung von RACADM.....	64
Erstes Startlaufwerk einstellen.....	64
Erstes Startgerät über die Web-Schnittstelle einrichten.....	65
Erstes Startgerät über RACADM festlegen.....	65
Einstellen des ersten Startgeräts unter Verwendung der virtuellen Konsole.....	65
Bildschirm „Letzter Absturz“ aktivieren.....	65
Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough.....	66
Aktivieren und Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung der Web-Schnittstelle.....	68
Aktivieren und Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung von RACADM.....	68
Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough unter Verwendung des Dienstprogramms für iDRAC-Einstellungen.....	68
Zertifikate abrufen.....	69
SSL-Serverzertifikate.....	69
Neue Zertifikatsignierungsanforderung erstellen.....	70
Serverzertifikat hochladen.....	71
Serverzertifikat anzeigen.....	72

Hochladen eines benutzerdefinierten Signaturzertifikats.....	72
Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat herunterladen	73
Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat löschen.....	73
Mehrere iDRAC7s über RACADM konfigurieren.....	73
iDRAC7-Konfigurationsdatei erstellen.....	74
Parsing-Regeln.....	75
iDRAC7-IP-Adresse ändern.....	76
Zugriff zum Ändern der iDRAC7-Konfigurationseinstellungen auf einem Host-System deaktivieren.....	77

Kapitel 5: Informationen zu iDRAC7 und zum Managed System anzeigen.....79

Zustand und Eigenschaften des Managed System anzeigen.....	79
System-Bestandsaufnahme anzeigen.....	79
Sensorinformationen anzeigen.....	80
Das System auf Frischlufttauglichkeit prüfen.....	82
Temperaturverlaufsdaten anzeigen.....	82
Temperaturdatenverlauf mit der iDRAC7-Weboberfläche anzeigen.....	83
Temperaturdatenverlauf über RACADM anzeigen.....	83
Bestandsaufnahme für Speichergeräte erstellen und Speichergeräte überwachen.....	84
Speichergeräte über die Web-Schnittstelle überwachen.....	84
Speichergerät über RACADM überwachen.....	85
Bestandsaufnahme für Netzwerkgeräte erstellen und Netzwerkgeräte überwachen.....	85
Netzwerkgeräte über die Web-Schnittstelle überwachen.....	85
Netzwerkgeräte über RACADM überwachen.....	85
Bestandsaufnahme und Überwachung von FC-HBA-Geräten.....	85
FC-HBA-Geräte mit der Web-Schnittstelle überwachen.....	86
Überwachung von FC-HBA-Geräten unter Verwendung von RACADM.....	86
Verbindungen der FlexAddress-Mezzanine-Kartenarchitektur anzeigen.....	86
iDRAC7-Sitzungen anzeigen oder beenden.....	87
iDRAC7-Sitzungen über die Web-Schnittstelle beenden.....	87
iDRAC7-Sitzungen über RACADM beenden.....	87

Kapitel 6: iDRAC7-Kommunikation einrichten.....89

Mit iDRAC7 über eine serielle Verbindung über ein DB9-Kabel kommunizieren.....	90
BIOS für serielle Verbindung konfigurieren.....	91
Serielle RAC-Verbindung aktivieren.....	91
Grundlegenden seriellen IPMI-Verbindungs- und -Terminalmodus aktivieren.....	91
Von der seriellen RAC-Verbindung auf die serielle Konsolenverbindung bei Verwendung eines DB9-Kabels umschalten.....	93
Von der seriellen Konsole auf die serielle RAC-Verbindung umschalten.....	94
Von der seriellen RAC-Verbindung auf die serielle Konsole umschalten.....	94
Mit iDRAC7 über IPMI SOL kommunizieren.....	94
BIOS für serielle Verbindung konfigurieren.....	94

iDRAC7 für die Verwendung von SOL konfigurieren.....	95
Unterstütztes Protokoll aktivieren.....	96
Mit iDRAC7 mithilfe von IPMI über LAN kommunizieren.....	100
IPMI über LAN über die Web-Schnittstelle konfigurieren.....	100
IPMI über LAN über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren.....	100
IPMI über LAN mithilfe von RACADM konfigurieren.....	101
Remote-RACADM aktivieren oder deaktivieren.....	101
Remote-RACADM über die Web-Schnittstelle aktivieren oder deaktivieren.....	101
Remote-RACADM über RACADM aktivieren oder deaktivieren.....	102
Lokalen RACADM deaktivieren.....	102
IPMI auf Managed System aktivieren.....	102
Linux während des Starts für die serielle Konsole konfigurieren.....	102
Anmeldung an der virtuellen Konsole nach dem Start aktivieren.....	103
Unterstützte SSH-Verschlüsselungsschemas.....	104
Authentifizierung über öffentlichen Schlüssel für SSH verwenden.....	104
Kapitel 7: Benutzerkonten und Berechtigungen konfigurieren.....	109
Lokale Benutzer konfigurieren.....	109
Lokale Benutzer über die iDRAC7-Web-Schnittstelle konfigurieren.....	109
Lokale Benutzer über RACADM konfigurieren.....	110
Konfigurieren von Active Directory-Benutzern.....	112
Voraussetzungen zur Verwendung der Active Directory-Authentifizierung des iDRAC7.....	113
Unterstützte Active Directory-Authentifizierungsmechanismen.....	115
Übersicht des Standardschema-Active Directory.....	115
Active Directory-Standardschema konfigurieren.....	117
Übersicht des Active Directory mit erweitertem Schema.....	120
Active Directory mit erweitertem Schema konfigurieren.....	122
Active Directory-Einstellungen testen.....	131
Konfigurieren von allgemeinen LDAP-Benutzern.....	131
Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mit der iDRAC7-Webschnittstelle.....	132
Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mittels RACADM.....	133
Einstellungen für LDAP-Verzeichnisdienst testen.....	133
Kapitel 8: iDRAC7 für die einfache Anmeldung oder Smart Card-Anmeldung konfigurieren.....	135
Voraussetzungen für die einmalige Active Directory-Anmeldung oder die Smart Card-Anmeldung.....	135
iDRAC7 als einen Computer in der Active Directory-Stammdomäne registrieren.....	135
Kerberos Keytab-Datei generieren.....	136
Active Directory-Objekte erstellen und Berechtigungen bereitstellen.....	137
Browser zum Aktivieren der Active Directory-SSO konfigurieren.....	137
iDRAC7-SSO-Anmeldung für Active Directory-Benutzer konfigurieren.....	137
iDRAC7-SSO-Anmeldung für Active Directory-Benutzer über die Web-Schnittstelle konfigurieren.....	138

iDRAC7 SSO-Anmeldung für Active Directory-Benutzer über RACADM konfigurieren.....	138
iDRAC7-Smart Card-Anmeldung für lokale Benutzer konfigurieren.....	138
Smart Card-Benutzerzertifikat hochladen.....	139
Vertrauenswürdige Zertifizierungsstellenzertifikat für Smart Card hochladen.....	139
iDRAC7-Smart-Card-Anmeldung für Active Directory-Benutzer konfigurieren.....	140
Smart Card-Anmeldung aktivieren oder deaktivieren.....	140
Smart Card-Anmeldung über die Web-Schnittstelle aktivieren oder deaktivieren.....	141
Smart Card-Anmeldung über RACADM aktivieren oder deaktivieren.....	141
Smart Card-Anmeldung über das Dienstprogramm für die iDRAC-Einstellungen aktivieren oder deaktivieren.....	141

Kapitel 9: iDRAC7 für das Versenden von Warnungen konfigurieren..... 143

Warnungen aktivieren und deaktivieren.....	143
Warnungen über die Web-Schnittstelle aktivieren oder deaktivieren.....	144
Warnungen über RACADM aktivieren oder deaktivieren.....	144
Warnungen über das Dienstprogramm für iDRAC-Einstellungen aktivieren oder deaktivieren.....	144
Warnungen filtern	144
Warnungen über die iDRAC7-Web-Schnittstelle filtern.....	144
Warnungen über RACADM filtern.....	145
Ereigniswarnungen einrichten.....	145
Ereigniswarnungen über die Web-Schnittstelle einrichten.....	145
Ereigniswarnungen über RACADM einrichten.....	146
Alarmwiederholungsereignis einrichten.....	146
Alarmwiederholungsereignis über die iDRAC7-Weboberfläche einrichten.....	146
Alarmwiederholungsereignisse über RACADM einrichten.....	146
Ereignismaßnahmen festlegen.....	146
Ereignismaßnahmen über die Web-Schnittstelle einrichten.....	147
Ereignismaßnahmen über RACADM einrichten.....	147
Einstellungen für E-Mail-Warnungs-SNMP-Trap oder IPMI-Trap konfigurieren.....	147
IP-basierte Warnziele konfigurieren.....	148
Konfigurieren von E-Mail-Benachrichtigungen.....	149
Konfigurieren von WS-Ereignisauslösung.....	151
IDs für Warnungsmeldung.....	151

Kapitel 10: Protokolle verwalten..... 155

Systemereignisprotokoll anzeigen.....	155
Systemereignisprotokoll über die Web-Schnittstelle anzeigen.....	155
Systemereignisprotokoll über RACADM anzeigen.....	155
Anzeigen des Systemereignisprotokolls unter Verwendung des Dienstprogramms für die iDRAC- Einstellungen.....	156
Lifecycle-Protokoll anzeigen	156
Lifecycle-Protokoll über die Web-Schnittstelle anzeigen.....	156

Lifecycle-Protokoll über RACADM anzeigen.....	157
Arbeitsanmerkungen hinzufügen.....	157
Remote-Systemprotokollierung konfigurieren.....	157
Remote-System-Protokollierung über die Web-Schnittstelle konfigurieren.....	158
Remote-Systemanmeldung über RACADM konfigurieren.....	158
Kapitel 11: Stromversorgung überwachen und verwalten.....	159
Stromversorgung überwachen.....	159
Stromversorgung über die Web-Schnittstelle überwachen.....	159
Stromversorgung über RACADM überwachen.....	160
Stromsteuerungsvorgänge ausführen.....	160
Stromsteuerungsvorgänge über die Web-Schnittstelle ausführen.....	160
Stromsteuerungsvorgänge über RACADM ausführen.....	160
Strombegrenzung.....	160
Strombegrenzung bei Blade-Servern.....	161
Strombegrenzungsrichtlinie anzeigen und konfigurieren.....	161
Netzteiloptionen konfigurieren.....	162
Netzteiloptionen über die Web-Schnittstelle konfigurieren.....	163
Netzteiloptionen über RACADM konfigurieren.....	163
Netzteiloptionen über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren.....	163
Netzschalter aktivieren oder deaktivieren.....	164
Kapitel 12: Virtuelle Konsole konfigurieren und verwenden.....	165
Unterstützte Bildschirmauflösungen und Bildwiederholfrquenzen.....	165
Web-Browser für die Verwendung der virtuellen Konsole konfigurieren.....	166
Web-Browser für die Verwendung des Java-Plugin konfigurieren.....	166
IE für die Verwendung des ActiveX-Plugin konfigurieren.....	167
Zertifizierungsstellenzertifikate auf die Management Station importieren.....	168
Virtuelle Konsole konfigurieren.....	169
Virtuelle Konsole über die Web-Schnittstelle konfigurieren.....	169
Virtuelle Konsole über RACADM konfigurieren.....	170
Vorschau der virtuellen Konsole.....	170
Virtuelle Konsole starten.....	170
Virtuelle Konsole über die Web-Schnittstelle starten.....	171
Virtuelle Konsole über URL starten.....	171
Viewer für virtuelle Konsole verwenden.....	172
Mauszeiger synchronisieren.....	172
Alle Tastenanschläge über die virtuelle Konsole führen.....	173
Kapitel 13: Virtuelle Datenträger verwalten.....	177
Unterstützte Laufwerke und Geräte.....	178
Virtuellen Datenträger konfigurieren.....	178

Virtuelle Datenträger über die iDRAC7-Web-Schnittstelle konfigurieren.....	178
Virtuelle Datenträger über RACADM konfigurieren.....	179
Virtuelle Datenträger über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren.....	179
Status des verbundenen Datenträgers und Systemantwort.....	179
Auf virtuellen Datenträger zugreifen.....	179
Virtuellen Datenträger über die virtuelle Konsole starten.....	179
Virtuellen Datenträger ohne virtuelle Konsole starten.....	180
Images von virtuellen Datenträgern hinzufügen.....	181
Images von virtuellen Datenträgern entfernen.....	181
Details zum virtuellen Gerät anzeigen.....	181
USB-Gerät zurücksetzen.....	181
Virtuelles Laufwerk zuordnen.....	182
Zuordnung für virtuelles Laufwerk aufheben.....	182
Startreihenfolge über das BIOS festlegen.....	183
Einmalstart für virtuelle Datenträger aktivieren.....	183
Kapitel 14: VMCLI-Dienstprogramm installieren und verwenden.....	185
VMCLI installieren.....	185
VMCLI-Dienstprogramm ausführen.....	185
VMCLI-Syntax.....	186
VMCLI-Befehle für den Zugriff auf virtuelle Datenträger	186
VMCLI: Betriebssystem-Shell-Optionen	187
Kapitel 15: vFlash SD-Karte verwalten.....	189
vFlash SD-Karten-Konfiguration.....	189
Eigenschaften der vFlash-SD-Karte anzeigen.....	189
Aktivieren oder Deaktivieren der vFlash-Funktionalität.....	190
vFlash SD-Karte initialisieren.....	191
Aktuellen Status über RACADM abrufen.....	192
vFlash-Partitionen verwalten.....	192
Leere Partition erstellen.....	192
Partition unter Verwendung einer Imagedatei erstellen.....	193
Partition formatieren.....	194
Verfügbare Partitionen anzeigen.....	195
Partition modifizieren.....	195
Partitionen verbinden oder trennen.....	196
Vorhandene Partitionen löschen.....	197
Partitionsinhalte herunterladen.....	198
Zu einer Partition starten.....	198
Kapitel 16: SMCLP verwenden.....	201
System-Verwaltungsfunktionen über SMCLP.....	201

SMCLP-Befehle ausführen.....	201
iDRAC7 SMCLP-Syntax.....	202
MAP-Adressbereich navigieren.....	204
Verb „show“ verwenden.....	205
Option -display verwenden.....	205
Option -level verwenden.....	205
Option -output verwenden.....	205
Anwendungsbeispiele.....	205
Server-Energieverwaltung.....	206
SEL-Verwaltung.....	206
MAP-Zielnavigation.....	207
Kapitel 17: Betriebssysteme bereitstellen.....	209
Betriebssystem mittels VMCLI bereitstellen	209
Betriebssystem über eine Remote-Dateifreigabe bereitstellen.....	210
Verwalten der Remote-Dateifreigabe (Remote File Share).....	211
Remote-Dateifreigabe über die Web-Schnittstelle konfigurieren.....	212
Remote-Dateifreigabe über RACADM konfigurieren.....	212
Betriebssystem über virtuelle Datenträger bereitstellen.....	213
Betriebssystem über mehrere Festplatten bereitstellen.....	213
Integriertes Betriebssystem auf SD-Karte bereitstellen.....	213
SD-Modul und Redundanz im BIOS aktivieren.....	214
Kapitel 18: Fehler auf Managed System über iDRAC7 beheben.....	215
Diagnosekonsole verwenden.....	215
POST-Codes anzeigen.....	215
Videos zum Startvorgang und zur Absturzerfassung anzeigen.....	216
Protokolle anzeigen.....	216
Bildschirm „Letzter Systemabsturz“ anzeigen.....	216
Status der Anzeige auf der Frontblende anzeigen.....	216
Status der LC-Anzeige auf der Frontblende des Systems anzeigen.....	217
Status der LE-Anzeige auf der Frontblende des Systems anzeigen.....	217
Anzeigen für Hardwareprobleme.....	218
Systemzustand anzeigen.....	218
Serverstatusbildschirm auf Fehlermeldungen überprüfen.....	219
iDRAC7 neu starten.....	219
iDRAC7 über die iDRAC7-Web-Schnittstelle zurücksetzen.....	219
iDRAC7 über RACADM zurücksetzen.....	219
Zurücksetzen des iDRAC7 auf die Werkeinstellungen.....	219
Zurücksetzen von iDRAC7 auf die Standardwerkeinstellungen unter Verwendung der iDRAC7-Web-Schnittstelle.....	219
iDRAC7 mithilfe des Dienstprogramms für iDRAC-Einstellungen auf Werkeinstellungen zurücksetzen.....	220

Kapitel 19: Häufig gestellte Fragen (FAQs)	221
System-Ereignisprotokoll.....	221
Netzwerksicherheit.....	221
Active Directory.....	222
Einfache Anmeldung.....	224
Smart Card-Anmeldung.....	226
Virtuelle Konsole.....	226
Virtueller Datenträger.....	229
vFlash-SD-Karte.....	232
SNMP-Authentifizierung.....	232
Speichergeräte.....	232
RACADM.....	232
Verschiedenes.....	233
Kapitel 20: Anwendungsszenarien	237
Fehler auf einem nicht zugreifbaren Managed System beheben.....	237
Systeminformationen abrufen und Systemzustand bewerten.....	237
Einrichten von Warnungen und Konfigurieren von E-Mail-Warnungen.....	238
Lifecycle-Protokoll und Systemereignisprotokoll anzeigen und exportieren.....	238
Schnittstellen zum Aktualisieren der iDRAC-Firmware.....	238
Ordnungsgemäßes Herunterfahren durchführen.....	238
Neues Administratorbenutzerkonto erstellen.....	239
Server-Remote-Konsole starten und ein USB-Laufwerk mounten.....	239
Bare Metal-Betriebssystem über verbundenen virtuellen Datenträger und Remote-Dateifreigabe installieren.....	239
Rack-Dichte verwalten.....	239
Neue elektronische Lizenz installieren.....	240

Übersicht

Der Integrated Dell Remote Access Controller 7 (iDRAC7) wurde entwickelt, um die Arbeit von Serveradministratoren produktiver zu gestalten und die allgemeine Verfügbarkeit von Dell-Servern zu verbessern. iDRAC7 weist Administratoren auf Serverprobleme hin, unterstützt sie bei der Ausführung von Remote-Server-Verwaltungsaufgaben und reduziert die Notwendigkeit, physisch auf den Server zuzugreifen.

iDRAC7 mit Lifecycle-Controller-Technologie ist Teil einer größeren Rechenzentrumslösung, die Sie dabei unterstützt, unternehmenskritische Anwendungen und Auslastungen jederzeit bereitzuhalten. Mit dieser Technologie können Administratoren Dell-Server von jedem Standort aus und ohne den Einsatz von Agenten bereitstellen, überwachen, verwalten, konfigurieren, aktualisieren, Instand setzen und Störungen auf diesen Servern beheben. Dabei ist es unerheblich, ob ein Betriebssystem oder ein Hypervisor vorhanden sind oder sie sich in einem betriebsfähigen Zustand befinden.

Verschiedene Produkte arbeiten mit dem iDRAC7 und dem Lifecycle-Controller zusammen, um IT-Vorgänge zu vereinfachen, darunter:

- Dell Management Plug-in für VMware vCenter
- Dell Repository Manager
- Dell Management Packs für Microsoft System Center Operations Manager (SCOM) und Microsoft System Center Configuration Manager (SCCM)
- BMC Bladelogic
- Dell OpenManage Essentials
- Dell OpenManage Power Center

Der iDRAC7 wird in den folgenden Varianten angeboten:

- Basic Management mit IPMI (standardmäßig für Server der 200-500 Serie verfügbar)
- iDRAC7 Express (standardmäßig für Rack- oder Tower-Server der 600 Serie oder höher verfügbar und für alle Blade-Server)
- iDRAC7 Enterprise (auf allen Servermodellen verfügbar)

Weitere Informationen finden Sie im *iDRAC7 Overview and Feature Guide* (iDRAC7-Überblicks- und Funktionshandbuch) unter dell.com/support/manuals.

Vorteile der Verwendung von iDRAC7 mit Lifecycle-Controller

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.
- Verbesserte integrierte Verwaltung über Lifecycle-Controller – Lifecycle-Controller bietet Bereitstellungsfunktionen und vereinfacht Wartungsaufgaben durch die Lifecycle-Controller-Benutzeroberfläche für die lokale Bereitstellung und über Schnittstellen für Remote-Dienste (WS-Management) für die Remote-Bereitstellung. Außerdem bietet Lifecycle-Controller eine Integration mit Dell OpenManage Essentials und Partner-Konsolen.

Weitere Informationen zur Lifecycle-Controller-Benutzeroberfläche finden Sie im *Lifecycle Controller User's Guide* (Lifecycle-Controller-Benutzerhandbuch), Informationen zu Remote-Diensten finden Sie im *Lifecycle Controller Remote Services User's Guide* (Lifecycle-Controller-Benutzerhandbuch für Remote-Dienste), jeweils unter dell.com/support/manuals.


Wichtige Funktionen

Zentrale Funktionen in iDRAC7:

 **ANMERKUNG:** Einige der Funktionen sind nur mit einer iDRAC7 Enterprise-Lizenz verfügbar. Für Informationen über die verfügbaren Funktionen der verschiedenen Lizenzen siehe [Lizenzen verwalten](#).

Bestandsaufnahme und Überwachung

- Zustand verwalteter Server anzeigen
- Netzwerkadapter zur Bestandsaufnahme und Überwachung und Speichersubsysteme (PERC und direkt angehängter Speicher) ohne Betriebssystemagenten.
- Anzeigen und Exportieren der aktuellen Bestandsliste.
- Anzeigen der Sensorinformationen wie beispielsweise Temperatur, Spannung und Eingriff.
- Überwachen des CPU-Status, automatische Prozessordrosselung und vorhergesagte Fehler.
- Anzeigen der Speicherinformation.
- Stromverbrauch überwachen und steuern
- Support für SNMPv3.
- Für Blade-Server: Web-Schnittstelle für Chassis Management Controller (CMC) starten und CMC-Informationen sowie WWN/MAC-Adressen anzeigen

 **ANMERKUNG:** CMC ermöglicht den Zugriff auf iDRAC7 über das M1000E-Gehäuse-LCD-Bedienfeld und über lokale Konsolenverbindungen. Weitere Informationen finden Sie im *Chassis Management Controller User's Guide* (Chassis Management Controller-Benutzerhandbuch) unter dell.com/support/manuals.

Bereitstellung

- vFlash SD-Kartenpartitionen verwalten
- Anzeigeeinstellungen für das Bedienfeld auf der Vorderseite konfigurieren
- Lifecycle Controller starten, mit dem Sie das BIOS und die unterstützten Netzwerk- und Speicheradapter konfigurieren und aktualisieren können
- iDRAC7-Netzwerkeinstellungen verwalten
- Virtuelle Konsole und virtuelle Datenträger konfigurieren und verwenden
- Betriebssysteme über die Remote-Dateifreigabe, über virtuelle Datenträger und VMCLI bereitstellen
- Aktivieren Sie die automatische Ermittlung.
- Ausführen der Serverkonfiguration unter Verwendung der Export- oder Import-XML-Profilfunktion durch RACADM und WS-MAN. Für mehr Informationen siehe *Lifecycle Controller Remote Services Quick Start Guide* (Lifecycle-Controller Remote-Dienste Schnellstarthandbuch).

Aktualisierung


- iDRAC7-Lizenzen verwalten
- Aktualisieren des BIOS und der Gerätefirmware für Geräte, die durch Lifecycle Controller unterstützt werden
- Aktualisierung oder Rollback für iDRAC7-Firmware durchführen
- Verwalten gestufter Aktualisierungen.
- Sicherung und Wiederherstellung des Serverprofils

Wartung und Fehlerbehebung

- Stromversorgungs-bezogene Vorgänge ausführen und Stromverbrauch überwachen
- Keine Abhängigkeit vom Server Administrator für die Generierung von Warnmeldungen
- Ereignisdaten protokollieren: Lifecycle- und RAC-Protokolle.
- Festlegen von E-Mail-Warnungen, IPMI-Warnungen, Remote System-Protokolle, WS-Ereignisprotokolle und SNMP-Traps (v1 und v2c) für Ereignisse und verbesserte E-Mail-Warnungsbenachrichtigung.
- Image des letzten Systemabsturzes erfassen
- Videos zur Start- und Absturzerfassung anzeigen

Konnektivität absichern

Die Sicherung des Zugriffs auf kritische Netzwerkressourcen hat Priorität. iDRAC7 implementiert einen Bereich mit Sicherheitsfunktionen, darunter:

- Benutzerdefinierte Signaturzertifikate für Secure Socket Layer (SSL).
- Signierte Firmware-Aktualisierungen
- Benutzerauthentifizierung durch Microsoft Active Directory, generischem Lightweight Directory Access Protocol (LDAP) Directory Service oder lokal verwalteten Benutzer-IDs und Kennwörtern.
- Zweifaktor-Authentifizierung über die Smart Card-Anmeldefunktion. Die Zweifaktor-Authentifizierung basiert auf der physischen Smart Card und der Smart Card-PIN.
- Authentifizierung über die einmalige Anmeldung und den öffentlichen Schlüssel
- Rollenbasierte Authentifizierung für die Konfiguration spezifischer Berechtigungen für jeden einzelnen Benutzer
- SNMPv3-Authentifizierung für Benutzerkonten, die lokal in iDRAC gespeichert sind. Es wird empfohlen, dies so zu benutzen, auch wenn die Option in den Standardeinstellungen deaktiviert ist.
- Benutzer-ID- und Kennwortkonfiguration
- Standardmäßige Anmeldekennwort-Modifikation.
- SMCLP- und Webschnittstellen, die 128-Bit- und 40-Bit-Verschlüsselung unterstützen (für Länder, in denen 128-Bit nicht zulässig ist) und den SSL 3.0-Standard verwenden.
- Konfiguration der Sitzungszeitüberschreitung (in Sekunden)
- Konfigurierbare IP-Schnittstellen (für HTTP, HTTPS, SSH, Telnet, virtuelle Konsole und virtuelle Datenträger).
-  **ANMERKUNG:** SSL-Verschlüsselung wird durch Telnet nicht unterstützt und ist standardmäßig deaktiviert.
- 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 iDRAC7 angeschlossen werden
- Dedizierter Gigabit-Ethernet-Adapter auf Rack- oder Tower-Servern mit Unternehmenslizenz.

Was ist neu in dieser Version?

Diese Version verfügt über die folgenden neuen Funktionen:

- Aktualisieren der Gerätefirmware für alle Geräte, die durch Lifecycle Controller unterstützt werden
- Anzeigen und Verwalten gestufter Firmwareaktualisierungen.

- Sicherung und Wiederherstellung des Serverprofils.
- Hardwarebestandsliste exportieren.
- Anzeigen der Bestandsaufnahmeinformation der Hardware und Firmware für zusätzliche Komponenten.
- Virtuelle Konsole:
 - Automatisches Sperren des Betriebssystems.
 - Skalieren des Viewers für die virtuelle Konsole.
 - Modifizierte Tastaturmakros.
 - Einstellen des ersten Startgeräts mithilfe des Viewers der virtuellen Konsole.
- Einstellung, mit der es iDRAC möglich ist, automatisch die Netzwerkkarte (NIC) auszuwählen (dedizierte NIC oder freigegebene LOM) basierend auf dem Linkstatus.
- Anzeigen der aktuell aktiven NIC.
- Aktivieren der Anzeige der virtuellen Konsole an der Frontblenden-LCD.
- Festlegen von Lifecycle Controller oder BIOS Boot Manager als erstes Startlaufwerk.
- Einstellen der Zeitzone und des Network Time Protocol (NTP).
- BS zu iDRAC Pass-Through aktivieren.
- Verbesserte Sicherheitsfunktionen wie z. B.:
 - Warnen des Benutzers, wenn die standardmäßigen Anmeldeinformationen genutzt werden, um sich bei iDRAC anzumelden.
 - Generieren und Verwenden des benutzerdefinierten SSL-Zertifikatssignaturzertifikats.
- Anzeigen der CPU-Details wie beispielsweise automatische Prozessordrosselung und vorhergesagte Fehler.
- Anzeigen von Funktionszustand und Zustandsmeldung für Dual Inline Memory Modules (DIMMs).
- Überwachen des Funktionszustandes und Anzeigen der Bestandsaufnahme für Fibre-Channel-Host-Bus-Adapter- (FC-HBA)Geräte.
- Aktivieren von SNMPv3-Authentifizierung für Benutzerkonten, die lokal in iDRAC gespeichert sind.
- Unterstützung für SNMP-Traps in v1- und v2-Format. Unterstützung für SNMP-Gets in v1-, v2- oder v3-Format oder nur in v3-Format.
- Senden von Warnungen im Remote-Zugriff an einen externen Server.
- Senden von WS-Ereignismeldungen. Diese Funktion ist zurzeit auf den Job-Kontrollwarnungstyp beschränkt.
- Zurücksetzen von iDRAC7 auf die Werkseinstellungen unter Verwendung der Diagnosekonsole.
- Für RACADM-Befehle den Anfangsbuchstaben schreiben und die Tabulatortaste drücken, um den Befehl abzuschließen. Den Befehl **cd** verwenden, um zwischen verschiedenen Ebenen zu wechseln.
- Die Serverkonfiguration mit Export- oder Import-XML-Profilfunktion durch RACADM oder WS-MAN durchführen.
- Unterstützung für Safari, Chrome und Mac OS X.

Verwandte Links

- [Aktualisieren der Gerätefirmware](#)
- [Anzeigen und Verwalten von gestuften Aktualisierungen](#)
- [Sichern und Wiederherstellen eines Serverprofils](#)
- [System-Bestandsaufnahme anzeigen](#)
- [Viewer für virtuelle Konsole verwenden](#)
- [LCD-Einstellung konfigurieren](#)
- [Erstes Startlaufwerk einstellen](#)
- [Das Konfigurieren von Zeitzone und NTP](#)
- [Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough](#)
- [Ändern des standardmäßigen Anmeldekennworts](#)
- [SSL-Serverzertifikate](#)
- [Sensorinformationen anzeigen](#)

[Bestandsaufnahme und Überwachung von FC-HBA-Geräten](#)

[Lokale Benutzer konfigurieren](#)

[Zurücksetzen von iDRAC7 auf die Standardwerkseinstellungen unter Verwendung der iDRAC7-Web-Schnittstelle](#)

Unterstützte Web-Browser

iDRAC7 wird auf folgenden Browsern unterstützt:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

Für eine Liste der unterstützten Versionen siehe die *Infodatei* unter dell.com/support/manuals.

Lizenzenverwaltung

Die iDRAC7-Funktionen richten sich nach der erworbenen Lizenz (Basisverwaltung, iDRAC7 Express, oder iDRAC7 Enterprise). Über die Schnittstellen können Sie nur auf lizenzierte Funktionen zugreifen, über die Sie iDRAC7 konfigurieren oder verwenden können. Dazu gehören z. B. die iDRAC7-Web-Schnittstelle, RACADM, WS-MAN, OpenManage Server Administrator, usw. Für bestimmte Funktionen, wie z. B. die dedizierte Netzwerkschnittstellenkarte (NIC) oder vFlash, benötigen Sie iDRAC-Schnittstellenkarten, die auf Servern der 200-500-Reihe optional sind.

Die Lizenzverwaltung und die Firmware-Aktualisierungsfunktion unter iDRAC7 können über die iDRAC7-Web-Schnittstelle und RACADM aufgerufen werden.

Lizenztypen

Die folgenden Lizenztypen sind verfügbar:

- 30-Tage-Testversion und Verlängerung – Diese Lizenz läuft nach 30 Tagen ab und kann um 30 weitere Tage verlängert werden. Evaluierungslizenzen sind zeitlich begrenzt und die Zeit, die für die Evaluierung zur Verfügung steht, reduziert sich sukzessive, wenn das System eingeschaltet ist.
- Dauerlizenz – Die Lizenz ist an die Service-Tag-Nummer gebunden und damit dauerhaft.


Lizenzen anfordern

Verwenden Sie zum Anfordern von Lizenzen eines der folgenden Verfahren:



- E-Mail – Die Lizenz ist an eine E-Mail angehängt, die nach der Anforderung der Lizenz durch das technische Support Center versendet wird.
- SB-Portal – Auf dem iDRAC7 steht ein Link zum SB-Portal zur Verfügung. Klicken Sie auf diesen Link, um im Internet das SB-Portal für Lizenzen zu öffnen. Derzeit können Sie das SB-Lizenzen-Portal nutzen, um Lizenzen abzurufen, die mit dem Server erworben wurden. Für den Kauf einer neuen Lizenz oder für die Erweiterung einer bereits bestehenden Lizenz müssen Sie entweder einen Vertriebsbeauftragten oder den technischen Support kontaktieren. Für weitere Informationen siehe die Online-Hilfe zur Seite des SB-Portals.
- Point-of-sale – Die Lizenz wird im Rahmen der Systembestellung angefordert.

Lizenzvorgänge

Bevor Sie die Lizenzverwaltungsschritte ausführen, müssen Sie sicherstellen, dass Sie die erforderlichen Lizenzen besitzen. Weitere Informationen finden Sie unter *Overview and Feature Guide* (Überblicks- und Funktionshandbuch) unter dell.com/support/manuals.

 **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 iDRAC7, RACADM, WS-MAN 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 auf einen lokalen Speicher, und importieren Sie sie über eine unterstützte Schnittstelle nach iDRAC7. Die Lizenz wird importiert, wenn Sie die Validierungsprüfungen bestanden hat.
 -  **ANMERKUNG:** Bei einigen neuen Funktionen ist für die Aktivierung dieser Funktionen ein Systemneustart erforderlich.
- Exportieren – Exportieren Sie die installierte Lizenz zu Sicherungszwecken oder für eine spätere Neuinstallation im Rahmen des Austauschs der Hauptplatine auf ein externes Speichergerät. Der Dateiname und das Format der exportierten Lizenz lauten wie folgt: <EntitlementID>.xml.
- Löschen – Löschen Sie die Lizenz, die mit einer Komponente verknüpft ist, wenn diese Komponente nicht vorhanden ist. Nach dem Löschen der Lizenz wird diese nicht mehr auf iDRAC7 gespeichert, und die Basisproduktfunktionen werden aktiviert.
- Ersetzen – Ersetzen Sie die Lizenz, um eine Evaluierungslizenz zu verlängern, um einen Lizenztyp zu ändern, z. B. eine Evaluierungslizenz in eine erworbene Lizenz, oder um eine abgelaufene Lizenz zu verlängern.
 - Eine Evaluierungslizenz kann durch eine umfangreichere Evaluierungslizenz oder eine erworbene Lizenz ersetzt werden.
 - Eine erworbene Lizenz kann durch eine aktualisierte Lizenz oder durch eine umfangreichere Lizenz ersetzt werden.
- 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 Sie *.dell.com zur Liste der vertrauenswürdigen Sites in den Sicherheitseinstellungen hinterlegen. Weitere Informationen finden Sie in der Internet Explorer-Online-Dokumentation.

Bei einer 1-zu-n-Implementierung können Sie Dell License Manager verwenden. Weitere Informationen finden Sie im *Dell License Manager User's Guide* (Dell License Manager-Benutzerhandbuch) unter dell.com/support/manuals.

Importieren der Lizenz nach Ersetzen der Hauptplatine

Sie können das Local iDRAC7 Enterprise License Installation Tool verwenden, wenn Sie die Hauptplatine kürzlich austauschen mussten und die iDRAC7 Enterprise-Lizenz lokal (ohne Netzwerkverbindung) neu installiert und die dedizierte NIC aktiviert werden muss. Dieses Dienstprogramm installiert eine 30-tägige Testversion der iDRAC7 Enterprise-Lizenz, womit Sie die Möglichkeit haben, iDRAC von freigegebener zu dedizierter NIC zurückzusetzen.

Für mehr Informationen zu diesem Dienstprogramm und wo Sie dieses Programm herunterladen können, klicken Sie hier.

Status und Zustand von Lizenzkomponenten und verfügbare Optionen

In der folgenden Tabelle wird die Liste der verfügbaren Lizenzvorgänge auf der Basis des Status oder des Zustands der Lizenz angezeigt.

Tabelle 1. Lizenzvorgänge auf der Basis des Status oder des Zustands

Status oder Zustand von Lizenz/Komponente	Importieren	Exportieren	Löschen	Ersetzen	Weitere Informationen
Nicht-Administrator-Anmeldung	Nein	Nein	Nein	Nein	Ja
Aktive Lizenz	Ja	Ja	Ja	Ja	Ja
Abgelaufene Lizenz	Nein	Ja	Ja	Ja	Ja
Lizenz installiert, jedoch fehlt Komponente	Nein	Ja	Ja	Nein	Ja

Lizenzen über die iDRAC7-Web-Schnittstelle verwalten

Um Lizenzen über die iDRAC7-Web-Schnittstelle zu verwalten, gehen Sie zu **Übersicht** → **Server** → **Lizenzen**.

Daraufhin werden auf der Seite **Lizenzen** die Lizenzen angezeigt, die mit den Geräten verknüpft sind, oder jene Lizenzen, die zwar installiert sind, für die das entsprechende Gerät im System jedoch nicht vorhanden ist. Weitere Informationen zum Importieren, Exportieren, Löschen oder Ersetzen einer Lizenz finden Sie in der *iDRAC7-Online-Hilfe*.

Lizenzen über RACADM verwalten

Um Lizenzen über RACADM zu verwalten, verwenden Sie den Unterbefehl **license**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Lizenzierbare Funktionen in iDRAC7

In der folgenden Tabelle werden die iDRAC7-Funktionen aufgeführt, die gemäß der erworbenen Lizenz aktiviert sind.

Tabelle 2. Lizenzierbare iDRAC7-Funktionen

Funktion	Basisverwaltung mit IPMI	iDRAC7 Express (Rack- und Tower-Server)	iDRAC7 Express (für Blade-Server)	iDRAC7 Enterprise
Schnittstellen- und Standardunterstützung				
IPMI 2.0	Ja	Ja	Ja	Ja
Web-basierte Schnittstelle [1]	Nein	Ja	Ja	Ja
SNMP	Nein	Ja	Ja	Ja
WS-MAN	Ja	Ja	Ja	Ja
SMASH-CLP (SSH)	Nein	Ja	Ja	Ja
RACADM (SSH, Lokal und Remote) [1]	Nein	Ja	Ja	Ja
Telnet	Nein	Ja	Ja	Ja
Konnektivität				

Funktion	Basisverwaltung mit IPMI	iDRAC7 Express (Rack- und Tower-Server)	iDRAC7 Express (für Blade-Server)	iDRAC7 Enterprise
Freigegebene oder Failover-Netzwerkmodi (nur Rack- und Tower-Server)	Ja	Ja	Nein	Ja
Dedizierte NIC	Nein	Nein	Ja [2]	Ja [2,6]
DNS	Ja	Ja	Ja	Ja
VLAN-Tagging	Ja	Ja	Ja	Ja
IPv4	Ja	Ja	Ja	Ja
IPv6	Nein	Ja	Ja	Ja
Dynamisches DNS	Nein	Ja	Ja	Ja
Sicherheit und Authentifizierung				
Rollenbasierte Autorität	Ja	Ja	Ja	Ja
Lokale Benutzer	Ja	Ja	Ja	Ja
Verzeichnisdienste (Active Directory und Allgemeiner LDAP)	Nein	Nein	Nein	Ja
SSL-Verschlüsselung	Ja	Ja	Ja	Ja
Zweifaktor-Authentifizierung [3]	Nein	Nein	Nein	Ja
Single Sign-On (SSO)	Nein	Nein	Nein	Ja
PK-Authentifizierung (für SSH)	Nein	Nein	Nein	Ja
Sicherheitssperre	Nein	Ja	Ja	Ja
Remote-Verwaltung und Störungsbeseitigung				
Integrierte Diagnose	Ja	Ja	Ja	Ja
Seriell über LAN (mit Proxy)	Ja	Ja	Ja	Ja
Seriell über LAN (kein Proxy)	Nein	Ja	Ja	Ja
Absturzbildschirm-Capture	Nein	Ja	Ja	Ja
Absturzvideo-Capture	Nein	Nein	Nein	Ja
Start-Capture	Nein	Nein	Nein	Ja
Virtuelle Datenträger [4]	Nein	Nein	Ja	Ja
Virtuelle Konsole [4]	Nein	Nein	Ja [5]	Ja
Konsolenzusammenarbeit [4]	Nein	Nein	Nein	Ja
Virtueller Ordner	Nein	Nein	Nein	Ja
Chat über virtuelle Konsole	Nein	Nein	Nein	Ja
Remote-Dateifreigabe	Nein	Nein	Nein	Ja
vFlash [6]	Nein	Nein	Nein	Ja
vFlash-Partitionen [6]	Nein	Nein	Nein	Ja
Auto-Ermittlung	Nein	Ja	Ja	Ja
Serverprofil sichern	Nein	Nein	Nein	Ja

Funktion	Basisverwaltung mit IPMI	iDRAC7 Express (Rack- und Tower-Server)	iDRAC7 Express (für Blade-Server)	iDRAC7 Enterprise
Parts Replacement [8]	Nein	Ja	Ja	Ja
Network Time Protocol (NTP)	Nein	Ja	Ja	Ja
Überwachung und Stromversorgung				
Sensorüberwachung und Warnmeldungen	Ja	Ja	Ja	Ja
Geräteüberwachung	Nein	Ja	Ja	Ja
Speicherüberwachung	Nein	Ja	Ja	Ja
Einzelne CPU und Speichersensoren	Ja	Ja	Ja	Ja
E-Mail-Warnungen	Nein	Ja	Ja	Ja
Historische Stromzähler	Ja	Ja	Ja	Ja
Strombegrenzung	Nein	Nein	Nein	Ja
Echtzeit-Stromüberwachung	Ja	Ja	Ja	Ja
Echtzeit-Stromdiagramme	Nein	Ja	Ja	Ja
Protokollierung				
System-Ereignisprotokoll	Ja	Ja	Ja	Ja
RAC-Protokoll [7]	Nein	Ja	Ja	Ja
Ablaufverfolgungsprotokoll [7]	Nein	Ja	Ja	Ja
Remote-Syslog	Nein	Nein	Nein	Ja

[1] Die Lizenzverwaltung und die Firmware-Aktualisierungsfunktion unter iDRAC7 können immer über die iDRAC7-Web-Schnittstelle und RACADM aufgerufen werden.

[2] Alle Blade-Server verwenden zu jedem Zeitpunkt dedizierte Netzwerkschnittstellenkarten für iDRAC7, die Geschwindigkeit ist jedoch auf 100 MB/s begrenzt. GIGABYTE-Ethernet-Karten können auf Blade-Servern aufgrund der Gehäusebeschränkungen nicht verwendet werden, sie können jedoch bei Rack- und Tower-Servern mit einer Unternehmenslizenz eingesetzt werden. LAN auf der Hauptplatine (LOM) ist für Blade-Server nicht aktiviert.

[3] Die Zweifaktor-Authentifizierung kann über Active-X aktiviert werden und unterstützt daher nur Internet Explorer.

[4] Virtuelle Konsole und der virtuelle Datenträger sind verfügbar, wobei sowohl das Java- als auch das Active-X-Plugin verwendet werden.

[5] Virtuelle Konsole für einzelne Benutzer mit Remote-Start.

[6] Auf einigen Systemen ist die optionale iDRAC7-Schnittstellenkarte erforderlich.

[7] RAC- und Ablaufverfolgungsprotokolle sind in der Basisversion über die WS-MAN verfügbar.

[8] Parts Replacement ist eine Funktion von Lifecycle Controller, der den Prozess der Teileerneuerung vereinfacht, indem die Firmwareebene und die Konfiguration des Ersatzteils wiederhergestellt wird. Für weitere Informationen siehe *Dell Lifecycle Controller User's Guide* (Lifecycle-Controller-Benutzerhandbuch) unter dell.com/support/manuals.

Schnittstellen und Protokoll für den Zugriff auf iDRAC7

In der folgenden Tabelle werden die Schnittstellen für den Zugriff auf iDRAC7 dargestellt.




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

Tabelle 3. Schnittstellen und Protokoll für den Zugriff auf iDRAC7

Schnittstelle oder Protokoll	Beschreibung
Dienstprogramm für iDRAC-Einstellungen	Verwenden Sie das Dienstprogramm für die iDRAC-Einstellungen, um Vor-Betriebssystemabläufe durchzuführen. Dieses Dienstprogramm bietet neben weiteren Funktionen teilweise die Funktionen, die über die DRAC7-Web-Schnittstelle verfügbar sind. Drücken Sie zum Zugreifen auf das Dienstprogramm für die iDRAC-Einstellungen während des Startvorgangs auf <F2> und klicken Sie dann auf iDRAC-Einstellungen auf der Seite für das System-Setup-Hauptmenü .
iDRAC7-Web-Schnittstelle	Über die iDRAC7-Web-Schnittstelle können Sie iDRAC7 verwalten und das Managed System überwachen. Der Browser verbindet sich über die HTTPS-Schnittstelle mit dem Web Server. Datenflüsse werden für Datenschutz und Integrität über die 128-Bit-SSL-Verschlüsselung verschlüsselt. Sämtliche Verbindungen zur HTTP-Schnittstelle werden auf HTTPS umgeleitet. Administratoren können ihr eigenes SSL-Zertifikat über einen SSL-CSR-Generierungsprozess hochladen, um den Web Server zu sichern. Die Standard-HTTP- und HTTPS-Schnittstelle kann geändert werden. Der Benutzerzugriff basiert auf den Benutzerberechtigungen.
RACADM	Verwenden Sie das Befehlszeilendienstprogramm für iDRAC7- und Server-Verwaltungsvorgänge. Sie können RACADM lokal und remote verwenden. <ul style="list-style-type: none"> Die lokale RACADM-Befehlszeilenschnittstelle wird auf verwalteten Systemen ausgeführt, auf dem Server Administrator installiert ist. Der lokale RACADM kommuniziert über die bandinterne IPMI-Host-Schnittstelle mit iDRAC7. Da es auf dem lokal verwalteten System installiert ist, müssen sich Benutzer zum Ausführen dieses Dienstprogramms am Betriebssystem anmelden. Ein Benutzer muss über umfassende Administratorberechtigungen verfügen oder ein Root-Benutzer sein, um dieses Dienstprogramm verwenden zu können. Remote-RACADM ist ein Client-Dienstprogramm, das auf einer Management Station ausgeführt wird. Es verwendet die bandexterne Netzwerkschnittstelle, um die RACADM-Befehle auf dem Managed System auszuführen, außerdem wird der HTTPS-Kanal verwendet. Die Option <code>-r</code> führt den RACADM-Befehl über ein Netzwerk aus. Sie können auf den Firmware-RACADM zugreifen, indem Sie sich über SSH oder Telnet bei iDRAC7 anmelden. Sie können die Firmware-RACADM-Befehle ohne Angabe der IP-Adresse, des Benutzernamens oder des Kennworts für iDRAC7 ausführen. Es ist nicht erforderlich, die IP-Adresse, den Benutzernamen oder das Kennwort für iDRAC7 anzugeben, um die Firmware-RACADM-Befehle auszuführen. Nachdem Sie die RACADM-Befehlseingabe aufgerufen haben, können Sie die Befehle ohne das Präfix „racadm“ direkt ausführen.
Server-LC-Anzeige/ Gehäuse-LC-Anzeige	Verwenden Sie die LC-Anzeige auf der Frontblende des Servers, um die folgenden Aktivitäten auszuführen: <ul style="list-style-type: none"> Warnungen, IP- oder MAC-Adresse für iDRAC7 oder benutzerprogrammierbare Zeichenfolgen anzeigen DHCP festlegen Statische IP-Einstellungen für iDRAC7 konfigurieren <p>Bei Blade-Servern befindet sich die LC-Anzeige auf der Frontblende des Gehäuses und wird von allen Blades gemeinsam verwendet.</p> <p>Um iDRAC ohne einen Neustart des Servers neu zu starten, halten Sie die  für 16 Sekunden gedrückt.</p>

Schnittstelle oder Protokoll	Beschreibung
CMC-Webschnittstelle	<p>Neben der Überwachung und der Verwaltung des Gehäuses können Sie die CMC-Web-Schnittstelle für die folgenden Aktivitäten verwenden:</p> <ul style="list-style-type: none"> • Status eines Managed System anzeigen • iDRAC7-Firmware anzeigen • iDRAC7-Netzwerkeinstellungen konfigurieren • Melden Sie sich bei der iDRAC7 Webschnittstelle an. • Managed System starten, anhalten oder zurücksetzen • BIOS, PERC und unterstützte Netzwerkadapter aktualisieren
Lifecycle-Controller	<p>Verwenden Sie Lifecycle, um iDRAC7-Konfigurationen zu verwenden. Drücken Sie zum Zugreifen auf Lifecycle Controller während des Startvorgangs auf <F10> und gehen Sie dann zu System-Setup → Erweiterte Hardware-Konfiguration → iDRAC-Einstellungen. Weitere Informationen finden Sie im <i>Lifecycle Controller User's Guide</i> (Lifecycle Controller-Benutzerhandbuch) unter dell.com/support/manuals.</p>
Telnet	<p>Verwenden Sie Telnet, um auf iDRAC7 zuzugreifen und RACADM- und SMCLP-Befehle auszuführen. Weitere Details zu RACADM finden Sie im <i>RACADM Command Line Reference Guide for iDRAC7 and CMC</i> (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals. Weitere Details zu SMCLP finden Sie unter SMCLP verwenden.</p> <p> ANMERKUNG: Telnet ist kein sicheres Protokoll und wird standardmäßig angezeigt. Telnet überträgt alle Daten, einschließlich Kennwörter, im Textformat. Bei der Übertragung von vertraulichen Informationen verwenden Sie die SSH-Schnittstelle.</p>
SSH	<p>Verwenden Sie SSH, um die RACADM- und SMCLP-Befehle auszuführen. Es bietet die gleichen Funktionen wie die Telnet-Konsole und verwendet für höhere Sicherheit eine verschlüsselte Transportebene. Der SSH-Dienst ist standardmäßig auf iDRAC7 aktiviert, er kann jedoch deaktiviert werden. iDRAC7 unterstützt ausschließlich die SSH-Version 2 mit DSA- und dem RSA-Host-Schlüsselalgorithmus. Es wird ein einziger 1024-Bit-DSA- und 1024-Bit-RSA-Host-Schlüssel generiert, wenn Sie iDRAC7 zum ersten Mal einschalten.</p>
IPMITool	<p>Verwenden Sie IPMITool für den Zugriff auf die Basisverwaltungsfunktionen für das Remote-System über iDRAC7. Die Schnittstelle umfasst lokales IPMI, IPMI über LAN, IPMI über serielle Verbindungen und Serielle Verbindung über LAN. Weitere Informationen zu IPMITool finden Sie im <i>Dell OpenManage Baseboard Management Controller Utilities User's Guide</i> (Benutzerhandbuch zu den Dienstprogrammen des Dell OpenManage Baseboard-Verwaltungs-Controllers) unter dell.com/support/manuals.</p>
VMCLI	<p>Verwenden Sie Befehlszeilenschnittstelle für virtuelle Datenträger (VMCLI) für den Zugriff auf einen Remote-Datenträger über die Managed Station und für die Bereitstellung von Betriebssystemen auf mehreren Managed Systems.</p>
SMCLP	<p>Verwenden Sie das Server Management Workgroup Server Management-Command Line Protocol (SMCLP), um Systemverwaltungsaufgaben auszuführen. Dieses Protokoll ist über SSH oder Telnet verfügbar. Weitere Informationen zu SMCLP finden Sie unter SMCLP verwenden.</p>
WS-MAN	<p>Die LC-Remote Services basieren auf dem WS-Management-Protokoll für 1-zu-n-Verwaltungsaufgaben. Sie müssen einen WS-MAN-Client verwenden, z. B. den WinRM-Client (Windows) oder den OpenWSMAN-Client (Linux), um die LC-Remote Services-Funktion zu verwenden. Sie können außerdem Power Shell und Python verwenden, um auf die WS-MAN-Schnittstelle zu schreiben.</p> <p>Web Services for Management (WS-Management) ist ein Simple Object Access Protocol (SOAP)-basiertes Protokoll, das für die Systemverwaltung verwendet wird. iDRAC7 verwendet WS-Management, um Distributed Management Task Force (DMTF) Common Information Model (CIM)-basierte Verwaltungsinformationen zu transportieren. Die CIM-Informationen</p>

Schnittstelle oder Protokoll	Beschreibung
	<p>definieren die Semantik und die Informationstypen, die in einem Managed System geändert werden können. Die über WS-Management verfügbaren Daten werden über die iDRAC7-Instrumentierungsschnittstelle bereitgestellt, die mit den DMTF-Profilen und Erweiterungsprofilen verknüpft ist.</p> <p>Weitere Informationen stehen zur Verfügung unter:</p> <ul style="list-style-type: none"> • Lifecycle Controller-Remote Services User's Guide (Lifecycle Controller-Remote-Dienste-Benutzerhandbuch) unter dell.com/support/manuals. • Lifecycle Controller Integration Best Practices Guide (Lifecycle Controller Integration Best Practices-Handbuch) unter dell.com/support/manuals. • Lifecycle Controller-Seite auf Dell TechCenter — delltechcenter.com/page/Lifecycle+Controller • Lifecycle Controller WS-Management Script Center – delltechcenter.com/page/Scripting+the+Dell+Lifecycle+Controller • MOFs und Profile – delltechcenter.com/page/DCIM.Library • DMTF-Website – www.dmtf.org/standards/profiles/

iDRAC7-Schnittstelleninformationen

Die folgenden Schnittstellen sind erforderlich, um auf iDRAC7 im Remote-Zugriff durch Firewalls zugreifen zu können. Dies sind die standardmäßigen Schnittstellen, durch die iDRAC7 auf Verbindungen hört. Für das weitere Vorgehen siehe [Dienste konfigurieren](#).

Tabelle 4. Schnittstellen, die iDRAC7 für Verbindungen hört

Schnittstellenummer	Funktion
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
5900*	Umleitung von Tastatur und Maus für die virtuelle Konsole, für virtuelle Datenträger, für virtuelle Ordner und die Remote-Dateifreigabe

* Konfigurierbare Schnittstelle

Die folgende Tabelle listet die Schnittstellen auf, die iDRAC7 als Client verwendet.

Tabelle 5. Schnittstellen, die iDRAC7 als Client verwendet

Schnittstellenummer	Funktion
25	SMTP
53	DNS
68	DHCP-zugewiesene IP-Adresse
69	TFTP
162	SNMP-Trap
445	Common Internet File System (CIFS)

Schnittstellenummer	Funktion
636	LDAP über SSL (LDAPS)
2049	Network File System (NFS)
123	Network Time Protocol (NTP)
3269	LDAPS für globalen Katalog (GC)

Weitere nützliche Dokumente

Zusätzlich zu diesem Handbuch bieten die folgenden, auf der Dell Support-Website unter dell.com/support/manuals verfügbaren Dokumente zusätzliche Informationen über das Setup und den Betrieb des iDRAC7 auf dem System. Auf der Seite **Handbücher** klicken Sie auf **Software** → **Systemverwaltung**. Klicken Sie auf den entsprechenden Produktlink auf der rechten Seite, um auf die Dokumente zuzugreifen:

- Die *iDRAC7-Online-Hilfe* bietet detaillierte Informationen und Beschreibungen zu den Feldern, die auf der iDRAC7-Web-Schnittstelle angezeigt werden. Sie können nach der Installation von iDRAC7 auf die Online-Hilfe zugreifen.
- Das *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC* enthält Informationen zu den RACADM-Unterbefehlen, den unterstützten Schnittstellen und iDRAC6-Eigenschaften-Datenbankgruppen und Objektdefinitionen.
- Das *Benutzerhandbuch zur Systemverwaltungsübersicht* bietet zusammengefasste Informationen zu den verschiedenen Software-Produkten, die für Systemverwaltungsaufgaben verfügbar sind.
- Das *Dell Lifecycle Controller User's Guide* (Lifecycle Controller-Benutzerhandbuch) enthält Informationen zur Verwendung der grafischen Benutzeroberfläche (GUI) von Lifecycle Controller.
- Die *Dell Lifecycle Controller Remote Services Quick Start Guide* (Dell Lifecycle Controller Remote-Dienste-Schnellstartanleitung) enthält einen Überblick der Möglichkeiten der Remote-Dienste, Informationen zum Einrichten der Remote-Dienste, Lifecycle Controller API und gibt Referenzen zu verschiedenen Ressourcen zum DELL Tech Center.
- Das *Dell Remote Access Configuration Tool User's Guide* (Benutzerhandbuch für das Remote-Zugriffs-Konfigurationshilfsprogramm von Dell) enthält Informationen zur Verwendung des Tools für die Ermittlung von iDRAC-IP-Adressen in Ihrem Netzwerk und zum Ausführen von 1-zu-n-Firmware-Aktualisierungen und Active Directory-Konfigurationen für die ermittelten IP-Adressen.
- Die *Dell Systems Software Support Matrix* bietet Informationen über die verschiedenen Dell-Systeme, über die von diesen Systemen unterstützten Betriebssysteme und über die Dell OpenManage-Komponenten, die auf diesen Systemen installiert werden können.
- Das *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*.
- Infodateien können vorhanden sein. Diese geben den letzten Stand der Änderungen am System oder an der Dokumentation wieder und enthalten erweitertes technisches Referenzmaterial für erfahrene Benutzer oder Techniker.
- Das *Glossar* enthält Informationen zu den in diesem Dokument verwendeten Begriffen.


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

- Das *iDRAC7-Übersichts- und Funktionshandbuch* enthält Informationen zu iDRAC7, zu lizenzierten Funktionen und zu Lizenzaktualisierungsoptionen.
- In den mit dem System gelieferten Sicherheitshinweisen finden Sie wichtige Informationen zur Sicherheit und zu den Betriebsbestimmungen. Weitere Betriebsbestimmungen finden Sie auf der Website zur Einhaltung

gesetzlicher Vorschriften unter www.dell.com/regulatory_compliance. Garantieinformationen können möglicherweise als separates Dokument beigelegt sein.

- In der zusammen mit der Rack-Lösung gelieferten *Anweisungen für die Rack-Montage* wird beschrieben, wie das System in einem Rack installiert wird.
- Das *Handbuch zum Einstieg* enthält eine Übersicht über die Systemfunktionen, die Einrichtung des Systems und technische Daten.
- Im *Benutzerhandbuch* erhalten Sie Informationen zu Systemfunktionen, zur Fehlerbehebung am System und zur Installation oder zum Austausch von Systemkomponenten.

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.

Dell stellt verschiedene onlinebasierte und telefonische Support- und Serviceoptionen bereit. Da die Verfügbarkeit dieser Optionen je nach Land und Produkt variiert, stehen einige Services in Ihrer Region möglicherweise nicht zur Verfügung. So erreichen Sie den Vertrieb, den Technischen Support und den Kundendienst von Dell:

1. Besuchen Sie www.dell.com/support.
2. Wählen Sie Ihre Supportkategorie.
3. Wählen Sie das Land bzw. die Region im Listenmenü „Choose a Country/Region“ (Land oder Region auswählen) am oberen Seitenrand aus.
4. Klicken Sie je nach Bedarf auf den entsprechenden Service- oder Support-Link.

Bei iDRAC7 anmelden

Sie können sich bei iDRAC7 als iDRAC7-Benutzer, als Microsoft Active Directory-Benutzer oder als Lightweight Directory Access Protocol (LDAP)-Benutzer anmelden. Der Standardbenutzername lautet „root“, und das Standardkennwort lautet „calvin“. Sie können sich auch über die einmalige Anmeldung (SSO) oder die Smart Card anmelden.


 **ANMERKUNG:** Sie müssen über Berechtigungen zum Anmelden bei iDRAC verfügen, um sich bei iDRAC7 anzumelden.


Verwandte Links

- [Anmelden als lokaler Benutzer, Active Directory-Benutzer oder LDAP-Benutzer bei iDRAC7](#)
- [Anmeldung beim iDRAC7 mit Smart Card](#)
- [Bei iDRAC7 über die einmalige Anmeldung anmelden](#)
- [Ändern des standardmäßigen Anmeldungskennworts](#)

Anmelden als lokaler Benutzer, Active Directory-Benutzer oder LDAP-Benutzer bei iDRAC7


Stellen Sie vor der Anmeldung bei iDRAC7 über die Web-Schnittstelle sicher, dass Sie einen unterstützten Web-Browser konfiguriert haben und dass das Benutzerkonto mit den erforderlichen Berechtigungen erstellt wurde.

 **ANMERKUNG:** Bei der Eingabe des Benutzernamens für einen Active Directory-Benutzer ist die Groß- und Kleinschreibung *nicht* relevant, beim Kennwort muss die Groß- und Kleinschreibung jedoch bei allen Benutzern beachtet werden.

 **ANMERKUNG:** Neben Active Directory werden auch die auf openLDAP, openDS, Novell eDir und Fedora basierenden Verzeichnisdienste unterstützt. Größer- und Kleiner-Zeichen (< und >) sind in Benutzernamen nicht zulässig.

So melden Sie sich als lokaler Benutzer, Active Directory-Benutzer oder LDAP-Benutzer bei iDRAC7 an:

1. Öffnen Sie einen unterstützten Webbrowser.
2. Geben Sie in das Feld **Adresse** `https://[iDRAC7-IP-Adresse]` ein und drücken Sie die <Eingabetaste>.

 **ANMERKUNG:** Wenn die Standard-HTTPS-Schnittstellenummer (Schnittstelle 443) geändert wurde, geben Sie Folgendes ein: `https://[iDRAC7-IP-Adresse]:[Schnittstellenummer]`, wobei `[iDRAC7-IP-Adresse]` für die iDRAC7-IPv4- oder die IPv6-Adresse und `[Schnittstellenummer]` für die HTTPS-Schnittstellenummer steht.

Die **Login**-Seite (Anmeldung) wird angezeigt.
3. Bei einem lokalen Benutzer:
 - Geben Sie in die Felder **Benutzername** und **Kennwort** Ihre Daten für den iDRAC7-Benutzernamen und das Kennwort ein.
 - Wählen Sie aus dem Drop-Down-Menü **Domäne** die Option **Dieser iDRAC** aus.
4. Geben Sie für einen Active Directory-Benutzer in die Felder **Benutzername** und **Kennwort** den Active Directory-Benutzer und das zugehörige Kennwort ein. Wenn Sie den Domänennamen als Teil des Benutzernamens

angegeben haben, wählen Sie **Dieser iDRAC** aus dem Drop-Down-Menü aus. Benutzernamen können in den folgenden Formaten angegeben werden: <Domäne>\<Benutzername>, <Domäne>/<Benutzername> oder <Benutzer>@<Domäne>.

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

Wenn die Domäne im Benutzernamen nicht angegeben ist, wählen Sie die Active Directory-Domäne aus dem Drop-Down-Menü **Domäne** aus.

5. Geben Sie für einen LDAP-Benutzer Ihren LDAP-Benutzernamen und das zugehörige Kennwort in die Felder **Benutzername** und **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 Benutzerberechtigungen bei iDRAC7 angemeldet. Wenn Sie sich mit Berechtigungen „Benutzer 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.

Verwandte Links

- [Benutzerkonten und Berechtigungen konfigurieren](#)
- [Ändern des standardmäßigen Anmeldungskennworts](#)
- [Konfigurieren von unterstützten Webbrowsern](#)

Anmeldung beim iDRAC7 mit Smart Card

Sie können sich über eine Smart Card bei iDRAC7 anmelden. Smart Cards verfügen über eine Zweifaktor-Authentifizierung (TFA) mit Sicherheit auf zwei Ebenen:

- Physisches Smart Card-Gerät.
- Geheimcode, z. B. ein Kennwort oder eine PIN.

Benutzer müssen ihre Anmeldeinformationen über die Smart Card und die PIN überprüfen.

Verwandte Links

- [Bei iDRAC7 über eine Smart Card als lokaler Benutzer anmelden](#)
- [Bei iDRAC7 über eine Smart Card als Active Directory-Benutzer anmelden](#)

Bei iDRAC7 über eine Smart Card als lokaler Benutzer anmelden

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

- Benutzer-Smart Card-Zertifikat und vertrauenswürdige Zertifikat der Zertifizierungsstelle nach iDRAC7 hochladen
- Smart Card-Anmeldung aktivieren


Die iDRAC7-Webschnittstelle zeigt die Smart Card-Anmeldeseite für alle Benutzer an, die für die Verwendung der Smart Card konfiguriert wurden.




ANMERKUNG: Abhängig von den Browser-Einstellungen werden Sie aufgefordert, das Smart Card Reader-ActiveX-Plugin herunterzuladen und zu installieren, wenn Sie diese Funktion zum ersten Mal anwenden.

So melden Sie sich bei iDRAC7 als lokaler Benutzer über eine Smart Card an:

1. Rufen Sie die iDRAC7-Web-Schnittstelle über den Link `https://[IP-Adresse]` auf. Die **iDRAC7**-Anmeldeseite wird eingeblendet und fordert Sie zum Einlegen der Smart Card auf.

 **ANMERKUNG:** Wenn die standardmäßige HTTPS-Schnittstellenummer (Schnittstelle 443) geändert wurde, geben Sie Folgendes ein: `https://[IP-Adresse]:[Schnittstellenummer]`, wobei [IP-Adresse] für die IP-Adresse des iDRAC7 und [Schnittstellenummer] für die HTTPS-Schnittstellenummer steht.

2. Legen Sie die Smart Card in das Laufwerk ein, und klicken Sie auf **Anmeldung**.
Sie werden daraufhin dazu aufgefordert, die PIN für die Smart Card einzugeben. Ein Kennwort wird nicht benötigt.
3. Geben Sie die PIN der Smart Card für lokale Smart Card-Benutzer ein.
Sie werden am iDRAC7 angemeldet.

 **ANMERKUNG:** Wenn Sie ein lokaler Benutzer sind, für den die Option **CRL-Prüfung für Smart Card-Anmeldung aktivieren** aktiviert ist, versucht iDRAC7, die Zertifikatsperrliste (CRL) herunterzuladen und überprüft die Zertifikatsperrliste (CRL) auf das Benutzerzertifikat. Die Anmeldung schlägt fehl, wenn das Zertifikat in der Zertifikatsperrliste als „Widerrufen“ gekennzeichnet ist oder wenn die Zertifikatsperrliste aus bestimmten Gründen nicht heruntergeladen werden kann.

Verwandte Links

- [Smart Card-Anmeldung aktivieren oder deaktivieren](#)
- [iDRAC7-Smart Card-Anmeldung für lokale Benutzer konfigurieren](#)


Bei iDRAC7 über eine Smart Card als Active Directory-Benutzer anmelden

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

- Laden Sie ein vertrauenswürdigen Zertifikat einer Zertifizierungsstelle (ein von einer Zertifizierungsstelle signiertes Active Directory-Zertifikat) nach iDRAC7 hoch.
- Konfigurieren Sie den DNS-Server.
- Aktivieren Sie die Active Directory-Anmeldung.
- Smart Card-Anmeldung aktivieren

So melden Sie sich über eine Smart Card als Active Directory-Benutzer bei iDRAC7 an:

1. Melden Sie sich über den Link `https://[IP-Adresse]` bei iDRAC7 an.
Die **iDRAC7-Anmeldeseite** wird eingeblendet und fordert Sie zum Einlegen der Smart Card auf.

 **ANMERKUNG:** Wenn die standardmäßige HTTPS-Schnittstellenummer (Schnittstelle 443) geändert wird, geben Sie Folgendes ein: `https://[IP-Adresse]:[Schnittstellenummer]`, wobei [IP-Adresse] für die iDRAC7-IP-Adresse und [Schnittstellenummer] für die HTTPS-Schnittstellenummer steht.

2. Legen Sie die Smart Card ein und klicken Sie auf **Anmeldung**.
Daraufhin wird das Popup-Fenster für die **PIN** angezeigt.
3. Geben Sie die PIN ein und klicken Sie auf **Senden**.
Sie sind über Ihre Active Directory-Anmeldedaten bei iDRAC7 angemeldet.

 **ANMERKUNG:**

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

Verwandte Links

- [Smart Card-Anmeldung aktivieren oder deaktivieren](#)
- [iDRAC7-Smart-Card-Anmeldung für Active Directory-Benutzer konfigurieren](#)

Bei iDRAC7 über die einmalige Anmeldung anmelden

Wenn die einmalige Anmeldung (SSO) aktiviert ist, können Sie sich ohne die Eingabe Ihrer Anmeldeinformationen für die Domänen-Benutzerauthentifizierung (also Benutzername und Kennwort) bei iDRAC7 anmelden.

Verwandte Links

[iDRAC7-SSO-Anmeldung für Active Directory-Benutzer konfigurieren](#)


Bei iDRAC7 SSO über die iDRAC7-Web-Schnittstelle anmelden


Bevor Sie sich über das Verfahren für die einmalige Anmeldung bei iDRAC7 anmelden, müssen Sie Folgendes sicherstellen:

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

So melden Sie sich über die Web-Schnittstelle bei iDRAC7 an:

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

 **ANMERKUNG:** Wenn die standardmäßige HTTPS-Schnittstellennummer (Schnittstelle 443) geändert wurde, geben Sie Folgendes ein: `https://[IP-Adresse]:[Schnittstellennummer]`, wobei [IP-Adresse] für die IP-Adresse des iDRAC7 und [Schnittstellennummer] für die HTTPS-Schnittstellennummer steht.

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

iDRAC7 meldet Sie mit den entsprechenden Microsoft Active Directory-Berechtigungen an und verwendet dabei die Anmeldeinformationen, die durch das Betriebssystem erfasst wurden, während Sie sich über ein gültiges Active Directory-Konto angemeldet haben.

Bei iDRAC7 SSO über die CMC-Web-Schnittstelle anmelden

Durch die Verwendung der SSO-Funktion können Sie die iDRAC7-Web-Schnittstelle über die CMC-Web-Schnittstelle starten. Ein CMC-Benutzer verfügt über CMC-Benutzerberechtigungen, wenn er iDRAC7 über CMC startet. Wenn das Benutzerkonto in CMC vorhanden ist, jedoch nicht in iDRAC, kann der Benutzer iDRAC7 dennoch über CMC starten.

Wenn iDRAC7-Netzwerk-LAN deaktiviert ist (LAN aktiviert = Nein), ist die SSO (Einzelanmeldung) nicht verfügbar.

Wenn der Server aus dem Gehäuse entfernt oder die iDRAC7-IP-Adresse geändert wird, oder wenn ein Problem bei der iDRAC7-Netzwerkverbindung vorliegt, wird die Option zum Starten von iDRAC7 in der CMC-Web-Schnittstelle ausgegraut dargestellt.


Weitere Informationen finden Sie im *Chassis Management Controller User's Guide* (Chassis Management Controller-Benutzerhandbuch) unter dell.com/support/manuals.

Über Remote-RACADM auf iDRAC7 zugreifen

Sie können Remote-RACADM für den Zugriff auf iDRAC7 über das RACADM-Dienstprogramm verwenden.

Weitere Informationen finden Sie im *RACADM Reference Guide for iDRAC7 and CMC* (RACADM-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.

Wenn die Management Station das iDRAC7-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 iDRAC7-Zertifikat handelt es sich um das Zertifikat, das iDRAC7 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.

Verwandte Links

[Zertifizierungsstellenzertifikat für die Verwendung von Remote-RACADM auf Linux validieren](#)

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 Standard-Zertifizierungsstellenzertifikat-Bundle auf der Management Station. Für RHEL5 64-bit lautet es beispielsweise **/etc/pki/tls/cert.pem**.
3. Hängen Sie das PEM-formatierte CA-Zertifikat an das CA-Zertifikat der Management Station an.
Verwenden Sie beispielsweise den CAT-Befehl: `cat testcacert.pem >> cert.pem`
4. Generieren Sie das Server-Zertifikat, und laden Sie es nach iDRAC7 hoch.

Über lokalen RACADM auf iDRAC7 zugreifen

Weitere Informationen zum Zugriff auf iDRAC7 über den lokalen RACADM finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Über Firmware-RACADM auf iDRAC7 zugreifen

Sie können die SSH- oder Telnet-Schnittstellen für den Zugriff auf iDRAC7 und zum Ausführen der Firmware-RACADM-Befehle verwenden. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Über SMCLP auf iDRAC7 zugreifen

SMCLP ist die Standard-Befehlszeileneingabe, wenn Sie sich über Telnet oder SSH bei iDRAC7 anmelden. Weitere Informationen finden Sie unter [SMCLP verwenden](#).

Anmeldung beim iDRAC7 mit Authentifizierung mit öffentlichem Schlüssel

Sie können sich über SSH beim iDRAC6 anmelden, ohne ein Kennwort einzugeben. Sie können auch einen einzelnen RACADM-Befehl als Befehlszeilenargument an die SSH-Anwendung senden. Die Befehlszeilenoptionen verhalten sich ähnlich wie Remote-RACADM, da die Sitzung endet, nachdem der Befehl ausgeführt wurde.

Zum Beispiel:

Anmeldung:

```
SSH-Benutzername@<Domäne>
```

oder

```
SSH-Benutzername@<IP_Adresse>
```

wobei IP-Adresse die IP-Adresse des iDRAC7 ist.

Senden von RACADM-Befehlen:

```
SSH-Benutzername@<Domäne> racadm getversion
```

```
SSH-Benutzername@<Domäne> racadm getsel
```

Verwandte Links

[Authentifizierung über öffentlichen Schlüssel für SSH verwenden](#)

Mehrere iDRAC7-Sitzungen

Aus der folgenden Tabelle können Sie eine Liste mit mehreren iDRAC7-Sitzungen entnehmen, die durch die Verwendung der diversen Schnittstellen möglich sind.

Tabelle 6. Mehrere iDRAC7-Sitzungen

Schnittstelle	Anzahl der Sitzungen
iDRAC7-Web-Schnittstelle	4
Remote-RACADM	4
Firmware-RACADM/SMCLP	SSH – 2 Telnet – 2 Seriell – 1

Ändern des standardmäßigen Anmeldungskennworts

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

- Sie sich bei iDRAC7 mit der Berechtigung „Benutzer konfigurieren“ anmelden.
- Die Warnungsfunktion des standardmäßigen Kennworts aktiviert ist.
- Anmeldeinformationen für das derzeitige aktive Konto root/calvin lauten.

Die gleiche Warnungsmeldung wird angezeigt, wenn Sie sich unter Verwendung von Active Directory oder LDAP anmelden. Konten von Active Directory oder LDAP werden nicht berücksichtigt, wenn bestimmt wird, ob irgendein Konto (lokal) root/calvin als Anmeldeinformationen hat. Es wird außerdem eine Warnungsmeldung angezeigt, wenn Sie sich bei iDRAC unter Verwendung von SSH, Telnet, Remote RACADM oder Web-Schnittstelle anmelden. Für Web-Interface, SSH und Telnet wird eine einzelne Warnungsmeldung für jede Sitzung angezeigt. Für Remote RACADM wird für jeden Befehl eine Warnungsmeldung angezeigt.

Um die Anmeldeinformationen zu ändern, müssen Sie über die Berechtigung „Benutzer konfigurieren“ verfügen.

Verwandte Links

[Aktivieren oder Deaktivieren der standardmäßigen Kennwortwarnungsmeldung](#)

Ändern des standardmäßigen Anmeldekennworts unter Verwendung von Web-Schnittstelle

Wenn Sie sich an die iDRAC7 Web-Schnittstelle anmelden und die Seite **Standardmäßige Kennwortwarnung** angezeigt wird, können Sie das Kennwort ändern. Gehen Sie dabei folgendermaßen vor:

1. Wählen Sie die Option **Standardmäßiges Kennwort ändern**.
2. Geben Sie im Feld **Neues Kennwort** das neue Kennwort ein.
Das Kennwort darf maximal 20 Zeichen lang sein. Die Zeichen sind maskiert. Folgende Zeichen werden unterstützt:
 - 0-9
 - A-Z
 - a-z
 - Sonderzeichen: +, &, ?, >, -, }, |, ,, !, (, ' ,, _ [, " , @, #,), *, ;, \$,], /, \$, %, =, <, :, {, |, \
3. Geben Sie in dem Feld **Kennwort bestätigen** das Kennwort erneut ein.
4. Klicken Sie auf **Fortfahren**. Das neue Kennwort ist konfiguriert und Sie sind bei 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 *iDRAC7-Online-Hilfe*.

Ändern eines in den Standardeinstellungen festgelegten Anmeldungskennworts unter Verwendung von RACADM

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

```
racadm set iDRAC.Users.<Index>.Password <Kennwort>
```

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

Lesen Sie für weitere Informationen das *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC).

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

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

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Benutzerkonfiguration**. Daraufhin wird die Seite **iDRAC-Einstellungen – Benutzerkonfiguration** angezeigt.
2. Geben Sie im Feld **Kennwort ändern** das neue Kennwort ein.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**. Die Details werden gespeichert.

Aktivieren oder Deaktivieren der standardmäßigen Kennwortwarnungsmeldung

Sie können die Anzeige der standardmäßigen Kennwortwarnungsmeldung aktivieren oder deaktivieren. Dafür benötigen Sie jedoch die Berechtigung „Benutzer konfigurieren“.

Aktivieren oder Deaktivieren einer standardmäßigen Kennwortwarnungsmeldung unter Verwendung der Web-Schnittstelle

So aktivieren oder deaktivieren Sie die Anzeige der standardmäßigen Kennwortwarnungsmeldung nach der Anmeldung bei iDRAC:


1. Gehen Sie zu **Übersicht** → **iDRAC Einstellungen** → **Benutzerauthentifizierung** → **Lokale Benutzer**. Die Seite **Benutzer** wird angezeigt.
2. Im Abschnitt **Standardmäßige Kennwortwarnung** die Option **Aktivieren** auswählen und anschließend auf **Anwenden** klicken, um die Anzeige der Seite **Standardmäßige Kennwortwarnung** anzuzeigen, wenn Sie sich bei iDRAC7 anmelden. Andernfalls klicken Sie auf **Deaktivieren**.
Alternativ können Sie, wenn diese Option aktiviert ist und Sie eine Anzeige der Warnmeldung für nachfolgende Anmeldungen vermeiden wollen, erst auf die Option **Diese Warnmeldung nicht noch einmal anzeigen** auf der Seite **Standardmäßigen Kennwortwarnung** und dann auf **Anwenden** klicken.

Aktivieren oder Deaktivieren der Warnungsmeldung zum Ändern des standardmäßigen Anmeldungskennworts unter Verwendung von RACADM

Um die Anzeige der Warnungsmeldung zum Ändern des standardmäßigen Anmeldekennworts unter Verwendung von RACADM zu aktivieren, verwenden Sie das Objekt `idrac.tuning.DefaultCredentialWarning`. Für weitere Informationen siehe *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Managed System und Management Station einrichten

Für die bandexterne Systemverwaltung über iDRAC7 müssen Sie iDRAC7 für die Remote-Zugriffsmöglichkeit konfigurieren, die Management Station und das Managed System einrichten und die unterstützten Web-Browser konfigurieren.


 **ANMERKUNG:** Bei Blade-Servern müssen Sie vor der Ausführung der Konfigurationsschritte die CMC- und E/A-Module im Gehäuse und das System physisch in das Gehäuse installieren.

Verwandte Links

- [iDRAC7-IP-Adresse einrichten](#)
- [Managed System einrichten](#)
- [Aktualisieren der Gerätefirmware](#)
- [Rollback der iDRAC7-Firmware durchführen](#)
- [Management Station einrichten](#)
- [Konfigurieren von unterstützten Webbrowsern](#)

iDRAC7-IP-Adresse einrichten

Sie müssen die anfänglichen Netzwerkeinstellungen auf der Basis Ihrer Netzwerkinfrastruktur konfigurieren, um die bilaterale Kommunikation mit iDRAC7 zu aktivieren. Sie können die IP-Adresse über eine der folgenden Schnittstellen einrichten:

- Dienstprogramm für die iDRAC-Einstellungen
- Lifecycle-Controller (siehe *Lifecycle-Controller-Benutzerhandbuch*)
- Dell Deployment Toolkit (siehe *Dell Deployment Toolkit-Benutzerhandbuch*)
- LC-Anzeige auf der Gehäuse- oder Server-Frontblende (siehe das *Hardware-Benutzerhandbuch* für das System)
 -  **ANMERKUNG:** Bei Blade-Servern können Sie die Netzwerkeinstellung über die Gehäuse-LC-Anzeige auf der Frontblende nur im Rahmen der Erstkonfiguration von CMC konfigurieren. Nach der Bereitstellung des Gehäuses können Sie iDRAC7 nicht mehr über die Gehäuse-LC-Anzeige auf der Frontblende neu konfigurieren.
- CMC-Web-Schnittstelle (siehe *Dell Chassis Management Controller Firmware-Benutzerhandbuch*)

Bei Rack- und Tower-Servern können Sie die IP-Adresse einrichten oder die iDRAC7-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 iDRAC7 einrichten.

Bei Blade-Servern wird standardmäßig die iDRAC7-Netzwerkschnittstelle angezeigt.

Nach der Konfiguration der iDRAC7-IP-Adresse:

- Stellen Sie sicher, dass Sie *nach dem Einrichten der iDRAC7-IP-Adresse den Benutzernamen und das Kennwort ändern*.
- Greifen Sie über die folgenden Schnittstellen auf iDRAC7 zu:

- iDRAC7 Web-Schnittstelle unter Verwendung eines unterstützten Browsers (Internet Explorer, Firefox, Chrome oder Safari)
- Secure Shell (SSH) – Erfordert einen Client, wie z. B. PuTTY auf Windows. SSH ist standardmäßig auf den meisten Linux-Systemen verfügbar, so dass kein Client benötigt wird.
- Telnet (muss aktiviert werden, da es standardmäßig deaktiviert ist)
- 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 von **support.dell.com** abgerufen werden kann)

Verwandte Links

- [iDRAC-IP-Adresse über das Dienstprogramm für die iDRAC-Einstellungen einrichten](#)
- [iDRAC7-IP-Adresse über die CMC-Web-Schnittstelle einrichten](#)
- [Auto-Ermittlung aktivieren](#)

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

So richten Sie die iDRAC7-IP-Adresse ein:

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

Verwandte Links

- [Netzwerkeinstellungen](#)
- [Allgemeine Einstellungen](#)
- [IPv4-Einstellungen](#)
- [IPv6-Einstellungen](#)
- [IPMI-Einstellungen](#)
- [VLAN-Einstellungen](#)


Netzwerkeinstellungen

So konfigurieren Sie die Netzwerkeinstellungen:




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

1. Wählen Sie unter **NIC aktivieren** die Option **Aktiviert** aus.
2. Wählen Sie aus dem Drop-Down-Menü **NIC-Auswahl** auf der Basis der Netzwerkanforderung eine der folgenden Schnittstellen aus:
 - **Dediziert** – Wählen Sie diese Option aus, um das Remote-Zugriffsgerät zu aktivieren und die auf dem Remote-Access-Controller (RAC) verfügbare dedizierte Netzwerkschnittstelle zu verwenden. Die DRAC-Schnittstelle wird nicht an das Host-Betriebssystem freigegeben und leitet den Verwaltungsverkehr zu einem separaten physischen Netzwerk, wodurch sie vom Anwendungsverkehr getrennt werden kann. Diese Option impliziert, dass die dedizierte iDRAC-Netzwerkschnittstelle den Datenverkehr getrennt von den LOM- oder NIC-Schnittstellen des Servers weiterleitet. Bei der Verwaltung des Netzwerkdatenverkehrs kann iDRAC über die Option „Dediziert“ im Vergleich zu den IP-Adressen, die dem Host-LOM oder den NICs zugewiesen werden, eine IP-Adresse vom gleichen Subnetz oder einem anderen Subnetz zugewiesen werden.

 **ANMERKUNG:** Diese Option ist nur auf Rack- oder Tower-Systemen mit einer iDRAC7 Enterprise-Lizenz verfügbar. Bei Blades ist diese Option standardmäßig verfügbar.

- 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. Blade-Server verwenden kein LOM für die Kommunikation mit iDRAC7.

3. Wählen Sie aus dem Drop-Down-Menü **Failover-Netzwerk** eine der verbleibenden LOMs aus. Wenn ein Netzwerk ausfällt, wird der Datenverkehr über das Failover-Netzwerk umgeleitet.

 **ANMERKUNG:** Wenn Sie in der Drop-Down-Liste **NIC-Auswahl** die Option **Dediziert** ausgewählt haben, wird diese Option ausgegraut dargestellt.

Wenn beispielsweise der iDRAC7-Netzwerkverkehr über LOM2 umgeleitet werden soll, wenn LOM1 ausgefallen ist, wählen Sie **LOM1** unter **NIC-Auswahl** und **LOM2** unter **Failover-Netzwerk** aus.

4. Wählen Sie unter **Automatische Verhandlung** die Option **Eingeschaltet** aus, wenn iDRAC7 den Duplexmodus und die Netzwerkgeschwindigkeit automatisch festlegen muss. Diese Option ist nur im dedizierten Modus verfügbar. Wenn sie aktiviert ist, legt iDRAC7 die Netzwerkgeschwindigkeit auf der Basis der Netzwerkgeschwindigkeit auf 10, 100 oder 1.000 MB/s fest.
5. Wählen Sie unter **Netzwerkgeschwindigkeit** entweder 10 oder 100 MB/s aus.

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

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

 **ANMERKUNG:** Wenn Sie **Automatische Verhandlung** ausgewählt haben, wird diese Option ausgegraut dargestellt.

Allgemeine Einstellungen

Wenn die Netzwerkinfrastruktur einen DNS-Server aufweist, registrieren Sie iDRAC7 auf diesem DNS. Hierbei handelt es sich um die anfänglichen Einstellungsanforderungen für erweiterte Funktionen, darunter „Verzeichnisdienste – Active Directory oder LDAP“, Einmalige Anmeldung und Smart Card.

So registrieren Sie iDRAC7:

1. **DRAC auf DNS registrieren** aktivieren.
2. Geben Sie den **DNS-DRAC-Namen** ein.

3. Wählen Sie **Domännennamen automatisch konfigurieren** aus, um den Domännennamen automatisch von DHCP abzurufen. Stellen Sie den **DNS-Domännennamen** andernfalls bereit.

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 zu iDRAC7 zuweisen kann. Wählen Sie ansonsten die Option **Deaktiviert** aus, und geben Sie die Werte für die folgenden Elemente ein:
 - Statische IP-Adresse
 - Statisches Gateway
 - Statische Subnetzmaske
3. Aktivieren Sie optional die Option **DHCP zum Abrufen der DNS-Server-Adresse verwenden**, so dass der DHCP-Server den **bevorzugten statischen DNS-Server** und den **alternativen statischen DNS-Server** zuweisen kann. Geben Sie ansonsten die IP-Adressen für **Statisch Bevorzugter DNS-Server** und **Statisch Alternativer DNS-Server** ein.

IPv6-Einstellungen

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

So konfigurieren Sie die IPv6-Einstellungen:

1. Wählen Sie die Option **Aktiviert** unter **IPv6 aktivieren** aus.
2. Damit der DHCPv6-Server die IP-Adresse, das Gateway und die Subnetzmaske iDRAC7 automatisch zuweisen kann, wählen Sie die Option **Aktiviert** unter **Auto-konfiguration aktivieren** aus. Falls diese Option aktiviert wird, werden die statischen Werte deaktiviert. Fahren Sie ansonsten mit dem nächsten Schritt für die Konfiguration über die statische IP-Adresse fort.
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 0 und 128 ein.
5. Geben Sie in das Feld **Statisches Gateway** die Gateway-Adresse ein.
6. Wenn Sie DHCP verwenden, aktivieren Sie die Option **DHCPv6 für das Abrufen von DNS-Server-Adressen einrichten**, um primäre und sekundäre DNS-Server-Adressen vom DHCPv6-Server abzurufen. Anderfalls wählen Sie **Deaktiviert** aus und gehen Sie folgendermaßen vor:
 - 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.

IPMI-Einstellungen

So aktivieren Sie die IPMI-Einstellungen:

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

VLAN-Einstellungen


Sie können iDRAC7 für die VLAN-Infrastruktur konfigurieren. So konfigurieren Sie die VLAN-Einstellungen:

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.

iDRAC7-IP-Adresse über die CMC-Web-Schnittstelle einrichten

So richten Sie die iDRAC7-IP-Adresse über die CMC-Web-Schnittstelle ein:

 **ANMERKUNG:** Sie müssen Administratorberechtigungen für die Gehäusekonfiguration (Chassis Configuration Administrator) besitzen, um iDRAC7-Netzwerkeinstellungen über den CMC vornehmen zu können.

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

 **ANMERKUNG:** Weitere Informationen finden Sie in der *iDRAC7 Online-Hilfe*.

7. Klicken Sie zum Speichern der Netzwerkinformationen auf **Anwenden**.
Weitere Informationen finden Sie im *Chassis Management Controller User's Guide* (Chassis Management Controller-Benutzerhandbuch) unter dell.com/support/manuals.

Auto-Ermittlung aktivieren

Die Funktion der Auto-Ermittlung erlaubt neu installierten Servern, automatisch die Remote-Verwaltungskonsole zu ermitteln, die den Bereitstellungsserver hostet. Der *Bereitstellungsserver* stellt iDRAC7 benutzerdefinierte Administrator-Anmeldeinformationen zur Verfügung, damit der nicht bereitgestellte Server durch die Verwaltungskonsole ermittelt und verwaltet werden kann. Weitere Informationen zur Auto-Ermittlung finden Sie im *Lifecycle Controller Remote Services User's Guide* (Lifecycle Controller Remote Services-Benutzerhandbuch) unter dell.com/support/manuals.




Die Auto-Ermittlung arbeitet mit einer statischen IP-Adresse. DHCP, DNS-Server oder der Standard-DNS-Host-Name ermitteln den Bereitstellungs-Server. Wenn DNS angegeben ist, wird die IP-Adresse für den Bereitstellungs-Server aus DNS abgerufen; die DHCP-Einstellungen werden nicht benötigt. Wenn der Bereitstellungs-Server angegeben ist, wird die Ermittlung übersprungen, so dass weder DHCP noch DNS erforderlich sind.

Sie können die Auto-Ermittlung über das Dienstprogramm für die iDRAC7-Einstellungen oder über Lifecycle Controller aktivieren. Weitere Informationen zur Verwendung von Lifecycle Controller finden Sie im *Lifecycle Controller User's Guide* (Lifecycle Controller-Benutzerhandbuch) unter dell.com/support/manuals.

Wenn die Auto-Ermittlung in den Werkseinstellungen nicht aktiviert ist, dann ist das standardmäßige Administratorkonto (Benutzername root und Kennwort calvin) aktiviert. Stellen Sie vor der Aktivierung der Auto-Ermittlung sicher, dass das

Administratorkonto deaktiviert ist. Wenn die Auto-Ermittlung in Lifecycle Controller aktiviert ist, werden alle Benutzerkonten in iDRAC deaktiviert, bis der Bereitstellungsserver *entdeckt* wurde.

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

1. Schalten Sie das verwaltete System ein.
2. Drücken Sie während des POST (Einschalt-Selbsttest) auf die Taste <F2 >, und gehen Sie dann zu **iDRAC - Einstellungen** → **Remote-Aktivierung** .
Daraufhin wird die Seite **iDRAC-Einstellungen – Remote-Aktivierung** angezeigt.
3. Aktivieren Sie die Auto-Ermittlung, geben Sie die IP-Adresse für den Bereitstellungs-Server ein, und klicken Sie auf **Zurück**.
 **ANMERKUNG:** Die Angabe der IP-Adresse für den Bereitstellungs-Server ist optional. Wenn Sie diese Adresse nicht angeben, wird sie über die DHCP- oder DNS-Einstellungen ermittelt (Schritt 7).
4. Klicken Sie auf **Netzwerk**.
Die Seite **iDRAC-Einstellungen Netzwerk** wird angezeigt.
5. NIC aktivieren
6. IPv4 aktivieren
 **ANMERKUNG:** IPv6 wird im Rahmen der Auto-Ermittlung nicht unterstützt.
7. Aktivieren Sie DHCP, und rufen Sie den Domännennamen, die DNS-Server-Adresse und den DNS-Domännennamen von DHCP ab.
 **ANMERKUNG:** Schritt 7 ist optional, wenn die IP-Adresse des Bereitstellungs-Servers in Schritt 3 angegeben wurde.

Management Station einrichten

Eine Management Station ist ein Computer, der für den Zugriff auf iDRAC7-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 der Infodatei.
2. Installieren und konfigurieren Sie einen unterstützten Webbrowser (Internet Explorer, Firefox, Chrome oder Safari).
3. Installieren Sie die aktuelle Java Runtime Environment (JRE) (erforderlich, wenn der Java-Plugin-Typ für den Zugriff auf iDRAC7 über einen Web-Browser verwendet wird).
4. Installieren Sie aus dem SYSMGMT-Ordner der *Dell Systems Management Tools and Documentation*-DVD die Komponenten „Remote-RACADM“ und „VMCLI“. Rufen Sie alternativ die **Setup**-Datei auf der DVD auf, um Remote-RACADM und weitere OpenManage-Software standardmäßig zu installieren. Weitere Informationen zu RACADM finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.
5. Installieren Sie nach Bedarf auch die folgenden Komponenten:
 - Telnet
 - SSH-Client
 - TFTP
 - Dell OpenManage Essentials


Verwandte Links

[VMCLI-Dienstprogramm installieren und verwenden](#)
[Konfigurieren von unterstützten Webbrowsern](#)

Per Remote auf iDRAC7 zugreifen

Für den Remote-Zugriff auf die iDRAC7-Web-Schnittstelle über eine Management Station müssen Sie sicherstellen, dass sich die Management Station auf dem gleichen Netzwerk wie iDRAC7 befindet. Beispiel:

- Blade-Server – Die Management Station muss sich auf dem gleichen Netzwerk wie CMC befinden. Weitere Informationen zum Isolieren des CMC-Netzwerks vom Netzwerk des Managed System finden Sie im *Chassis Management Controller User's Guide* (Chassis Management Controller-Benutzerhandbuch) unter dell.com/support/manuals.
- Rack- und Tower-Server – Definieren Sie die iDRAC7-Schnittstelle auf LOM1, und stellen Sie sicher, dass sich die Management Station auf dem gleichen Netzwerk wie iDRAC7 befindet.

 **ANMERKUNG:** Wenn das System auf iDRAC7 Enterprise hochgestuft wird, können Sie die iDRAC7-Netzwerkschnittstelle auf **Dediziert** definieren.

Verwenden Sie für den Zugriff auf die Managed System-Konsole über eine Management Station die virtuelle Konsole über die iDRAC7-Web-Schnittstelle.

Verwandte Links

[Virtuelle Konsole starten](#)

[Netzwerkeinstellungen](#)

Managed System einrichten

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

- Lokaler RACADM
- Server Administrator

Weitere Informationen zum Server Administrator finden Sie im *Dell OpenManage Server Administrator User's Guide* (Dell OpenManage Server Administrator-Benutzerhandbuch) unter dell.com/support/manuals.

Verwandte Links

[Einstellungen für lokales Administratorkonto ändern](#)

Einstellungen für lokales Administratorkonto ändern

Nachdem Sie die iDRAC7-IP-Adresse festgelegt haben, können Sie die Einstellungen für das lokale Administratorkonto (hier Benutzer 2) über das Dienstprogramm für die iDRAC-Einstellungen ändern. Gehen Sie dazu wie folgt vor:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Benutzerkonfiguration**. Daraufhin wird die Seite **iDRAC-Einstellungen – Benutzerkonfiguration** angezeigt.
2. Geben Sie den **Benutzernamen**, die **LAN-Benutzerberechtigungen**, die **Benutzerberechtigungen für die seriellen Schnittstellen** und das **Kennwort** an.
Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
Mit diesem Schritt sind die Einstellungen für das lokale Administratorkonto konfiguriert.

Standort für das Managed System einrichten

Sie können die Standortdetails des Managed System im Rechenzentrum über die iDRAC7-Web-Schnittstelle 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 in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Eigenschaften** → **Details**. Die Seite **Systemdetails** wird angezeigt.
2. Geben Sie unter **Systemstandort** die Standortdetails für das Managed System im Rechenzentrum ein. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC7-Online-Hilfe*.
3. Klicken Sie auf **Anwenden**. Daraufhin werden die Details zum Systemstandort in iDRAC7 gespeichert.

Standort für Managed System über RACADM einrichten

Verwenden Sie die Gruppenobjekte `System.Location`, um die Details für den Systemstandort anzugeben. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

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 des Managed System im Rechenzentrum ein. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**. Die Details werden gespeichert.

Systemleistung und Stromverbrauch optimieren

Über das Dienstprogramm für die iDRAC-Einstellungen können Sie die Leistung optimieren und die maximale Temperatur für den Luftaustritt festlegen sowie die Lüftergeschwindigkeit des Managed System festlegen. Gehen Sie dazu wie folgt vor:

1. Gehen Sie im Dienstprogramm für die iDRAC -Einstellungen zu **Thermisch**. Die Seite **iDRAC-Einstellungen Thermisch** wird angezeigt.
2. Legen Sie die Einstellungen für „Thermisch“, „Benutzeroption“ und „Lüfter“ fest. Weitere Informationen finden Sie in der *Online-Hilfe zu den iDRAC-Einstellungen*.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**. Die Konfiguration der Temperatureinstellungen ist damit abgeschlossen.

Konfigurieren von unterstützten Webbrowsers

iDRAC7 wird auf den Webbrowsern Internet Explorer, Mozilla Firefox, Google Chrome und Safari unterstützt. Für weitere Informationen über Versionen siehe die *Infodatei* unter dell.com/support/manuals.

Wenn Sie von einer Management Station aus, die über einen Proxyserver mit dem Internet verbunden ist, eine Verbindung zur iDRAC7-Webschnittstelle herstellen, muss der Webbrowser so konfiguriert werden, dass er von diesem Server aus auf das Internet zugreifen kann. Dieser Abschnitt enthält Information zur Konfiguration von Internet Explorer. So konfigurieren Sie den Internet Explorer-Web-Browser:

1. Gehen Sie im Web-Browser zu **Extras** → **Internetoptionen** → **Sicherheit** → **Lokales Netzwerk**.
2. Klicken Sie auf **Stufe anpassen**, wählen Sie **Mittelhoch** und klicken Sie dann auf **Zurücksetzen**. Klicken Sie zum Bestätigen auf **OK**. Klicken Sie auf **Stufe anpassen**, um das Dialogfeld erneut zu öffnen.
3. Führen Sie einen Bildlauf zum Abschnitt „ActiveX-Steuerelemente und Plugins“ durch, und legen Sie Folgendes fest:

 **ANMERKUNG:** Die Einstellungen im Status „Mittelhoch (Standard)“ richten sich nach der jeweiligen IE-Version.

- Automatische Eingabeaufforderung für ActiveX-Steuerelemente: Aktivieren
- Binär- und Skript-Verhalten: Aktivieren
- Signierte ActiveX-Steuerelemente herunterladen: Bestätigen
- ActiveX-Steuerelemente initialisieren und ausführen, die nicht als sicher gekennzeichnet sind: Bestätigen
- ActiveX-Steuerelemente und Plug-ins ausführen: Aktivieren
- ActiveX-Steuerelemente ausführen, die für Skripting sicher sind: Aktivieren

Unter **Downloads**:

- Automatische Eingabeaufforderung für Datei-Downloads: Aktivieren
- Datei-Download: Aktivieren
- Schriftart-Download: Aktivieren

Unter **Verschiedenes**:

- META-AKTUALISIERUNG zulassen: Aktivieren
- Skripting von Web-Browser-Steuerung für Internet Explorer zulassen: Aktivieren
- Skript-initiierte Fenster ohne Größen- bzw. Positionsbeschränkungen zulassen: Aktivieren
- Keine Eingabeaufforderungen für die Client-Zertifikatsauswahl anzeigen, wenn keine Zertifikate vorliegen, oder wenn nur ein einziges Zertifikat vorhanden ist: Aktivieren
- Programme und Dateien in einem IFRAME starten: Aktivieren
- Dateien nach Inhalt, nicht nach Dateierweiterung öffnen: Aktivieren
- Softwarekanal-Berechtigungen: Niedrige Sicherheitsstufe
- Unverschlüsselte Formulardaten zulassen: Aktivieren
- Pop-up-Blocker verwenden: Deaktivieren

Unter **Skripting**:

- Aktives Skripting: Aktivieren
 - Zugriff auf Zwischenablage zulassen: Aktivieren
 - Scripting von Java-Applets: Aktivieren
4. Gehen Sie zu **Extras** → **Internetoptionen** → **Erweitert**.
 5. Unter **Browsen**:
 - URLs immer als UTF-8 senden: markiert
 - Skriptdebugging deaktivieren (Internet Explorer): markiert
 - Skriptdebugging deaktivieren (Andere): markiert

- Zu jedem Skript-Fehler eine Benachrichtigung anzeigen: nicht markiert
- Aktivieren von Installation nach Bedarf (Andere): markiert
- Seitenübergänge aktivieren: aktiviert
- Browser-Erweiterungen von Drittanbietern aktivieren: markiert
- Verknüpfungen im gleichen Fenster öffnen: nicht markiert

Unter **Einstellungen für HTTP 1.1:**

- HTTP 1.1 verwenden: markiert
- HTTP 1.1 über Proxy-Verbindungen verwenden: markiert

Unter **Java (Sun):**

- JRE 1.6.x_yz verwenden: markiert (optional; Version kann unterschiedlich sein)

Unter **Multimedia:**

- Automatische Bildgrößenanpassung aktivieren: markiert
- Animationen auf Webseiten abspielen: markiert
- Videos auf Webseiten abspielen: markiert
- Bilder anzeigen: markiert

Unter „Sicherheit“:

- Auf gesperrte Zertifikate von Herausgebern überprüfen: nicht markiert
- Signaturen von heruntergeladenen Programmen überprüfen: nicht markiert
- Signaturen von heruntergeladenen Programmen überprüfen: nicht markiert
- SSL 2.0 verwenden: nicht markiert
- SSL 3.0 verwenden: markiert
- TLS 1.0 verwenden: markiert
- Zu ungültigen Standortzertifikaten Warnungen ausgeben: markiert
- Beim Wechsel zwischen sicherem und nicht sicherem Modus warnen: markiert
- Warnung ausgeben, wenn Einreichung des Formulars umgeleitet wird: markiert



ANMERKUNG: Zum Ändern der Einstellungen wird empfohlen, sich mit den daraus resultierenden Folgen vertraut zu machen. Wenn Sie beispielsweise Popups blockieren, werden Teile der iDRAC7-Web-Schnittstelle möglicherweise nicht ordnungsgemäß ausgeführt.

6. Klicken Sie auf **Anwenden** und dann auf **OK**.
7. Klicken Sie auf die Registerkarte **Verbindungen**.
8. Klicken Sie unter **LAN-Einstellungen (Lokales Netzwerk)** auf **LAN-Einstellungen**.
9. Ist das Kästchen **Proxyserver verwenden** markiert, wählen Sie **Proxyserver für lokale Adressen umgehen** aus.
10. Klicken Sie zweimal auf **OK**.
11. Schließen Sie den Browser und starten Sie ihn anschließend neu. So stellen Sie sicher, dass alle Änderungen wirksam werden.


Verwandte Links

- [Lokalisierte Versionen der Webschnittstelle anzeigen](#)
- [iDRAC7 zur Liste vertrauenswürdiger Domänen hinzufügen](#)
- [Weiße Liste-Funktion in Firefox deaktivieren](#)

iDRAC7 zur Liste vertrauenswürdiger Domänen hinzufügen

Wenn Sie auf die iDRAC7-Web-Schnittstelle zugreifen, werden Sie dazu aufgefordert, die iDRAC7-IP-Adresse zur Liste der vertrauenswürdigen Domänen hinzuzufügen, wenn die IP-Adresse in der Liste nicht enthalten ist. Klicken Sie nach Abschluss dieses Vorgangs auf **Aktualisieren**, oder starten Sie den Web-Browser, um eine Verbindung zur iDRAC7-Web-Schnittstelle aufzubauen.

Bei einigen Betriebssystemen kann es vorkommen, dass Internet Explorer 8 Sie nicht dazu auffordert, eine iDRAC7-IP-Adresse zur Liste vertrauenswürdiger Domänen hinzuzufügen, obwohl sich die IP-Adresse nicht in der Liste befindet.

 **ANMERKUNG:** Wenn Sie sich an der iDRAC7-Webschnittstelle mit einem Zertifikat anmelden wollen, dem der Browser nicht vertraut, wird die Zertifikatfehlerwarnung des Browsers nach dem Bestätigen der ersten Meldung möglicherweise ein zweites Mal angezeigt. Dies ist das erwartete Verhalten zur Sicherheitsgewährleistung.

Um bei Internet Explorer 8 die iDRAC7-IP-Adresse zur Liste der vertrauenswürdigen Domänen hinzuzufügen, gehen Sie folgendermaßen vor:

1. Wählen Sie **Extras** → **Internetoptionen** → **Sicherheit** → **Vertrauenswürdige Sites** → **Sites** aus.
2. Geben Sie die IP-Adresse des iDRAC7 in das Feld **Diese Website zur Zone hinzufügen** ein.
3. Klicken Sie auf **Hinzufügen**, dann auf **OK** und schließlich auf **Schließen**.
4. Klicken Sie auf **OK** und aktualisieren Sie dann den Browser.

Weißer 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 Virtuellen Konsolen-Viewers für jeden besuchten iDRAC7 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 auf <Eingabe>:
3. Machen Sie in der Spalte **Einstellungsname** den Eintrag **xpinstall.whitelist.required** auffindig und doppelklicken Sie darauf.
Die Werte für **Einstellungsname**, **Status**, **Typ** und **Wert** ändern sich zu fett gedrucktem Text. Der Wert **Status** ändert sich zu Vom Benutzer festgelegt, und der **Wert** ändert sich zu `false` (falsch).
4. Machen Sie in der Spalte **Einstellungsname** den Eintrag `xpinstall.enabled` auffindig.
Stellen Sie sicher, dass der **Wert** `true` (wahr) ist. Ist dies nicht der Fall, doppelklicken Sie auf `xpinstall.enabled`, um den **Wert** auf `true` (wahr) zu setzen.

Lokalisierte Versionen der Webschnittstelle anzeigen

Die iDRAC7-Webschnittstelle wird in den folgenden Sprachen unterstützt:

- Englisch (en-us)
- Französisch (fr)
- Deutsch (de)
- Spanisch (es)
- Japanisch (ja)

- Vereinfachtes Chinesisch (zh-cn)

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

Die iDRAC7-Webschnittstelle wurde für den Einsatz mit den jeweiligen Tastaturbelegungen für die unterstützten Sprachvarianten entwickelt. Einige Funktionen der iDRAC6-Webschnittstelle, wie z. B. Virtuelle Konsole, können zusätzliche Schritte für den Zugriff auf bestimmte Funktionen/Buchstaben erfordern. Andere Tastaturen werden nicht unterstützt und können ggf. unerwartete Probleme verursachen.



ANMERKUNG: Lesen Sie in der Dokumentation zum Browser nach, wie verschiedene Sprachen konfiguriert und eingerichtet werden, und lassen Sie sich lokalisierte Versionen der iDRAC7-Webschnittstelle anzeigen.

Aktualisieren der Gerätefirmware

Unter Verwendung von iDRAC7 können Sie die Firmware von iDRAC7, BIOS und sämtlichen Geräten aktualisieren, die durch Lifecycle Controller unterstützt werden, z. B.:

- Lifecycle-Controller
- Diagnose
- Treiberpaket des Betriebssystems
- Netzwerkschnittstellenkarte (NIC)
- RAID-Controller

Die benötigte Firmware muss zu iDRAC hochgeladen werden. Nach dem Hochladen wird die aktuelle Version der Firmware, die auf dem Gerät installiert wurde, und die verwendete Version angezeigt. Wenn die hochgeladene Firmwareversion nicht gültig ist, wird eine Fehlermeldung angezeigt. Aktualisierungen, bei denen kein Neustart erforderlich ist, werden sofort angewendet. Aktualisierungen, bei denen ein Neustart des Systems erforderlich ist, werden gestuft und beim nächsten Systemneustart ausgeführt. Es ist nur ein Systemneustart erforderlich, um alle Aktualisierungen durchzuführen.

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)
- **.d7**
- **USC**
- **.pm**

Für Dateien mit der Erweiterung **.exe** müssen Sie über die Berechtigung Systemsteuerung verfügen. Die lizenzierte Remote-Firmwareaktualisierungsfunktion und Lifecycle Controller müssen aktiviert sein.

Für Dateien mit der Erweiterung **.d7**, **.usc** und **.pm** müssen Sie über die Berechtigung zur Konfiguration verfügen.

Verwandte Links

[Herunterladen der Gerätefirmware](#)

[Aktualisieren der Gerätefirmware über die iDRAC7-Web-Schnittstelle](#)

[Aktualisieren der Gerätefirmware über RACADM](#)

[Firmware über die CMC-Web-Schnittstelle aktualisieren](#)


[Firmware über DUP aktualisieren](#)

[Firmware über Remote-RACADM aktualisieren](#)

[Firmware über die Lifecycle-Controller-Remote-Dienste aktualisieren](#)

Herunterladen der Gerätefirmware

Das Format der von Ihnen heruntergeladenen Image-Datei richtet sich nach dem verwendeten Aktualisierungsverfahren:

- iDRAC7-Web-Schnittstelle – Laden Sie das Binärpaket, das als selbstextrahierendes Archiv gepackt ist, herunter. Die Standard-Firmware-Image-Datei trägt den Namen **firmitmg.d7**.
 **ANMERKUNG:** Das gleiche Dateiformat wird für die Wiederherstellung von iDRAC7 über die CMC-Web-Schnittstelle verwendet.
- Managed System – Laden Sie das Betriebssystem-spezifische Dell Update Package (DUP) herunter. Die Dateierweiterungen lauten **.bin** für Linux-Betriebssysteme und **.exe** für Windows-Betriebssysteme.
- Lifecycle-Controller – Laden Sie die aktuelle Katalogdatei und die DUPs herunter, und verwenden Sie die Funktion *Plattformaktualisierung* in Lifecycle-Controller, um die Gerätefirmware zu aktualisieren. Weitere Informationen zur Funktion „Plattformaktualisierung“ finden Sie im *Lifecycle Controller User's Guide* (Lifecycle-Controller-Benutzerhandbuch) unter dell.com/support/manuals.

Aktualisieren der Gerätefirmware über die iDRAC7-Web-Schnittstelle

Zum Aktualisieren der Gerätefirmware unter Verwendung von iDRAC7 Web-Schnittstelle:

1. Gehen Sie zu **Übersicht** → **iDRAC Einstellungen** → **Aktualisieren und Zurücksetzen** → **Aktualisierung**. Die Seite **Firmware-Aktualisierung** wird angezeigt.
2. Klicken Sie auf **Durchsuchen**, wählen Sie die Firmware-Image-Datei für die gewünschte Komponente aus und klicken Sie dann auf **Hochladen**.
3. Nachdem der Vorgang abgeschlossen ist, zeigt der Abschnitt **Aktualisierungsdetails** jede hochgeladene Firmwaredatei und den zugehörigen Status an. Für mehr Informationen über die Felder siehe *iDRAC7 Online-Hilfe*.
4. Sie können die erforderliche Firmware Datei, die aktualisiert werden soll, auswählen und eine der folgenden Optionen anklicken:
 - Für Firmwareimages, bei denen kein Neustart des Hostsystems erforderlich ist, klicken Sie auf **Installieren**. Zum Beispiel, **.d7** Firmwaredatei.
 - Für Firmwareimages, bei denen ein Neustart des Hostsystems erforderlich ist, klicken Sie auf **Installieren und Neustart** oder **Beim nächsten Systemstart installieren**.
 - Um die Aktualisierung der Firmware abzubrechen, klicken Sie auf **Abbrechen**.

Wenn Sie auf **Installieren und Neustart** oder **Beim nächsten Systemstart installieren** klicken, wird die Meldung *Aktualisierung der Jobwarteschlange* angezeigt.

5. Klicken Sie auf **Jobwarteschlange**, um die Seite **Jobwarteschlange** anzuzeigen, wo Sie die gestuften Firmware-Aktualisierungen verwalten oder auf **OK** klicken können, um die aktuelle Seite neu zu laden und den Status der Firmwareaktualisierung anzuzeigen.

Verwandte Links

- [Aktualisieren der Gerätefirmware](#)
- [Anzeigen und Verwalten von gestuften Aktualisierungen](#)
- [Herunterladen der Gerätefirmware](#)

Aktualisieren der Gerätefirmware über RACADM

Um die Gerätefirmware unter Verwendung von RACADM zu aktualisieren, verwenden Sie den Unterbefehl **update**. Für weitere Informationen siehe *RACADM Reference Guide for iDRAC7 and CMC* (RACADM Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Firmware über die CMC-Web-Schnittstelle aktualisieren

Sie können die iDRAC7-Firmware für Blade-Server über die CMC-Web-Schnittstelle aktualisieren.

So aktualisieren Sie die iDRAC7-Firmware über die CMC-Web-Schnittstelle:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Gehen Sie zu **Server** → **Übersicht** → **<Servername>**.
Die Seite **Serverstatus** wird angezeigt.
3. Klicken Sie auf **iDRAC-Web-Schnittstelle starten**, und führen Sie dann die **iDRAC-Firmware-Aktualisierung** aus.

Verwandte Links

[Aktualisieren der Gerätefirmware](#)

[Herunterladen der Gerätefirmware](#)

[Aktualisieren der Gerätefirmware über die iDRAC7-Web-Schnittstelle](#)

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 iDRAC7-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`

So aktualisieren Sie iDRAC7 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

So führen Sie eine Aktualisierung über RACADM durch:

1. Laden Sie das Firmware-Image auf den TFTP oder einen FTP-Server herunter. Beispiel: `C:\downloads\firmimg.d7`
2. Führen Sie den folgenden RACADM-Befehl aus:

TFTP-Server:

- Verwenden des Befehls **fwupdate**: `racadm -r <iDRAC7 IP-Adresse> -u <Benutzername> -p <Kennwort> fwupdate -g -u -a <Pfad>`
 , wobei *Pfad* der Speicherort auf dem TFTP-Server ist, auf dem **firmimg.d7** gespeichert ist.
- Verwenden des Befehls **update**: `racadm -r <iDRAC7 IP-Adresse> -u <Benutzername> -p <Kennwort> update -f <Dateiname>`

FTP-Server

- Verwenden des Befehls **fwupdate**: `racadm -r <iDRAC7-IP-Adresse> -u <Benutzername> -p <Kennwort> fwupdate -f <FTP-Server-IP-Adresse> <FTP-Server-Benutzername> <FTP-Server-Kennwort> -d <Pfad>`
 , wobei *Pfad* der Speicherort auf dem FTP-Server ist, auf dem **firmimg.d7** gespeichert ist.
- Verwenden des Befehls **update**: `racadm -r <iDRAC7 IP-Adresse> -u <Benutzername> -p <Kennwort> update -f <Dateiname>`

Weitere Informationen über den Befehl **fwupdate** finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Firmware über die Lifecycle-Controller-Remote-Dienste aktualisieren

Für Informationen zur Aktualisierung der Firmware unter Verwendung von Lifecycle Controller-Remote-Dienste siehe *Lifecycle Controller Remote Services Quick Start Guide* (Lifecycle-Controller Remote-Dienste Schnellstarthandbuch) unter dell.com/support/manuals.

Anzeigen und Verwalten von gestuften Aktualisierungen

Sie können die geplanten Aufgaben anzeigen und löschen, einschließlich der Konfiguration und Aktualisierung von Aufgaben. Dies ist eine lizenzierte Funktion. Alle Aufgaben, die in der Warteschlange sind und während des nächsten Neustarts ausgeführt werden sollen, können gelöscht werden.

Verwandte Links

[Aktualisieren der Gerätefirmware](#)

Anzeigen und Verwalten gestufter Aktualisierungen unter Verwendung der iDRAC7 Web-Schnittstelle

Zum Anzeigen der geplanten Aufgaben unter Verwendung von iDRAC Web-Schnittstelle, gehen Sie zu **Übersicht** → **Server** → **Jobwarteschleife**. Die Seite **Jobwarteschleife** zeigt den Status der Jobs in der Jobwarteschleife des Lifecycle Controllers an. Für mehr Informationen zu den angezeigten Feldern siehe die *iDRAC7 Online-Hilfe*.

Um einen oder mehrere Jobs zu löschen, wählen Sie einen oder mehrere Jobs aus und klicken Sie auf **Löschen**. Die Seite wird neu geladen und der ausgewählte Job wird aus der Jobwarteschleife von Lifecycle Controller entfernt. Sie können alle Jobs in der Warteschleife löschen, die während des nächsten Systemstarts ausgeführt werden sollen. Sie können keine aktiven Jobs mit dem Status *Wird ausgeführt* oder *Wird heruntergeladen* löschen.

Sie müssen die Berechtigung „Serversteuerung“ besitzen, um Jobs löschen zu können.

Anzeigen und Verwalten gestufter Aktualisierungen unter Verwendung von RACADM

Zur Anzeige der gestuften Aktualisierungen unter Verwendung von RACADM verwenden Sie den Unterbefehl **jobqueue**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.

Rollback der iDRAC7-Firmware durchführen

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

- iDRAC7-Web-Schnittstelle
- CMC-Webschnittstelle
- RACADM-Befehlszeilenschnittstelle (iDRAC7 und CMC)
- Life Cycle Controller
- Lifecycle Controller-Remote-Dienste

Verwandte Links

[Rollback für die Firmware über die iDRAC7-Web-Schnittstelle durchführen](#)

[Rollback der Firmware über die CMC-Web-Schnittstelle durchführen](#)


[Rollback der Firmware über RACADM durchführen](#)

[Rollback der Firmware über Lifecycle-Controller durchführen](#)

[Rollback der Firmware über die Remote-Dienste für den Lifecycle Controller durchführen](#)

Rollback für die Firmware über die iDRAC7-Web-Schnittstelle durchführen

So führen Sie ein Firmware-Rollback über die iDRAC7-Web-Schnittstelle durch:


 **ANMERKUNG:** Derzeit wird ein Rollback nur für die Firmware von iDRAC7 und nicht für die Firmware eines anderen Geräts unterstützt.


1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Aktualisierung und Rollback** → **Rollback**.

Die Seite **Rollback** zeigt die aktuellen und die vorhergehenden Firmware-Versionen an.

2. Klicken Sie auf **Next (Weiter)**.

Der iDRAC7 startet nach Durchführung des Rollbacks neu.

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

 **ANMERKUNG:** Wenn die iDRAC7-Konfiguration auf die Standardwerte zurückgesetzt wird, wird die iDRAC7-IP-Adresse auf 192.168.0.120 zurückgesetzt. Sie können über diese IP-Adresse auf iDRAC7 zugreifen oder die iDRAC7-Adresse über einen lokalen RACADM oder die Taste F2 neu konfigurieren (für Remote-RACADM ist der Netzwerkzugriff erforderlich).

3. Nachdem der Rollback-Vorgang abgeschlossen ist, wird iDRAC7 zurückgesetzt. Sie müssen zum Verwenden von iDRAC7 das aktuelle Browser-Fenster schließen und eine neue Verbindung über ein neues Browser-Fenster aufbauen.
4. Gehen Sie zum Anzeigen der iDRAC7-Firmware-Version auf eine der folgenden Seiten:
 - Gehen Sie zu **Übersicht** → **Server** → **Eigenschaften** → **Zusammenfassung**, und zeigen Sie die Firmware-Version im Abschnitt **Server-Informationen** an.

- Gehen Sie zu **Übersicht** → **iDRAC-Einstellungen** → **Eigenschaften**, und zeigen Sie die Firmware-Version im Abschnitt **Integrated Dell Remote Access Controller 7** an.

Rollback der Firmware über die CMC-Web-Schnittstelle durchführen

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

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Gehen Sie zu **Server-Übersicht** → **<Server-Name>**.
Die Seite **Serverstatus** wird angezeigt.
3. Klicken Sie auf **iDRAC-Web-Schnittstelle starten**, und führen Sie das iDRAC7-Firmware-Rollback aus.

Rollback der Firmware über RACADM durchführen

Sie können ein Rollback der iDRAC-Firmware auf eine frühere Firmware-Version nur unter Verwendung von RACADM durchführen. Dazu verwenden Sie den Befehl **fwupdate**. Weitere Informationen finden Sie unter *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.

Rollback der Firmware über Lifecycle-Controller durchführen

Weitere Informationen finden Sie im *Lifecycle-Controller User's Guide* (Lifecycle-Controller Benutzerhandbuch) unter dell.com/support/manuals.

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

Informationen finden Sie im *Lifecycle Controller Remote Services Quick Start Guide* (Lifecycle-Controller Remote-Dienste Schnellstarthandbuch) unter dell.com/support/manuals.

iDRAC7 wiederherstellen


iDRAC7 unterstützt zwei Betriebssystem-Images, um ein startfähiges iDRAC7 sicherzustellen. Gehen Sie bei einem nicht vorhersehbaren Fehler mit schwerwiegenden Folgen und dem Verlust der beiden Startpfade wie folgt vor:

- Der iDRAC7-Bootloader erkennt, dass kein startfähiges Image vorhanden ist.
- Die Systemzustands- und Identifizierungs-LED leuchtet etwa im Halbsekundentakt auf. (Die LED befindet sich auf der Rückseite von Rack- und Tower-Systemen sowie auf der Vorderseite eines Blade-Servers.)
- Der Bootloader fragt den SD-Kartensteckplatz ab.
- Formatieren Sie eine SD-Karte mit FAT über ein Windows-Betriebssystem oder EXT3 über ein Linux-Betriebssystem.
- Kopieren Sie das Image **firmimg.d7** auf die SD-Karte.
- Legen Sie die SD-Karte in den Server ein.
- Bootloader erkennt die SD-Karte, schaltet die blinkende LED auf eine dauerhaft gelbe Anzeige, liest das Image „firmimg.d7“, programmiert iDRAC7 um und startet iDRAC7 neu.

TFTP-Server verwenden

Sie können den Trivial File Transfer Protocol (TFTP)-Server zum Hoch- und Herunterstufen der iDRAC7-Firmware oder zum Installieren von Zertifikaten verwenden. Er wird in den SM-CLP and RACADM-Befehlszeilenschnittstellen

verwendet, um Dateien von und nach iDRAC7 zu übertragen. Der Zugriff auf den TFTP-Server muss über eine iDRAC7-IP-Adresse oder einen DNS-Namen aktiviert werden.

 **ANMERKUNG:** Wenn Sie die iDRAC7-Web-Schnittstelle zum Übertragen von Zertifikaten und zum Aktualisieren der Firmware verwenden, wird der TFTP-Server nicht benötigt.

Sie können den Befehl `netstat -a` auf Windows- oder Linux-Betriebssystemen verwenden, um zu ermitteln, ob ein TFTP-Server ausgeführt wird. Die Standardschnittstelle für TFTP ist 69. Wenn der TFTP-Server nicht ausgeführt wird, führen Sie einen der folgenden Schritte aus:

- Suchen Sie im Netzwerk, in dem ein TFTP-Dienst ausgeführt wird, einen anderen Computer.
- Installieren Sie einen TFTP-Server auf dem Betriebssystem.

Sichern und Wiederherstellen eines Serverprofils

Sie können die Systemkonfiguration sichern, einschließlich der installierten Firmware-Images auf verschiedenen Komponenten und den Konfigurationseinstellungen dieser Komponenten. Die Sicherung erstellt eine einzelne Datei, die Sie auf einer vFlash-SD-Karte oder einer Netzwerkfreigabe (CIFS oder NFS) speichern können.

Vor der Durchführung eines Sicherungsvorgangs auf eine vFlash-SD-Karte achten Sie auf Folgendes:

- Eine von Dell unterstützte vFlash-SD-Karte ist eingelegt und initialisiert.
- Die vFlash-SD-Karte verfügt über ausreichend Speicherplatz zur Speicherung der Sicherungsdatei.

Die Sicherungsdatei enthält verschlüsselte, sensible Benutzerdaten, Konfigurationsinformationen und Firmware-Images, die Sie für den Wiederherstellungsvorgang nutzen können.

Stellen Sie vor dem Durchführen eines Wiederherstellungsvorgangs sicher, dass der Lifecycle-Controller aktiviert ist.

Für den Wiederherstellungsvorgang müssen der Service-Tag und der Service-Tag in der Sicherungsdatei identisch sein. Der Wiederherstellungsvorgang gilt für alle Systemkomponenten, die gleich sind und sich am gleichen Ort (z. B. im gleichen Steckplatz) wie in der Sicherungsdatei festgehalten befinden. Wenn sich Komponenten unterscheiden oder sich nicht am gleichen Ort befinden, werden sie nicht modifiziert und im Lifecycle-Protokoll werden Wiederherstellungsfehler protokolliert.

Sichern des Serverprofils unter Verwendung der iDRAC7-Web-Schnittstelle

So sichern Sie das Serverprofil mithilfe der iDRAC7-Web-Schnittstelle:

1. Gehen Sie zu **Übersicht** → **iDRAC-Einstellungen** → **Backup und Wiederherstellen** .
Die Seite **Backup und Wiederherstellen eines Serverprofils** wird angezeigt.
2. Wählen Sie **Backup** aus.
3. Wählen Sie eine der folgenden Optionen aus, um das Sicherungsdatei-Image zu speichern:
 - Netzwerkfreigabe, um das Sicherungsdatei-Image auf einer CIFS- oder NFS-Freigabe zu speichern.
 - vFlash
4. Geben Sie Name und Verschlüsselungspassphrase (optional) der Sicherungsdatei ein.
5. Wenn als Speicherort der Datei **Netzwerk** ausgewählt wird, geben Sie die Netzwerkeinstellungen ein.
Weitere Informationen zu den Feldern finden Sie in der *iDRAC7 Online-Hilfe*.
6. Klicken Sie auf **Serverprofil Backup**.
Der Backup-Vorgang wird initiiert und Sie können den Status auf der Seite **Job-Warteschlange** anzeigen. Nach einem erfolgreichen Vorgang wird die Sicherungsdatei am angegebenen Ort gespeichert.

Sichern des Serverprofils unter Verwendung von RACADM

Zur Sicherung des Serverprofils mithilfe von RACADM verwenden Sie den Befehl **systemconfig backup**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.

Sichern des Serverprofils unter Verwendung der iDRAC7-Web-Schnittstelle

Die Sicherungsdatei wird zur Wiederherstellung des Systems verwendet.

So sichern und stellen Sie das Serverprofil mithilfe der iDRAC7-Web-Schnittstelle wieder her:

1. Gehen Sie zu **Übersicht** → **iDRAC-Einstellungen** → **Backup und Wiederherstellen**. Die Seite **Backup und Wiederherstellen eines Serverprofils** wird angezeigt.
2. Wählen Sie **Wiederherstellen**.
3. Wählen Sie eine der folgenden Optionen, um den Speicherort der Sicherungsdatei anzugeben:
 - Netzwerkressource
 - vFlash
4. Geben Sie Name und Entschlüsselungspassphrase (optional) der Sicherungsdatei ein.
5. Wenn als Speicherort der Datei **Netzwerk** ausgewählt wird, geben Sie die Netzwerkeinstellungen ein. Weitere Informationen zu den Feldern finden Sie in der *iDRAC7 Online-Hilfe*.
6. Wählen Sie eine der folgenden Optionen:
 - **Beibehalten** - Die bestehende Konfiguration der Festplatte und die Festplattendaten werden beibehalten.
 - **Löschen und ersetzen** - Das System wird durch die Daten aus der Sicherungsimagedatei ersetzt.
7. Klicken Sie auf **Serverprofil wiederherstellen**. Der Wiederherstellungsvorgang wird initiiert.

Wiederherstellen des Serverprofils unter Verwendung von RACADM

Zur Wiederherstellung des Serverprofils mithilfe von RACADM verwenden Sie den Befehl **systemconfig restore**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CM* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.

Sequenz für den Wiederherstellungsvorgang

Die Sequenz für den Wiederherstellungsvorgang sieht wie folgt aus:

1. Das Host-System fährt herunter.
2. Die Informationen aus der Sicherheitsdatei werden zur Wiederherstellung des Lifecycle-Controllers verwendet.
3. Das Host-System wird eingeschaltet.
4. Der Wiederherstellungsprozess von Firmware und Konfiguration für das Gerät wird abgeschlossen.
5. Das Host-System fährt herunter.
6. Der Wiederherstellungsprozess von iDRAC-Firmware und Konfiguration wird abgeschlossen.
7. Der iDRAC startet neu.
8. Das wiederhergestellte Host-System wird eingeschaltet, um den Normalbetrieb wiederaufzunehmen.

iDRAC7 über andere Systemverwaltungs-Tools überwachen

Sie können iDRAC7 über IT Assistant, Dell Verwaltung Konsole und Dell OpenManage Essentials entdecken und überwachen. Sie können außerdem das Dell Remote Access Configuration Tool (DRACT) verwenden, um iDRACs zu entdecken, die Firmware zu aktualisieren und Active Directory einzurichten. Weitere Informationen finden Sie in den jeweiligen Benutzerhandbüchern.

iDRAC7 konfigurieren


Mit iDRAC7 können Sie iDRAC7-Eigenschaften konfigurieren, Benutzer einrichten und Warnungen für die Ausführung von Remote-Verwaltungsaufgaben einrichten.

Stellen Sie vor der Konfiguration von iDRAC7 sicher, dass die iDRAC7-Netzwerkeinstellungen und ein unterstützter Browser konfiguriert und die erforderlichen Lizenzen aktualisiert sind. Weitere Informationen zu den lizenzierbaren Funktionen in iDRAC7 finden Sie unter [Lizenzen verwalten](#).

Sie können iDRAC7 über die folgenden Komponenten konfigurieren:

- iDRAC7-Web-Schnittstelle
- RACADM
- Remote-Dienste (siehe *Dell Lifecycle Controller Remote Services-Benutzerhandbuch*)
- IPMITool (siehe *Benutzerhandbuch zu den Dienstprogrammen des Dell OpenManage Baseboard Management Controller*)

So konfigurieren Sie iDRAC7:

1. Melden Sie sich bei iDRAC7 an.
2. Ändern der Netzwerkeinstellungen falls erforderlich.
 -  **ANMERKUNG:** Sollten Sie im Rahmen der Einrichtung der iDRAC7-IP-Adresse iDRAC7-Netzwerkeinstellungen über das Dienstprogramm für die iDRAC-Einstellungen konfiguriert haben, können Sie diesen Schritt übergehen.
3. Konfigurieren Sie Schnittstellen für den Zugriff auf iDRAC7.
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 iDRAC7 auf:
 - Serielle IPMI- oder RAC-Verbindung
 - Serielle IPMI-Verbindung über LAN
 - IPMI über LAN
 - SSH- oder Telnet-Client
8. Erforderliche Zertifikate abrufen.
9. Fügen Sie iDRAC7-Benutzer mit Berechtigungen hinzu, und konfigurieren Sie diese.
10. Konfigurieren und aktivieren Sie E-Mail-Warnungen, SNMP-Traps oder IPMI-Warnungen.
11. Einrichten der Strombegrenzungsrichtlinie falls erforderlich.
12. Bildschirm des letzten Systemabsturzes anzeigen
13. Konfigurieren Sie ggf. die virtuelle Konsole und die virtuellen Datenträger.
14. Konfigurieren Sie ggf. die vFlash SD-Karte.
15. Richten Sie ggf. das erste Startlaufwerk ein.
16. Stellen Sie das Betriebssystem ggf. auf iDRAC-Passthrough.

Verwandte Links

[Bei iDRAC7 anmelden](#)
[Netzwerkeinstellungen ändern](#)
[Dienste konfigurieren](#)
[Anzeige auf der Frontblende konfigurieren](#)
[Standort für das Managed System einrichten](#)
[Das Konfigurieren von Zeitzone und NTP](#)
[iDRAC7-Kommunikation einrichten](#)
[Benutzerkonten und Berechtigungen konfigurieren](#)
[Stromversorgung überwachen und verwalten](#)
[Bildschirm „Letzter Absturz“ aktivieren](#)
[Virtuelle Konsole konfigurieren und verwenden](#)
[Virtuelle Datenträger verwalten](#)
[vFlash SD-Karte verwalten](#)
[Erstes Startlaufwerk einstellen](#)
[Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough](#)
[iDRAC7 für das Versenden von Warnungen konfigurieren](#)

iDRAC7-Informationen anzeigen

Sie können die iDRAC7-Basiseigenschaften anzeigen.

iDRAC7-Informationen über die Web-Schnittstelle anzeigen

Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Eigenschaften**, um die folgenden Informationen in Bezug auf iDRAC7 anzuzeigen. Weitere Informationen zu den Eigenschaften finden Sie in der *iDRAC7-Online-Hilfe*.

- Gerätetyp
- Hardware- und Firmware-Version
- Letzte Firmware-Aktualisierung
- RAC-Uhrzeit
- Anzahl von möglichen aktiven Sitzungen
- Anzahl von aktuellen Sitzungen
- LAN ist aktiviert oder deaktiviert
- IPMI-Version
- Informationen über die Benutzerschnittstelle in der Titelleiste
- Netzwerkeinstellungen
- IPv4-Einstellungen
- IPv6-Einstellungen


iDRAC7-Informationen über RACADM anzeigen

Weitere Informationen zum Anzeigen von iDRAC7-Informationen über RACADM finden Sie in den Unterbefehlen `getsysinfo` oder `get` im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Netzwerkeinstellungen ändern

Nach der Konfiguration der iDRAC7-Netzwerkeinstellungen über das Dienstprogramm für die iDRAC-Einstellungen können Sie auch die Einstellungen über die iDRAC7-Web-Schnittstelle, über RACADM, über den Lifecycle-Controller, über das Dell Deployment Toolkit und (nach dem Starten des Betriebssystems) über Server Administrator ändern. Weitere Informationen zu den Tools und den Berechtigungseinstellungen finden Sie in den entsprechenden Benutzerhandbüchern.

Zum Ändern der Netzwerkeinstellungen über die iDRAC7-Web-Schnittstelle oder RACADM müssen Sie über Berechtigungen zum **Konfigurieren** verfügen.

 **ANMERKUNG:** Durch das Ändern der Netzwerkeinstellungen werden möglicherweise die aktuellen Netzwerkverbindungen mit iDRAC7 beendet.

Netzwerkeinstellungen über die Web-Schnittstelle ändern

So ändern Sie die iDRAC7-Netzwerkeinstellungen:


1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk**. 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 **Automatisch dedizierte NIC** unter **Netzwerkeinstellungen** auswählen, ändert iDRAC seine NIC-Auswahl zur Verwendung der dedizierte NIC, wenn bei ihm die NIC-Auswahl als freigegebenes LOM (1, 2, 3 oder 4) angegeben ist und ein Link auf der dedizierten NIC des iDRAC erkannt wird. Wird kein Link auf der dedizierten NIC erkannt, verwendet iDRAC das freigegebene LOM. Der Wechsel von freigegebener zu dedizierter Zeitüberschreitung dauert fünf Sekunden und von dedizierter zu freigegebener 30 Sekunden. Sie können diesen Zeitüberschreitungswert mithilfe von RACADM oder WS-MAN konfigurieren.

Weitere Informationen zu den verschiedenen Feldern finden Sie in der *iDRAC7-Online-Hilfe*.

Netzwerkeinstellungen über einen lokalen RACADM ändern

Geben Sie Folgendes ein, um eine Liste verfügbarer Netzwerkeigenschaften zu erstellen:

 **ANMERKUNG:** Sie können entweder die Befehle **getconfig** und **config** oder die Befehle **get** und **set** mit den RACADM-Objekten verwenden.

- Verwenden des Befehls **getconfig**: `racadm getconfig -g cfgLanNetworking`
- Verwenden des Befehls **get**: `racadm get iDRAC.Nic`

Wenn DHCP zur Ermittlung einer IP-Adresse verwendet werden soll, kann der folgende Befehl zum Schreiben des Objekts **cfgNicUseDhcp** oder **DHCPEnable** und zum Aktivieren dieser Funktion verwendet werden:

- Verwenden des Befehls **config**: `racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1`
- Verwenden des Befehls **set**: `racadm set iDRAC.IPv4.DHCPEnable 1`

Im folgenden Beispiel wird gezeigt, wie der Befehl zur Konfiguration benötigter LAN-Netzwerkeigenschaften verwendet werden kann:

- Verwenden des Befehls **config**:

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1 racadm config -g  
cfgLanNetworking -o cfgNicIpAddress 192.168.0.120 racadm config -g
```

```

cfgLanNetworking -o cfgNicNetmask 255.255.255.0 racadm config -g
cfgLanNetworking -o cfgNicGateway 192.168.0.120 racadm config -g
cfgLanNetworking -o cfgNicUseDHCP 0 racadm config -g cfgLanNetworking -o
cfgDNSServersFromDHCP 0 racadm config -g cfgLanNetworking -o
cfgDNSServer1 192.168.0.5 racadm config -g cfgLanNetworking -o
cfgDNSServer2 192.168.0.6 racadm config -g cfgLanNetworking -o
cfgDNSRegisterRac 1 racadm config -g cfgLanNetworking -o cfgDNSRacName
RAC-EK00002 racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP
0 racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN

```

- **Verwenden des Befehls `set`:**

```

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 `cfgNicEnable` oder `iDRAC.Nic.Enable` auf `0` gesetzt wird, wird das iDRAC7-LAN selbst dann deaktiviert, wenn DHCP aktiviert ist.


IP-Filterung und IP-Blockierung konfigurieren

Verwenden Sie neben der Benutzerauthentifizierung die folgenden Optionen für zusätzliche Sicherheit, während Sie auf iDRAC7 zugreifen:

- Mit IP-Filterung können Sie den IP-Adressbereich der Clients beschränken, die auf iDRAC7 zugreifen. Dabei wird die IP-Adresse einer eingehenden Anmeldung mit dem angegebenen Bereich verglichen, und der Zugang zu iDRAC7 wird nur über eine Management Station genehmigt, deren IP-Adresse sich innerhalb dieses Bereichs befindet. Alle anderen Anmeldeanfragen werden abgelehnt.
- Durch IP-Blockierung wird dynamisch festgestellt, wenn von einer bestimmten IP-Adresse aus übermäßige Anmeldefehlversuche auftreten und die Adresse eine bestimmte Zeit lang blockiert bzw. daran gehindert wird, eine Anmeldung am iDRAC7 durchzuführen. Sie enthält:
 - Die Anzahl zulässiger Anmeldefehlschläge.
 - Die Zeitspanne in Sekunden, während der diese Fehler auftreten müssen.
 - Die Zeitdauer in Sekunden, während der die blockierte IP-Adresse daran gehindert wird, eine Sitzung herzustellen, nachdem die zulässige Anzahl von Fehlern überschritten wurde (`cfgRacTuneIpBlkPenaltyTime`)

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

 **ANMERKUNG:** Wenn Anmeldeversuche von der Client-IP-Adresse abgelehnt werden, können einige SSH-Clients die Meldung anzeigen: `ssh exchange identification: Verbindung vom Remote-Host geschlossen.`

 **ANMERKUNG:** Wenn Sie das Dell Deployment Toolkit (DTK) verwenden, finden Sie weitere Informationen zu den Berechtigungen im *Dell Deployment Toolkit-Benutzerhandbuch*.

IP-Filterung und IP-Blockierung über die iDRAC7-Web-Schnittstelle konfigurieren

Sie müssen über Berechtigungen zum Konfigurieren von iDRAC7 verfügen, um diese Schritte auszuführen.

So konfigurieren Sie IP-Filterung und IP-Blockierung:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Netzwerk**.

Die Seite **Netzwerk** wird angezeigt.

2. Klicken Sie auf **Erweiterte Einstellungen**.

Die Seite **Netzwerksicherheit** wird angezeigt.

3. Geben Sie die Einstellungen für die IP-Filterung und die IP-Blockierung an.

Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC7-Online-Hilfe*.

4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

IP-Filterung und IP-Blockierung über RACADM konfigurieren

Sie müssen über Berechtigungen zum Konfigurieren von iDRAC7 verfügen, um diese Schritte auszuführen.

Um die IP-Filterung und IP-Blockierung zu konfigurieren, verwenden Sie die folgenden RACADM-Objekte:

- Mit dem Befehl **config**:
 - `cfgRacTuneIpRangeEnable`
 - `cfgRacTuneIpRangeAddr`
 - `cfgRacTuneIpRangeMask`
 - `cfgRacTuneIpBlkEnable`
 - `cfgRacTuneIpBlkFailCount`
 - `cfgRacTuneIpBlkFailWindow`
- Verwenden Sie mit dem Befehl **set** die Objekte der Gruppe **iDRAC.IPBlocking**:
 - `RangeEnable`
 - `RangeAddr`
 - `RangeMask`
 - `BlockEnable`
 - `FailCount`
 - `FailWindow`
 - `PenaltyTime`

Die Eigenschaft **cfgRacTuneIpRangeMask** oder die **RangeMask** wird sowohl auf die eingehende IP-Adresse als auch auf die **cfgRacTuneIpRangeAddr** oder **RangeAddr**-Eigenschaften angewendet. Sind die Ergebnisse identisch, wird für die eingehende Anmeldeaufforderung der Zugriff auf den iDRAC7 zugelassen. Anmeldung von IP-Adressen außerhalb dieses Bereichs führen zu einer Fehlermeldung.

Die Anmeldung wird fortgeführt, wenn der folgende Ausdruck Null entspricht:

- Verwenden der Legacy-Syntax: `cfgRacTuneIpRangeMask & (<eingehende IP-Adresse> ^ cfgRacTuneIpRangeAddr)`
- Verwenden der neuen Syntax: `RangeMask & (<eingehende IP-Adresse> ^ RangeAddr)`

wobei **&** das binäre UND der Mengen und **^** das binäre ausschließliche ODER ist.

Beispiele für die IP-Filterung

- Die folgenden RACADM-Befehle blockieren alle IP-Adressen außer 192.168.0.57:
 - Verwenden des Befehls **config**:

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1 racadm
config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57 racadm
config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```

- Verwenden des Befehls **set**:


```
racadm set iDRAC.IPBlocking.RangeEnable 1 racadm set
iDRAC.IPBlocking.RangeAddr 192.168.0.57 racadm set
iDRAC.IPBlocking.RangeMask 255.255.255.255
```
- Zur Beschränkung von Anmeldungen auf einen Satz von vier angrenzenden IP-Adressen (z. B. 192.168.0.212 bis 192.168.0.215) wählen Sie alle außer den niederwertigsten zwei Bits in der Maske aus:
 - Verwenden des Befehls **set**:


```
racadm set iDRAC.IPBlocking.RangeEnable 1 racadm set
iDRAC.IPBlocking.RangeAddr 192.168.0.212 racadm set
iDRAC.IPBlocking.RangeMask 255.255.255.252
```

Das letzte Byte der Bereichsmaske ist auf 252 eingestellt, das Dezimaläquivalent von 11111100b.

Beispiele für die IP-Blockierung

- Im folgenden Beispiel wird die IP-Adresse einer Management Station fünf Minuten lang vor der Einrichtung einer Sitzung bewahrt, wenn die Einrichtung innerhalb einer Minute fünf Mal gescheitert ist.
 - Verwenden des Befehls **config**:


```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1 racadm
config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5 racadm config -
g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60
```
 - Verwenden des Befehls **set**:


```
racadm set iDRAC.IPBlocking.RangeEnable 1 racadm set
iDRAC.IPBlocking.FailCount 5 racadm set iDRAC.IPBlocking.FailWindow
60
```
- Das folgende Beispiel verhindert mehr als drei Fehlversuche innerhalb einer Minute und verhindert für eine Stunde weitere Anmeldeversuche.
 - Verwenden des Befehls **config**:


```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkEnable 1 racadm
config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3 racadm config -
g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60 racadm config -g
cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 3600
```
 - Verwenden des Befehls **set**:


```
racadm set iDRAC.IPBlocking.BlockEnable 1 racadm set
iDRAC.IPBlocking.FailCount 3 racadm set iDRAC.IPBlocking.FailWindow
60 racadm set iDRAC.IPBlocking.PenaltyTime 3600
```

Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.

Dienste konfigurieren

Sie können die folgenden Dienste auf iDRAC7 konfigurieren und aktivieren:

- Lokale Kommunikation – Deaktivieren Sie den Zugriff auf die iDRAC7-Konfiguration (vom Host-System) über den lokalen RACADM und das Dienstprogramm für iDRAC-Einstellungen.
- Web Server — Zugang zur iDRAC7-Weboberfläche aktivieren. Wenn Sie die Option deaktivieren, aktivieren Sie den Web Server wieder über den lokalen RACADM, da die Deaktivierung des Web Servers auch den Remote-RACADM deaktiviert.
- SSH – Greifen Sie über die Firmware-RACADM auf iDRAC7 zu.
- Telnet – Greifen Sie über die Firmware-RACADM auf iDRAC7 zu.
- Remote-RACADM – Greifen Sie per remote auf iDRAC7 zu.

- SNMP-Agent – Aktiviert Unterstützung für SNMP-Anfragen (GET-, GETNEXT- und GETBULK-Vorgänge) in iDRAC7.
- Automatischer System-Wiederherstellungsagent – Aktivieren Sie den Bildschirm mit dem letzten Systemabsturz.

Services unter Verwendung der Webschnittstelle konfigurieren

Dienste über die iDRAC7-Web-Schnittstelle konfigurieren:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Dienste**. Die Seite **Dienste** wird angezeigt.
2. Geben Sie die erforderlichen Informationen ein und klicken Sie auf **Übernehmen**. Weitere Informationen zu den verschiedenen Einstellungen finden Sie in der *iDRAC7-Online-Hilfe*.

Dienste über RACADM konfigurieren

So aktivieren und konfigurieren Sie die verschiedenen Dienste mit RACADM:

- Verwenden Sie die folgenden Objekte mit dem Befehl **config**:
 - cfgRacTuneLocalConfigDisable
 - cfgRacTuneCtrlEConfigDisable
 - cfgSerialSshEnable
 - cfgRacTuneSshPort
 - cfgSsnMgtSshIdleTimeout
 - cfgSerialTelnetEnable
 - cfgRacTuneTelnetPort
 - cfgSsnMgtTelnetIdleTimeout
 - cfgRacTuneWebserverEnable
 - cfgSsnMgtWebserverTimeout
 - cfgRacTuneHttpPort
 - cfgRacTuneHttpsPort
 - cfgRacTuneRemoteRacadmEnable
 - cfgSsnMgtRacadmTimeout
 - cfgOobSnmpAgentEnable
 - cfgOobSnmpAgentCommunity
- Verwenden Sie die Objekte in den folgenden Objektgruppen mit dem Befehl **set**:
 - iDRAC.LocalSecurity
 - iDRAC.LocalSecurity
 - iDRAC.SSH
 - iDRAC.Webserver
 - iDRAC.Telnet
 - iDRAC.Racadm
 - iDRAC.SNMP

Weitere Informationen zu diesen Objekten finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Anzeige auf der Frontblende konfigurieren

Sie können die Anzeige der LC- und LE-Anzeigen auf der Frontblende des Managed System konfigurieren.

Bei Rack- und Tower-Servern sind zwei Frontblendentypen verfügbar:

- LC-Anzeige auf der Frontblende und System-ID-LED
- LE-Anzeige auf der Frontblende und System-ID-LED

Bei Blade-Servern ist nur die System-ID-LED auf der Frontblende des Servers verfügbar, da das Blade-Gehäuse mit einer LC-Anzeige ausgerüstet ist.

Verwandte Links

[LCD-Einstellung konfigurieren](#)

[LED-Einstellung für die System-ID konfigurieren](#)

LCD-Einstellung konfigurieren

Sie können eine Standardzeichenkette, wie z. B. den iDRAC-Namen, die IP-Adresse, usw. oder eine benutzerdefinierte Zeichenkette auf der LC-Anzeige auf der Frontblende des Managed System definieren und anzeigen.

Einstellungen für die LC-Anzeige über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die LC-Anzeige auf der Frontblende eines Servers:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Hardware** → **Frontblende**.
2. Wählen Sie im Abschnitt **Einstellungen für LC-Anzeige** über das Drop-Down-Menü **Nachricht auf der Startseite einrichten** einen der folgenden Aspekte aus:

- Service-Tag-Nummer (Standardeinstellung)
- Asset Tag
- DRAC-MAC-Adresse
- DRAC-IPv4-Adresse
- DRAC-IPv6-Adresse
- Systemstrom
- Umgebungstemperatur
- Systemmodell
- Host-Name
- Benutzerdefiniert
- Keine

Wenn Sie **Benutzerdefiniert** auswählen, geben Sie die erforderliche Nachricht in das Textfeld ein.

Wenn Sie **Keine** auswählen, wird die Nachricht auf der Startseite nicht auf der LC-Anzeige auf der Frontblende angezeigt.

3. Aktivieren Sie die Anzeige der virtuellen Konsole (optional). Bei Aktivierung zeigen der Abschnitt **Live-Status** an der Frontblende und die LCD-Anzeige am Server die Meldung `Sitzung der virtuellen Konsole aktiv` an, wenn es eine aktive Sitzung der virtuellen Konsole gibt.
4. Klicken Sie auf **Anwenden**.
Die LC-Anzeige auf der Frontblende des Servers zeigt die konfigurierte Nachricht für die Startseite an.

LCD-Einstellungen über RACADM konfigurieren

Um die Anzeige des LCD-Bedienfelds auf der Vorderseite des Servers zu konfigurieren, verwenden Sie die Objekte in der Gruppe **System.LCD**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

LCD-Einstellungen über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren

So konfigurieren Sie die LC-Anzeige auf der Frontblende eines Servers:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Frontblendensicherheit**. Die Seite **iDRAC-Einstellungen.Frontblendensicherheit** wird angezeigt.
2. Aktivieren oder deaktivieren Sie den Netzschalter.
3. Geben Sie folgendes an:
 - Zugang zur Frontblende
 - LCD-Meldungszeichenkette
 - Systemstromeinheiten, Umgebungstemperatureinheiten und Fehleranzeige
4. Aktivieren oder deaktivieren Sie die Anzeige der virtuellen Konsole. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.
5. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

LED-Einstellung für die System-ID konfigurieren

Aktivieren oder deaktivieren Sie für die Identifizierung eines Servers das Blinken der System-ID-LED auf dem Managed System.

LED-Einstellung für die System-ID über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die LE-Anzeige für die System-ID:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Hardware** → **Frontblende**. Daraufhin wird die Seite **Frontblende** angezeigt.
2. Wählen Sie im Abschnitt **LED-Einstellungen für die System-ID** beliebige der folgenden Optionen aus, um das Blinken der LED zu aktivieren oder zu deaktivieren:
 - Blinken ausgeschaltet
 - Blinken eingeschaltet
 - Blinken einschalten bei Zeitüberschreitung von einem Tag
 - Blinken einschalten bei Zeitüberschreitung von einer Woche
 - Blinken einschalten bei Zeitüberschreitung von einem Monat
3. Klicken Sie auf **Anwenden**. Das Blinken der LED auf der Frontblende ist konfiguriert.

LED-Einstellung der System-ID über RACADM konfigurieren

Um die System-ID-LED zu konfigurieren, verwenden Sie den Befehl **setled**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Das Konfigurieren von Zeitzone und NTP

Sie können die Zeitzone in iDRAC konfigurieren und die iDRAC-Zeit synchronisieren, indem Sie das Network Time Protocol (NTP) anstelle von BIOS oder Host-Systemzeiten verwenden.

Sie müssen über die Berechtigung zur Konfiguration verfügen, um die Zeitzone oder NTP-Einstellungen zu konfigurieren.

Konfigurieren von Zeitzone und NTP unter Verwendung der iDRAC- Web-Schnittstelle

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

1. Gehen Sie zu **Übersicht** → **iDRAC-Einstellungen** → **Eigenschaften** → **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 konfigurieren, aktivieren Sie NTP, geben Sie die NTP-Serveradressen ein und klicken Sie dann auf **Anwenden**.
Weitere Informationen zu den Feldern finden Sie unter *iDRAC7 Online Hilfe*.

Konfigurieren von Zeitzone und NTP unter Verwendung von RACADM

Um Zeitzone und NTP mithilfe von RACADM zu konfigurieren, verwenden Sie die Objekte in der Gruppe **iDRAC.Time** und **iDRAC.NTPConfigGroup** mit dem Befehl **set**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Erstes Startlaufwerk einstellen

Sie können das erste Startgerät für den nächsten Start einmalig oder für alle folgenden Starts einstellen. Basierend auf dieser Auswahl können Sie das erste Startgerät für das System einrichten. Das System startet vom ausgewählten Gerät beim nächsten und den folgenden Starts und bleibt als erstes Startgerät in der BIOS-Startreihenfolge bestehen, bis es wieder mit der iDRAC7-Web-Schnittstelle oder der 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
- Remote-Dateifreigabe
- Lokale SD-Karte
- vFlash
- Lifecycle-Controller
- BIOS Boot Manager



ANMERKUNG: Die Einstellungen für das erste Startgerät in der iDRAC7-Web-Schnittstelle überschreiben die Starteinstellungen im System-BIOS.

Erstes Startgerät über die Web-Schnittstelle einrichten

So richten Sie das erste Startgerät über die iDRAC7-Web-Schnittstelle ein:

1. Gehen Sie zu **Übersicht** → **Server** → **Einrichtung** → **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 den Startvorgang vom ausgewählten Startgerät beim nächsten Starten nur einmal auszuführen, wählen Sie **Einmalstart** aus. Daraufhin startet das System vom ersten Startgerät gemäß der BIOS-Startreihenfolge.
Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC7-Online-Hilfe*.

Erstes Startgerät über RACADM festlegen

- Um das erste Startgerät festzulegen, verwenden Sie das Objekt **cfgServerFirstBootDevice**.
- Um den einmaligen Start für ein Gerät einzurichten, verwenden Sie das Objekt **cfgServerBootOnce**.

Weitere Informationen zu diesen Objekten finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Einstellen des ersten Startgeräts unter Verwendung der virtuellen Konsole

Sie können das Gerät, von dem aus gestartet werden soll, auswählen, während der Server im Viewer für die virtuelle Konsole angezeigt wird, bevor er seine Startsequenz durchläuft. Sie können bei allen unterstützten Geräten, die unter [Erstes Startgerät einstellen](#) aufgelistet sind, einen Einmalstart durchführen.

So stellen Sie das erste Startgerät mithilfe der virtuellen Konsole ein:

1. Starten Sie die virtuelle Konsole.
2. Stellen Sie im Viewer der virtuellen Konsole im Menü **Nächster Start** das gewünschte Gerät als erstes Startgerät ein.

Bildschirm „Letzter Absturz“ aktivieren

Um den Grund für den Absturz eines Managed System zu beheben, können Sie das Image des Systemabsturzes über iDRAC7 erfassen.

So aktivieren Sie den Bildschirm für den letzten Absturz:

1. Installieren Sie über die *Dell Systems Management Tools and Documentation*-DVD den Server Administrator auf dem Managed System.
Weitere Informationen hierzu finden Sie im *Dell OpenManage Server Administrator Installation Guide* (Dell OpenManage Server Administrator-Installationshandbuch) unter dell.com/support/manuals.
2. Stellen Sie im Fenster „Starten und Wiederherstellen“ unter **Windows** sicher, dass die Option für den automatischen Neustart nicht ausgewählt ist.
Nähere Informationen erhalten Sie in der Windows Dokumentation.

3. Verwenden Sie Server Administrator, um den Zeitgeber für die **automatische Wiederherstellung** zu aktivieren, stellen Sie die automatische Wiederherstellung auf **Zurücksetzen, Ausschalten** oder **Aus- und einschalten** ein und stellen Sie den Zeitgeber in Sekunden ein (ein Wert zwischen 60 und 480).

Weitere Informationen hierzu finden Sie im *Dell OpenManage Server Administrator Installation Guide* (Dell OpenManage Server Administrator-Installationshandbuch) unter dell.com/support/manuals.

4. Aktivieren Sie die Option **Automatisches Herunterfahren und Wiederherstellen** (ASR) über eine der folgenden Komponenten:
 - Server Administrator – Weitere Informationen finden Sie im *Dell OpenManage Server Administrator User's Guide* (Dell OpenManage Server Administrator-Benutzerhandbuch) unter dell.com/support/manuals.
 - Lokaler RACADM – Verwenden Sie den folgenden Befehl:

```
racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1
```

5. Aktivieren Sie **Automatischer System-Wiederherstellungsagent**. Gehen Sie dazu zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Dienste**, wählen Sie **Aktivieren** aus, und klicken Sie auf **Anwenden**.

Aktivieren oder Deaktivieren des Betriebssystems zum iDRAC-Passthrough

Bei Servern, die Network-Daughter-Card- (NDC) oder integrierte LAN-On-Motherboard- (LOM) Geräte aufweisen, können Sie die Funktion Betriebssystem zu iDRAC-Passthrough aktivieren, die eine bidirektionale bandinterne Hochgeschwindigkeitskommunikation zwischen iDRAC7 und dem Host-Betriebssystem mittels eines freigegebenen LOM (Rack- oder Tower-Server) oder einer dedizierten NIC (Rack-, Tower- oder Blade-Server) ermöglicht. Diese Funktion ist mit der iDRAC7 Enterprise-Lizenz verfügbar.

Wenn der Browser durch eine dedizierte NIC aktiviert wurde, kann dieser im Host-Betriebssystem gestartet werden und dann auf die iDRAC-Web-Schnittstelle zugreifen. Die dedizierte NIC für die Blade-Server findet sich im Chassis Management Controller.

Das Wechseln zwischen dedizierter NIC und freigegebenem LOM erfordert keinen Neustart oder Reset des Host-Betriebssystems oder des iDRAC.

Der Kanal kann folgendermaßen aktiviert werden:

- iDRAC-Web-Schnittstelle
- RACADM oder WS-MAN (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 die XML-Konfigurationsdatei über RACADM oder WS-MAN verwenden und wenn die Netzwerkeinstellungen in dieser Datei geändert wurden, dann müssen Sie 15 Sekunden warten, um entweder die Funktion des Betriebssystems zum iDRAC-Passthrough zu aktivieren oder die IP-Adresse des Host-Betriebssystems einzustellen.

Vor Aktivierung des Betriebssystems zum iDRAC-Passthrough stellen Sie Folgendes sicher:

- Host-Betriebssystem und iDRAC7 befinden sich auf dem gleichen Subnetz.
- Die IP-Adresse des Host-Betriebssystems ist konfiguriert.
- Sie verfügen über die Berechtigung zum Konfigurieren.

Wenn Sie diese Funktion aktivieren:

- Im freigegebenen Modus wird die IP-Adresse des Host-Betriebssystems automatisch bestückt.
- 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.

Nach Aktivierung der Funktion von Betriebssystem zu iDRAC-Passthrough gehen Sie bei einer Funktionsstörung wie folgt vor:

- Überprüfen Sie, ob das dedizierte NIC-Kabel des iDRAC richtig verbunden ist.
- Stellen Sie sicher, dass mindestens ein LOM aktiv ist.

Die folgende Tabelle bietet eine Liste der Karten, die die Funktion von Betriebssystem zu iDRAC-Passthrough unterstützen.

Tabelle 7 : Betriebssystem zu iDRAC-Passthrough – Unterstützte Karten

Kategorie	Hersteller	Typ
NDC	Broadcom	<ul style="list-style-type: none"> • 57800S QP rNDC (10G BASE-T + 1G BASE-T) • 57800S QP rNDC (10G SFP+ + 1G BASE-T) • 5720 QP rNDC 1G BASE-T • 57810S DP bNDC KR • 57840 4x10G SFP+ (Sirius) • 57840 4x10G KR (Regulus)
	Intel	<ul style="list-style-type: none"> • i540 QP rNDC (10G BASE-T + 1G BASE-T) • i350 QP rNDC 1G BASE-T • i520 DP bNDC KR • x520 2X10G SFP+ / i350 2X1G Base-T (Saiph)
	QLogic	10G DP bNDC KR
Zusatzkarte	Broadcom	<ul style="list-style-type: none"> • 5719 QP 1G Mezz • 57810S DP 10G KR Mezz
	Intel	<ul style="list-style-type: none"> • DP 10Gb KR Mezz • i350 QP 1G Mezz
	QLogic	<ul style="list-style-type: none"> • DP 10Gb SFP+/DA CNA Mezz • QME2662 FC16 • QME2572 FC8
	Emulex	LPM16002
NIC	Broadcom	<ul style="list-style-type: none"> • 57810 DP 10G SFP+ ADAPTER • 57810C DP 10G BASE-T ADAPTER • 5720 DP 1G ADAPTER • 5719 QP 1G ADAPTER
	Intel	<ul style="list-style-type: none"> • X540 DP 10G BASE-T ADAPTER • I350 DP 1G ADAPTER • I350 QP 1G ADAPTER • X520 DP 10G SFP+ ADAPTER
	QLogic	DP 10Gb SFP+/DA CNA ADAPTER

Kategorie	Hersteller	Typ
PCIe	Emulex	LPe16000
	QLogic	<ul style="list-style-type: none"> • QLE2660 FC16 • QLE2662 FC16 • QLE2560 FC8 • QLE2562 FC8

Die folgenden Karten unterstützen nicht die Funktion von Betriebssystem zu iDRAC-Passthrough:

- Intel 10 Gig bNDC.
- Intel rNDC (Elk Flat rNDC) mit zwei Controllern – 10G-Controller unterstützen nicht.
- Qlogic bNDC Part # D90TX.

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

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

1. Gehen Sie zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Betriebssystem zu iDRAC-Passthrough**. Die Seite **Betriebssystem zu iDRAC-Passthrough** wird angezeigt.
2. Wählen Sie **Aktivieren**. Die konfigurierte IP-Adresse des Host-Betriebssystems wird im Feld **IP-Adresse Betriebssystem** angezeigt. Zur Deaktivierung wählen Sie **Deaktivieren** aus und fahren mit Schritt 4 fort.
3. Klicken Sie auf **Netzwerkverbindung testen**, um zu überprüfen, ob iDRAC sich ordnungsgemäß mit der IP-Adresse verbinden kann.
4. Klicken Sie auf **Anwenden**. Betriebssystem zu iDRAC-Passthrough ist aktiviert.

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

Um das Betriebssystem zum iDRAC-Passthrough unter Verwendung von RACADM zu aktivieren oder zu deaktivieren, verwenden Sie die Objekte in der Gruppe **iDRAC.OS-BMC**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

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 **Betriebssystem zu iDRAC-Passthrough**. Die Seite **iDRAC-Einstellungen.Betriebssystem zu iDRAC-Passthrough** wird angezeigt.
2. Wählen Sie **Aktiviert**, um das Betriebssystem zum iDRAC-Passthrough zu aktivieren. Ansonsten wählen Sie **Deaktiviert**. Die konfigurierte IP-Adresse des Host-Betriebssystems wird im Feld **IP-Adresse Betriebssystem** angezeigt.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**. Die Details sind damit gespeichert.

Zertifikate abrufen

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

Tabelle 8. Zertifikattypen auf der Basis des Anmeldetyps

Anmeldetyp	Zertifikattyp	Abrufmöglichkeit
Einmalige Anmeldung über Active Directory	Vertrauenswürdigen Zertifizierungsstellenzertifikat	Zertifikatsignierungsanforderung (CSR) generieren und diese von einer Zertifizierungsstelle signieren lassen
Smart Card-Anmeldung als lokaler oder Active Directory-Benutzer	<ul style="list-style-type: none"> Benutzerzertifikat Vertrauenswürdigen Zertifizierungsstellenzertifikat 	<ul style="list-style-type: none"> Benutzerzertifikat – Smart Card-Benutzerzertifikat als Base64-kodierte Datei unter Verwendung der Kartenverwaltungssoftware exportieren, die durch den Smart Card-Anbieter bereitgestellt wird Vertrauenswürdigen Zertifizierungsstellenzertifikat – Dieses Zertifikat wird von einer Zertifizierungsstelle ausgegeben.
Active Directory-Benutzeranmeldung	Vertrauenswürdigen Zertifizierungsstellenzertifikat	Dieses Zertifikat wird durch eine Zertifizierungsstelle ausgegeben.
Lokale Benutzeranmeldung	SSL-Zertifikat	Zertifikatsignierungsanforderung (CSR) generieren und diese von einer vertrauenswürdigen Zertifizierungsstelle signieren lassen
		 ANMERKUNG: iDRAC7 wird mit einem standardmäßigen selbstsignierten SSL-Server-Zertifikat ausgeliefert. Dieses Zertifikat wird vom iDRAC7 Web-Server, von virtuellen Datenträgern und der virtuellen Konsole verwendet.

Verwandte Links

[SSL-Serverzertifikate](#)

[Neue Zertifikatsignierungsanforderung erstellen](#)

SSL-Serverzertifikate

iDRAC7 beinhaltet einen Web Server, der für die Verwendung des Branchenstandard-SSL-Sicherheitsprotokolls für die Übertragung von verschlüsselten Daten über ein Netzwerk konfiguriert ist. 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

^Der Verschlüsselungsprozess bietet ein hohes Maß an Datenschutz. iDRAC7 wendet den 128-Bit-SSL-Verschlüsselungsstandard an. Hierbei handelt es sich um die sicherste Form der Verschlüsselung, die allgemein für Internet-Browser in Nordamerika verfügbar ist.

iDRAC7 Web Server verfügt standardmäßig über ein von Dell selbst signiertes, eindeutiges digitales SSL-Zertifikat. Sie können das standardmäßige SSL-Zertifikat durch ein von einer bekannten Zertifizierungsstelle signiertes Zertifikat ersetzen. Eine Zertifizierungsstelle ist ein Geschäftsunternehmen, das anerkannterweise hohe Standards bei der verlässlichen Prüfung, Identifikation und anderen wichtigen Sicherheitskriterien erfüllt. Beispiele für Zertifizierungsstellen sind Thawte und VeriSign. Um den Vorgang zum Erhalt eines von einer Zertifizierungsstelle signierten Zertifikats zu beginnen, nutzen Sie entweder die Web-Schnittstelle von iDRAC7 oder die RACADM-Schnittstelle, um eine Zertifikatsignieranforderung (CSR) mit den Informationen Ihres Unternehmens zu erzeugen. Dann senden Sie die erzeugte CSR an eine Zertifizierungsstelle wie VeriSign oder Thawte ab. Nachdem Sie das von der Zertifizierungsstelle signierte SSL-Zertifikat erhalten haben, laden Sie es in iDRAC hoch.

Für jeden iDRAC, dem die Management Station vertrauen soll, muss das jeweilige iDRAC-SSL-Zertifikat im Zertifikatspeicher der Management Station platziert werden. Wenn das SSL-Zertifikat auf den Management Stations installiert ist, können unterstützte Browser auf iDRAC ohne Zertifikatswarnungen zugreifen.

Sie können zur Signierung des SSL-Zertifikats auch ein benutzerdefiniertes Signaturzertifikat hochladen, anstatt auf das Standardsignaturzertifikat für diese Funktion zurückzugreifen. Durch Import eines benutzerdefinierten Signaturzertifikats in alle Management Stations wird allen iDRACs, die dieses benutzerdefinierte Signaturzertifikat verwenden, vertraut. Falls ein benutzerdefiniertes Signaturzertifikat hochgeladen wird, wenn bereits ein benutzerdefiniertes SSL-Zertifikat in Verwendung ist, dann wird das benutzerdefinierte SSL-Zertifikat deaktiviert und ein einmaliges, automatisch erzeugtes SSL-Zertifikat wird verwendet, das mit dem benutzerdefinierten Signaturzertifikat signiert ist. Sie können das benutzerdefinierte Signaturzertifikat herunterladen (ohne den privaten Schlüssel). Sie können ein bestehendes benutzerdefiniertes Signaturzertifikat auch löschen. Nach Löschen des benutzerdefinierten 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 dem 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).

Verwandte Links

[Neue Zertifikatsignierungsanforderung erstellen](#)

[Serverzertifikat hochladen](#)

[Serverzertifikat anzeigen](#)

[Hochladen eines benutzerdefinierten Signaturzertifikats](#)

[Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat herunterladen](#)

[Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat löschen](#)

Neue Zertifikatsignierungsanforderung erstellen

Eine CSR ist eine digitale Anforderung eines SSL-Serverzertifikats von einer Zertifizierungsstelle (CA). SSL-Serverzertifikate ermöglichen Clients des Servers, die Identität des Servers als vertrauenswürdig einzustufen und eine verschlüsselte Sitzung mit dem Server auszuhandeln.

Nachdem die Zertifizierungsstelle eine Zertifikatsignierungsanforderung erhalten hat, verifiziert und bestätigt sie die darin enthaltenen Informationen. Wenn der Anmeldende die Sicherheitsstandards der Zertifikatzertifizierungsstelle erfüllt, gibt die Zertifikatzertifizierungsstelle ein digital signiertes SSL-Serverzertifikat aus, das den Server des Anmeldenden beim Aufbau von SSL-Verbindungen über Browser, die auf Management Stations ausgeführt werden, eindeutig identifiziert.

Nach der Genehmigung der Zertifikatsignierungsanforderung (CSR) und der Ausgabe des Serverzertifikats durch die Zertifikatzertifizierungsstelle kann die CSR auf iDRAC7 hochgeladen werden. Die Informationen, die zum Generieren der

CSR verwendet und auf der iDRAC7-Firmware gespeichert werden, müssen mit den Informationen auf dem SSL-Serverzertifikat übereinstimmen, dies bedeutet, dass das Zertifikat mithilfe der durch iDRAC7 erstellte CSR generiert worden sein muss.

Verwandte Links

[SSL-Serverzertifikate](#)

CSR unter Verwendung der Webschnittstelle erstellen

Um neue CSR zu erstellen:



ANMERKUNG: Jede neue Zertifikatsignierungsanforderung überschreibt alle vorangegangenen, in der Firmware gespeicherten Daten. Die Informationen in der Zertifikatsignierungsanforderung müssen den Informationen im Zertifikat entsprechen. Andernfalls akzeptiert der iDRAC7 nicht das Zertifikat.

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **SSL**, 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 *iDRAC7 Online-Hilfe*.
3. Klicken Sie auf **Erstellen**. Es wird eine neue CSR erzeugt. Speichern Sie sie in der Management Station.

CSR über RACADM generieren

Um eine CSR unter Verwendung von RACADM zu erzeugen, verwenden Sie die Objekte in der Gruppe **cfgRacSecurity** mit dem Befehl **config** oder die Objekte in der Gruppe **iDRAC.Security** mit dem Befehl **set** und verwenden Sie dann den Befehl **sslcsrgen**, um die CSR zu erzeugen. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Serverzertifikat hochladen

Nach der Generierung einer Zertifikatsignierungsanforderung (CSR) können Sie das signierte SSL-Serverzertifikat auf die iDRAC7-Firmware hochladen. iDRAC7 wird zurückgesetzt, nachdem Sie das Zertifikat hochgeladen haben. iDRAC7 akzeptiert nur X509, Base 64-kodierte Web Server-Zertifikate.



VORSICHT: Während des Resets ist iDRAC7 für einige Minuten nicht verfügbar.

Verwandte Links

[SSL-Serverzertifikate](#)

Serverzertifikat über die Web-Schnittstelle hochladen

So laden Sie das SSL-Serverzertifikat hoch:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **SSL**, wählen Sie **Serverzertifikat hochladen** aus, und klicken Sie dann 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 die iDRAC7-Firmware hochgeladen und ersetzt das bereits vorhandene Zertifikat.

Serverzertifikat über RACADM hochladen

Um das SSL-Serverzertifikat hochzuladen, verwenden Sie den Befehl **sslcertupload**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Serverzertifikat anzeigen

Sie können das SSL-Serverzertifikat anzeigen, das derzeit in iDRAC7 verwendet wird.

Verwandte Links

[SSL-Serverzertifikate](#)

Serverzertifikat über die Web-Schnittstelle anzeigen

Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **SSL**. Die Seite **SSL** zeigt oben auf der Seite das SSL-Serverzertifikat an, das derzeit verwendet wird.

Serverzertifikat über RACADM anzeigen

Um das SSL-Serverzertifikat anzuzeigen, verwenden Sie den Befehl **sslcertview**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Hochladen eines benutzerdefinierten Signaturzertifikats

Sie können ein benutzerdefiniertes Signaturzertifikat hochladen, um das SSL-Zertifikat zu signieren.

Hochladen von benutzerdefinierten Signaturzertifikaten mithilfe der Web-Schnittstelle

So laden Sie ein benutzerdefiniertes Signaturzertifikat mithilfe der iDRAC7-Web-Schnittstelle hoch:

1. Gehen Sie zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **SSL**.
Die Seite **SSL** wird angezeigt.
2. Wählen Sie unter **Benutzerdefiniertes SSL-Zertifikatssignaturzertifikat Benutzerdefiniertes SSL-Zertifikatssignaturzertifikat hochladen** aus und klicken Sie auf **Weiter**.
Die Seite **Benutzerdefiniertes SSL-Zertifikatssignaturzertifikat hochladen** wird angezeigt.
3. Klicken Sie auf **Durchsuchen** und wählen Sie das benutzerspezifische SSL-Zertifikat 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 zu den Resets von iDRAC und iDRAC hochgeladen. Während des Resets ist iDRAC für einige Minuten nicht verfügbar.

Hochladen eines benutzerdefinierten SSL-Zertifikatssignaturzertifikats unter Verwendung von RACADM

Um das benutzerdefinierte SSL-Zertifikatssignaturzertifikat mit RACADM hochzuladen, verwenden Sie den Unterbefehl **sslcertupload**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat herunterladen

Sie können das benutzerdefinierte Signaturzertifikat mithilfe der iDRAC7-Web-Schnittstelle oder RACADM herunterladen.

Benutzerdefiniertes Signierungszertifikat herunterladen

So laden Sie Benutzerdefinierte Signierungszertifikate unter Verwendung der iDRAC7 Webschnittstelle herunter:

1. Gehen Sie zu **Überblick** → **iDRAC-Einstellungen** → **Netzwerk** → **SSL**.
Die Seite **SSL** wird angezeigt.
2. Wählen Sie unter **Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat** die Option **Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat herunterladen** und klicken Sie auf **Weiter**.
Ein Fenster öffnet sich, über das Sie das benutzerdefinierte Signierungszertifikat an den Speicherort Ihrer Wahl speichern können.

Herunterladen eines benutzerdefinierten SSL-Zertifikatssignaturzertifikats unter Verwendung von RACADM

Um das benutzerdefinierte SSL-Zertifikatssignaturzertifikat herunterzuladen, verwenden Sie den Unterbefehl **sslcertdownload**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Benutzerdefiniertes SSL-Zertifikat Signierungszertifikat löschen

Sie können ein bestehendes benutzerdefiniertes Signierungszertifikat auch unter Verwendung der iDRAC7 Webschnittstelle oder RACADM löschen.

Löschen von benutzerdefinierten Signaturzertifikaten

So löschen Sie ein benutzerdefiniertes Signaturzertifikat mithilfe der iDRAC7-Web-Schnittstelle:


1. Gehen Sie zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **SSL**.
Die Seite **SSL** wird angezeigt.
2. Wählen Sie unter **Benutzerdefiniertes SSL-Zertifikatssignaturzertifikat** **Benutzerdefiniertes SSL-Zertifikatssignaturzertifikat löschen** aus und klicken Sie auf **Weiter**.
Das benutzerdefinierte Signaturzertifikat wird von iDRAC gelöscht. iDRAC wird darauf zurückgesetzt, das selbst signierte Standard-SSL-Zertifikat zu verwenden, das vom Web Server automatisch erzeugt wird. iDRAC ist während des Zurücksetzens nicht verfügbar.

Löschen eines benutzerdefinierten SSL-Zertifikatssignaturzertifikats unter Verwendung von RACADM

Um das benutzerdefinierte SSL-Zertifikatssignaturzertifikat mit RACADM zu löschen, verwenden Sie den Unterbefehl **sslcertdelete**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Mehrere iDRAC7s über RACADM konfigurieren

Sie können einen oder mehrere iDRAC7s mit identischen Eigenschaften über RACADM konfigurieren. Wenn Sie einen spezifischen iDRAC7 über seine Gruppen-ID und die Objekt-ID abfragen, erstellt RACADM die Konfigurationsdatei **.cfg** aus den abgerufenen Informationen. Der Dateiname kann durch den Benutzer festgelegt werden. Importieren Sie die Datei für identische Konfigurationen auf andere iDRAC7s.


 **ANMERKUNG:** Einige Konfigurationsdateien enthalten einmalige iDRAC7-Informationen (z. B. die statische IP-Adresse), die Sie ändern müssen, bevor Sie die Datei auf andere iDRAC7s exportieren.


Sie können auch die XML-Datei der Systemkonfiguration verwenden, um mehrere iDRACs mit RACADM zu konfigurieren. Die XML-Datei der Systemkonfiguration enthält die Informationen zur Komponentenkonfiguration und die Datei wird verwendet, um die Konfiguration für BIOS, iDRAC, RAID und NIC anzuwenden, indem die Datei in ein Zielsystem importiert wird. Weitere Informationen finden Sie im Whitepaper *XML Configuration Workflow*, das unter dell.com/support/manuals oder im Dell Tech Center verfügbar ist.

So konfigurieren Sie mehrere iDRAC7s unter Verwendung der **.cfg**-Datei:

1. Fragen Sie den Ziel-iDRAC7, der die erforderlichen Konfiguration enthält, über den folgenden Befehl ab: `racadm getconfig -f myfile.cfg`.


Der Befehl fordert die iDRAC7-Konfiguration an und generiert die Datei **myfile.cfg**. Falls erforderlich, können Sie die Datei mit einem anderen Namen konfigurieren.

 **ANMERKUNG:** Das Umleiten der iDRAC7-Konfiguration zu einer Datei unter Verwendung von `getconfig -f` wird nur bei den lokalen und Remote-RACADM-Schnittstellen unterstützt.

 **ANMERKUNG:** Die erstellte **.cfg**-Datei enthält keine Benutzerkennwörter.

Der Befehl **getconfig** zeigt alle Konfigurationseigenschaften in einer Gruppe (angegeben nach Gruppenname und Index) und alle Konfigurationseigenschaften für einen Benutzer nach Benutzername an.

2. Ändern Sie die Konfigurationsdatei mit einem einfachen Texteditor (optional).

 **ANMERKUNG:** Es wird empfohlen, diese Datei mit einem einfachen Texteditor zu bearbeiten. Das RACADM-Dienstprogramm verwendet einen ASCII-Text-Parser. Jede Formatierung verursacht Störungen bei der Analyse und kann die RACADM-Datenbank beschädigen.

3. Verwenden Sie die neue Konfigurationsdatei, um den Ziel-iDRAC7 über den folgenden Befehl zu ändern: `racadm config -f myfile.cfg`

Durch diesen Befehl werden die Informationen in den anderen iDRAC7 geladen. Sie können den **config**-Unterbefehl verwenden, um die Benutzer- und Kennwortdatenbank mit Server Administrator zu synchronisieren.

4. Setzen Sie den Ziel-iDRAC7 über den folgenden Befehl zurück: `racadm racreset`

iDRAC7-Konfigurationsdatei erstellen

Die Konfigurationsdatei **.cfg** kann:

- Erstellt
- Abgerufen vom Befehl `racadm getconfig -f <filename>.cfg` oder `racadm get -f <filename>.cfg`
- Abgerufen vom Befehl `racadm getconfig -f <filename>.cfg` oder `racadm get -f <filename>.cfg` und dann bearbeitet

Weitere Informationen zu den Befehlen **getconfig** und **get** finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Die **.cfg**-Datei wird zunächst geparkt, um zu prüfen, ob gültige Gruppen und Objektamen vorhanden sind und ob einige einfache Syntaxregeln befolgt werden. Fehler werden mit der Zeilennummer markiert, in der der Fehler ermittelt wurde. Eine Meldung beschreibt das Problem. Die vollständige Datei wird auf Richtigkeit geparkt und alle Fehler werden angezeigt. Schreibbefehle werden nicht zum iDRAC7 übertragen, wenn in der **.cfg**-Datei ein Fehler festgestellt wird. Der Benutzer muss alle Fehler vor der Verwendung der Datei zum Konfigurieren von iDRAC7 korrigieren. Verwenden Sie die Option `-c` für den Unterbefehl `config`. Dadurch wird die Syntax überprüft, es werden jedoch keine Schreibvorgänge zum iDRAC7 vorgenommen.

Verwenden Sie die folgenden Richtlinien zum Erstellen einer **.cfg**-Datei:

- Wenn der Parser auf eine indizierte Gruppe trifft, wird der Index der Gruppe als Anker verwendet. Sämtliche Modifizierungen der Objekte innerhalb der indizierten Gruppe werden ebenfalls mit dem Indexwert assoziiert. Beispiel:

- Wenn Sie den Befehl **getconfig** verwendet haben:

```
[cfgUserAdmin] # cfgUserAdminIndex=11 cfgUserAdminUserName= #
cfgUserAdminPassword=***** (Write-Only) cfgUserAdminEnable=0
cfgUserAdminPrivilege=0x00000000 cfgUserAdminIpmiLanPrivilege=15
cfgUserAdminIpmiSerialPrivilege=15 cfgUserAdminSolEnable=0
```

- Wenn Sie den Befehl **get** verwendet haben:

```
[idrac.users.16] Enable=Disabled IpmiLanPrivilege=15
IpmiSerialPrivilege=15 !!Password=***** (Write-Only)
Privilege=0x0 SNMPv3AuthenticationType=SHA SNMPv3Enable=Disabled
SNMPv3PrivacyType=AES SolEnable=Disabled UserName=
```

- Die Indizes sind vom Typ Nur-Lesen und können nicht modifiziert werden. Objekte der indizierten Gruppe sind an den Index gebunden, unter dem sie aufgeführt sind, und alle gültigen Konfigurationen des Objektwerts gelten nur für diesen bestimmten Index.
- Für jede indizierte Gruppe steht ein vordefinierter Satz von Indizes zur Verfügung. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.
- Verwenden Sie den Unterbefehl `racresetcfg`, um iDRAC7 auf die Standardeinstellung zurückzusetzen und führen Sie dann den Befehl `racadm config -f <filename>.cfg` oder `racadm set -f <filename>.cfg` aus. Stellen Sie sicher, dass die Datei **.cfg** alle erforderlichen Objekte, Benutzer, Indizes und anderen Parameter enthält.



VORSICHT: Verwenden Sie den Unterbefehl `racresetcfg`, um die Datenbank und die iDRAC7-NIC-Einstellungen auf die Standardeinstellungen zurückzusetzen und alle Benutzer und Benutzerkonfigurationen zu entfernen. Während der Stammbenutzer verfügbar ist, werden die Einstellungen anderer Benutzer ebenfalls auf die Standardeinstellungen zurückgesetzt.

Parsing-Regeln

- Alle Zeilen, die mit `#` beginnen, werden als Kommentare behandelt. Eine Kommentarzeile muss in Spalte 1 beginnen. Ein `„#“`-Zeichen in jeder anderen Spalte wird als das Zeichen `#` behandelt. Einige Modemparameter können `„#“`-Zeichen in der Zeichenkette enthalten. Ein Escape-Zeichen ist nicht erforderlich. Sie können einen **.cfg**-Befehl aus einem `racadm getconfig -f <Dateiname>.cfg`-Befehl erstellen und dann einen `racadm config -f <Dateiname>.cfg`-Befehl auf einem anderen iDRAC7 ausführen, ohne dass Sie Escape-Zeichen hinzufügen müssen. Beispiel:

```
#
# Dies ist eine Anmerkung
[cfgUserAdmin]
cfgUserAdminPageModemInitString=<Modem init # Dies ist kein Kommentar>
```

- Alle Gruppeneinträge müssen in `[" und "]`-Zeichen eingeschlossen sein. Das Anfangszeichen `[`, das einen Gruppennamen anzeigt, *muss* in Spalte eins sein. Der Gruppename *muss* vor allen anderen Objekten in dieser Gruppe angegeben werden. Objekte, die keinen zugewiesenen Gruppennamen enthalten, erzeugen Fehler. Die Konfigurationsdaten sind in Gruppen angeordnet, die im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist, definiert sind. Das folgende Beispiel zeigt einen Gruppennamen, ein Objekt und den Eigenschaftswert des Objekts an.

```
[cfgLanNetworking] -{Gruppenname}
cfgNicIpAddress=143.154.133.121 {Objektname}
```

- Alle Parameter werden als „Objekt=Wert“-Paare ohne Leerzeichen zwischen „Objekt“, „=“ und „Wert“ angegeben.
Leerzeichen nach dem Wert werden ignoriert. Ein Leerzeichen innerhalb einer Wertezeichenkette bleibt unverändert. Jedes Zeichen rechts von „=“ wird wie vorhanden angenommen (zum Beispiel, ein zweites „=“ oder ein „#“, „[“,]“ und so weiter).

Siehe Beispiel unter vorherigem Punkt.

Der Befehl `racadm getconfig -f <Dateiname>.cfg` setzt einen Kommentar vor die Index-Objekte, durch die dem Benutzer die enthaltenen Kommentare angezeigt werden.

Um den Inhalt einer indizierten Gruppe anzuzeigen, verwenden Sie den folgenden Befehl:

```
racadm getconfig -g <Gruppenname> -i <Index 1-16>
```

- Für indizierte Gruppen muss es sich bei dem Objektanker um das erste Objekt nach dem „[]“-Paar handeln. Im Folgenden finden Sie Beispiele für aktuelle indizierte Gruppen:

```
[cfgUserAdmin]
cfgUserAdminIndex=11
```

Wenn Sie `racadm getconfig -f <MeinBeispiel>.cfg` eingeben, erstellt der Befehl eine **.cfg**-Datei für die aktuelle iDRAC7-Konfiguration. Diese Konfigurationsdatei kann als Beispiel und Ausgangspunkt für Ihre eindeutige **.cfg**-Datei verwendet werden.

iDRAC7-IP-Adresse ändern

Wenn Sie die iDRAC6-IP-Adresse in der Konfigurationsdatei ändern, entfernen Sie alle unnötigen `<Variable>=Wert`-Einträge. Es verbleibt lediglich die tatsächliche Bezeichnung der variablen Gruppe mit „[“ und „]“ zusammen mit den beiden `<Variable>=Wert`-Einträgen, die sich auf die IP-Adressenänderung beziehen.

Zum Beispiel:


```
#
# Objektgruppe "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

Die Datei wird aktualisiert wie folgt:

```
#
# Objektgruppe "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# Kommentar, der Rest dieser Zeile wird ignoriert
cfgNicGateway=10.35.9.1
```

Mit dem Befehl `racadm config -f myfile.cfg` wird die Datei geparkt, und Fehler werden nach Zeilennummer identifiziert. Eine korrekte Datei aktualisiert die richtigen Einträge. Außerdem kann derselbe `getconfig`-Befehl (siehe vorheriges Beispiel) zur Bestätigung der Aktualisierung verwendet werden.


Mit dieser Datei können Sie unternehmensweite Änderungen herunterladen oder neue Systeme über das Netzwerk konfigurieren.

 **ANMERKUNG:** „Anchor“ ist ein interner Ausdruck und darf nicht in der Datei verwendet werden.

Zugriff zum Ändern der iDRAC7-Konfigurationseinstellungen auf einem Host-System deaktivieren

Sie können den Zugriff zum Ändern der iDRAC7-Konfigurationseinstellungen über einen lokalen RACADM oder ein Dienstprogramm für iDRAC-Einstellungen deaktivieren. Außerdem können Sie diese Konfigurationseinstellungen anzeigen. Gehen Sie dazu wie folgt vor:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Dienste**.
2. Wählen eine oder beide der folgenden Maßnahmen aus:
 - **Lokale iDRAC-Konfiguration unter Verwendung der iDRAC-Einstellungen deaktivieren** – Deaktiviert den Zugriff zum Ändern der Konfigurationseinstellungen im Dienstprogramm für die iDRAC-Einstellungen.
 - **Lokale iDRAC-Konfiguration unter Verwendung von RACADM deaktivieren** – Deaktiviert den Zugriff zum Ändern der Konfigurationseinstellungen im lokalen RACADM.
3. Klicken Sie auf **Anwenden**.

 **ANMERKUNG:** Wenn der Zugriff zum Ändern deaktiviert ist, können Sie Server Administrator oder IPMITool nicht zum Ändern der iDRAC7-Konfigurationen verwenden. Sie können jedoch IPMI-über-LAN verwenden

Informationen zu iDRAC7 und zum Managed System anzeigen

Sie können den Zustand und die Eigenschaften für iDRAC7 und das Managed System, außerdem die Bestandsliste zu Hardware und Firmware, den Zustand des Sensors, die Speichergeräte und die Netzwerkgeräte anzeigen. Darüber hinaus können Sie Benutzersitzungen anzeigen und beenden. Bei Blade-Servern können Sie außerdem Informationen zur Flex-Adresse anzeigen.

Verwandte Links

- [Zustand und Eigenschaften des Managed System anzeigen](#)
- [System-Bestandsaufnahme anzeigen](#)
- [Sensorinformationen anzeigen](#)
- [Das System auf Frischlufttauglichkeit prüfen](#)
- [Temperaturverlaufsdaten anzeigen](#)
- [Bestandsaufnahme für Speichergeräte erstellen und Speichergeräte überwachen](#)
- [Bestandsaufnahme für Netzwerkgeräte erstellen und Netzwerkgeräte überwachen](#)
- [Bestandsaufnahme und Überwachung von FC-HBA-Geräten](#)
- [Verbindungen der FlexAddress-Mezzanine-Kartenarchitektur anzeigen](#)
- [iDRAC7-Sitzungen anzeigen oder beenden](#)

Zustand und Eigenschaften des Managed System anzeigen

Wenn Sie sich bei der iDRAC7-Web-Schnittstelle anmelden, können Sie auf der Seite **Systemzusammenfassung** den Zustand des Managed System und Basis-iDRAC7-Informationen anzeigen, eine Vorschau auf die virtuelle Konsole abrufen, Arbeitnotizen hinzufügen und anzeigen und Aufgaben schnell starten, wie z. B. aus- und einschalten, Protokolle anzeigen, Firmware aktualisieren und iDRAC7 zurücksetzen.

Gehen Sie zum Aufrufen der Seite **Systemzusammenfassung** zu **Übersicht** → **Server** → **Eigenschaften** → **Zusammenfassung**. Daraufhin wird die Seite **Systemzusammenfassung** angezeigt. Weitere Informationen finden Sie in der *iDRAC7-Online-Hilfe*.

Außerdem können Sie die Basis-Systemzusammenfassungsinformationen über das Dienstprogramm für die iDRAC-Einstellungen anzeigen. Gehen Sie dazu im Dienstprogramm für die iDRAC-Einstellungen zu **Systemzusammenfassung**. Daraufhin wird die Seite **iDRAC-Einstellungen – Systemzusammenfassung** angezeigt. Weitere Informationen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

System-Bestandsaufnahme anzeigen

Sie können die Informationen zu den auf dem Managed System installierten Hardware- und Firmware-Komponenten anzeigen. Gehen Sie dazu in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Eigenschaften** → **System-Bestandsaufnahme**. Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der *iDRAC7-Online-Hilfe*. Der Abschnitt Hardware-Bestandsaufnahme zeigt die Informationen für die folgenden Komponenten an, die auf dem Managed System verfügbar sind:


- iDRAC

- RAID-Controller
- Batterien
- CPUs
- DIMMs
- HDDs
- NICs (integriert und eingebettet)
- Videokarte
- SD-Karte
- Netzteile
- Lüfter
- Fibre-Channel-HBAs
- USB

Der Abschnitt Firmware-Bestandsaufnahme zeigt die Firmware-Version für die folgenden Komponenten:

- BIOS
- Lifecycle-Controller
- iDRAC
- BS-Treiberpaket
- 32-Bit Diagnose
- System CPLD
- PERC-Controller
- Batterien
- Physische Laufwerke
- Netzteil
- NIC
- Fibre-Channel
- Rückwandplatine
- Gehäuse

Wenn Sie Hardware-Komponente ersetzen oder die Firmware-Versionen aktualisieren, müssen Sie sicherstellen, dass Sie die Option **System-Bestandsaufnahme beim Neustart erstellen** (CSIOR) aktivieren und ausführen, um eine System-Bestandsaufnahme beim Neustart zu erstellen. Melden Sie sich nach einigen Minuten bei iDRAC7 an, und navigieren Sie zur Seite **System-Bestandsaufnahme**, um die Details anzuzeigen. Es kann in Abhängigkeit von der auf dem Server installierten Hardware bis zu fünf Minuten dauern, bis die Informationen angezeigt werden.


 **ANMERKUNG:** CSIOR-Option ist standardmäßig aktiviert.

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


Sensorinformationen anzeigen

Die folgenden Sensoren unterstützen Sie bei der Überwachung des Zustands des verwalteten Systems:

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

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

- **Lüfter** (nur für Rack- und Tower-Server verfügbar) – Bietet Informationen zu Lüftern in Systemen – Lüfterredundanz und Lüfterliste, in der die Lüftergeschwindigkeit und die Schwellenwerte angezeigt werden.
- **CPU** – Zeigt den Funktionszustand und den allgemeinen Zustand der CPUs im Managed System an. Zeigt Informationen zur automatischen Prozessordrosselung an und vorhergesagte Fehler.
- **Speicher** – Zeigt den Funktionszustand und den allgemeinen Zustand der im Managed System vorhandenen Speichermodule mit zwei Kontaktanschlusssreihen (Dual In-line Memory Module, DIMM) an.
- **Eingriff** – Zeigt Informationen über das Gehäuse an.
- **Netzteil** (nur für Tack- und Tower-Server) – Bietet Informationen zu den Netzteilen und dem Status der Netzteilredundanz.

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

- **Entfernbarer Flash Media** – Bietet Informationen zu den internen SD-Modulen – vFlash und Internal Dual SD Module (IDSMD).
 - Wenn IDSMD-Redundanz aktiviert ist, werden die folgenden IDSMD-Sensorstatus angezeigt: IDSMD-Redundanzstatus, IDSMD SD1 und IDSMD SD2. Wenn Redundanz deaktiviert ist, wird nur IDSMD SD1 angezeigt.
 - Wenn IDSMD-Redundanz beim Einschalten des Systems oder nach dem Zurücksetzen von iDRAC deaktiviert wird, wird der IDSMD SD1-Sensorstatus nur angezeigt, wenn eine Karte eingesetzt wird.
 - Wenn IDSMD-Redundanz aktiviert ist, während zwei SD-Karten im IDSMD vorhanden sind, und sich eine SD-Karte im *Online*-Modus befindet, während sich die andere Karte im *Offline*-Modus befindet, ist ein Neustart des Systems erforderlich, um die Redundanz zwischen den beiden SD-Karten im IDSMD wiederherzustellen. Nach der Wiederherstellung der Redundanz befinden sich beide SD-Karten im IDSMD wieder im *Online*-Modus.
 - Während der Wiederherstellung der Redundanz zwischen zwei SD-Karten, die sich im IDSMD befinden, wird der IDSMD-Status nicht angezeigt, da die IDSMD-Sensoren ausgeschaltet sind.
 - Die Systemereignisprotokolle (SEL) für eine schreibgeschützte oder beschädigte SD-Karte im IDSMD-Modul werden erst wiederholt, nachdem sie durch das Ersetzen der SD-Karte durch eine beschreibbare und funktionsfähige SD-Karte gelöscht wurden.
- **Temperatur** – Bietet Informationen zu den Lufteintritts- und Luftaustrittstemperaturen auf der Systemplatine (nur bei Rack- und Tower-Servern). Die Temperaturmessung zeigt an, ob sich der Status des Messgeräts innerhalb der vordefinierten Warnwerts oder des kritischen Schwellenwerts befindet.
- **Spannung** – Zeigt den Status und die Messwerte des Spannungssensors für verschiedene Systemkomponenten an.


Aus der folgenden Tabelle können Sie entnehmen, wie die Sensorinformationen über die iDRAC7-Web-Schnittstelle oder über RACADM abgelesen werden. Weitere Informationen zu den auf der Web-Schnittstelle angezeigten Eigenschaften finden Sie auf den entsprechenden Seiten in der *iDRAC7-Online-Hilfe*.

Tabelle 9. Abrufen von Sensorinformationen über die Web-Schnittstelle und RACADM

Sensorinformationen anzeigen für	über die Web-Schnittstelle	RACADM verwenden
Batterien	Übersicht → Hardware → Batterien	Verwenden Sie den Befehl getsensorinfo . Bei Netzteilen können Sie außerdem den Befehl System.Power.Supply mit dem Unterbefehl get verwenden. Weitere Informationen finden Sie im <i>RACADM Command Line Reference Guide for iDRAC7 and CMC</i> (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.
Lüfter	Overview → Hardware → Fans	
CPU	Overview → Hardware → CPU	
Speicher	Overview → Hardware → Memory	
Eingriff	Overview → Server → Intrusion	
Netzteile	Overview → Hardware → Power Supplies	
Wechselbarer Flash-Datenträger	Overview → Hardware → Removable Flash Media	
Temperatur	Overview → Server → Power/ Thermal → Temperatures	
Spannung	Overview → Server → Power/ Thermal → Voltages	

Das System auf Frischlufttauglichkeit prüfen

Die Frischluftkühlung kühlt die Systeme im Datenzentrum direkt mit Außenluft. Frischlufttaugliche Systeme können oberhalb ihres normalen Betriebstemperaturbereichs betrieben werden (Temperaturen bis zu 113 °F (45 °C)).

 **ANMERKUNG:** Frischluftkonfigurationen werden für 135W-CPUs, PCIe-SSDs, GPU-Karten und LR-DIMMs nicht unterstützt. Informationen zu den unterstützten Frischluftkonfigurationen erhalten Sie von Dell.

So prüfen Sie das System auf Frischlufttauglichkeit:

1. Gehen Sie in der iDRAC7-Weboberfläche auf **Übersicht** → **Server** → **Leistung / Wärme** → **Temperaturen**. Die **Temperatur**-Seite wird angezeigt.
2. Im Bereich **Frischluft** wird angezeigt, ob das System frischlufttauglich ist oder nicht.

Temperaturverlaufsdaten anzeigen

Sie können den prozentualen Zeitanteil anzeigen lassen, während dessen das System bei Umgebungstemperaturen oberhalb des normalerweise unterstützten Temperaturschwellenwertes betrieben wurde. Zur Temperaturüberwachung werden die Messwerte des Sensors für die Einlasstemperatur auf der Systemplatine für einen bestimmten Zeitraum erfasst. Die Datenaufnahme beginnt, wenn das System nach der Auslieferung zum ersten Mal eingeschaltet wird. Die Daten werden für den Zeitraum erfasst und angezeigt, während dessen das System eingeschaltet war. Sie können die überwachte Einlasstemperatur für die vergangenen sieben Jahre verfolgen und speichern.



ANMERKUNG: Sie können den Verlauf der Einlasstemperatur auch für System verfolgen, die nicht frischlufttauglich sind.

Es werden zwei Temperaturbereiche erfasst:

- Warnbereich - besteht aus der Zeitdauer, während derer ein System oberhalb des Sensorwarnschwellenwerts für die Einlasstemperatur betrieben wurde. Das System darf in zwölf Monaten 10% der Zeit im Warnbereich betrieben werden.
- Kritischer Bereich - besteht aus der Zeitdauer, während derer ein System oberhalb des kritischen Sensorwarnschwellenwerts für die Einlasstemperatur betrieben wurde. Das System darf in zwölf Monaten 1% der Zeit im kritischen Bereich betrieben werden, wozu auch die Zeit im Warnbereich zählt.

Die erfassten Daten werden in einer Grafik dargestellt, in der auch die 10%- und die 1%-Schwellenwerte wiedergegeben sind. Die protokollierten Temperaturdaten können nur vor der Auslieferung vom Werk gelöscht werden.

Ein Ereignis wird erzeugt, wenn das System für eine angegebene Betriebsdauer weiterhin oberhalb des Schwellenwerts für die normalerweise unterstützte Temperatur betrieben wird. Wenn die Durchschnittstemperatur während der angegebenen Betriebsdauer größer oder gleich dem Warnschwellenwert ($\geq 8\%$) oder dem kritischen Schwellenwert ($\geq 0,8\%$) liegt, wird ein Ereignis im Lifecycle-Protokoll protokolliert und die entsprechende SNMP-Trap erstellt. Hierzu zählen folgende Ereignisse:

- Warnereignis, wenn die Einlasstemperatur während 8% oder mehr der vergangenen 12 Monate oberhalb des Warnschwellenwertes lag.
- Kritisches Ereignis, wenn die Einlasstemperatur während 10% oder mehr der vergangenen 12 Monate oberhalb des Warnschwellenwertes lag.
- Warnereignis, wenn die Einlasstemperatur während 0,8% oder mehr der vergangenen 12 Monate oberhalb des kritischen Schwellenwertes lag.
- Kritisches Ereignis, wenn die Einlasstemperatur während 1% oder mehr der vergangenen 12 Monate oberhalb des kritischen Schwellenwertes lag.

Sie können den iDRAC auch so konfigurieren, dass weitere kritische Ereignisse erzeugt werden. Weitere Informationen hierzu finden Sie im Abschnitt [Alarmwiederholungseignis einrichten](#).

Temperaturdatenverlauf mit der iDRAC7-Weboberfläche anzeigen

So zeigen Sie den Verlauf der Temperaturdaten an:

1. Gehen Sie in der iDRAC7-Weboberfläche auf **Übersicht** → **Server** → **Leistung / Wärme** → **Temperaturen**. Die **Temperatur**-Seite wird angezeigt.
2. Im Bereich **Verlauf der Systemplatineeinlasstemperatur** wird in einem grafischen Schaubild die gespeicherte Einlasstemperatur (Durchschnitts- und Spitzenwerte) für den letzten Tag, die letzten 30 Tage und das letzte Jahr angezeigt.

Weitere Informationen finden Sie in der *iDRAC7-Online-Hilfe*.



ANMERKUNG: Nach einer Aktualisierung der iDRAC-Firmware oder einem Reset des iDRAC werden manche Temperaturdaten möglicherweise nicht mehr im Schaubild angezeigt.

Temperaturdatenverlauf über RACADM anzeigen

Verwenden Sie den Unterbefehl **inlettemphistory** um den Datenverlauf über RACADM anzuzeigen. Weitere Informationen hierzu finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für den iDRAC7 und CMC).

Bestandsaufnahme für Speichergeräte erstellen und Speichergeräte überwachen

Sie können den Zustand remote überwachen und die Bestandsaufnahme für die folgenden Comprehensive Embedded Management (CEM)-aktivierten Speichergeräte im Managed System über die iDRAC7-Web-Schnittstelle oder über RACADM anzeigen:

- RAID-Controller mit Batterien
- Gehäuse mit Gehäuseverwaltungsmodulen (EMMs), Netzteile, Lüftersonde und Temperatursonde
- Physische Laufwerke
- Virtuelle Laufwerke

WS-MAN zeigt die Informationen für die meisten Speichergeräte jedoch im System an.

iDRAC7 führt Bestands- und Überwachungsaufgaben für die PERC 8-RAID-Controller-Reihe mit den folgenden Modellen aus: H310, H710, H710P und H810. Controller, die kein Comprehensive Embedded Management (CEM) unterstützen, sind Internal Tape Adapters (ITAs) und SAS 6 GB/s HBA.

Es werden auch Informationen zu kürzlich aufgetretenen Speicherereignissen und zur Topologie der Speichergeräte angezeigt.

Für Speicherereignisse werden Warnungen und SNMP-Traps angezeigt. Diese Ereignisse werden im Lifecycle-Protokoll erfasst.

Weitere konzeptionelle Informationen finden Sie im *OpenManage Storage Management User's Guide* (OpenManage Storage Management-Benutzerhandbuch) unter dell.com/support/manuals.

Speichergeräte über die Web-Schnittstelle überwachen

So zeigen Sie die Speichergeräteinformationen über die Web-Schnittstelle an:

- Gehen Sie zu **Übersicht** → **Speicher** → **Zusammenfassung**, um eine Zusammenfassung zu den Speicherkomponenten und den kürzlich protokollierten Ereignissen anzuzeigen. Diese Seite wird automatisch alle 30 Sekunden aktualisiert.
- Gehen Sie zu **Übersicht** → **Speicher** → **Topologie**, um die hierarchisch-physische Ansicht der Aggregation mit den wichtigsten Speicherkomponenten anzuzeigen.
- Gehen Sie zu **Übersicht** → **Speicher** → **Physische Festplatten**, um Informationen zu den physischen Festplatten anzuzeigen. Daraufhin wird die Seite **Physische Festplatten** angezeigt.
- Gehen Sie zu **Übersicht** → **Speicher** → **Virtuelle Festplatten**, um Informationen zu virtuellen Festplatten anzuzeigen. Daraufhin wird die Seite **Virtuelle Festplatten** angezeigt.
- Gehen Sie zu **Übersicht** → **Speicher** → **Controller**, um Informationen zu den RAID-Controllern anzuzeigen. Daraufhin wird die Seite **Controller** angezeigt.
- Gehen Sie zu **Übersicht** → **Speicher** → **Gehäuse**, um Informationen zu den Gehäusen anzuzeigen. Daraufhin wird die Seite **Gehäuse** angezeigt.

Sie können Filter verwenden, um spezifische Geräteinformationen anzuzeigen.

Weitere Informationen zu den angezeigten Eigenschaften und zur Verwendung der Filteroptionen finden Sie in der *iDRAC7-Online-Hilfe*.

Speichergerät über RACADM überwachen

Um die Speichergeräteinformationen anzuzeigen, verwenden Sie den Befehl **raid**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Bestandsaufnahme für Netzwerkgeräte erstellen und Netzwerkgeräte überwachen

Sie können den Zustand remote überwachen und die Bestandsaufnahme für die folgenden Netzwerkgeräte im Managed System anzeigen:


- Netzwerkadapter (NICs)
- Konvergente Netzwerkadapter (CNAs)
- LAN auf Hauptplatinen (LOMs)
- Netzwerktochterkarten (NDCs)
- Mezzanine-Karten (nur für Blade-Server)

Für jedes Gerät können Sie die folgenden Informationen zu den Schnittstellen und unterstützten Partitionen abrufen:

- Link-Status
- Eigenschaften
- Einstellungen und Funktionen
- Empfangs- und Übertragungsstatistiken

Netzwerkgeräte über die Web-Schnittstelle überwachen

Um die Netzwerkgeräteinformationen über die Web-Schnittstelle anzuzeigen, gehen Sie zu **Übersicht** → **Hardware** → **Netzwerkgeräte**. Daraufhin wird die Seite **Netzwerkgeräte** angezeigt. Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der *iDRAC7-Online-Hilfe*.

 **ANMERKUNG:** Wenn der **BS-Treiberzustand** den Status als „Betriebsbereit“ darstellt, werden der Betriebssystem-Treiberstatus oder der UEFI-Treiberstatus angezeigt.

Netzwerkgeräte über RACADM überwachen

Um die Netzwerkgeräteinformationen anzuzeigen, verwenden Sie die Befehle **hwinventory** und **nicstatistics**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Zusätzliche Eigenschaften werden möglicherweise angezeigt, wenn Sie RACADM oder WS-MAN neben den auf der iDRAC7-Web-Schnittstelle angezeigten Eigenschaften verwenden.

Bestandsaufnahme und Überwachung von FC-HBA-Geräten

Sie können den Funktionszustand und die Bestandsaufnahme der Fibre Channel Host Bus Adapter- (FC HBA) Geräte im Managed System anzeigen. Die FC HBAs von Emulex und QLogic (außer FC8) werden unterstützt. Für jedes FC-HBA-Gerät können Sie die folgenden Informationen zu den Ports anzeigen lassen.

- Linkstatus und Information
- Schnittstellen-Eigenschaften
- Empfangs- und Übertragungsstatistiken

FC-HBA-Geräte mit der Web-Schnittstelle überwachen

Um die FC-HBA-Geräteinformationen mit der Web-Schnittstelle überwachen zu können, gehen Sie zu **Übersicht** → **Hardware** → **Fibre-Channel**. Die Seite FC wird angezeigt. Für mehr Informationen zu den angezeigten Eigenschaften siehe *iDRAC7 Online-Hilfe*.

Im Seitennamen werden auch die Steckplatznummer, die angibt, wo das FC-HBA-Gerät verfügbar ist, und der Typ des FC-HBA-Geräts angezeigt.

Überwachung von FC-HBA-Geräten unter Verwendung von RACADM

Um die FC-HBA-Geräteinformationen mit RACADM anzuzeigen, verwenden Sie den Unterbefehl **hwinventory**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Verbindungen der FlexAddress-Mezzanine-Kartenarchitektur anzeigen

In Blade Servern ermöglicht FlexAddress die Verwendung von beständigen, dem Gehäuse zugewiesenen World-Wide-Namen und MAC-Adressen (WWN/MAC) für jede verwaltete Server-Anschlussverbindung.

Sie können die folgenden Informationen für jede installierte eingebettete Ethernet- und optionalen Mezzanine-Kartenschnittstelle anzeigen:

- Strukturen, mit denen die Karten verbunden sind
- Strukturtyp
- MAC-Adressen, die Servern, Gehäusen oder remote zugewiesen sind

Um Flex-Adressinformationen in iDRAC7 anzuzeigen, konfigurieren und aktivieren Sie die Flex-Adress-Funktion über den Chassis Management Controller (CMC). Weitere Informationen finden Sie im *Dell Chassis Management Controller User Guide* (Dell Chassis Management Controller-Benutzerhandbuch) unter dell.com/support/manuals. Alle aktiven Sitzungen für die virtuelle Konsole oder virtuellen Datenträger werden beendet, wenn die FlexAddress-Einstellung aktiviert oder deaktiviert ist.



ANMERKUNG: Um Fehler zu vermeiden, die zu einer Stromunterversorgung auf dem verwalteten System führen können, *muss* der richtige Mezzanine-Kartentyp für jede Anschluss- und Architekturverbindung installiert sein.

Die FlexAddress-Funktion ersetzt die Server-zugewiesenen MAC-Adressen durch Gehäuse-zugewiesene MAC-Adressen und wird für den iDRAC7 zusammen mit Blade-LOMs, Mezzanine-Karten und E/A-Modulen eingesetzt. Die Funktion FlexAddress des iDRAC unterstützt die Bewahrung der steckplatzspezifischen MAC-Adressen für iDRACs in einem Gehäuse. Die Gehäuse-zugewiesene MAC-Adresse wird im permanenten CMC-Speicher abgelegt und bei einem iDRAC7-Start oder einer Aktivierung der CMC-FlexAddress an den iDRAC7 gesendet.

Wenn CMC Gehäusen zugewiesene MAC-Adressen aktiviert, zeigt iDRAC7 die **MAC-Adresse** auf den folgenden Seiten an:

- **Übersicht** → **Server** → **Einstellungen Details** → **iDRAC Information**.
- **Übersicht** → **Server** → **Einstellungen WWN/MAC**.
- **Overview** → **iDRAC Settings** → **Properties iDRAC Information** → **Current Network Settings**.

- **Übersicht** → **iDRAC Einstellungen** → **Netzwerk Netzwerk** → **Netzwerk Einstellungen**.

△ **VORSICHT:** Wenn Sie bei aktivierter FlexAddress zwischen Server-zugewiesener MAC-Adresse und Gehäuse-zugewiesener MAC-Adresse umschalten oder umgekehrt, ändert sich auch die iDRAC7-IP-Adresse.

iDRAC7-Sitzungen anzeigen oder beenden

Sie können die Anzahl der Benutzer anzeigen, die derzeit bei iDRAC7 angemeldet sind, und die Benutzersitzungen beenden.

iDRAC7-Sitzungen über die Web-Schnittstelle beenden

Benutzer ohne Administratorberechtigungen benötigen eine Berechtigung zum Konfigurieren von iDRAC7, um iDRAC7-Sitzungen über die iDRAC7-Web-Schnittstelle beenden zu können.

So zeigen Sie die iDRAC7-Sitzungen an und beenden sie:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Sitzungen**.
Daraufhin werden auf der Seite **Sitzungen** die Sitzungs-ID, der Benutzername, die IP-Adresse und der Sitzungstyp angezeigt. Weitere Informationen zu diesen Eigenschaften finden Sie in der *iDRAC7-Online-Hilfe*.
2. Klicken Sie zum Beenden der Sitzung in der Spalte **Beenden** auf das Papierkorbsymbol für eine Sitzung.

iDRAC7-Sitzungen über RACADM beenden

Sie benötigen Administratorberechtigungen, um iDRAC7-Sitzungen über RACADM beenden zu können.

Verwenden Sie zum Anzeigen der aktuellen Benutzersitzungen den Befehl **getssninfo**.

Verwenden Sie zum Beenden einer Benutzersitzung den Befehl **closesessn**.

Weitere Informationen zu diesen Befehlen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

iDRAC7-Kommunikation einrichten

Sie können über eine der folgenden Modi mit iDRAC7 kommunizieren:

- iDRAC7-Web-Schnittstelle
- Serielle Verbindung mithilfe eines DB9-Kabels (serielle RAC-Verbindung oder serielle IPMI-Verbindung) – nur für Rack- und Tower-Server
- Serielle IPMI-Verbindung über LAN
- IPMI über LAN
- Remote-RACADM
- Lokaler RACADM
- Remote-Dienste

Eine Übersicht über die unterstützten Protokolle und Befehle sowie die jeweiligen Voraussetzungen finden Sie in der folgenden Tabelle.

Tabelle 10. Kommunikationsmodi – Übersicht

Kommunikationsmodus	Unterstütztes Protokoll	Unterstützte Befehle	Voraussetzung
iDRAC7-Web-Schnittstelle	Internet-Protokolle (https)	-	Webserver
Serielle Verbindung über Null-Modem-DB9-Kabel	Protokoll für serielle Verbindung	RACADM SMCLP IPMI	Teil der iDRAC7-Firmware Serielle RAC- oder IPMI-Verbindungen sind aktiviert.
Serielle IPMI-Verbindung über LAN	Intelligent Platform Management Bus-Protokoll SSH Telnet	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.
SMCLP	SSH Telnet	SMCLP	SSH oder Telnet auf iDRAC7 sind aktiviert.
Remote-RACADM	HTTPS	Remote-RACADM	Remote-RACADM ist installiert und aktiviert.
Firmware RACADM	SSH Telnet	Firmware RACADM	Firmware-RACADM ist installiert und aktiviert.
Lokaler RACADM	IPMI	Lokaler RACADM	Lokaler RACADM ist installiert.
Remote-Dienste [1]	WS-MAN	WinRM (Windows) OpenWSMAN (Linux)	WinRM ist installiert (Windows), oder OpenWSMAN ist installiert (Linux).

Kommunikationsmodus	Unterstütztes Protokoll	Unterstützte Befehle	Voraussetzung
---------------------	-------------------------	----------------------	---------------

[1] Weitere Informationen finden Sie im *Lifecycle Controller Remote Services User's Guide* (Dell Lifecycle Controller Remote Services-Benutzerhandbuch) unter dell.com/support/manuals.

Verwandte Links

- [Mit iDRAC7 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 iDRAC7 über IPMI SOL kommunizieren](#)
- [Mit iDRAC7 mithilfe von IPMI über LAN kommunizieren](#)
- [Remote-RACADM aktivieren oder deaktivieren](#)
- [Lokalen RACADM deaktivieren](#)
- [IPMI auf Managed System aktivieren](#)
- [Linux während des Starts für die serielle Konsole konfigurieren](#)
- [Unterstützte SSH-Verschlüsselungsschemas](#)

Mit iDRAC7 über eine serielle Verbindung über ein DB9-Kabel kommunizieren

Sie können jede der folgenden Kommunikationsmethoden verwenden, um Systemverwaltungsaufgaben über eine serielle Verbindung auf den Rack- und Tower-Servern durchzuführen:

- Serielle RAC-Verbindung
- Serielle IPMI-Verbindung – Grundlegender Modus „Direktverbindung“ und Terminalmodus „Direktverbindung“



ANMERKUNG: Bei Blade-Servern wird die serielle Verbindung über das Gehäuse aufgebaut. Weitere Informationen finden Sie im *Chassis Management Controller User's Guide* (Chassis Management Controller-Benutzerhandbuch) unter dell.com/support/manuals.

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.
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, an welcher Stelle des Startvorgangs sich das verwaltete System derzeit befindet, wird entweder der POST-Bildschirm oder der Betriebssystembildschirm angezeigt. Die Anzeige richtet sich nach der Konfiguration: SAC für Windows und Linux-Textmodusbildschirme für Linux.


4. Aktivieren Sie serielle RAC- oder IPMI-Verbindungen auf iDRAC7.

Verwandte Links

- [BIOS für serielle Verbindung konfigurieren](#)
- [Serielle RAC-Verbindung aktivieren](#)
- [Grundlegenden seriellen IPMI-Verbindungs- und -Terminalmodus aktivieren](#)

BIOS für serielle Verbindung konfigurieren


So konfigurieren Sie das BIOS für serielle Verbindungen:

 **ANMERKUNG:** Dies gilt nur für iDRAC7 auf Rack- und Tower-Servern.

1. Schalten Sie das System ein oder starten Sie es neu.
2. Drücken Sie <F2>.
3. Gehen Sie zu **System-BIOS-Einstellungen** → **Serielle Kommunikation**.
4. Wählen Sie **Externer serieller Konnektor** auf **Remote-Zugriffsggerät** aus.
5. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
6. Drücken Sie auf die Esc-Taste, um das **System-Setup**-Programm zu beenden.

Serielle RAC-Verbindung aktivieren

Nach der Konfiguration der seriellen Verbindung im BIOS aktivieren Sie die serielle RAC-Verbindung in iDRAC7.

 **ANMERKUNG:** Dies gilt nur für iDRAC7 auf Rack- und Tower-Servern.

Serielle RAC-Verbindungen über die Web-Schnittstelle aktivieren

So aktivieren Sie die serielle RAC-Verbindung:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Serielle Verbindung**.
Die Seite **Seriell** 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 IPMI-Einstellungen konfiguriert.


Serielle RAC-Verbindung über RACADM aktivieren

Um die serielle RAC-Verbindung über RACADM zu aktivieren, nutzen Sie eine der folgenden Optionen:

- Verwenden Sie die Objekte in der Gruppe **cfgSerial** mit dem Befehl **config**.
- Verwenden Sie die Objekte in der Gruppe **iDRAC.Serial** mit dem Befehl **set**.

Grundlegenden seriellen IPMI-Verbindungs- und -Terminalmodus aktivieren

Konfigurieren Sie zum Aktivieren der seriellen IPMI-Weiterleitung des BIOS an iDRAC7 die serielle IPMI-Verbindung in den folgenden iDRAC7-Modi:

 **ANMERKUNG:** Dies gilt nur für iDRAC7 auf Rack- und Tower-Servern.

- Grundlegender IPMI-Modus - Unterstützt eine binäre Schnittstelle für Programmzugriff, z. B. die IPMI-Shell (ipmish), die zum Lieferumfang des Baseboard-Verwaltungsdienstprogramms (BMU) gehört. Beispiel: Führen Sie zum Ausdrucken des Systemereignisprotokolls mittels ipmish über den grundlegenden IPMI-Modus den folgenden Befehl aus:

```
ipmish -com 1 -baud 57600 -flow cts -u root -p calvin sel get
```
- IPMI-Terminalmodus – Unterstützt ASCII-Befehle, die von einem seriellen Terminal gesendet werden. Dieser Modus unterstützt eine begrenzte Anzahl von Befehlen (einschließlich der Stromsteuerung) und Raw-IPMI-

Befehle, die als hexadezimale ASCII-Zeichen eingegeben werden. Mit dieser Funktion können Sie die Startsequenzen für das Betriebssystem bis zum BIOS anzeigen, wenn Sie sich über SSH oder Telnet bei iDRAC7 anmelden.

Verwandte Links

[BIOS für serielle Verbindung konfigurieren](#)

[Zusätzliche Einstellungen für den seriellen IPMI-Terminalmodus](#)

Serielle Verbindung über die Web-Schnittstelle aktivieren

Stellen Sie sicher, dass Sie die serielle RAC-Schnittstelle für die Aktivierung der seriellen IPMI-Verbindung deaktivieren. So konfigurieren Sie die Einstellungen für die seriellen IPMI-Verbindungen:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Serielle Verbindung**.
2. Legen Sie unter **Serielle IPMI-Verbindung** die Werte für die Attribute fest. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC7-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 Sie dann den IPMI-Modus unter Verwendung einer der folgenden Befehle:

- Verwenden des Befehls **config**:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode <0 oder 1>
```

wobei *0* für den Terminalmodus und *1* für den Basismodus steht.
- Verwenden des Befehls **set**:

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

```
racadm set iDRAC.IPMISerial.ConnectionMode < 0 or 1>
```

wobei *0* für den Terminalmodus und *1* für den Basismodus steht.

Einstellungen für serielle IPMI-Verbindung über RACADM aktivieren

So konfigurieren Sie die Einstellungen für die serielle IPMI-Verbindung mit dem Befehl **set** oder **config**:

1. Ändern Sie den Modus für die serielle IPMI-Verbindung über den folgenden Befehl auf die gewünschte Einstellung:
 - Verwenden des Befehls **config**:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```
 - Verwenden des Befehls **set**:

```
racadm set iDRAC.Serial.Enable 0
```
2. Stellen Sie die IPMI-Seriell-Baudrate ein:
 - Verwenden des Befehls **config**:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <Baudrate>
```
 - Verwenden des Befehls **set**:

```
racadm set iDRAC.IPMISerial.BaudRate <Baudrate>
```wobei *<Baudrate>* 9600, 19200, 57600 oder 115200 Bits pro Sekunde ist.
3. Aktivieren Sie die Hardware-Datenflusssteuerung auf der seriellen IPMI:
 - Verwenden des Befehls **config**:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1
```
 - Verwenden des Befehls **set**:

```
racadm set iDRAC.IPMISerial.FlowControl 1
```

4. Stellen Sie die Mindestberechtigungsebene auf dem seriellen IPMI-Kanal ein:
 - Verwenden des Befehls **config**: `racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <Level>`
 - Verwenden des Befehls **set**: `racadm set iDRAC.IPMISerial.ChanPrivLimit <Level>`

wobei <Level> 2 (Benutzer), 3 (Operator), oder 4 (Administrator) ist.

5. Stellen Sie sicher, dass der serielle MUX (externer serieller Konnektor) über das BIOS-Setup-Programm ordnungsgemäß für das Remote-Zugriffsggerät eingestellt ist, um das BIOS für die serielle Verbindung zu konfigurieren.

Weitere Informationen über diese Eigenschaften finden Sie in der IPMI 2.0-Spezifikation.

Zusätzliche Einstellungen für den seriellen IPMI-Terminalmodus

In diesem Abschnitt finden Sie zusätzliche Konfigurationseinstellungen für den seriellen IPMI-Terminalmodus.

Zusätzliche Einstellungen für den seriellen IPMI-Terminalmodus über die Web-Schnittstelle konfigurieren

So legen Sie die Terminalmoduseinstellungen fest:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Seriell**. Die Seite **Serial** wird angezeigt.
2. Aktivieren Sie „Serielle IPMI-Verbindung“.
3. Klicken Sie auf **Terminalmoduseinstellungen**. Daraufhin wird die Seite **Terminalmoduseinstellungen** angezeigt.
4. Legen Sie die folgenden Werte fest:
 - Zeilenbearbeitung
 - Löschtesteuerung
 - Echo-Steuerung
 - Handshaking-Steuerung
 - Neue Zeilenreihenfolge
 - Neue Zeilenfolgen eingeben

Weitere Informationen zu diesen Optionen finden Sie in der *iDRAC7-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-Zugriffsggerät eingestellt ist, um das BIOS für die serielle Verbindung zu konfigurieren.

Zusätzliche Einstellungen für den seriellen IPMI-Terminalmodus über RACADM konfigurieren

Um die Einstellungen für den Terminalmodus zu konfigurieren, führen Sie den Befehl: `racadm config cfgIpmiSerial` aus.

Von der seriellen RAC-Verbindung auf die serielle Konsolenverbindung bei Verwendung eines DB9-Kabels umschalten

iDRAC7 unterstützt Escape-Tastensequenzen, mit denen Sie zwischen der seriellen RAC-Schnittstellenkommunikation und der seriellen Konsole auf den Rack- und Tower-Servern umschalten können.

Von der seriellen Konsole auf die serielle RAC-Verbindung umschalten

Um vom Modus der seriellen Konsole auf die serielle RAC-Schnittstellenkommunikation umzuschalten, verwenden Sie die folgende Tastenfolge:

<Esc> +<UMSCH> <9>

Mit der obigen Tastenfolge rufen Sie entweder die iDRAC-Anmeldeaufforderung auf (wenn der iDRAC auf den seriellen RAC-Modus gesetzt ist) oder den seriellen Anschlussmodus, in dem Terminalbefehle abgeben werden können (wenn der iDRAC auf den seriellen IPMI-Terminalmodus bei Direktverbindung eingestellt ist).

Von der seriellen RAC-Verbindung auf die serielle Konsole umschalten

Um vom Modus der seriellen RAC-Schnittstellenkommunikation auf den Modus der seriellen Konsole umzuschalten, verwenden Sie die folgende Tastenfolge:

<Esc> +<UMSCH> <q>

Verwenden Sie im Terminalmodus zum Umschalten der Verbindung zum Modus „Serielle Konsole“:

<Esc> +<UMSCH> <q>

So kehren Sie zum Terminalmodus zurück, wenn Sie über den Modus „Serielle Konsole“ verbunden sind:

<Esc> +<UMSCH> <9>

Mit iDRAC7 über IPMI SOL kommunizieren

Mit der seriellen IPMI über LAN-Verbindung kann die textbasierte Konsole eines Managed System serielle Daten über das dedizierte oder freigegebene bandexterne Ethernet-Verwaltungsnetzwerk von iDRAC7 umleiten. Mit der Verwendung von SOL können Sie Folgendes ausführen:

- 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 iDRAC7 für die Verwendung von SOL.
3. Aktivieren Sie ein unterstütztes Protokoll (SSH, Telnet, IPMItool).

Verwandte Links


[BIOS für serielle Verbindung konfigurieren](#)


[iDRAC7 für die Verwendung von SOL konfigurieren](#)

[Unterstütztes Protokoll aktivieren](#)

BIOS für serielle Verbindung konfigurieren

So konfigurieren Sie das BIOS für serielle Verbindungen:

 **ANMERKUNG:** Dies gilt nur für iDRAC7 auf Rack- und Tower-Server.

1. Schalten Sie das System ein oder starten Sie es neu.
2. Drücken Sie <F2>.
3. Gehen Sie zu **System-BIOS-Einstellungen** → **Serielle Kommunikation**.
4. Legen Sie die folgenden Werte fest:
 - Serielle Kommunikation – Eingeschaltet mit Konsolenumleitung
 - Adresse der seriellen Schnittstelle – COM2
 -  **ANMERKUNG:** Sie können die **serielle Kommunikation** auf **Eingeschaltet mit serieller Umleitung über COM1** einstellen, wenn das **Adressfeld des seriellen Anschlusses, Serielles Gerät2**, auch auf COM1 eingestellt ist.
 - Externer serieller Anschluss - Serielles Gerät2
 - Failsafe-Baud-Rate – 115.200
 - Remote-Terminaltyp... vt100/vt220
 - Umleitung nach Start – Aktiviert
5. Klicken Sie auf **Zurück** und dann auf **Fertigstellen**.
6. Klicken Sie auf **Ja**, um die Änderungen zu speichern.
7. Drücken Sie auf die Esc-Taste, um das **System-Setup**-Programm zu beenden.

iDRAC7 für die Verwendung von SOL konfigurieren

Sie können die SOL-Einstellungen in iDRAC7 über die Web-Schnittstelle, über RACADM oder über das Dienstprogramm für die iDRAC-Einstellungen festlegen.

iDRAC7 für die Verwendung von SOL über die iDRAC7-Web-Schnittstelle konfigurieren

Um IPMI Seriell über LAN (SOL) zu konfigurieren:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle nach **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Serielle Verbindung 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 Einstellungen für IPMI SOL sind damit konfiguriert. Diese Werte unterstützen Sie bei der Verbesserung der Leistung.
Weitere Informationen zu diesen Optionen finden Sie in der *iDRAC7-Online-Hilfe*.


iDRAC7 für die Verwendung von SOL unter Verwendung von RACADM konfigurieren

Um IPMI Seriell über LAN (SOL) zu konfigurieren:

1. IPMI-Seriell-Über-LAN aktivieren:
 - Verwenden des Befehls **config**: `racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1`
 - Verwenden des Befehls **set**: `racadm set iDRAC.IPMISol.Enable 1`
2. Aktualisieren Sie die IPMI-SOL-Mindestberechtigungsebene:

- Verwenden des Befehls **config**: `racadm config -g cfgIpmiSol o cfgIpmiSolMinPrivilege <Ebene>`
- Verwenden des Befehls **set**: `racadm set iDRAC.IPMSol.MinPrivilege 1`


wobei <Ebene> 2 (Benutzer), 3 (Operator), 4 (Administrator) ist.

 **ANMERKUNG:** Die Mindestberechtigungsebene für IPMI SOL bestimmt die Mindestberechtigung für die Aktivierung von IPMI SOL. Weitere Informationen finden Sie in den technischen Daten zu IPMI 2.0.

3. Aktualisieren Sie die IPMI-SOL-Baudrate:

- Verwenden des Befehls **config**: `racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <Baudrate>`
- Verwenden des Befehls **set**: `racadm set iDRAC.IPMSol.BaudRate <Baudrate>`


wobei <Baudrate> 9600, 19200, 57600 oder 115200 Bits pro Sekunde ist.

 **ANMERKUNG:** Um die serielle Konsole über LAN umzuleiten, stellen Sie sicher, dass die SOL-Baudrate mit der Baudrate des verwalteten Systems übereinstimmt.

4. Aktivieren Sie SOL für jeden Benutzer:

- Verwenden des Befehls **config**: `racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <ID> 2`
- Verwenden des Befehls **set**: `racadm set iDRAC.Users.<ID>.SolEnable 2`

wobei <ID> die eindeutige Benutzer-ID ist.

 **ANMERKUNG:** Um die serielle Konsole über LAN umzuleiten, stellen Sie sicher, dass die SOL-Baudrate mit der Baudrate des verwalteten Systems übereinstimmt.

Unterstütztes Protokoll aktivieren

Die unterstützten Protokolle sind IPMI, SSH und Telnet.

Unterstütztes Protokoll über die Web-Schnittstelle aktivieren

Um SSH oder Telnet zu aktivieren, gehen Sie zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Dienste**, und wählen Sie die Option **Aktiviert** für SSH oder Telnet aus.

Gehen Sie zum Aktivieren von IPMI zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk**, und wählen Sie **IPMI über LAN aktivieren** aus. Stellen Sie außerdem sicher, dass der Wert für den **Verschlüsselungsschlüssel** vollständig aus Nullen besteht, oder drücken Sie auf die Rückschritttaste, um den Wert so zu ändern, dass er ausschließlich Nullen enthält.

Unterstütztes Protokoll über RACADM aktivieren

Führen Sie zum Aktivieren von SSH oder Telnet den folgenden Befehl aus:

- Telnet:
 - Verwenden des Befehls **config**: `racadm config -g cfgSerial -o cfgSerialTelnetEnable 1`
 - Verwenden des Befehls **set**: `racadm set iDRAC.Telnet.Enable 1`
- SSH:
 - Verwenden des Befehls **config**: `racadm config -g cfgSerial -o cfgSerialSshEnable 1`
 - Verwenden des Befehls **set**: `racadm set iDRAC.SSH.Enable 1`

Geben Sie zum Ändern des SSH-Anschlusses Folgendes ein:

- Verwenden des Befehls **config**: `racadm config -g cfgRacTuning -o cfgRacTuneSshPort <Portnummer>`
- Verwenden des Befehls **set**: `racadm set iDRAC.SSH.Port <Portnummer>`

Sie können u. a. die folgenden Tools verwenden:

- IPMItool zur Verwendung des IPMI-Protokolls
- Putty/OpenSSH zur Verwendung der SSH- oder Telnet-Protokolle

Verwandte Links

[SOL über das IPMI-Protokoll](#)

[SOL unter Verwendung der SSH- oder Telnet-Protokolle](#)

SOL über das IPMI-Protokoll

IPMItool <--> LAN/WAN-Verbindung <--> iDRAC7

Das IPMI-basierte SOL-Dienstprogramm, IPMItool, verwendet RMCP+, das unter Verwendung von UDP-Datengrammen an Anschluss 623 geliefert wird. RMCP+ bietet verbesserte Authentifizierung, Datenintegritätsprüfungen und Verschlüsselung sowie die Fähigkeit, verschiedene Arten von Nutzlasten zu tragen. 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 Zeichenkette mit 40 Nullen.

Eine RMCP+-Verbindung zu iDRAC7 muss über den Verschlüsselungsschlüssel (Schlüsselgenerator-Schlüssel) verschlüsselt werden. Sie können den Verschlüsselungsschlüssel über die iDRAC7-Web-Schnittstelle oder das Dienstprogramm für die iDRAC-Einstellungen konfigurieren.

So starten Sie eine SOL-Sitzung mithilfe von IPMItool von einer Management Station aus:

 **ANMERKUNG:** Falls erforderlich, können Sie die Standard-SOL-Zeitüberschreitung unter **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Dienste** ändern.

1. Installieren Sie IPMITool über die *Dell Systems Management Tools and Documentation-DVD*. Weitere Anweisungen finden Sie im *Software-Schnellinstallationshandbuch*.
2. Führen Sie über die Befehlseingabe (Windows oder Linux) den folgenden Befehl zum Starten von SOL über iDRAC7 aus: `ipmitool -H <iDRAC7-IP-Adresse> -I lanplus -U <Anmeldename> -P <Anmeldekennwort> sol activate`
Mit diesem Befehl wird eine Verbindung von der Management Station zur seriellen Schnittstelle des Managed System hergestellt.
3. Drücken Sie zum Beenden einer SOL-Sitzung über IPMItool nacheinander auf <~> und <.>. Daraufhin wird die SOL-Sitzung geschlossen.


 **ANMERKUNG:** Wenn sich eine SOL-Sitzung nicht beenden lässt, setzen Sie iDRAC7 zurück, und warten Sie etwa zwei Minuten, bis der Startvorgang vollständig abgeschlossen ist.

SOL unter Verwendung der SSH- oder Telnet-Protokolle

Secure Shell (SSH) sind Netzwerkprotokolle, die zum Ausführen der Kommunikation über Befehlszeilen mit iDRAC7 verwendet werden. Sie können Remote-RACADM- und SMCLP-Befehle über eine dieser Schnittstellen parsen.

SSH bietet im Vergleich zu Telnet die größere Sicherheit. iDRAC7 unterstützt nur die SSH-Version 2 mit Kennwortauthentifizierung. Diese Funktion ist standardmäßig aktiviert. iDRAC7 unterstützt bis zu zwei SSH-Sitzungen und zwei Telnet-Sitzungen gleichzeitig. Aus Sicherheitsgründen wird empfohlen, SSH zu verwenden, da es sich bei Telnet nicht um ein sicheres Protokoll handelt. Sie müssen Telnet nur dann verwenden, wenn Sie den SSH-Client nicht installieren können oder davon ausgehen, dass Ihre Netzwerkinfrastruktur sicher ist.

Verwenden Sie Open Source-Programme, wie z. B. PuTTY oder OpenSSH, die SSH- und Telnet-Netzwerkprotokolle auf einer Management Station für die Verbindungsaufnahme mit iDRAC7 unterstützen.

 **ANMERKUNG:** Führen Sie OpenSSH über einen VT100- oder ANSI-Terminalemulator auf Windows aus. Wenn Sie OpenSSH an der Windows-Befehlseingabe ausführen, können Sie nicht auf den vollen Funktionsumfang zugreifen (einige Tasten reagieren nicht, und einige Grafiken werden nicht angezeigt).

Bevor Sie SSH oder Telnet für die Kommunikation mit iDRAC7 verwenden, müssen Sie die folgenden Schritte ausführen:

1. BIOS für die Aktivierung der seriellen Konsole konfigurieren
2. SOL in iDRAC7 konfigurieren
3. SSH oder Telnet über die iDRAC7-Web-Schnittstelle oder RACADM aktivieren
Client für Telnet (Schnittstelle 23)/SSH (Schnittstelle 22) <--> WAN-Verbindung <--> iDRAC7

Durch das IPMI-basierte SOL, das das SSH- oder Telnet-Protokoll verwendet, erübrigt sich der Bedarf an einem zusätzlichen Dienstprogramm, da die Seriell-auf-Netzwerk-Umsetzung innerhalb von iDRAC7 erfolgt. Die von Ihnen verwendete SSH- oder Telnet-Konsole muss in der Lage sein, die von der seriellen Schnittstelle des verwalteten Systems eingehenden Daten zu interpretieren und zu beantworten. Die serielle Schnittstelle hängt sich in der Regel an eine Shell, die ein ANSI- oder VT100/VT220-Terminal simuliert. Die serielle Konsole wird automatisch auf die SSH- oder Telnet-Konsole umgeleitet.

Verwandte Links

[SOL über PuTTY auf Windows verwenden](#)


[SOL über OpenSSH oder Telnet auf Linux verwenden](#)

SOL über PuTTY auf Windows verwenden

So starten Sie IPMI SOL über PuTTY auf einer Windows-Management Station:

 **ANMERKUNG:** Falls erforderlich, können Sie die Standardeinstellung für Zeitüberschreitungen für SSH oder Telnet über **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Dienste** ändern.

1. Führen Sie für die Verbindungsaufnahme zu iDRAC7 den folgenden Befehl aus: `putty.exe [-ssh | -telnet] <Anmeldename>@<iDRAC7-IP-Adresse> <Schnittstellename>`

 **ANMERKUNG:** Die Angabe der Schnittstellenummer ist optional. Sie wird nur dann benötigt, wenn die Schnittstellenummer neu zugewiesen wird.

2. Führen Sie den Befehl `console com2` oder den Befehl `connect` aus, um SOL zu starten und das verwaltete System zu starten.

Es wird eine SOL-Sitzung von der Management Station zum verwalteten System unter Verwendung des SSH- oder des Telnet-Protokolls geöffnet. Folgen Sie zum Aufrufen der iDRAC7-Befehlszeilenkonsole der ESC-Tastensequenz. Verhaltensweisen von PuTTY und SOL-Verbindungen:

- Während Sie im Rahmen des POST auf das verwaltete System zugreifen, falls die Funktionstasten und Keypad-Option unter PuTTY wie folgt eingestellt sind:
 - * VT100+ – F2 erfolgreich, F12 nicht erfolgreich
 - * ESC[n~ – F12 erfolgreich, F2 jedoch nicht erfolgreich
- Wenn unter Windows die Emergency Management System (EMS)-Konsole unmittelbar nach dem Neustart eines Hosts geöffnet wird, wird das Special Admin Console (SAC)-Terminal möglicherweise beschädigt. Beenden Sie die SOL-Sitzung, schließen Sie das Terminal, öffnen Sie ein anderes Terminal, und starten Sie die SOL-Sitzung über den gleichen Befehl.

Verwandte Links


[Verbindung zur SOL-Sitzung in der iDRAC7-Befehlszeilenkonsole abbrechen](#)

SOL über OpenSSH oder Telnet auf Linux verwenden

So verwenden Sie SOL über OpenSSH oder Telnet auf einer Linux-Management Station:


 **ANMERKUNG:** Falls erforderlich, können Sie die Standardzeitüberschreitung für SSH- oder Telnet-Sitzungen unter **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Dienste** ändern.

1. Starten Sie eine Shell.
2. Stellen Sie eine Verbindung zu iDRAC7 über den folgenden Befehl her:
 - SSH: `ssh <iDRAC7-IP-Adresse>-l <Anmeldename>`
 - Telnet: `telnet <iDRAC7-IP-Adresse>`

 **ANMERKUNG:** Wenn Sie die Standardanschlussnummer für den Telnet-Dienst (Anschluss 23) geändert haben, fügen Sie die Anschlussnummer am Ende des Telnet-Befehls hinzu.

3. Geben Sie zum Starten von SOL an der Befehlseingabeaufforderung einen der folgenden Befehle ein:
 - `connect`
 - `console com2`

Mit diesen Befehlen wird iDRAC7 mit der SOL-Schnittstelle des verwalteten Systems verbunden. Sobald eine SOL-Sitzung aufgebaut wurde, steht die iDRAC7-Befehlszeilenkonsole nicht mehr zur Verfügung. Führen Sie die Escape-Sequenz ordnungsgemäß aus, um die iDRAC7-Befehlszeilenkonsole zu öffnen. Die Escape-Sequenz wird außerdem auf dem Bildschirm angezeigt, sobald eine SOL-Sitzung aufgebaut wurde. Wenn das verwaltete System ausgeschaltet ist, kann der Aufbau der SOL-Sitzung einen Moment dauern.

 **ANMERKUNG:** Sie können entweder Konsole com1 oder Konsole com2 verwenden, um SOL zu starten. Starten Sie den Server neu, um die Verbindung herzustellen.

Der Befehl `console -h com2` zeigt den Inhalt des seriellen Verlaufspuffers an, bevor er auf Eingaben über die Tastatur oder neue Zeichen vom seriellen Anschluss wartet.

Die Standard- (und gleichzeitig Maximal-) -Größe des Verlaufspuffers beträgt 8.192 Zeichen. Sie können diese Zahl über den folgenden Befehl auf einen geringeren Wert herabsetzen:

```
racadm config -g cfgSerial -o cfgSerialHistorySize <Zahl>
```

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

Verwandte Links

[Virtuelle Telnet-Konsole verwenden](#)

[Die Rücktaste für die Telnet-Sitzung konfigurieren](#)

[Verbindung zur SOL-Sitzung in der iDRAC7-Befehlszeilenkonsole abbrechen](#)

Virtuelle Telnet-Konsole verwenden

Einige Telnet-Clients auf Microsoft-Betriebssystemen zeigen den BIOS-Setup-Bildschirm eventuell nicht richtig an, wenn die virtuelle BIOS-Konsole auf die VT100/VT220-Emulation eingestellt ist. Wenn dieses Problem auftritt, können Sie die Anzeige aktualisieren, indem Sie die BIOS-Konsolenumleitung auf ANSI-Modus ändern. Um dieses Verfahren im BIOS-Setup-Menü auszuführen, wählen Sie **Virtuelle Konsole** → **Remote-Terminaltyp** → **ANSI** aus.

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.

So verwenden Sie virtuelle Telnet-Konsole:

1. Aktivieren Sie **Telnet** in den **Windows-Komponentendiensten**.
2. Stellen Sie eine Verbindung zu iDRAC7 über den folgenden Befehl her: `telnet <IP-Adresse>:<Schnittstellennummer>`, wobei `IP-Adresse` für die IP-Adresse des iDRAC7 und

Schnittstellenummer für die Telnet-Schnittstellenummer steht (wenn Sie eine neue Schnittstelle verwenden).

Die Rücktaste für die Telnet-Sitzung konfigurieren

Je nach verwendetem Telnet-Client kann die Verwendung der Rücktaste zu unerwarteten Ergebnissen führen. Die Sitzung kann beispielsweise ein `^h`-Echo verursachen. Die meisten Microsoft- und Linux-Telnet-Clients können jedoch für die Verwendung der Rücktaste konfiguriert werden.

Um eine Linux Telnet-Sitzung für die Verwendung der Rückschritttaste zu konfigurieren, öffnen Sie eine Befehlseingabe, und geben Sie den Befehl `stty erase ^h` ein. Geben Sie an der Eingabeaufforderung den Befehl `telnet` ein.

So konfigurieren Sie Microsoft-Telnet-Clients zur Verwendung der Rücktaste:

1. Öffnen Sie ein Eingabeaufforderungsfenster (falls erforderlich).
2. Wenn Sie keine Telnet-Sitzung ausführen, geben Sie `telnet` ein. Wenn Sie hingegen eine Telnet-Sitzung ausführen, drücken Sie auf die Tastenkombination `<Strg><]>`.
3. Geben Sie an der Eingabeaufforderung den Befehl `set bsasdel` ein.
Daraufhin wird die Meldung `Rückschritttaste wird als Löschen gesendet` angezeigt.

Verbindung zur SOL-Sitzung in der iDRAC7-Befehlszeilenkonsole abbrechen

Die Befehle zum Trennen einer SOL-Sitzung basieren auf dem Dienstprogramm. 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 iDRAC7-Befehlszeilenkonsole.

- Drücken Sie zum Beenden einer SOL-Umleitung auf die `<Eingabetaste>`, dann auf `<Esc>` und schließlich auf `<␣>`. Daraufhin werden die SOL-Sitzungen geschlossen.
- Um eine SOL-Sitzung über Telnet auf Linux zu beenden, halten Sie die Tastenkombination `<Strg>+]` gedrückt. Daraufhin wird die Telnet-Befehlseingabe angezeigt. Geben Sie `quit` ein, um Telnet zu beenden.
- Wenn eine SOL-Sitzung im Dienstprogramm nicht vollständig beendet wurde, sind andere SOL-Sitzungen möglicherweise nicht verfügbar. Um dieses Problem zu lösen, beenden Sie die Befehlszeilenkonsole in der Web-Schnittstelle unter **Übersicht** → **iDRAC-Einstellungen** → **Sitzungen**.

Mit iDRAC7 mithilfe von IPMI über LAN kommunizieren

Sie müssen IPMI über LAN für iDRAC7 konfigurieren, um IPMI-Befehle über LAN-Kanäle auf beliebigen externen Systemen zu aktivieren oder zu deaktivieren. Wenn die Konfiguration nicht abgeschlossen ist, können die externen Systeme nicht über die IPMI-Befehle mit dem iDRAC7-Server kommunizieren.

IPMI über LAN über die Web-Schnittstelle konfigurieren

So konfigurieren Sie IPMI über LAN:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk**. Die Seite **Netzwerk** wird angezeigt.
2. Geben Sie unter **IPMI-Einstellungen** die Attributwerte an, und klicken Sie dann auf **Anwenden**. Weitere Informationen zu diesen Optionen finden Sie in der *iDRAC7-Online-Hilfe*. Die IPMI über LAN-Einstellungen werden konfiguriert.

IPMI über LAN über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren


So konfigurieren Sie IPMI über LAN:

1. Gehen Sie im **Dienstprogramm für die iDRAC-Einstellungen** zu **Netzwerk**.
Die Seite **iDRAC-Netzwerkeinstellungen** wird angezeigt.
2. Geben Sie die erforderlichen Werte für die **IPMI-Einstellungen** ein.
Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
Die IPMI über LAN-Einstellungen werden konfiguriert.

IPMI über LAN mithilfe von RACADM konfigurieren


So konfigurieren Sie IPMI über LAN mit dem Befehl **set** oder **config**:

1. IPMI-Über-LAN aktivieren:
 - Verwenden des Befehls **config**: `racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1`
 - Verwenden des Befehls **set**: `racadm set iDRAC.Racadm.Enable 1`

 **ANMERKUNG:** Diese Einstellung bestimmt die IPMI-Befehle, die von der IPMI-über-LAN-Schnittstelle ausgeführt werden können. Weitere Informationen finden Sie in den IPMI 2.0-Angaben unter intel.com.
2. Aktualisieren Sie die IPMI-Kanalberechtigungen:
 - Verwenden des Befehls **config**: `racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <level>`
 - Verwenden des Befehls **set**: `racadm set iDRAC.IPMILan.PrivLimit <level>`

<level> steht für eines der folgenden Elemente: 2 (Benutzer), 3 (Operator) oder 4 (Administrator)
3. Stellen Sie den IPMI-LAN-Kanalverschlüsselungsschlüssel ein, falls erforderlich:
 - Verwenden des Befehls **config**: `racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <Schlüssel>`
 - Verwenden des Befehls **set**: `racadm set iDRAC.IPMILan.EncryptionKey <Schlüssel>`

wobei <Schlüssel> ein aus 20 Zeichen bestehender Verschlüsselungsschlüssel in einem gültigen Hexadezimalformat ist.

 **ANMERKUNG:** Die iDRAC7-IPMI unterstützt das RMCP+-Protokoll. Weitere Informationen finden Sie in den IPMI 2.0-Angaben unter intel.com.

Remote-RACADM aktivieren oder deaktivieren

Sie können Remote-RACADM über die iDRAC7-Web-Schnittstelle oder RACADM aktivieren oder deaktivieren. Sie können bis zu fünf Remote-RACADM-Sitzungen gleichzeitig ausführen.

Remote-RACADM über die Web-Schnittstelle aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie Remote-RACADM:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Dienste**.
Die Seite **Dienste** wird angezeigt.
2. Wählen Sie unter **Remote-RACADM** die Option **Aktiviert** oder die Option **Deaktiviert** aus.
3. Klicken Sie auf **Anwenden**.

Entsprechend Ihrer Auswahl ist Remote-RACADM damit aktiviert oder deaktiviert.


Remote-RACADM über RACADM aktivieren oder deaktivieren

Die RACADM-Remotefähigkeit ist standardmäßig aktiviert. Wenn Sie deaktiviert ist, geben Sie einen der folgenden Befehle ein:

- Verwenden des Befehls **config**: `racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 1`
- Verwenden des Befehls **set**: `racadm set iDRAC.Racadm.Enable 1`

Um die Remotefähigkeit zu deaktivieren, geben Sie einen der folgenden Befehle ein:

- Verwenden des Befehls **config**: `racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0`
- Verwenden des Befehls **set**: `racadm set iDRAC.Racadm.Enable 0`

 **ANMERKUNG:** Es wird empfohlen, diese Befehle auf Ihrem lokalen System auszuführen.

Lokalen RACADM deaktivieren


Der lokale RACADM ist standardmäßig aktiviert. Weitere Informationen zum Deaktivieren finden Sie unter [Zugriff zum Ändern der iDRAC7-Konfigurationseinstellungen auf dem Host-System deaktivieren](#).

IPMI auf Managed System aktivieren

Verwenden Sie auf einem Managed System Dell Open Manage Server Administrator, um IPMI zu aktivieren oder zu deaktivieren. Weitere Informationen finden Sie im *Dell Open Manage Server Administrator's User Guide* (Dell Open Manage Server Administrator-Benutzerhandbuch) unter dell.com/support/manuals.

Linux während des Starts für die serielle Konsole konfigurieren

Die folgenden Schritte beziehen sich speziell auf den Linux Grand Unified Bootloader (GRUB). Ähnliche Änderungen sind erforderlich, um einen anderen Bootloader zu verwenden.

 **ANMERKUNG:** Beim Konfigurieren des Client-VT100-Emulationsfensters stellen Sie das Fenster bzw. die Anwendung, die die umgeleitete virtuelle Konsole anzeigt, auf 25 Reihen x 80 Spalten ein, um eine ordnungsgemäße Textanzeige sicherzustellen. Andernfalls werden einige Textanzeigen möglicherweise nicht richtig dargestellt.

Bearbeiten Sie die Datei `/etc/grub.conf` wie folgt:

1. Suchen Sie in der Datei die Abschnitte zur allgemeinen Einstellung und fügen Sie Folgendes hinzu:
`serial --unit=1 --speed=57600 terminal --timeout=10 serial`
2. Hängen Sie zwei Optionen an die Kernel-Zeile an:
`kernel console=ttyS1,115200n8r console=tty1`
3. Deaktivieren Sie die grafische GRUB-Schnittstelle und verwenden Sie die textbasierte Schnittstelle. Andernfalls wird der GRUB-Bildschirm nicht in der virtuellen RAC-Konsole angezeigt. Zum Deaktivieren der grafischen Schnittstelle kommentieren Sie die Zeile aus, die mit `splashimage` beginnt.

Das folgende Beispiel enthält ein Beispiel einer `/etc/grub.conf`-Datei, die die in diesem Verfahren beschriebenen Änderungen zeigt.

```
# grub.conf generated by anaconda # Note that you do not have to rerun grub
after making changes to this file # NOTICE: You do not have a /boot
```

```

partition. This means that all # kernel and initrd paths are relative to /,
e.g. # root (hd0,0) # kernel /boot/vmlinuz-version ro root=/dev/sdal #
initrd /boot/initrd-version.img #boot=/dev/sda default=0 timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz serial --unit=1 --speed=57600
terminal --timeout=10 serial title Red Hat Linux Advanced Server (2.4.9-e.
3smp) root (hd0,0) kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sdal
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/sdal 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.

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 10:0:wait:/etc/rc.d/rc 0 11:1:wait:/etc/rc.d/rc 1 12:2:wait:/etc/
rc.d/rc 2 13:3:wait:/etc/rc.d/rc 3 14:4:wait:/etc/rc.d/rc 4 15:5:wait:/etc/
rc.d/rc 5 16:6:wait:/etc/rc.d/rc 6 #Things to run in every runlevel. ud::once:/
sbin/update ud::once:/sbin/update #Trap CTRL-ALT-DELETE ca::ctrlaltdel:/sbin/
shutdown -t3 -r now #When our UPS tells us power has failed, assume we have a
few #minutes of power left. Schedule a shutdown for 2 minutes from now. #This
does, of course, assume you have power installed and your #UPS is connected and
working correctly. pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System
Shutting Down" #If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"


#Run gettys in standard runlevels co:2345:respawn:/sbin/agetty -h -L 57600
ttyS1 ansi 1:2345:respawn:/sbin/mingetty tty1 2:2345:respawn:/sbin/mingetty
tty2 3:2345:respawn:/sbin/mingetty tty3 4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5 6:2345:respawn:/sbin/mingetty tty6 #Run xdm
in runlevel 5 #xdm is now a separate service x:5:respawn:/etc/X11/prefdm -
nodaemon

```

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
```

Unterstützte SSH-Verschlüsselungsschemas

Um mit iDRAC7 über das SSH-Protokoll zu kommunizieren, unterstützt es verschiedene Verschlüsselungsschemas, die in der folgenden Tabelle aufgelistet sind.

Tabelle 11. SSH-Verschlüsselungsschemas

| Schematyp | Schema |
|-------------------------------|--|
| Asymmetrische Verschlüsselung | Diffie-Hellman DSA/DSS 512-1024 (zufällige) Bits nach NIST-Spezifizierung |
| Symmetrische Verschlüsselung | <ul style="list-style-type: none">• AES256-CBC• RIJNDAEL256-CBC• AES192-CBC• RIJNDAEL192-CBC• AES128-CBC• RIJNDAEL128-CBC• BLOWFISH-128-CBC• 3DES-192-CBC• ARCFOUR-128 |
| Meldungsintegrität | <ul style="list-style-type: none">• HMAC-SHA1-160• HMAC-SHA1-96• HMAC-MD5-128• HMAC-MD5-96 |
| Authentifizierung | Kennwort |
| PKA-Authentifizierung | Paare mit öffentlich-privaten Schlüsseln |


Authentifizierung über öffentlichen Schlüssel für SSH verwenden


iDRAC7 unterstützt die Authentifizierung mit öffentlichem Schlüssel (PKA) über SSH. Das ist eine lizenzierte Funktion. Wenn PKA über SSH eingerichtet ist und korrekt verwendet wird, müssen Sie bei der Anmeldung am iDRAC7 keinen Benutzernamen und kein Kennwort eingeben. Das ist sehr nützlich für automatisierte Skripts zur Durchführung verschiedener Funktionen. Die hochgeladenen Schlüssel müssen im RFC 4716- oder openssh-Format sein. Wenn sie dieses Format nicht aufweisen, müssen die Schlüssel in dieses Format konvertiert werden.

In allen Szenarios muss ein Paar aus einem privaten und einem öffentlichen Schlüssel auf der Management Station generiert werden. Der öffentliche Schlüssel wird auf den lokalen iDRAC7-Benutzer hochgeladen, und der private Schlüssel wird durch den SSH-Client verwendet, um eine vertrauenswürdige Beziehung zwischen der Management Station und iDRAC7 aufzubauen.

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 im Normalfall für Benutzer reserviert, die Mitglieder der Administratorbenutzergruppe auf iDRAC sind. Es kann jedoch auch Benutzern der Gruppe 'Benutzerdefiniert' diese Berechtigung zugewiesen werden. Ein Benutzer mit dieser Berechtigung kann die Konfiguration beliebiger Benutzer modifizieren. Hierzu zählen das Erstellen oder Löschen beliebiger Benutzer, SSH-Schlüssel-Verwaltung für Benutzer usw. Weisen Sie diese Berechtigung daher mit Bedacht zu.

 **VORSICHT:** Die Möglichkeit, SSH-Schlüssel hochzuladen, anzuzeigen und/oder zu löschen basiert auf der Benutzerberechtigung "Benutzer konfigurieren". Diese Berechtigung ermöglicht Benutzern, den SSH-Schlüssel eines anderen Benutzers zu konfigurieren. Erteilen Sie diese Berechtigung mit Bedacht.

Generieren öffentlicher Schlüssel für Windows


So verwenden Sie die Anwendung *PuTTY-Schlüsselgenerator* zum Erstellen des Grundschlüssels:

1. Starten Sie die Anwendung und wählen Sie entweder SSH-2 RSA oder SSH-2 DSA als Typ des zu generierenden Schlüssels aus (SSH-1 wird nicht unterstützt). RSA und DSA sind die einzigen unterstützten Schlüsselerstellungsalgorithmen.
2. Geben Sie die Anzahl Bits für den Schlüssel ein. Bei RSA liegen sie zwischen 768 und 4.096 Bits, bei DSA hingegen bei 1.024 Bits.
3. Klicken Sie auf **Generieren** und bewegen Sie die Maus gemäß Anleitung im Fenster. Die Schlüssel wurden erstellt.
4. Sie können das Schlüsselanmerkungsfeld ändern.
5. Geben Sie eine Passphrase zur Sicherung des Schlüssels ein.
6. Speichern Sie den öffentlichen und den privaten Schlüssel.

Generieren öffentlicher Schlüssel für Linux


Um die Anwendung *ssh-keygen* für die Erstellung des Basisschlüssels zu verwenden, öffnen Sie ein Terminalfenster, und geben Sie an der Shell-Eingabeaufforderung den Befehl `ssh-keygen -t rsa -b 1024 -C testing` ein, wobei:

- `-t` entweder für *dsa* oder für *rsa* steht.
- `-b` die Bit-Verschlüsselungsgröße zwischen 768 und 4096 angibt.
- `-C` das Ändern der Anmerkung des öffentlichen Schlüssels ermöglicht und optional ist.

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

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

 **VORSICHT:** Schlüssel, die über die Linux Management Station über den Befehl „ssh-keygen“ generiert werden, liegen im Nicht-4716-Format vor. Konvertieren Sie diese Schlüssel über den Befehl `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub` in das 4716-Format. Nehmen Sie keine Änderungen an den Berechtigungen für diese Schlüsseldatei vor. Die Konvertierung muss über Standardberechtigungen erfolgen.

 **ANMERKUNG:** iDRAC7 unterstützt nicht die ssh-agent-Weiterleitung von Schlüsseln.

SSH-Schlüssel hochladen

Sie können bis zu 4 öffentliche Schlüssel *pro Benutzer* hochladen, die über eine SSH-Schnittstelle verwendet werden können. Stellen Sie sicher, dass Sie sich vor dem Hinzufügen öffentlicher Schlüssel unbedingt die Schlüssel ansehen, ob sie bereits eingerichtet sind, sodass kein Schlüssel 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. iDRAC7 prüft nicht, ob vorherige Schlüssel gelöscht wurden, bevor neue Schlüssel hinzugefügt werden. Wenn ein neuer Schlüssel hinzugefügt wird, kann dieser nicht verwendet werden, wenn die SSH-Schnittstelle aktiviert ist.

SSH-Schlüssel über die Web-Schnittstelle hochladen

So laden Sie SSH-Schlüssel hoch:


1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Benutzerauthentifizierung** → **Lokale Benutzer**.
Die Seite **Benutzer** wird angezeigt.
2. In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.
Die Seite **Benutzer-Hauptmenü** wird angezeigt.
3. Wählen Sie unter **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 iDRAC7 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.

- Lokaler RACADM: `racadm sshpkauth -i <2 to 16> -k <1 to 4> -f <Dateiname>`
- Remote-RACADM über Telnet oder SSH: `racadm sshpkauth -i <2 to 16> -k <1 to 4> -t <Schlüsseltext>`

Beispiel: Um einen gültigen Schlüssel für die Benutzer-ID 2 auf iDRAC7 für den ersten Schlüsselsektor mithilfe einer Datei hochzuladen, führen den folgenden Befehl aus:

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

 **ANMERKUNG:** Die Option `-f` wird für Telnet/ssh/seriellen RACADM nicht unterstützt.

SSH-Schlüssel anzeigen

Sie können die Schlüssel anzeigen, die nach iDRAC7 hochgeladen wurden.

SSH-Schlüssel über die Web-Schnittstelle anzeigen

So zeigen Sie die SSH-Schlüssel an:

1. Gehen Sie in der Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Benutzerauthentifizierung** → **Lokale Benutzer**.
Die Seite **Benutzer** wird angezeigt.
2. In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.
Die Seite **Benutzer-Hauptmenü** wird angezeigt.
3. Wählen Sie unter **SSH-Schlüsselkonfiguration** die Option **SSH-Schlüssel anzeigen/entfernen** aus, und klicken Sie dann auf **Weiter**.
Daraufhin wird die Seite **SSH-Schlüssel anzeigen/entfernen** mit den Schlüsseldetails angezeigt.

SSH-Schlüssel über RACADM anzeigen

Führen Sie zum Anzeigen der SSH-Schlüssel den folgenden Befehl aus:

- Spezifischer Schlüssel – `racadm sshpkauth -i <2 bis 16> -v -k <1 bis 4>`

- Alle Schlüssel `-racadm sshpkauth -i <2 bis 16> -v -k all`

SSH-Schlüssel löschen

Bevor Sie die öffentlichen Schlüssel löschen, müssen Sie sicherstellen, dass Sie die Schlüssel anzeigen, wenn sie eingerichtet sind, so dass ein Schlüssel nicht versehentlich gelöscht werden kann.

SSH-Schlüssel über die Web-Schnittstelle löschen

So löschen Sie SSH-Schlüssel:

1. Gehen Sie in der Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Benutzerauthentifizierung** → **Lokale Benutzer** .
Die Seite **Benutzer** wird angezeigt.
2. In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.
Die Seite **Benutzer-Hauptmenü** wird angezeigt.
3. Wählen Sie unter **SSH-Schlüsselkonfiguration** die Option **SSH-Schlüssel anzeigen/entfernen** aus, und klicken Sie dann auf **Weiter**.
Daraufhin werden auf der Seite **SSH-Schlüssel anzeigen/entfernen** die Schlüsseldetails angezeigt.
4. Wählen Sie für die zu löschenden Schlüssel die Option **Entfernen** aus, und klicken Sie dann auf „Anwenden“.
Die ausgewählten Schlüssel werden daraufhin gelöscht.

SSH-Schlüssel über RACADM löschen

Führen Sie zum Löschen der SSH-Schlüssel die folgenden Befehle aus:

- Spezifischer Schlüssel `-racadm sshpkauth -i <2 bis 16> -d -k <1 bis 4>`
- Alle Schlüssel `-racadm sshpkauth -i <2 bis 16> -d -k all`

Benutzerkonten und Berechtigungen konfigurieren

Sie können Benutzerkonten mit spezifischen Berechtigungen (*rollenbasierten Berechtigungen*) einrichten, um Ihr System über iDRAC7 zu verwalten und um die Systemsicherheit zu gewährleisten. Standardmäßig ist iDRAC7 mit einem lokalen Administratorkonto konfiguriert. Der Standardbenutzername lautet *root*, und das Kennwort lautet *calvin*. Als Administrator können Sie Benutzerkonten einrichten, damit andere Benutzer auf iDRAC7 zugreifen können.

Sie können lokale Benutzer oder Verzeichnisdienste einrichten, wie z. B. Microsoft Active Directory oder LDAP, um Benutzerkonten einzurichten. Durch die Verwendung eines Verzeichnisdienstes verfügen Sie über einen zentralen Standort für die Verwaltung berechtigter Benutzerkonten.

iDRAC7 unterstützt den rollenbasierten Zugriff auf Benutzer mit einem Satz aus zugewiesenen Berechtigungen. Die folgenden Rollen sind verfügbar: Administrator, Operator, Schreibgeschützt oder Kein/e/r. Die Rolle definiert den Umfang der zugewiesenen Berechtigungen.

Verwandte Links


[Lokale Benutzer konfigurieren](#)

[Konfigurieren von Active Directory-Benutzern](#)

[Konfigurieren von allgemeinen LDAP-Benutzern](#)


Lokale Benutzer konfigurieren

Sie können in iDRAC7 bis zu 16 lokale Benutzer mit spezifischen Zugriffsberechtigungen konfigurieren. Bevor Sie einen iDRAC7-Benutzer erstellen, müssen Sie überprüfen, ob etwaige aktuelle Benutzer vorhanden sind. Sie können Benutzernamen, Kennwörter und Rollen mit den Berechtigungen für diese Benutzer definieren. Die Benutzernamen und Kennwörter können über sichere iDRAC7-Schnittstellen geändert werden (z. B. über die Web-Schnittstelle, RACADM oder WS-MAN). Sie können auch SNMPv3 Authentifizierung für jeden Benutzer aktivieren oder deaktivieren.

 **ANMERKUNG:** Die SNMPv3-Funktion ist lizenziert und ist zusammen mit der iDRAC7 Enterprise-Lizenz verfügbar.

Lokale Benutzer über die iDRAC7-Web-Schnittstelle konfigurieren

So fügen Sie lokale iDRAC7-Benutzer hinzu und konfigurieren sie:

 **ANMERKUNG:** Sie müssen die Berechtigung „Benutzer konfigurieren“ besitzen, um einen iDRAC7-Benutzer zu erstellen.

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Benutzerauthentifizierung** → **Lokale Benutzer**.

Die Seite **Benutzer** wird angezeigt.


2. In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.

 **ANMERKUNG:** Benutzer 1 ist für den anonymen IPMI-Benutzer reserviert; diese Konfiguration kann nicht geändert werden.

Die Seite **Benutzer-Hauptmenü** wird angezeigt.

3. Wählen Sie **Benutzer konfigurieren** aus, und klicken Sie dann auf **Weiter**.
Die Seite **Benutzerkonfiguration** wird angezeigt.
4. Aktivieren Sie die Benutzer-ID und geben Sie Benutzernamen, Kennwort und Zugriffsberechtigungen des Benutzers an. Sie können auch SNMPv3-Authentifizierung für den Benutzer aktivieren. Weitere Informationen finden Sie in der *iDRAC7 Online-Hilfe*.
5. Klicken Sie auf **Anwenden**. Der Benutzer wird mit den erforderlichen Berechtigungen erstellt.

Lokale Benutzer über RACADM konfigurieren


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

Sie können einen oder mehrere iDRAC7-Benutzer über RACADM konfigurieren.

Um mehrere iDRAC7-Benutzer mit identischen Konfigurationseinstellungen zu konfigurieren, führen Sie eines der folgenden Verfahren aus:

- Erstellen Sie mit Hilfe der RACADM-Beispiele in diesem Abschnitt eine Stapeldatei mit RACADM-Befehlen, und führen Sie diese Stapeldatei dann auf jedem verwalteten System aus.
- Erstellen Sie die iDRAC7-Konfigurationsdatei und führen Sie unter Verwendung derselben Konfigurationsdatei den Unterbefehl **racadm config** oder **racadm set** auf den einzelnen verwalteten Systemen aus.

Wenn Sie einen neuen iDRAC7 konfigurieren oder den Befehl **racadm racresetcfg** verwendet haben, ist der einzige aktuelle Benutzer **root** mit dem Kennwort **calvin**. Der Unterbefehl **racresetcfg** setzt den iDRAC7 auf die ursprünglichen Standardwerte zurück.

 **ANMERKUNG:** Benutzer können im Laufe der Zeit aktiviert und deaktiviert werden. Infolgedessen kann ein Benutzer auf jedem iDRAC7 eine unterschiedliche Indexnummer besitzen.

Geben Sie zum Überprüfen, ob ein Benutzer existiert, bei der Eingabeaufforderung den folgenden Befehl ein:

- Verwenden des Befehls **config**: `racadm getconfig -u <Benutzername>`
- Verwenden des Befehls **get**: `racadm get -u <Benutzername>`

ODER

Geben Sie den folgenden Befehl einmal für jeden Index von (1-16) ein:

- Verwenden des Befehls **config**: `racadm getconfig -g cfgUserAdmin -i <Index>`
- Verwenden des Befehls **get**: `racadm get iDRAC.Users.<Index>.UserName`

 **ANMERKUNG:** Sie können auch `racadm getconfig -f <myfile.cfg>` oder `racadm get -f <myfile.cfg>` eingeben und die Datei **myfile.cfg** anzeigen bzw. bearbeiten, die alle iDRAC7-Konfigurationsparameter enthält.

Mehrere Parameter und Objekt-IDs werden mit ihren aktuellen Werten angezeigt. Die Objekte von Bedeutung sind:

- Wenn Sie den Befehl **getconfig** verwendet haben:
`cfgUserAdminIndex=XX`
`cfgUserAdminUserName=`
- Wenn Sie den Befehl **get** verwendet haben:
`iDRAC.Users.UserName=`

Wenn das Objekt **cfgUserAdminUserName** keinen Wert besitzt, steht diese Indexnummer, die durch das Objekt **cfgUserAdminIndex** angezeigt wird, zur Verfügung. Wenn hinter dem "=" ein Name steht, wird dieser Index von diesem Benutzernamen verwendet.

Wenn Sie einen Benutzer mit dem Unterbefehl **racadm config** manuell aktivieren oder deaktivieren, *mus*s der Index mit der Option **-i** angegeben werden.

Beobachten Sie, ob das im vorausgehenden Beispiel angezeigte Objekt **cfgUserAdminIndex** das Zeichen **#** enthält. Es weist darauf hin, dass es sich um ein schreibgeschütztes Objekt handelt. Ebenso kann der Index nicht angegeben werden, wenn der Befehl **racadm config -f racadm.cfg** zur Angabe einer beliebigen Anzahl von zu schreibenden Gruppen/Objekten verwendet wird. Dieses Verhalten bietet größere Flexibilität bei der Konfiguration mehrerer iDRAC7 mit denselben Einstellungen.

iDRAC7-Benutzer über RACADM hinzufügen

Führen Sie zum Hinzufügen eines neuen Benutzers zum RAC folgende Schritte aus:

1. Legen Sie den Benutzernamen fest.
2. Legen Sie das Kennwort fest.
3. Legen Sie folgende Benutzerberechtigungen fest:
 - iDRAC7
 - LAN
 - Serielle Schnittstelle
 - Seriell über LAN
4. Aktivieren Sie den Benutzer.

Beispiel:

Im folgenden Beispiel wird beschrieben, wie man einen neuen Benutzer namens "John" mit dem Kennwort "123456" und ANMELDE-Berechtigungen am RAC hinzufügt.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 jan
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 jan
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x00000001
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminIpmiLanPrivilege 0x00000001
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminIpmiSerialPrivilege 0x00000001
racadm config -g cfgUserAdmin -i 1 -o cfgUserAdminSolEnable 0x00000001
racadm config -g cfgUserAdmin -i 1 -o cfgUserAdminEnable 0x00000001
```

Verwenden Sie zur Überprüfung einen der folgenden Befehle:

```
racadm getconfig -u john
racadm getconfig -g cfgUserAdmin -i 2
```

Weitere Informationen zu RACADM-Befehlen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.

iDRAC7 Benutzer mit Berechtigungen aktivieren

Um einen Benutzer mit spezifischen administrativen Berechtigungen (rollenbasierte Autorität) zu aktivieren:




ANMERKUNG: Sie können die Befehle **getconfig** und **config** oder die Befehle **get** und **set** verwenden.

1. Machen Sie zuerst einen verfügbaren Benutzer-Index mithilfe der Befehlssyntax ausfindig:
 - Verwenden des Befehls **getconfig**: `racadm getconfig -g cfgUserAdmin -i <Index>`
 - Verwenden des Befehls **get**: `racadm get iDRAC.Users <Index>`


2. Geben Sie die folgenden Befehle mit dem neuen Benutzernamen und dem neuen Kennwort ein.

- Verwenden des Befehls **config**: `racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <Index> <Benutzerberechtigungs-Bitmaskenwert>`
- Verwenden des Befehls **set**: `racadm set iDRAC.Users.<Index>.Privilege <Benutzerberechtigungs-Bitmaskenwert>`

 **ANMERKUNG:** Eine Liste gültiger Bit-Maskenwerte für spezifische Benutzerberechtigungen ist im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) enthalten, das unter dell.com/support/manuals verfügbar ist. Der Standard-Berechtigungs Wert ist 0, was darauf hinweist, dass der Benutzer über keine aktivierten Berechtigungen verfügt.

Konfigurieren von Active Directory-Benutzern

Wenn Ihre Firma die Microsoft Active Directory-Software verwendet, kann die Software so konfiguriert werden, dass sie Zugriff auf iDRAC7 bietet. Sie können dann bestehenden Benutzern im Verzeichnisdienst iDRAC7-Benutzerberechtigungen erteilen und diese steuern. Das ist eine lizenzierte Funktion.

 **ANMERKUNG:** Die Verwendung der Active Directory-Software zum Erkennen von iDRAC7 Benutzern wird von den Betriebssystemen Microsoft Windows 2000, Windows Server 2003 und Windows Server 2008 unterstützt.

Sie können die Benutzerauthentifizierung über Active Directory konfigurieren, um sich am iDRAC7 anzumelden. Rollenbasierte Autorität kann bereitgestellt werden, die es einem Administrator ermöglicht, spezifische Berechtigungen für jeden Benutzer zu konfigurieren.

Die Rollen- und Berechtigungsnamen für iDRAC7 wurden im Vergleich zu früheren Servergenerationen geändert. Die Rollennamen lauten:

Tabelle 12. iDRAC7-Rollen

| Aktuelle Generation | Vorherige Generation | Benutzerberechtigungen |
|---------------------|----------------------|---|
| Administrator | Administrator | Anmelden, Konfigurieren, Benutzer konfigurieren, Protokolle, Systemsteuerung, Auf virtuelle Konsole zugreifen, Auf virtuelle Datenträger zugreifen, Systemvorgänge, Debug |
| Operator | Hauptbenutzer | Anmelden, Konfigurieren, Systemsteuerung, Auf virtuelle Konsole zugreifen, Auf virtuelle Datenträger zugreifen, Systemvorgänge, Debug |
| Schreibgeschützt | Gastbenutzer | Anmelden |
| Keine | Keine | Keine |

Tabelle 13. iDRAC7-Benutzerberechtigungen

| Aktuelle Generation | Vorherige Generation | Beschreibung |
|------------------------|-----------------------------------|---|
| Anmelden | Am iDRAC anmelden | Ermöglicht dem Benutzer, sich am iDRAC anzumelden. |
| Konfigurieren | iDRAC konfigurieren | Ermöglicht dem Benutzer, den iDRAC zu konfigurieren. |
| Benutzer konfigurieren | Benutzer konfigurieren | Ermöglicht dem Benutzer, bestimmten Benutzern den Zugriff auf das System zu erlauben. |
| Protokolle | Protokolle löschen | Aktiviert den Benutzer zum Löschen des Systemereignisprotokolls (SEL). |
| Systemsteuerung | Serversteuerungsbefehle ausführen | Ermöglicht Aus- und Einschalten des Host-Systems. |

| Aktuelle Generation | Vorherige Generation | Beschreibung |
|-------------------------------------|--|--|
| Auf die virtuelle Konsole zugreifen | Auf die Umleitung der virtuellen Konsole zugreifen (bei Blade-Servern)
Auf die virtuelle Konsole zugreifen (bei Rack- oder Tower-Servern) | Ermöglicht dem Benutzer, die virtuelle Konsole auszuführen. |
| Auf virtuelle Datenträger zugreifen | Auf virtuelle Datenträger zugreifen | Ermöglicht dem Benutzer, virtuelle Datenträger auszuführen und zu verwenden. |
| Systemvorgänge | Testwarnungen | Ermöglicht vom Benutzer initiierte und erzeugte Ereignisse und die Informationen werden als asynchrone Benachrichtigung versendet und protokolliert. |
| Debug | Diagnosebefehle ausführen | Ermöglicht dem Benutzer, Diagnosebefehle auszuführen. |

Verwandte Links

- [Voraussetzungen zur Verwendung der Active Directory-Authentifizierung des iDRAC7](#)
- [Unterstützte Active Directory-Authentifizierungsmechanismen](#)

Voraussetzungen zur Verwendung der Active Directory-Authentifizierung des iDRAC7

Um die Active Directory-Authentifizierungsfunktion auf dem iDRAC7 verwenden zu können, stellen Sie sicher, dass Sie:

- eine Active Directory-Infrastruktur bereitgestellt haben. Weitere Informationen finden Sie auf der Microsoft-Website.
- PKI in die Active Directory-Infrastruktur integriert haben. iDRAC7 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.
- Hat die Secure Socket Layer (SSL) auf allen Domänen-Controllern aktiviert, mit denen sich iDRAC7 zur Authentifizierung mit allen Domänen-Controllern verbindet.

Verwandte Links

- [SSL auf Domänen-Controller aktivieren](#)

SSL auf Domänen-Controller aktivieren

Wenn Benutzer durch das iDRAC6 gegen einen Active Directory-Domänen-Controller authentifiziert werden, wird eine SSL-Sitzung mit dem Domänen-Controller gestartet. Der Domänen-Controller muss ein von der Zertifizierungsstelle (CA) signiertes Zertifikat erstellen – das Stammzertifikat, das auch in das iDRAC6 geladen wird. Damit also die iDRAC6-Authentifizierung auf einem *beliebigen* Domänen-Controller möglich ist – egal, ob es sich um den Stamm-Domänen-Controller oder den untergeordneten Domänen-Controller handelt – muss dieser Domänen-Controller ein SSL-aktiviertes, von der CA der Domäne signiertes SSL-Zertifikat aufweisen.

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 iDRAC7 exportieren
3. SSL-Zertifikat der iDRAC7-Firmware importieren

Verwandte Links

- [SSL-Zertifikat für jeden Domänen-Controller installieren](#)


[Das CA-Stammzertifikat des Domänen-Controllers zu iDRAC7 exportieren](#)
[SSL-Zertifikat der iDRAC7-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 klicken Sie dann auf **Fertigstellen**. Daraufhin wird das SSL-Zertifikat installiert.

Das CA-Stammzertifikat des Domänen-Controllers zu iDRAC7 exportieren

 **ANMERKUNG:** Wenn Ihr System Windows 2000 ausführt oder Sie eine eigenständige CA verwenden, können die nachfolgenden Schritte variieren.


So exportieren Sie das Stamm-Zertifizierungsstellenzertifikat des Domänen-Controllers nach iDRAC7:

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** auf Windows 2000-Systemen) 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 **Fertigstellen**, 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 iDRAC7.

SSL-Zertifikat der iDRAC7-Firmware importieren

Das iDRAC7-SSL-Zertifikat ist identisch mit dem Zertifikat, das für den iDRAC7-Web Server verwendet wird. Alle iDRAC7-Controller werden mit einem selbstsignierten Standard-Zertifikat versendet.

Wenn der Active Directory-Server so eingestellt ist, dass der Client während der Initialisierungsphase einer SSL-Sitzung authentifiziert wird, muss das iDRAC7-Serverzertifikat auf den Active Directory-Domänen-Controller hochgeladen werden. Dieser zusätzliche Schritt ist nicht erforderlich, wenn das Active Directory während der Initialisierungsphase einer SSL-Sitzung keine Client-Authentifizierung ausführt.

 **ANMERKUNG:** Wenn Ihr System Windows 2000 ausführt, können die folgenden Schritte abweichen.



ANMERKUNG: Wenn das SSL-Zertifikat der iDRAC7-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 iDRAC7-Firmware in alle Listen vertrauenswürdiger Zertifikate der Domänen-Controller:

1. Laden Sie das iDRAC7 SSL-Zertifikat unter Verwendung des folgenden RACADM-Befehls herunter:
`racadm sslcertdownload -t 0x1 -f <RAC-SSL-Zertifikat>`
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** und klicken Sie auf **Importieren**.
4. Klicken Sie auf **Weiter** und suchen Sie die SSL-Zertifikatdatei.
5. Installieren Sie das iDRAC7-SSL-Zertifikat in der **vertrauenswürdigen Stammzertifizierungsstelle** der einzelnen Domänen-Controller.

Wenn Sie Ihr eigenes Zertifikat installiert haben, stellen Sie sicher, dass die Zertifizierungsstelle, die das Zertifikat signiert hat, in der Liste **Vertrauenswürdige Stammzertifizierungsstellen** aufgeführt ist. Wenn die Zertifizierungsstelle nicht auf der Liste ist, müssen Sie sie auf allen Domänen-Controllern installieren.

6. Klicken Sie auf **Weiter** und wählen Sie aus, ob Windows den Zertifikatspeicher automatisch aufgrund des Zertifikattyps auswählen soll, oder suchen Sie selbst nach einem Speicher.
7. Klicken Sie auf **Fertigstellen**, und klicken Sie dann auf **OK**. Das SSL-Zertifikat für die iDRAC7-Firmware wird in alle Listen mit vertrauenswürdigen Zertifikaten für Domänen-Controller importiert.

Unterstützte Active Directory-Authentifizierungsmechanismen

Sie können mit Active Directory den Benutzerzugriff auf iDRAC7 mittels zweier Methoden definieren:

- Die *Standardschemalösung*, die nur Microsoft-Standard-Active Directory-Gruppenobjekte verwendet.
- Lösung *Erweitertes Schema*, die über benutzerdefinierte Active Directory-Objekte verfügt. Alle Zugriffssteuerungsobjekte werden im Active Directory verwahrt. Bei der Konfiguration des Benutzerzugangs auf verschiedenen iDRAC7-Karten mit unterschiedlichen Ebenen der Benutzerberechtigung besteht maximale Flexibilität.

Verwandte Links

[Übersicht des Standardschema-Active Directory](#)

[Übersicht des Active Directory mit erweitertem Schema](#)

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 iDRAC7.

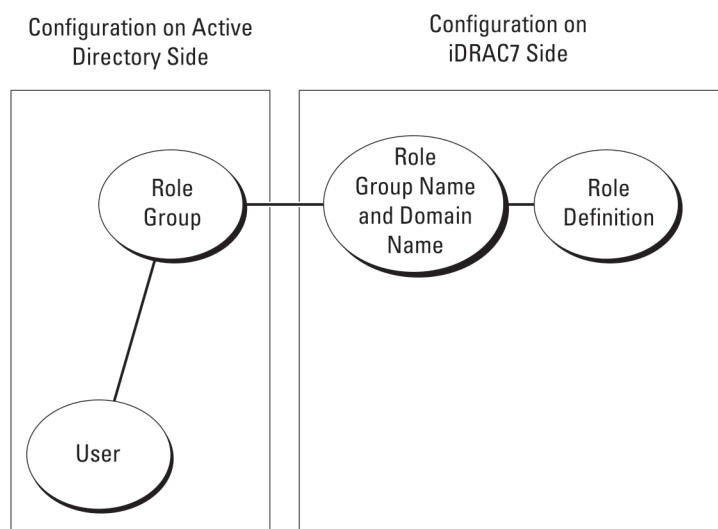


Abbildung 1. Konfiguration des iDRAC7 mit Active Directory Standardschema

In Active Directory wird ein Standardgruppenobjekt als Rollengruppe verwendet. Ein Benutzer, der Zugang zum iDRAC7 hat, ist ein Mitglied der Rollengruppe. Um diesem Benutzer Zugriff auf einen bestimmten iDRAC6 zu gewähren, muss der Rollengruppenname und dessen Domänenname auf dem jeweiligen iDRAC6 konfiguriert werden. Die Rolle und die Berechtigungsebene wird auf jedem iDRAC und nicht im Active Directory definiert. Sie können bis zu fünf Rollengruppen für jeden iDRAC7 konfigurieren. Tabellen-Referenznummer zeigt die Standard-Rollengruppen-Berechtigungen.

Tabelle 14. Standardeinstellungsberechtigungen der Rollengruppe

| Rollengruppen | Standard-Berechtigungsebene | Gewährte Berechtigungen | Bitmaske |
|----------------|-----------------------------|---|------------|
| Rollengruppe 1 | kein | Am iDRAC anmelden, iDRAC konfigurieren, Benutzer konfigurieren, Protokolle löschen, Serversteuerungsbefehle ausführen, auf virtuelle Konsole zugreifen, auf virtuellen Datenträger zugreifen, Warnungen testen, Diagnosebefehle ausführen | 0x000001ff |
| Rollengruppe 2 | kein | Am iDRAC anmelden, iDRAC konfigurieren, Serversteuerungsbefehle ausführen, auf virtuelle Konsole zugreifen, auf virtuellen Datenträger zugreifen, Warnungen testen, Diagnosebefehle ausführen | 0x000000f9 |
| Rollengruppe 3 | kein | Am iDRAC anmelden | 0x00000001 |
| Rollengruppe 4 | kein | Keine zugewiesenen Berechtigungen | 0x00000000 |
| Rollengruppe 5 | kein | Keine zugewiesenen Berechtigungen | 0x00000000 |



ANMERKUNG: Die Bitmasken-Werte werden nur verwendet, wenn das Standardschema mit RACADM eingerichtet wird.

Einfache Domänen (Single Domains) und mehrfache Domänen (Multiple Domains)

Wenn sich alle Anmeldebenutzer und Rollengruppen sowie die verschachtelten Gruppen in derselben Domäne befinden, müssen lediglich die Adressen der Domänen-Controller auf dem iDRAC7 konfiguriert werden. In diesem Muster einer einfachen Domäne wird jede Art von Gruppe unterstützt.

Wenn alle Anmeldebenutzer und Rollengruppen oder beliebige der verschachtelten Gruppen mehreren Domänen angehören, müssen Server-Adressen des Globalen Katalogs auf dem iDRAC7 konfiguriert werden. In diesem Muster mehrfacher Domänen müssen alle Rollengruppen und, falls vorhanden, alle verschachtelten Gruppen einer Universalgruppe angehören.

Active Directory-Standardschema konfigurieren

So konfigurieren Sie iDRAC7 für den Zugriff auf eine Active Directory-Anmeldung:

1. Öffnen Sie auf einem Active Directory-Server (Domänen-Controller) das Active Directory-Benutzer- und -Computer-Snap-In.
2. Erstellen Sie eine Gruppe, oder wählen Sie eine vorhandene Gruppe aus. Fügen Sie den Active Directory-Benutzer als Mitglied der Active Directory-Gruppe für den Zugriff auf iDRAC7 hinzu.
3. Konfigurieren Sie den Gruppennamen, den Domännennamen und die Rollenberechtigungen auf iDRAC7 über die iDRAC7-Web-Schnittstelle oder RACADM.

Verwandte Links

[Active Directory mit Standardschema unter Verwendung der iDRAC7-Webschnittstelle konfigurieren](#)
[Konfiguration des Active Directory mit Standardschema unter Verwendung von RACADM](#)

Active Directory mit Standardschema unter Verwendung der iDRAC7-Webschnittstelle konfigurieren



ANMERKUNG: Weitere Informationen zu den verschiedenen Feldern finden Sie in der *iDRAC7-Online-Hilfe*.

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Benutzerauthentifizierung** → **Verzeichnisdienste** → **Microsoft Active Directory**.
Die **Active Directory-Zusammenfassungsseite** wird angezeigt.
2. Klicken Sie auf **Active Directory konfigurieren**.
Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 1 von 4 wird angezeigt.
3. Aktivieren Sie optional die Zertifikatüberprüfung, und laden Sie das durch die Zertifizierungsstelle signierte digitale Zertifikat hoch, das im Rahmen der Initiierung von SSL-Verbindungen bei der Kommunikation mit dem Active Directory (AD)-Server verwendet wird. Aus diesem Grund müssen die Domänen-Controller und die FQDN des globalen Katalogs angegeben werden. Dies folgt im nächsten Schritt. Folglich sollte die DNS in den Netzwerkeinstellungen ordnungsgemäß konfiguriert werden.
4. Klicken Sie auf **Weiter**.
Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 2 von 4 wird angezeigt.
5. Aktivieren Sie Active Directory, und geben Sie die Standortinformationen zu den Active Directory-Servern und -Benutzerkonten an. Geben Sie außerdem an, wie lange iDRAC7 bei der Anmeldung bei iDRAC7 auf Antworten von Active Directory warten muss.



ANMERKUNG: Wenn die Zertifikatüberprüfung aktiviert ist, geben Sie die Adressen des Domain Controller Server und die FQDN des globalen Katalogs an. Stellen Sie sicher, dass DNS unter **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** ordnungsgemäß konfiguriert ist.

6. Klicken Sie auf **Weiter**. Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 3 von 4 wird angezeigt.

7. Wählen Sie **Standardschema** aus, und klicken Sie auf „Weiter“.
Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 4a von 4** wird angezeigt.
8. Geben Sie den Standort der globalen Katalogserver für Active Directory an, und geben Sie außerdem die Berechtigungsgruppen an, die für die Autorisierung von Benutzern verwendet werden.
9. Klicken Sie auf eine **Rollengruppe**, um die Steuerungsauthentifizierungsrichtlinie für Benutzer unter dem Standardschemacode zu konfigurieren.
Die Seite **Active Directory-Konfiguration und -Verwaltung Schritt 4b von 4** wird angezeigt.
10. 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.
11. Klicken Sie auf **Fertigstellen**. Daraufhin werden die Active Directory-Einstellungen für das Standardschema konfiguriert.

Konfiguration des Active Directory mit Standardschema unter Verwendung von RACADM

So konfigurieren Sie iDRAC7 Active Directory mit Standardschema unter Verwendung von RACADM:

1. Führen Sie an der RACADM-Befehlszeileingabe die folgenden Befehle aus:
 - Verwenden des Befehls **config**:


```
racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g
cfgActiveDirectory -o cfgADType 2 racadm config -g cfgStandardSchema -
i <Index> -o cfgSSADRoleGroupName <allgemeiner Name der Rollengruppe>
racadm config -g cfgStandardSchema -i <Index> -o
cfgSSADRoleGroupDomain <vollqualifizierter Domänenname> racadm config -
g cfgStandardSchema -i <Index> -o cfgSSADRoleGroupPrivilege
<Bitmaskenwert für bestimmte Rollengruppenberechtigungen> racadm
config -g cfgActiveDirectory -o cfgADDomainController1
<vollqualifizierter Domänenname oder IP-Adresse des Domänen-
Controllers> racadm config -g cfgActiveDirectory -o
cfgADDomainController2 <vollqualifizierter Domänenname oder IP-Adresse
des Domänen-Controllers> racadm config -g cfgActiveDirectory -o
cfgADDomainController3 <vollqualifizierter Domänenname oder IP-Adresse
des Domänen-Controllers> racadm config -g cfgActiveDirectory -o
cfgADGlobalCatalog1 <vollqualifizierter Domänenname oder IP-Adresse
des Domänen-Controllers> racadm config -g cfgActiveDirectory -o
cfgADGlobalCatalog2 <vollqualifizierter Domänenname oder IP-Adresse
des Domänen-Controllers> racadm config -g cfgActiveDirectory -o
cfgADGlobalCatalog3 <vollqualifizierter Domänenname oder IP-Adresse
des Domänen-Controllers>
```
 - Verwenden des Befehls **set**:


```
racadm set iDRAC.ActiveDirectory.Enable 1 racadm set
iDRAC.ActiveDirectory.Schema 2 racadm set iDRAC.ADGroup.Name
<allgemeiner Name der Rollengruppe> racadm set iDRAC.ADGroup.Domain
<vollqualifizierter Domänenname> racadm set iDRAC.ADGroup.Privilege
<Bitmaskenwert für bestimmte Rollengruppenberechtigungen> racadm set
iDRAC.ActiveDirectory.DomainController1 <vollqualifizierter
Domänenname oder IP-Adresse des Domänen-Controllers> racadm set
iDRAC.ActiveDirectory.DomainController2 <vollqualifizierter
Domänenname oder IP-Adresse des Domänen-Controllers> racadm set
iDRAC.ActiveDirectory.DomainController3 <vollqualifizierter
Domänenname oder IP-Adresse des Domänen-Controllers> racadm set
iDRAC.ActiveDirectory.GlobalCatalog1 <vollqualifizierter Domänenname
oder IP-Adresse des Domänen-Controllers> racadm set
iDRAC.ActiveDirectory.GlobalCatalog2 <vollqualifizierter Domänenname
oder IP-Adresse des Domänen-Controllers> racadm set
iDRAC.ActiveDirectory.GlobalCatalog3 <vollqualifizierter Domänenname
oder IP-Adresse des Domänen-Controllers>
```

Informationen zu Bitmaskenwerten für spezifische Rollengruppenberechtigungen finden Sie unter [Standardeinstellungsberechtigungen der Rollengruppe](#).

Geben Sie unbedingt den FQDN des Domänen-Controllers ein, nicht den FQDN der Domäne selbst. Geben Sie z.B. `servername.dell.com` ein und nicht `dell.com`.

Es muss mindestens eine der Adresse konfiguriert werden. iDRAC7 versucht so lange, nacheinander mit allen konfigurierten Adressen eine Verbindung herzustellen, bis eine Verbindung erfolgreich hergestellt wurde. Im Standardschema handelt es sich um die Adressen der Domänen-Controller, auf denen sich die Benutzerkonten und die Rollengruppen befinden.

Im Standardschema ist der Global Catalog Server nur erforderlich, wenn die Benutzerkonten und Rollengruppen in verschiedenen Domänen liegen. Im Falle mehrerer Domänen wie hier kann nur die Universalgruppe verwendet werden.

Der FQDN oder die IP-Adresse, den/die Sie in diesem Feld angeben, sollte mit dem Feld "Servername" oder "Alternativer Servername" des Zertifikats Ihres Domänen-Controllers übereinstimmen, wenn Sie die Überprüfung des Zertifikats aktiviert haben.

Wenn Sie für den SSL-Handshake die Zertifikatsvalidierung deaktivieren möchten, geben Sie den folgenden RACADM-Befehl ein:

- Verwenden des Befehls **config**: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0`
- Verwenden des Befehls **set**: `racadm set iDRAC.ActiveDirectory.CertValidationEnable 0`


In diesem Fall brauchen Sie kein CA-Zertifikat zu laden.

So erzwingen Sie die Zertifikatsvalidierung während eines SSL-Handshake (optional):

- Verwenden des Befehls **config**: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1`
- Verwenden des Befehls **set**: `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-Zertifikat>
```

 **ANMERKUNG:** Wenn die Zertifikatsvalidierung aktiviert ist, geben Sie die Adressen des Domain Controller Server und die FQDN des globalen Katalogs an. Stellen Sie sicher, dass DNS unter **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** ordnungsgemäß konfiguriert ist.

Die Verwendung des folgenden RACADM-Befehls kann optional sein.

```
racadm sslcertdownload -t 0x1 -f <RAC-SSL-Zertifikat>
```

2. Wenn DHCP auf dem iDRAC7 aktiviert ist und Sie den vom DHCP-Server bereitgestellten DNS verwenden möchten, geben Sie folgenden RACADM-Befehl ein:

- Verwenden des Befehls **config**: `racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1`
- Verwenden des Befehls **set**: `racadm set iDRAC.IPv4.DNSFromDHCP 1`

3. Wenn DHCP auf dem iDRAC7 deaktiviert ist oder Sie die DNS IP-Adresse manuell eingeben möchten, geben Sie die folgenden RACADM-Befehle ein:

- Verwenden des Befehls **config**:
`racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0`
`racadm config -g cfgLanNetworking -o cfgDNSServer1 <primäre DNS-IP-Adresse>`
`racadm config -g cfgLanNetworking -o cfgDNSServer2 <sekundäre DNS-IP-Adresse>`

- Verwenden des Befehls **set**:

```
racadm set iDRAC.IPv4.DNSFromDHCP 0 racadm set
iDRAC.IPv4.DNSFromDHCP.DNS1 <primäre DNS-IP-Adresse> racadm set
iDRAC.IPv4.DNSFromDHCP.DNS2 <sekundäre DNS-IP-Adresse>
```

4. Wenn Sie eine Liste von Benutzerdomänen konfigurieren möchten, sodass für die Anmeldung an der Webschnittstelle nur der Benutzername eingegeben werden muss, geben Sie den folgenden Befehl ein:

- Verwenden des Befehls **config**: `racadm config -g cfgUserDomain -o cfgUserDomainName <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers> -i <Index>`
- Verwenden des Befehls **set**: `racadm set iDRAC.UserDomain.<Index>.Name <vollqualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>`

Sie können bis zu 40 Benutzerdomänen mit Indexzahlen zwischen 1 und 40 konfigurieren.

Übersicht des Active Directory mit erweitertem Schema

Für die Verwendung der Lösung mit dem erweiterten Schema benötigen Sie die Active Directory-Schema-Erweiterung.

Active Directory-Schemaerweiterungen

Bei den Active Directory-Daten handelt es sich um eine verteilte Datenbank von *Attributen* und *Klassen*. Das Active Directory-Schema enthält die Regeln, die den Typ der Daten bestimmen, die der Datenbank hinzugefügt werden können bzw. darin gespeichert werden. Die Benutzerklasse ist ein Beispiel einer *Klasse*, die in der Datenbank gespeichert wird. Beispielhafte Attribute der Benutzerklasse sind der Vorname, der Nachname bzw. die Telefonnummer des Benutzers. Sie können die Active Directory-Datenbank erweitern, indem Sie Ihre eigenen einzigartigen *Attribute* und *Klassen* für besondere Anforderungen hinzufügen. Dell hat das Schema um die erforderlichen Änderungen zur Unterstützung von Remote-Management-Authentifizierung und -Autorisierung erweitert.

Jedes *Attribut* bzw. jede *Klasse*, das/die zu einem vorhandenen Active Directory-Schema hinzugefügt wird, muss mit einer eindeutigen ID definiert werden. Um branchenweit eindeutige IDs zu gewährleisten, unterhält Microsoft eine Datenbank von Active Directory-Objektbezeichnern (OIDs). Wenn also Unternehmen das Schema erweitern, sind diese Erweiterungen eindeutig und ergeben keine Konflikte. Um das Schema im Active Directory von Microsoft zu erweitern, hat Dell eindeutige OIDs (Namenserweiterungen) und eindeutig verlinkte Attribut-IDs für die Attribute und Klassen erhalten, die dem Verzeichnisdienst hinzugefügt werden.

- Erweiterung ist: dell
- Basis-OID lautet: 1.2.840.113556.1.8000.1280
- Der RAC-LinkID-Bereich ist: 12070 bis 12079

Übersicht über die iDRAC7-Schemaerweiterungen

Dell hat das Schema um *Zuordnungs*-, *Geräte*- und *Berechtigungseigenschaften* erweitert. Die *Zuordnungseigenschaft* wird zur Verknüpfung der Benutzer oder Gruppen mit einem spezifischen Satz an Berechtigungen für ein oder mehrere iDRAC7-Geräte verwendet. Dieses Modell ist unkompliziert und gibt dem Administrator höchste Flexibilität bei der Verwaltung verschiedener Benutzergruppen, iDRAC7-Berechtigungen und iDRAC7-Geräten im Netzwerk.

Für jedes iDRAC7 des Netzwerkes, das Sie zur Authentifizierung und Autorisierung in Active Directory integrieren möchten, müssen Sie mindestens ein Zuordnungsobjekt und ein iDRAC7-Geräteobjekt erstellen. Sie können mehrere Zuordnungsobjekte erstellen, wobei jedes Zuordnungsobjekt nach Bedarf mit beliebig vielen Benutzern, Benutzergruppen, oder iDRAC7-Geräteobjekten verbunden werden kann. Die Benutzer und iDRAC7-Benutzergruppen können Mitglieder beliebiger Domänen im Unternehmen sein.

Jedes Zuordnungsobjekt darf jedoch nur mit einem Berechtigungsobjekt verbunden werden (bzw. jedes Zuordnungsobjekt kann Benutzer, Benutzergruppen oder iDRAC7-Geräteobjekte nur mit einem Berechtigungsobjekt

verbinden). Dies ermöglicht dem Administrator, die Berechtigungen jedes Benutzers über spezielle iDRAC6-Geräte zu steuern.

Das iDRAC6-Geräteobjekt ist die Verknüpfung zur iDRAC6-Firmware für die Abfrage des Active Directory auf Authentifizierung und Autorisierung. Wenn ein iDRAC7 dem Netzwerk hinzugefügt wird, muss der Administrator den iDRAC7 und sein Geräteobjekt mit seinem Active Directory-Namen so konfigurieren, dass Benutzer Authentifizierung und Genehmigung bei Active Directory ausführen können.

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

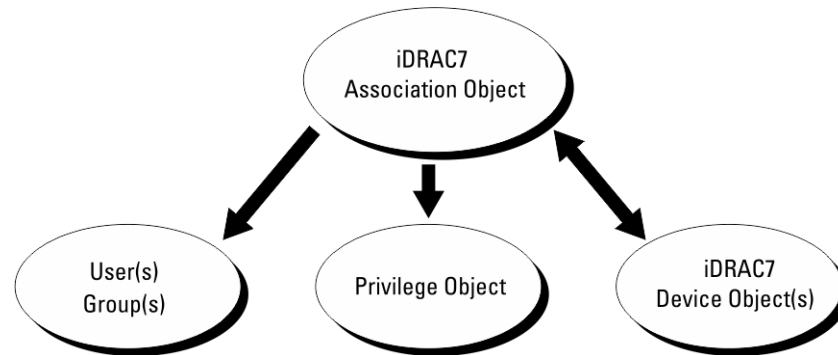


Abbildung 2. Typisches Setup für Active Directory-Objekte

Sie können eine beliebige Anzahl an Zuordnungsobjekten erstellen. Es ist jedoch erforderlich, dass Sie mindestens ein Zuordnungsobjekt erstellen, und Sie müssen ein iDRAC7-Geräteobjekt für jedes iDRAC7 auf dem Netzwerk haben, das zum Zweck der Authentifizierung und Autorisierung mit dem iDRAC7 mit dem Active Directory integriert werden soll.

Das Zuordnungsobjekt lässt ebenso viele oder wenige Benutzer bzw. Gruppen und auch iDRAC7-Geräteobjekte zu. Das Zuordnungsobjekt enthält jedoch nur ein Berechtigungsobjekt pro Zuordnungsobjekt. Das Zuordnungsobjekt verbindet die Benutzer, die Berechtigungen auf iDRAC7-Geräten haben.

Über die Dell-Erweiterung zum ADUC MMC Snap-In können nur Berechtigungsobjekte und iDRAC7-Objekte derselben Domäne mit dem Verbindungsobjekt verbunden werden. Mit der Dell-Erweiterung können keine Gruppen oder iDRAC7-Objekte aus anderen Domänen als Produktmitglied des Verbindungsobjektes hinzugefügt werden.

Wenn Sie Universalgruppen von unterschiedlichen Domänen hinzufügen, erstellen Sie ein Zuordnungsobjekt mit Universalreichweite. Die durch das Dell Schema Extender-Dienstprogramm erstellten Standardzuordnungsobjekte sind lokale Domänengruppen und funktionieren nicht mit Universalgruppen anderer Domänen.

Benutzer, Benutzergruppen oder verschachtelte Benutzergruppen jeglicher Domäne können dem Verbindungsobjekt hinzugefügt werden. Lösungen mit erweitertem Schema unterstützen jede Art von Benutzergruppe sowie jede Benutzergruppe, die über mehrere Domänen verschachtelt und von Microsoft Active Directory zugelassen ist.

Unter Verwendung des erweiterten Schemas Berechtigungen ansammeln

Die Methode zur Authentifizierung des erweiterten Schemas unterstützt das Ansammeln von Berechtigungen über unterschiedliche Berechtigungsobjekte, die mit demselben Benutzer über verschiedene Zuordnungsobjekte in Verbindung stehen. Mit anderen Worten sammelt die Authentifizierung des erweiterten Schemas Berechtigungen an, um dem Benutzer den Supersatz aller zugewiesener Berechtigungen zu ermöglichen, die den verschiedenen, demselben Benutzer zugeordneten Berechtigungsobjekten entsprechen.

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

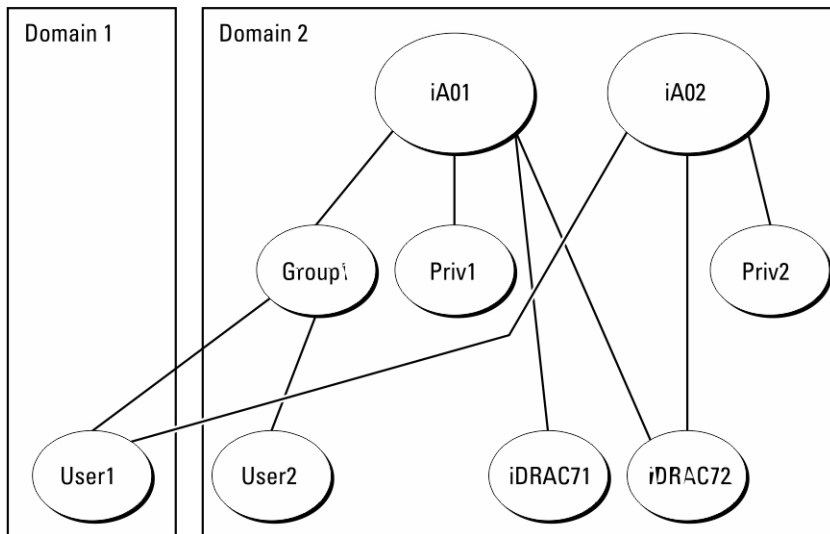


Abbildung 3. Ansammeln von Berechtigungen für einen Benutzer

Die Abbildung stellt zwei Zuordnungsobjekte dar – A01 und A02. Benutzer1 ist über beide Verbindungsobjekte mit iDRAC72 verbunden.

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

In diesem Beispiel verfügt Benutzer1 über die Berechtigungen von Priv1 und Priv2 auf dem iDRAC2. Benutzer1 hat ausschließlich Priv1-Berechtigungen auf dem iDRAC1. Benutzer2 hat die Berechtigungen von Priv1 sowohl auf dem iDRAC1 als auch auf dem iDRAC2. Diese Darstellung zeigt auch, dass Benutzer1 einer anderen Domäne und auch einer Gruppe angehören kann.

Active Directory mit erweitertem Schema konfigurieren

So konfigurieren Sie Active Directory für den Zugriff auf iDRAC7:


1. Erweitern des Active Directory-Schemas.
2. Active Directory-Benutzer und Computer-Snap-In erweitern
3. Fügen Sie dem Active Directory die iDRAC 7-Benutzer und ihre Berechtigungen hinzu.
4. Konfigurieren Sie die iDRAC7 Active Directory-Eigenschaften über die iDRAC7-Web-Schnittstelle oder RACADM.


Verwandte Links

- [Übersicht des Active Directory mit erweitertem Schema](#)
- [Dell-Erweiterung zu Active Directory Benutzer- und Computer-Snap-In installieren](#)
- [iDRAC7-Benutzer und -Berechtigungen zum Active Directory hinzufügen](#)
- [Active Directory mit erweitertem Schema unter Verwendung der iDRAC7-Webschnittstelle konfigurieren](#)
- [Konfiguration des Active Directory mit erweitertem Schema unter Verwendung von RACADM](#)

Erweitern des Active Directory-Schemas

Mit der Erweiterung des Active Directory-Schemas werden eine Dell-Organisationseinheit, Schemaklassen und -attribute sowie Beispielberechtigungen und Zuordnungsobjekte zum Active Directory-Schema hinzugefügt. Bevor Sie das Schema erweitern, müssen Sie sicherstellen, dass Sie Schema-Admin-Berechtigungen auf dem Schema Master-FSMO-Rollenbesitzer (Flexible Single Master Operation) der Domänenstruktur besitzen.

 **ANMERKUNG:** Stellen Sie sicher, dass die Schema-Erweiterung für dieses Produkt sich von den Vorgänger-Generationen der Dell Remote Management-Produkte unterscheidet. Das vorherige Schema kann bei diesem Produkt nicht verwendet werden.

 **ANMERKUNG:** Eine Erweiterung des neuen Schemas ändert nichts an den Vorgängerversionen des Produktes.

Sie können das Schema mit einer der folgenden Methoden erweitern:

- Dell Schema Extender-Dienstprogramm
- LDIF-Script-Datei

Die Dell-Organisationseinheit wird dem Schema nicht hinzugefügt, wenn Sie die LDIF-Skriptdatei verwenden.

Die LDIF-Dateien und Dell Schema Extender befinden sich auf der DVD *Dell Systems Management Tools and Documentation* in den folgenden jeweiligen Verzeichnissen:

- **DVD-Laufwerk:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files**
- **<DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender**

Lesen Sie zur Verwendung der LDIF-Dateien die Anleitungen in der Infodatei im Verzeichnis **LDIF_Files**.

Sie können Schema Extender oder die LDIF-Dateien an einem beliebigen Standort kopieren und ausführen.

Dell Schema Extender verwenden

 **VORSICHT:** Das Dienstprogramm Dell Schema Extender verwendet die Datei **SchemaExtenderOem.ini**. Um sicherzustellen, dass das Dell Schema Extender-Dienstprogramm richtig funktioniert, modifizieren Sie den Namen dieser Datei nicht.

1. Klicken Sie im **Begrüßungsbildschirm** auf **Weiter**.
2. Lesen Sie die Warnung und vergewissern Sie sich, dass Sie sie verstehen und klicken Sie dann auf **Weiter**.
3. Wählen Sie **Aktuelle Anmeldeinformationen Verwenden** aus, oder geben Sie einen Benutzernamen und ein Kennwort mit Schema-Administratorrechten ein.
4. Klicken Sie auf **Weiter**, um Dell Schema Extender auszuführen.
5. Klicken Sie auf **Fertigstellen**.

Das Schema wird erweitert. Um die Schema-Erweiterung zu überprüfen, verwenden Sie die Microsoft-Verwaltungskonsolle (MMC) und das Active Directory-Schema-Snap-In, um zu prüfen, ob [Klassen und Attribute](#) vorhanden sind: Näheres zur Benutzung der Verwaltungskonsolle (MMC) und des Active Directory-Schema-Snap-In finden Sie in der Microsoft-Dokumentation.

Klassen und Attribute

Tabelle 15. 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 16. dellRacDevice Class

| | |
|--------------|---|
| OID | 1.2.840.113556.1.8000.1280.1.7.1.1 |
| Beschreibung | Das iDRAC-Gerät muss im Active Directory als dellIDRACDevice konfiguriert sein. Mit dieser Konfiguration kann der iDRAC CMC Lightweight Directory Access Protocol (LDAP)-Abfragen an das Active Directory senden. |
| Klassentyp | Strukturklasse |
| SuperClasses | dellProduct |
| Attribute | dellSchemaVersion
dellRacType |

Tabelle 17. dellIDRACAssociationObject Class

| | |
|--------------|--|
| OID | 1.2.840.113556.1.8000.1280.1.7.1.2 |
| Beschreibung | Repräsentiert das Dell-Zuordnungsobjekt. Das Zuordnungsobjekt ist die Verbindung zwischen Benutzern und Geräten. |
| Klassentyp | Strukturklasse |
| SuperClasses | Gruppe |
| Attribute | dellProductMembers
dellPrivilegeMember |

Tabelle 18. dellIRAC4Privileges Class

| | |
|--------------|--|
| OID | 1.2.840.113556.1.8000.1280.1.1.1.3 |
| Beschreibung | Legt die Berechtigungen für iDRAC6 fest (Autorisierungsrechte) |
| Klassentyp | Erweiterungsklasse |
| SuperClasses | kein |
| Attribute | dellIsLoginUser
dellIsCardConfigAdmin
dellIsUserConfigAdmin
dellIsLogClearAdmin
dellIsServerResetUser
dellIsConsoleRedirectUser
dellIsVirtualMediaUser
dellIsTestAlertUser
dellIsDebugCommandAdmin |

Tabelle 19. 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 |

| | |
|--------------|------------------------------------|
| OID | 1.2.840.113556.1.8000.1280.1.1.1.4 |
| SuperClasses | Benutzer |
| Attribute | dellRAC4Privileges |

Tabelle 20. 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 21. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden

| Attributname/Beschreibung | Zugewiesener OID/Syntax-Objektkennzeichner | Einzelbewertung |
|---|---|-----------------|
| dellPrivilegeMember
Die Liste von dellPrivilege-Objekten, die zu diesem Attribut gehören. | 1.2.840.113556.1.8000.1280.1.1.2.1
Eindeutiger Name (LDAPTYPE_DN
1.3.6.1.4.1.1466.115.121.1.12) | FALSE |
| dellProductMembers
Liste der dellRacDevice- und DelliDRACDevice-Geräteobjekte, die dieser Rolle angehören. 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 |
| dellsLoginUser
TRUE, wenn der Benutzer Anmelde-rechte auf dem Gerät hat. | 1.2.840.113556.1.8000.1280.1.1.2.3
Boolesch (LDAPTYPE_BOOLEAN
1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dellsCardConfigAdmin
TRUE, wenn der Benutzer Kartenkonfigurationsrechte auf dem Gerät hat. | 1.2.840.113556.1.8000.1280.1.1.2.4
Boolesch (LDAPTYPE_BOOLEAN
1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dellsUserConfigAdmin
TRUE, wenn der Benutzer Benutzerkonfigurationsrechte auf dem Gerät hat. | 1.2.840.113556.1.8000.1280.1.1.2.5
Boolesch (LDAPTYPE_BOOLEAN
1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dellsLogClearAdmin
TRUE, wenn der Benutzer Protokolllöschungsrechte auf dem Gerät hat. | 1.2.840.113556.1.8000.1280.1.1.2.6
Boolesch (LDAPTYPE_BOOLEAN
1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dellsServerResetUser
TRUE, wenn der Benutzer Server-Reset-Rechte auf dem Gerät hat. | 1.2.840.113556.1.8000.1280.1.1.2.7
Boolesch (LDAPTYPE_BOOLEAN
1.3.6.1.4.1.1466.115.121.1.7) | TRUE |

| Attributname/Beschreibung | Zugewiesener OID/Syntax-Objektkennzeichner | Einzelbewertung |
|--|--|-----------------|
| dellConsoleRedirectUser
TRUE, wenn der Benutzer über Virtuelle-Konsole-Rechte auf dem Gerät verfügt. | 1.2.840.113556.1.8000.1280.1.1.2.8
Boolesch (LDAPTYPE_BOOLEAN
1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dellVirtualMediaUser
TRUE, wenn der Benutzer Rechte für den virtuellen Datenträger auf dem Gerät hat. | 1.2.840.113556.1.8000.1280.1.1.2.9
Boolesch (LDAPTYPE_BOOLEAN
1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dellTestAlertUser
TRUE, wenn der Benutzer Testwarnungsbenutzerrechte auf dem Gerät hat. | 1.2.840.113556.1.8000.1280.1.1.2.10
Boolesch (LDAPTYPE_BOOLEAN
1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dellDebugCommandAdmin
TRUE, wenn der Benutzer Debug-Befehl-Admin-Rechte auf dem Gerät hat. | 1.2.840.113556.1.8000.1280.1.1.2.11
Boolesch (LDAPTYPE_BOOLEAN
1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dellSchemaVersion
Die aktuelle Schemaversion wird verwendet, um das Schema zu aktualisieren. | 1.2.840.113556.1.8000.1280.1.1.2.12
Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING
1.2.840.113556.1.4.905) | TRUE |
| dellRacType
Dieses Attribut ist der aktuelle RAC-Typ für das dellRacDevice-Objekt und der Rückwärtslink zum dellAssociationObjectMembers-Vorwärtslink. | 1.2.840.113556.1.8000.1280.1.1.2.13
Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING
1.2.840.113556.1.4.905) | TRUE |
| dellAssociationMembers
Liste der dellAssociationObjectMembers, die diesem Produkt angehören. Dieses Attribut ist die Rückwärtsverknüpfung zum verknüpften dellProductMembers-Attribut.
Link-ID: 12071 | 1.2.840.113556.1.8000.1280.1.1.2.14
Eindeutiger Name (LDAPTYPE_DN
1.3.6.1.4.1.1466.115.121.1.12) | FALSE |

Dell-Erweiterung zu Active Directory Benutzer- und Computer-Snap-In installieren

Wenn Sie das Schema im Active Directory erweitern, müssen Sie auch das Active Directory-Benutzer- und -Computer-Snap-In erweitern, so dass der Administrator iDRAC7-Geräte, Benutzer und Benutzergruppen, iDRAC7-Zuordnungen und iDRAC7-Berechtigungen verwalten kann.

Wenn Sie die Systems Management Software mit der DVD *Dell Systems Management Tools and Documentation* installieren, können Sie das Snap-In erweitern, indem Sie während des Installationsverfahrens die Option **Snap-In von Active Directory-Benutzern und -Computern** auswählen. Das Schnellinstallationshandbuch zu Dell OpenManage-Software enthält zusätzliche Anleitungen zur Installation von Systemverwaltungssoftware. Die Snap-In-Installation für 64-Bit-Versionen von Windows finden Sie unter:

<DVD-Laufwerk>\SYSTEMGMTManagementStation\support\OMActiveDirectory_SnapIn64

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

iDRAC7-Benutzer und -Berechtigungen zum Active Directory hinzufügen

Mit dem von Dell erweiterten Active Directory-Benutzer- und -Computer-Snap-In können Sie iDRAC7-Benutzer und -Berechtigungen hinzuzufügen, indem Sie Gerät-, Zuordnungs- und Berechtigungsobjekte erstellen. Um die einzelnen Objekte hinzuzufügen, führen Sie folgende Verfahren durch:

- Erstellen eines iDRAC7-Geräteobjekts
- Erstellen eines Berechtigungsobjekts
- Erstellen eines Zuordnungsobjekts
- Einem Zuordnungsobjekt Objekte hinzufügen

Verwandte Links

[Hinzufügen von Objekten zu einem Zuordnungsobjekt](#)

[iDRAC7-Geräteobjekt erstellen](#)

[Berechtigungsobjekt erstellen](#)

[Zuordnungsobjekt erstellen](#)


iDRAC7-Geräteobjekt erstellen

So erstellen Sie ein iDRAC7-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**.
Das Fenster **Neues Objekt** wird angezeigt.
3. Geben Sie einen Namen für das neue Objekt ein. Dieser Name muss mit dem iDRAC7-Namen identisch sein, den Sie im Rahmen der Konfiguration der Active Directory-Eigenschaften über die iDRAC7-Web-Schnittstelle 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-Verwaltungsobjekt erweitert** aus.
Das Fenster **Neues Objekt** wird angezeigt.
3. Geben Sie einen Namen für das neue Objekt ein.
4. Wählen Sie **Berechtigungsobjekt** und klicken Sie auf OK.
5. Klicken Sie mit der rechten Maustaste auf das Berechtigungsobjekt, das Sie erstellt haben, und wählen Sie **Eigenschaften** aus.
6. Klicken Sie auf die Registerkarte **Remote-Verwaltungsberechtigungen**, und weisen Sie die Berechtigungen für den Benutzer oder die Gruppe zu.

Zuordnungsobjekt erstellen

So erstellen Sie ein Zuordnungsobjekt:

 **ANMERKUNG:** Das iDRAC7-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.

Verwandte Links

[Benutzerzugriffsberechtigungen für verknüpfte Objekte bereitstellen](#)

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-Editor**. Daraufhin wird das Fenster **ADSI-Editor** angezeigt.
2. Wechseln Sie im rechten Bereich zum angelegten Zuordnungsobjekt, klicken Sie auf die rechte Maustaste und wählen Sie **Eigenschaften**.
3. Klicken Sie in der Registerkarte **Sicherheit** auf **Hinzufügen**.
4. Geben Sie `Authentifizierte Benutzer` ein, klicken Sie auf **Namen überprüfen**, und klicken Sie dann auf **OK**. Die authentifizierten Benutzer werden zur Liste der **Gruppen- oder Benutzernamen** hinzugefügt.
5. Klicken Sie auf **OK**.

Hinzufügen von Objekten zu einem Zuordnungsobjekt

Durch die Verwendung des Fensters **Zuordnungsobjekt-Eigenschaften** können Sie Benutzer oder Benutzergruppen, Berechtigungsobjekte und iDRAC7-Geräte oder iDRAC7-Gerätegruppen zuordnen.

Sie können Benutzergruppen und iDRAC7-Geräte hinzufügen.

Verwandte Links

[Benutzer oder Benutzergruppen hinzufügen](#)

[Berechtigungen hinzufügen](#)

[Hinzufügen von iDRAC7-Geräten oder iDRAC7-Gerätegruppen](#)

Benutzer oder Benutzergruppen hinzufügen

So fügen Sie Benutzer oder Benutzergruppen hinzu:

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

Berechtigungen hinzufügen

So fügen Sie Berechtigungen hinzu:

Klicken Sie auf das Register **Berechtigungsobjekt**, um das Berechtigungsobjekt der Zuordnung hinzuzufügen, welche die Berechtigungen des Benutzers bzw. der Benutzergruppe bei Authentifizierung eines iDRAC7-Geräts definiert. Einem Zuordnungsobjekt kann nur ein Berechtigungsobjekt hinzugefügt werden.

1. Wählen Sie das Register **Berechtigungsobjekt** und klicken Sie auf **Hinzufügen**.
2. Geben Sie den Namen des Berechtigungsobjekts ein und klicken Sie auf **OK**.
3. Klicken Sie auf das Register **Berechtigungsobjekt**, um das Berechtigungsobjekt der Zuordnung hinzuzufügen, welche die Berechtigungen des Benutzers bzw. der Benutzergruppe bei Authentifizierung eines iDRAC7-Geräts definiert. Einem Zuordnungsobjekt kann nur ein Berechtigungsobjekt hinzugefügt werden.

Hinzufügen von iDRAC7-Geräten oder iDRAC7-Gerätegruppen

Um iDRAC7-Geräte oder iDRAC7-Gerätegruppen hinzuzufügen:

1. Wählen Sie die Registerkarte **Produkte** und klicken Sie auf **Hinzufügen**.
2. Geben Sie die Namen der iDRAC7-Geräte oder iDRAC7-Gerätegruppen ein und klicken Sie auf **OK**.
3. Im Fenster **Eigenschaften** klicken Sie auf **Anwenden** und dann auf **OK**.
4. Wählen Sie das Register **Produkte** und fügen Sie ein iDRAC7-Gerät hinzu, das mit dem Netzwerk verbunden ist, das den definierten Benutzern oder Benutzergruppen zur Verfügung steht. Einem Zuordnungsobjekt können mehrere iDRAC7-Geräte hinzugefügt werden.

Active Directory mit erweitertem Schema unter Verwendung der iDRAC7-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 *iDRAC7-Online-Hilfe*.

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Benutzerauthentifizierung** → **Verzeichnisdienste** → **Microsoft Active Directory**.

Die **Active Directory**-Zusammenfassungsseite wird angezeigt.

2. Klicken Sie auf **Active Directory konfigurieren**.

Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 1 von 4 wird angezeigt.

3. 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.

4. Klicken Sie auf **Weiter**.

Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 2 von 4 wird angezeigt.

5. Geben Sie die Speicherortinformationen für die Active Directory (AD)-Server und Benutzerkonten an. Geben Sie außerdem die Dauer an, die iDRAC7 im Rahmen des Anmeldeprozesses auf Antworten von AD warten muss.



ANMERKUNG: Wenn die Zertifikatvalidierung aktiviert ist, geben Sie die Adressen des Domain Controller Server und von FQDN an. Stellen Sie sicher, dass DNS unter **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** ordnungsgemäß konfiguriert ist.

6. Klicken Sie auf **Weiter**. Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 3 von 4 wird angezeigt.

7. Wählen Sie **Erweitertes Schema** aus, und klicken Sie auf **Weiter**.

Die Seite **Active Directory-Konfiguration und -Verwaltung** Schritt 4 von 4 wird angezeigt.

8. Geben Sie den Namen und den Speicherort des iDRAC7-Geräteobjekts unter Active Directory (AD) an, und klicken Sie auf **Fertigstellen**.

Die Active Directory-Einstellungen für den Modus „Erweitertes Schema“ wird konfiguriert.

Konfiguration des Active Directory mit erweitertem Schema unter Verwendung von RACADM

So konfigurieren Sie Active Directory mit erweitertem Schema unter Verwendung von RACADM:

1. Öffnen Sie eine Eingabeaufforderung und geben Sie die folgenden RACADM-Befehle ein:


- Verwenden des Befehls **config**:

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g
cfgActiveDirectory -o cfgADType 1 racadm config -g cfgActiveDirectory -
o cfgADName <allgemeiner RAC-Name> racadm config -g
cfgActiveDirectory -o cfgADDomain <vollständig qualifizierter
Domänenname> racadm config -g cfgActiveDirectory -o
cfgADDomainController1 <vollständig qualifizierter Domänenname oder IP-
Adresse des Domänen-Controllers> racadm config -g cfgActiveDirectory -
```

```
o cfgADDomainController2 <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers> racadm config -g cfgActiveDirectory -o cfgADDomainController3 vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
```


– Verwenden des Befehls **set**:

```
racadm set iDRAC.ActiveDirectory.Enable 1 racadm set iDRAC.ActiveDirectory.Schema 2 racadm set iDRAC.ActiveDirectory.RacName <allgemeiner RAC-Name> racadm set iDRAC.ActiveDirectory.RacDomain <vollständig qualifizierter Domänenname> racadm set iDRAC.ActiveDirectory.DomainController1 <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers> racadm set iDRAC.ActiveDirectory.DomainController2 <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers> racadm set iDRAC.ActiveDirectory.DomainController3 <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>
```

 **ANMERKUNG:** Sie müssen mindestens eine der drei Adressen konfigurieren. iDRAC7 versucht so lange, nacheinander mit jeder der konfigurierten Adressen eine Verbindung herzustellen, bis eine Verbindung hergestellt werden konnte. Mit erweitertem Schema sind dies der FQDN oder die IP-Adresse des Domänen-Controllers, auf dem sich das iDRAC7-Gerät befindet.

So deaktivieren Sie die Zertifikatvalidierung während eines SSL-Handshake (optional):

- Verwenden des Befehls **config**: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0`
- Verwenden des Befehls **set**: `racadm set iDRAC.ActiveDirectory.CertValidationEnable 0`


 **ANMERKUNG:** In diesem Fall brauchen Sie kein CA-Zertifikat zu laden.

So erzwingen Sie die Zertifikatvalidierung während eines SSL-Handshake (optional):

- Verwenden des Befehls **config**: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1`
- Verwenden des Befehls **set**: `racadm set iDRAC.ActiveDirectory.CertValidationEnable 1`

In diesem Fall müssen Sie ein Zertifizierungsstellenzertifikat hochladen:

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

 **ANMERKUNG:** Wenn die Zertifikatvalidierung aktiviert ist, geben Sie die Adressen des Domain Controller Server und von FQDN an. Stellen Sie sicher, dass DNS unter **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** ordnungsgemäß konfiguriert ist.

Die Verwendung des folgenden RACADM-Befehls kann optional sein.

```
racadm sslcertdownload -t 0x1 -f <RAC-SSL-Zertifikat>
```

2. Wenn DHCP auf dem iDRAC7 aktiviert ist und Sie den vom DHCP-Server bereitgestellten DNS verwenden möchten, geben Sie folgenden RACADM-Befehl ein:

- Verwenden des Befehls **config**: `racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1`
- Verwenden des Befehls **set**: `racadm set iDRAC.IPv4.DNSFromDHCP 1`

3. Wenn DHCP auf dem iDRAC7 deaktiviert ist oder Sie ihre DNS IP-Adresse manuell eingeben möchten, arbeiten Sie mit den folgenden RACADM-Befehlen:

- Verwenden des Befehls **config**:
`racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0 racadm config -g cfgLanNetworking -o cfgDNSServer1 <primäre DNS-IP-Adresse>`

```
racadm config -g cfgLanNetworking -o cfgDNSServer2 <sekundäre DNS-IP-Adresse>
```

- **Verwenden des Befehls `set`:**

```
racadm set iDRAC.IPv4.DNSFromDHCP 0 racadm set  
iDRAC.IPv4.DNSFromDHCP.DNS1 <primäre DNS-IP-Adresse> racadm set  
iDRAC.IPv4.DNSFromDHCP.DNS2 <sekundäre DNS-IP-Adresse>
```

4. Möchten Sie eine Liste mit Benutzerdomänen konfigurieren, sodass für die Anmeldung an der iDRAC7-Webschnittstelle nur der Benutzername eingegeben werden muss, verwenden Sie dazu den folgenden Befehl:

- **Verwenden des Befehls `config`:** `racadm config -g cfgUserDomain -o cfgUserDomainName <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers> -i <Index>`
- **Verwenden des Befehls `set`:** `racadm set iDRAC.UserDomain.<Index>.Name <vollständig qualifizierter Domänenname oder IP-Adresse des Domänen-Controllers>`

Sie können bis zu 40 Benutzerdomänen mit Indexpunkten zwischen 1 und 40 konfigurieren.

5. Drücken Sie die **Eingabetaste**, um die Konfiguration des Active Directory mit erweitertem Schema abzuschließen.

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 iDRAC7-Web-Schnittstelle testen

So testen Sie die Active Directory-Einstellungen:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Benutzerauthentifizierung** → **Verzeichnisdienste** → **Microsoft Active Directory**.

Die **Active Directory**-Zusammenfassungsseite wird angezeigt.

2. Klicken Sie auf **Testeinstellungen**.
3. Geben Sie einen Test-Benutzernamen (z. B. **Benutzername@domain.com**) und ein Kennwort ein, und klicken Sie dann auf **Test starten**. Daraufhin werden detaillierte Testergebnisse und ein Testprotokoll angezeigt. Überprüfen Sie gegebenenfalls die einzelnen Fehlermeldungen und mögliche Lösungen im Testprotokoll.

 **ANMERKUNG:** Wenn die Active Directory-Einstellungen überprüft werden und dabei "Zertifikatsüberprüfung aktiviert" ausgewählt ist, erfordert iDRAC7, 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 iDRAC7 nicht mit dem Active Directory-Server kommunizieren kann.

Active Directory-Einstellungen über RACADM testen


Um die Active Directory-Einstellungen zu testen, verwenden Sie den Befehl `testfeature`. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Konfigurieren von allgemeinen LDAP-Benutzern

iDRAC7 bietet eine allgemeine Lösung zur Unterstützung LDAP-basierter Authentifizierung (Lightweight Directory Access Protocol). Für diese Funktion ist auf Ihren Verzeichnisdiensten keine Schemaerweiterung erforderlich.

Um die iDRAC7 LDAP-Implementierung generisch zu gestalten, werden die Gemeinsamkeiten der verschiedenen Verzeichnisdienste dazu genutzt, Benutzer in Gruppen zusammenzufassen und danach die Beziehung zwischen Benutzer und Gruppe festzulegen. Die Verzeichnisdienst-spezifische Maßnahme ist hierbei das Schema. Es können

beispielsweise verschiedene Attributnamen für die Gruppe, Benutzer und die Verbindung zwischen dem Benutzer und der Gruppe vergeben werden. Diese Maßnahmen können im iDRAC7 konfiguriert werden.

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

Verwandte Links

[Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mit der iDRAC7-Webschnittstelle](#)

[Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mittels RACADM](#)

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mit der iDRAC7-Webschnittstelle


So konfigurieren Sie den generischen LDAP-Verzeichnisdienst über die Web-Schnittstelle:

 **ANMERKUNG:** Weitere Informationen zu den verschiedenen Feldern finden Sie in der *iDRAC7-Online-Hilfe*.

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Benutzerauthentifizierung** → **Verzeichnisdienste** → **Generischer LDAP-Verzeichnisdienst**.

Die Seite **Generisches LDAP - Konfiguration und Verwaltung** zeigt die aktuellen Einstellungen für das generische LDAP an.

2. Klicken Sie auf **Generischen LDAP-Verzeichnisdienst konfigurieren**.
3. Aktivieren Sie optional Zertifikatsvalidierung und laden Sie das digitale Zertifikat hoch, das Sie zum Aufbau von SSL-Verbindungen bei der Kommunikation mit einem generischen LDAP-Server verwendet haben.


 **ANMERKUNG:** Bei dieser Version wird eine LDAP-Bindung, die nicht auf einem SSL-Anschluss basiert, nicht unterstützt. Nur LDAP über SSL wird unterstützt.

4. Klicken Sie auf **Weiter**.

Die Seite **Allgemeines LDAP – Konfiguration und Verwaltung** Schritt 2 von 3 wird angezeigt.

5. Aktivieren Sie die generische LDAP-Authentifizierung, und geben Sie die Speicherortinformationen zu den generischen LDAP-Servern und -Benutzerkonten an.

 **ANMERKUNG:** Wenn die Zertifikatsvalidierung aktiviert ist, geben Sie die FQDN des LDAP-Servers an, und stellen Sie sicher, dass DNS unter **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** korrekt konfiguriert ist.

 **ANMERKUNG:** Bei dieser Version werden verschachtelte Gruppen nicht unterstützt. Die Firmware sucht nach dem Mitglied der Gruppe, das dem Benutzer-DN entspricht. Weiterhin wird nur Einzeldomäne unterstützt. Übergreifende Domänen werden nicht unterstützt.


6. Klicken Sie auf **Weiter**.

Die Seite **Allgemeines LDAP – Konfiguration und Verwaltung** Schritt 3a von 3 wird angezeigt.

7. Klicken Sie auf **Rollengruppe**.

Die Seite **Allgemeines LDAP – Konfiguration und Verwaltung** Schritt 3b von 3 wird angezeigt.

8. 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 Rollengruppeneinstellungen werden gespeichert. Die Seite **Allgemeines LDAP - Konfiguration und Verwaltung – Schritt 3a von 3** zeigt die Rollengruppeneinstellungen an.

9. Wenn Sie weitere Rollengruppen konfigurieren möchten, wiederholen Sie die Schritte 7 und 8.
10. Klicken Sie auf **Fertigstellen**. Der generische LDAP-Verzeichnisdienst ist damit konfiguriert.

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mittels RACADM

So konfigurieren Sie den LDAP Directory-Dienst:

- Verwenden Sie die Objekte in den Gruppen **cfgLdap** und **cfgLdapRoleGroup** mit dem Befehl **config**.
- Verwenden Sie die Objekte in den Gruppen **iDRAC.LDAP** und **iDRAC.LDAPRole** mit dem Befehl **set**.

Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.

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.


Einstellungen des LDAP-Verzeichnisdienstes über die iDRAC7-Web-Schnittstelle testen


So testen Sie die Einstellungen für den LDAP-Verzeichnisdienst:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Benutzerauthentifizierung** → **Verzeichnisdienste** → **Allgemeiner LDAP-Verzeichnisdienst**.

Die Seite **Generisches LDAP - Konfiguration und Verwaltung** zeigt die aktuellen Einstellungen für das generische LDAP an.

2. Klicken Sie auf **Einstellungen testen**.
3. Geben Sie den Benutzernamen und das Kennwort eines Verzeichnisbenutzers ein, der zur Überprüfung der LDAP-Einstellungen ausgewählt wurde. Das Format hängt davon ab, welches *Attribut der Benutzeranmeldung* verwendet wird, und der eingegebene Benutzername muss dem Wert des gewählten Attributs entsprechen.

 **ANMERKUNG:** Wenn die LDAP-Einstellungen überprüft werden und dabei "Zertifikatsüberprüfung aktiviert" ausgewählt ist, erfordert iDRAC7, 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 iDRAC6 nicht mit dem LDAP-Server kommunizieren kann.

 **ANMERKUNG:** Wenn generisches LDAP aktiviert ist, versucht iDRAC7 zunächst, den Benutzer als Verzeichnis-Benutzer anzumelden. Schlägt dies fehl, wird die Suche nach lokalen Benutzern aktiviert.

Die Testergebnisse und das Testprotokoll werden angezeigt.

LDAP-Verzeichnisdiensteinstellungen über RACADM testen

Um die LDAP-Verzeichnisdiensteinstellungen zu testen, verwenden Sie den Befehl `testfeature`. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

iDRAC7 für die einfache Anmeldung oder Smart Card-Anmeldung konfigurieren

In diesem Abschnitt erhalten Sie Informationen zur Konfiguration von iDRAC7 für die Smart Card-Anmeldung (für lokale und Active Directory-Benutzer) und die einmalige Anmeldung (SSO, für Active Directory-Benutzer.) Die SSO- und Smart Card-Anmeldungen sind lizenzierte Funktionen.

iDRAC7 unterstützt die Kerberos-basierte Active Directory-Authentifizierung für die Unterstützung von Smart Card- und SSO-Anmeldungen. Weitere Informationen zu Kerberos finden Sie auf der Microsoft-Website.

Verwandte Links

[iDRAC7-SSO-Anmeldung für Active Directory-Benutzer konfigurieren](#)


[iDRAC7-Smart Card-Anmeldung für lokale Benutzer konfigurieren](#)

[iDRAC7-Smart-Card-Anmeldung für Active Directory-Benutzer konfigurieren](#)

Voraussetzungen für die einmalige Active Directory-Anmeldung oder die Smart Card-Anmeldung

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

- Synchronisieren Sie die iDRAC7-Zeit mit der Zeit des Active Directory-Domänen-Controllers. Wenn nicht, schlägt die Kerberos-Authentifizierung auf iDRAC7 fehl. Sie können die Funktion für Zeitzone und NTP verwenden, um die Zeit zu synchronisieren. Siehe dazu [Konfigurieren von Zeitzone und NTP](#).
- Registrieren Sie den iDRAC7 als Computer in der Active Directory-Root-Domäne.
- Generieren Sie eine Keytab-Datei über das Ktpass-Tool.
- Um die einmalige Anmeldung für das erweiterte Schema zu aktivieren, stellen Sie sicher, dass die Option **Diesem Benutzer für die Delegation zu einem beliebigen Dienst vertrauen (nur Kerberos)** auf der Registerkarte **Delegation** für den Keytab-Benutzer ausgewählt ist. Diese Registerkarte ist erst verfügbar, nachdem die Keytab-Datei über das ktpass-Dienstprogramm erstellt wurde.
- Konfigurieren Sie den Browser für die Aktivierung der SSO-Anmeldung.
- Erstellen Sie die Active Directory-Objekte, und stellen Sie die erforderlichen Berechtigungen bereit.
- Konfigurieren Sie für SSO auf den DNS-Servern die Zone für die Rückwärtssuche für das Subnetz, auf dem sich iDRAC7 befindet.

 **ANMERKUNG:** Wenn der Host-Name mit der DNS-Rückwärtssuche nicht übereinstimmt, schlägt die Kerberos-Authentifizierung fehl.

Verwandte Links

[Browser zum Aktivieren der Active Directory-SSO konfigurieren](#)

[iDRAC7 als einen Computer in der Active Directory-Stammdomäne registrieren](#)

[Kerberos Keytab-Datei generieren](#)

[Active Directory-Objekte erstellen und Berechtigungen bereitstellen](#)

iDRAC7 als einen Computer in der Active Directory-Stammdomäne registrieren

So registrieren Sie iDRAC7 in der Active Directory-Stammdomäne:

1. Klicken Sie auf **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Netzwerk**.
Die Seite **Netzwerk** wird angezeigt.
2. Stellen Sie eine gültige IP-Adresse für den **bevorzugten/alternativen DNS-Server** bereit. Dieser Wert steht für eine gültige IP-Adresse für den DNS-Server, der Teil der Stammdomäne ist.
3. Wählen Sie **iDRAC auf DNS registrieren** aus.
4. Geben Sie einen gültigen **DNS-Domännennamen** an.
5. 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 *iDRAC7-Online-Hilfe*.

Kerberos Keytab-Datei generieren

Zur Unterstützung der SSO- und Smart Card-Anmeldungs-Authentifizierung unterstützt iDRAC7 die Konfiguration zur Selbstaktivierung als Kerberos-Dienst in einem Windows-Kerberos-Netzwerk. Die Kerberos-Konfiguration am iDRAC6 umfasst dieselben Schritte wie die Konfiguration eines Kerberos-Dienstes als Sicherheitsprinzipal in Windows Server Active Directory auf einem Nicht-Windows-Server.

Mit dem *ktpass*-Hilfsprogramm (wird von Microsoft als Teil der Server-Installations-CD/DVD bereitgestellt) werden die Bindungen des Dienstprinzipalnamens (SPN =Service Principal Name) zu einem Benutzerkonto erstellt und die Vertrauensinformationen in eine MIT-artige Kerberos-*Keytab*-Datei exportiert, die eine Vertrauensbeziehung zwischen einem externen Benutzer oder System und dem Schlüsselverteilungscenter (KDC = Key Distribution Centre) aktiviert. Die Keytab-Datei enthält einen kryptografischen Schlüssel, der zum Verschlüsseln der Informationen zwischen Server und KDC dient. Das Hilfsprogramm "ktpass" ermöglicht es UNIX-basierten Diensten, die Kerberos-Authentifizierung unterstützen, die von einem Kerberos-KDC-Dienst für Windows Server bereitgestellten Interoperabilitätsfunktionen zu verwenden. Weitere Informationen zum Dienstprogramm **ktpass** finden Sie auf der Microsoft-Website unter: [technet.microsoft.com/en-us/library/cc779157\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc779157(WS.10).aspx)


Sie müssen vor dem Erstellen einer Keytab-Datei ein Active Directory-Benutzerkonto zur Benutzung mit der Option **-mapuser** des Befehls *ktpass* einrichten. Außerdem müssen Sie denselben Namen verwenden wie den iDRAC7-DNS-Namen, zu dem Sie die erstellte Keytab-Datei hochladen.

So generieren Sie eine Keytab-Datei mithilfe des *ktpass*-Tools:

1. Führen Sie das Dienstprogramm *ktpass* auf dem Domänen-Controller (Active Directory-Server) aus, auf dem Sie den iDRAC7 einem Benutzerkonto 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 DES-CBC-MD5 -ptype
KRB5_NT_PRINCIPAL -pass [password] +DesOnly -out c:\krbkeytab
```


Der Verschlüsselungstyp lautet DES-CBC-MD5. Der Prinzipaltyp lautet KRB5_NT_PRINCIPAL. Die Eigenschaften des Benutzerkontos, dem der Dienstprinzipalname zugeordnet ist, muss die Eigenschaft DES-Verschlüsselungstypen für dieses Konto verwenden aktiviert haben.

 **ANMERKUNG:** Verwenden Sie – gemäß dem Beispiel – Kleinbuchstaben für den **iDRAC7-Namen** und die **Service-Prinzip-Bezeichnung** und Großbuchstaben für den Domännennamen.

3. Führen Sie den folgenden Befehl aus:

```
C:\>setspn -a HTTP/idrac7name.domainname.com username
```

Es wird eine Keytab-Datei generiert.

 **ANMERKUNG:** Wenn beim iDRAC7-Benutzer, für den die Keytab-Datei erstellt wird, Probleme auftreten, erstellen Sie bitte einen neuen Benutzer und eine neue Keytab-Datei. Wenn dieselbe Keytab-Datei, die ursprünglich erstellt wurde, erneut ausgeführt wird, wird sie nicht korrekt konfiguriert.

Active Directory-Objekte erstellen und Berechtigungen bereitstellen

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 Zuordnungsobjekt im Active Directory-Server.
2. Einstellung von Zugangsberechtigungen für das angelegte Berechtigungsobjekt. Es wird empfohlen, keine Administratorberechtigungen zu vergeben, da hiermit einige Sicherheitsprüfungen umgangen werden könnten.
3. Ordnen Sie das Geräteobjekt und das Berechtigungsobjekt mit dem Zuordnungsobjekt zu.
4. Fügen Sie dem Geräteobjekt den vorherigen SSO-Benutzer (anmeldender Benutzer) zu.
5. Vergeben Sie die Zugangsberechtigung zum Zugriff auf das angelegte Zuordnungsobjekt an *authentifizierte Benutzer*.

Verwandte Links

[iDRAC7-Benutzer und -Berechtigungen zum Active Directory hinzufügen](#)

Browser zum Aktivieren der Active Directory-SSO konfigurieren

In diesem Abschnitt werden die Browser-Einstellungen für Internet Explorer und Firefox für die Aktivierung von Active Directory SSO angezeigt.



ANMERKUNG: Google Chrome und Safari unterstützen Active Directory für die SSO-Anmeldung nicht.

Internet Explorer für die Aktivierung von Active Directory SSO konfigurieren

So konfigurieren Sie die Browser-Einstellungen für Internet Explorer:

1. Navigieren Sie im Internet Explorer zu **Lokales Intranet**, und klicken Sie dann auf **Sites**.
2. Wählen Sie nur die folgenden Optionen aus:
 - Schließen Sie alle lokalen (Intranet-) Sites ein, die nicht auf anderen Zonen aufgeführt sind.
 - Schließen Sie alle Sites ein, die den Proxy-Server umgehen.
3. Klicken Sie auf **Erweitert**.
4. Fügen Sie alle betreffenden Domännennamen ein, die für iDRAC7-Instanzen, die Teil der SSO-Konfiguration sind, verwendet werden (z. B. **myhost.example.com**.)
5. Klicken Sie auf **Schließen** und anschließend auf **OK** zweimal.

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** `network.negotiate` ein.
3. Fügen Sie den iDRAC7-Namen zu `network.negotiate-auth.trusted-uris` (kommaseparierte Liste verwenden) hinzu.
4. Fügen Sie den iDRAC7-Namen zu `network.negotiate-auth.elegation-uris` (kommaseparierte Liste verwenden) hinzu.

iDRAC7-SSO-Anmeldung für Active Directory-Benutzer konfigurieren

Stellen Sie vor der Konfiguration von iDRAC7 für die Active Directory-SSO-Anmeldung sicher, dass alle Voraussetzungen erfüllt sind.


Sie können iDRAC7 für Active Directory-SSO konfigurieren, wenn Sie ein Benutzerkonto auf der Basis von Active Directory einrichten.

Verwandte Links

- [Voraussetzungen für die einmalige Active Directory-Anmeldung oder die Smart Card-Anmeldung](#)
- [Active Directory mit Standardschema unter Verwendung der iDRAC7-Webschnittstelle konfigurieren](#)
- [Konfiguration des Active Directory mit Standardschema unter Verwendung von RACADM](#)
- [Active Directory mit erweitertem Schema unter Verwendung der iDRAC7-Webschnittstelle konfigurieren](#)
- [Konfiguration des Active Directory mit erweitertem Schema unter Verwendung von RACADM](#)

iDRAC7-SSO-Anmeldung für Active Directory-Benutzer über die Web-Schnittstelle konfigurieren

So konfigurieren Sie iDRAC7 für die Active Directory-SSO-Anmeldung:

 **ANMERKUNG:** Weitere Informationen zu diesen Optionen finden Sie in der *iDRAC7-Online-Hilfe*.

- Überprüfen Sie, ob der iDRAC7-DNS-Name mit dem vollständigen, qualifizierten iDRAC7-Domänennamen übereinstimmt. Gehen Sie dazu in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Netzwerk**, und rufen Sie die Eigenschaft **DNS-Domänenname** ab.
- 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.

iDRAC7 SSO-Anmeldung für Active Directory-Benutzer über RACADM konfigurieren

Neben den im Rahmen der Konfiguration von Active Directory ausgeführten Schritten führen Sie zum Aktivieren von SSO den folgenden Befehl aus:

- Verwenden des **config**-Befehls:

```
racadm config -g cfgActiveDirectory -o cfgADSSOEnable 1
```
- Verwenden des **set**-Befehls:

```
racadm set iDRAC.ActiveDirectory.SSOEnable 1
```

iDRAC7-Smart Card-Anmeldung für lokale Benutzer konfigurieren

So konfigurieren Sie einen lokalen iDRAC7-Benutzer für die Smart Card-Anmeldung:

- Laden Sie das Smart Card-Benutzerzertifikat und das vertrauenswürdige Zertifizierungsstellenzertifikat nach iDRAC7 noch.
- Smart Card-Anmeldung aktivieren

Verwandte Links

- [Zertifikate abrufen](#)
- [Smart Card-Benutzerzertifikat hochladen](#)
- [Smart Card-Anmeldung aktivieren oder deaktivieren](#)

Smart Card-Benutzerzertifikat hochladen

Bevor Sie das Benutzerzertifikat hochladen, stellen Sie sicher, dass das Benutzerzertifikat des Smart Card-Anbieters im Base64-Format vorliegt.

Verwandte Links

[Zertifikate abrufen](#)

Smart Card-Benutzerzertifikat über die Web-Schnittstelle hochladen

So laden Sie ein Smart Card-Benutzerzertifikat hoch:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Benutzerauthentifizierung** → **Lokaler Benutzer**.
Die Seite **Benutzer** wird angezeigt.
2. In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.
Die Seite **Benutzer-Hauptmenü** wird angezeigt.
3. Wählen Sie unter **Smart Card-Konfigurationen** die Option **Benutzerzertifikat hochladen** aus, und klicken Sie dann auf **Weiter**.
Daraufhin wird die Seite **Benutzerzertifikat hochladen** angezeigt.
4. Führen Sie einen Suchlauf durch, wählen Sie dann das Base64-Benutzerzertifikat aus, und 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 Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

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.

Verwandte Links

[Zertifikate abrufen](#)

Vertrauenswürdige Zertifizierungsstellenzertifikat für Smart Card über die Web-Schnittstelle hochladen

So laden Sie ein vertrauenswürdige Zertifizierungsstellenzertifikat für die Smart Card-Anmeldung hoch:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk** → **Benutzerauthentifizierung** → **Lokaler Benutzer**.
Die Seite **Benutzer** wird angezeigt.
2. In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer.
Die Seite **Benutzer-Hauptmenü** wird angezeigt.
3. Wählen Sie unter **Smart Card-Konfiguration** die Option **Zertifikat einer vertrauenswürdigen Zertifizierungsstelle hochladen** aus, und klicken Sie dann auf **Weiter**.
Daraufhin wird die Seite **Zertifikat einer vertrauenswürdigen Zertifizierungsstelle hochladen** angezeigt.
4. Suchen Sie das vertrauenswürdige Zertifizierungsstellenzertifikat, und klicken Sie auf **Anwenden**.

Vertrauenswürdige Zertifizierungsstellenzertifikat für Smart Card über RACADM hochladen

Um ein vertrauenswürdige Zertifikat einer vertrauenswürdigen Zertifizierungsstelle für die Smart Card-Anmeldung hochzuladen, verwenden Sie das Objekt **usercertupload**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

iDRAC7-Smart-Card-Anmeldung für Active Directory-Benutzer konfigurieren

Vor der Konfiguration der iDRAC7-Smart-Card-Anmeldung für Active Directory-Benutzer müssen Sie sicherstellen, dass die erforderlichen Voraussetzungen erfüllt sind.

So konfigurieren Sie iDRAC7 für die Smart Card-Anmeldung:

1. Führen Sie über die iDRAC7-Web-Schnittstelle, 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 vertrauenswürdige, von einer Zertifikatzertifizierungsstelle signiertes Zertifikat hoch.
 - Laden Sie die Keytab-Datei hoch.
2. Aktivieren Sie die Smart Card-Anmeldung. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC7-Online-Hilfe*.

Verwandte Links

[Smart Card-Anmeldung aktivieren oder deaktivieren](#)

[Zertifikate abrufen](#)

[Kerberos Keytab-Datei generieren](#)

[Active Directory mit Standardschema unter Verwendung der iDRAC7-Webschnittstelle konfigurieren](#)

[Konfiguration des Active Directory mit Standardschema unter Verwendung von RACADM](#)

[Active Directory mit erweitertem Schema unter Verwendung der iDRAC7-Webschnittstelle konfigurieren](#)

[Konfiguration des Active Directory mit erweitertem Schema unter Verwendung von RACADM](#)

Smart Card-Anmeldung aktivieren oder deaktivieren

Vor der Aktivierung oder Deaktivierung der Smart Card-Anmeldung für iDRAC7 müssen Sie Folgendes sicherstellen:

- Die iDRAC7-Berechtigungen sind konfiguriert.
- Die lokale iDRAC7-Benutzerkonfiguration oder die Active Directory-Benutzerkonfiguration mit den entsprechenden Zertifikaten ist abgeschlossen.



ANMERKUNG: Wenn die Smart Card-Anmeldung aktiviert ist, sind SSH, Telnet, IPMI über LAN, Serielle Verbindung über LAN und Remote-RACADM deaktiviert. Zur Erinnerung: Wenn die Smart Card-Anmeldung deaktiviert ist, werden die Schnittstellen nicht automatisch aktiviert.

Verwandte Links

[Zertifikate abrufen](#)

[iDRAC7-Smart-Card-Anmeldung für Active Directory-Benutzer konfigurieren](#)

[iDRAC7-Smart Card-Anmeldung für lokale Benutzer konfigurieren](#)

Smart Card-Anmeldung über die Web-Schnittstelle aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die Smart Card-Anmeldefunktion:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle nach **Übersicht** → **iDRAC-Einstellungen** → **Benutzerauthentifizierung** → **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. Wählen Sie ansonsten die Option **Deaktiviert** aus.
Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC7-Online-Hilfe*.
3. Klicken Sie auf **Übernehmen**, um die Einstellungen zu übernehmen.
Bei nachfolgenden Anmeldeversuchen über die iDRAC7-Web-Schnittstelle werden Sie dazu aufgefordert, eine Smart Card-Anmeldung auszuführen.

Smart Card-Anmeldung über RACADM aktivieren oder deaktivieren

Zur Aktivierung der Smart Card-Anmeldung nutzen Sie einen der folgenden Befehle:

- Verwenden Sie die Objekte in der Gruppe **cfgSmartCard** mit dem Befehl **config**.
- Verwenden Sie die Objekte in der Gruppe **iDRAC.SmartCard** mit dem Befehl **set**.

Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.

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 die Option **Aktiviert** aus, um die Smart Card-Anmeldung zu aktivieren. Oder wählen Sie **Deaktiviert** aus.
Weitere Informationen zu diesen 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.

iDRAC7 für das Versenden von Warnungen konfigurieren

Sie können Warnungen und Maßnahmen für bestimmte Ereignisse festlegen, die auf dem Managed System auftreten. Ein Ereignis tritt auf, wenn der Status einer Systemkomponente vom vordefinierten Zustand abweicht. Wenn ein Ereignis mit einem Ereignisfilter übereinstimmt und Sie diesen Filter für die Generierung einer Warnung konfiguriert haben (per E-Mail, SNMP-Trap, IPMI-Warnung, Remote-Systemprotokolle oder WS-Ereignisse), wird eine Warnung an ein oder mehrere konfigurierte Ziele versendet. Wenn der gleiche Ereignisfilter auch zum Ausführen einer Maßnahme (z. B. Neustart, Aus- und Einschalten oder Ausschalten des Systems) konfiguriert wurde, wird diese Maßnahme ausgeführt. Sie können für jedes Ereignis nur eine Maßnahme festlegen.

So konfigurieren Sie iDRAC7 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-Warnung, IPMI-Warnung, SNMP-Trap, Remote System-Protokoll und/oder WS-Ereignis-Einstellungen.
4. Aktivieren Sie die folgenden Ereigniswarnungen und Maßnahmen:
 - Senden Sie eine E-Mail-Wanung, IPMI-Warnung, SNMP-Traps, Remote System-Protokolle oder WS-Ereignisse 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.

Verwandte Links

[Warnungen aktivieren und deaktivieren](#)

[Warnungen filtern](#)

[Ereigniswarnungen einrichten](#)

[Alarmwiederholungseignis einrichten](#)

[Einstellungen für E-Mail-Warnungs-SNMP-Trap oder IPMI-Trap konfigurieren](#)

[Remote-Systemprotokollierung konfigurieren](#)

[Konfigurieren von WS-Ereignisauslösung](#)

[IDs für Warnungsmeldung](#)

Warnungen aktivieren und deaktivieren

Zum Senden einer Warnung an konfigurierte Ziele oder zum Ausführen einer Ereignismaßnahme müssen Sie die globale Warnoption aktivieren. Diese Eigenschaft überschreibt die individuell festgelegten Warnungen oder Ereignismaßnahmen.

Verwandte Links

[Warnungen filtern](#)

[Einstellungen für E-Mail-Warnungs-SNMP-Trap oder IPMI-Trap konfigurieren](#)

Warnungen über die Web-Schnittstelle aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die Generierung von Warnungen:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Warnungen**. Daraufhin wird die Seite **Warnungen** 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.

Warnungen über RACADM aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die Erzeugung von Warnungen oder Ereignismaßnahmen mithilfe des Befehls **config**:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```

So aktivieren oder deaktivieren Sie die Erzeugung von Warnungen oder Ereignismaßnahmen mithilfe des Befehls **set**:

```
racadm set iDRAC.IPMILan.AlertEnable 1
```

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 Warnungsgenerierung oder die Ereignismaßnahme zu aktivieren. Wählen Sie ansonsten **Deaktiviert** aus. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**. Die Warnungseinstellungen sind damit konfiguriert.

Warnungen filtern

Sie können Warnungen auf der Basis der Kategorie und des Schweregrads filtern.

Verwandte Links

[Warnungen aktivieren und deaktivieren](#)

[Einstellungen für E-Mail-Warnungs-SNMP-Trap oder IPMI-Trap konfigurieren](#)

Warnungen über die iDRAC7-Web-Schnittstelle filtern

So filtern Sie Warnungen auf der Basis der Kategorie und des Schweregrads:



ANMERKUNG: Selbst wenn Sie als Benutzer nur über Leseberechtigungen verfügen, können Sie die Warnungen filtern.

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Warnungen** . Daraufhin wird die Seite **Warnungen** angezeigt.
2. Wählen Sie unter **Warnungsfilter** eine oder mehrere der folgenden Kategorien aus:
 - Systemzustand
 - Lagerung
 - Konfiguration
 - Audit
 - Updates
 - Arbeitsnotizen
3. Wählen Sie eine oder mehrere der folgenden Schweregrade aus:
 - Informativ
 - Warnung
 - Kritisch
4. Klicken Sie auf **Übernehmen**.
Der Abschnitt **Warnungsergebnisse** zeigt die Ergebnisse auf der Basis der ausgewählten Kategorie und des Schweregrads an.

Warnungen über RACADM filtern

Um die Warnungen zu filtern, verwenden Sie die den Befehl **eventfilters**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Ereigniswarnungen einrichten

Sie können Ereigniswarnungen, wie z. B. E-Mail-Warnungen, IPMI-Warnungen, SNMP-Traps, Remote System-Protokolle und WS-Ereignisse so einstellen, dass sie an die konfigurierten Ziele gesendet werden.

Verwandte Links

- [Warnungen aktivieren und deaktivieren](#)
- [Einstellungen für E-Mail-Warnungs-SNMP-Trap oder IPMI-Trap konfigurieren](#)
- [Warnungen filtern](#)
- [Remote-Systemprotokollierung konfigurieren](#)
- [Konfigurieren von WS-Ereignisauslösung](#)

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 zu **Übersicht** → **Server** → **Warnungen**.
Die Seite **Warnungen** wird angezeigt.
3. Wählen Sie unter **Warnergebnisse** eine oder alle der folgenden Warnungen für die benötigten Ereignisse aus:
 - E-Mail-Warnung
 - SNMP-Trap
 - IPMI-Warnung


- Remote System-Protokoll
 - WS-Ereignisauslösung
4. Klicken Sie auf **Anwenden**.
Die Einstellung wird gespeichert.
 5. Wählen Sie im Abschnitt **Warnungen** die Option **Aktivieren** aus, um Warnungen an konfigurierte Ziele zu senden.
 6. Optional können Sie ein Testereignis versenden. Geben Sie in das Feld **Meldungs-ID für Testereignis** die Meldungs-ID ein, um zu testen, ob die Warnung erzeugt wird, und klicken Sie auf **Test**. Eine Liste der Meldungs-IDs finden Sie im *Event Messages Guide* (Handbuch für Ereignismeldungen) unter dell.com/support/manuals.

Ereigniswarnungen über RACADM einrichten

Zur Einrichtung einer Ereigniswarnung verwenden Sie den Befehl **eventfilters**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Alarmwiederholungsereignis einrichten

Sie können den iDRAC so konfigurieren, dass in bestimmten Intervallen weitere Ereignisse erzeugt werden, wenn das System weiterhin oberhalb eines Schwellenwertes für die Einlasstemperatur betrieben wird. Das Standardintervall beträgt 30 Tage. Der zulässige Bereich beträgt 0 bis 365 Tage. Ein Wert von „0“ bedeutet, dass die Ereigniswiederholung deaktiviert ist.

 **ANMERKUNG:** Sie müssen die Berechtigung zum Konfigurieren des iDRAC („Configure iDRAC“) besitzen, um den Wert für die Alarmwiederholung einzustellen.

Alarmwiederholungsereignis über die iDRAC7-Weboberfläche einrichten

So legen Sie einen Wert für die Alarmwiederholung fest:

1. Gehen Sie in der iDRAC7-Weboberfläche zu **Übersicht** → **Server** → **Alarmer** → **Alarmwiederholung**.
Die Seite **Alarmwiederholung** wird angezeigt.
2. Geben Sie in der Spalte **Wiederholung** einen Wert für die Alarmerhäufigkeit für die gewünschte Kategorie, den Alarm und die Schweregrade ein.
Weitere Informationen finden Sie in der *iDRAC7-Online-Hilfe*.
3. Klicken Sie auf **Anwenden**.
Die Einstellungen für die Alarmwiederholung werden gespeichert.

Alarmwiederholungsereignisse über RACADM einrichten

Verwenden Sie den Unterbefehl **eventfilters**, um über den RACADM Alarmwiederholungsereignisse einzurichten. Weitere Informationen hierzu finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für den iDRAC7 und CMC).

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.

Verwandte Links

[Warnungen filtern](#)

[Warnungen aktivieren und deaktivieren](#)

Ereignismaßnahmen über die Web-Schnittstelle einrichten

So richten Sie eine Ereignismaßnahme ein:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Warnungen** . Daraufhin wird die Seite **Warnungen** angezeigt.
2. Wählen Sie unter **Warnergebnisse** 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

Zur Konfiguration einer Ereignismaßnahme können Sie Folgendes nutzen:

- den Befehl **eventfilters**.
- das Objekt **cfglpmiPefAction** mit dem Befehl **config**.

Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.

Einstellungen für E-Mail-Warnungs-SNMP-Trap oder IPMI-Trap konfigurieren

Die Management Station verwendet Traps der Art „Simple Network Management Protocol“ (SNMP) und „Intelligent Platform Management Interface“ (IPMI), um Daten vom iDRAC7 zu empfangen. Bei Systemen mit einer größeren Anzahl an Knoten ist es für eine Management Station möglicherweise nicht effizient, jeden einzelnen iDRAC7 in Bezug auf einen potenziell möglichen Zustand abzufragen. Ereignis-Traps können eine Management Station beispielsweise mit einem Lastenausgleich zwischen Knoten oder durch das Generieren einer Warnung unterstützen, wenn ein Authentifizierungsfehler auftritt.

Sie können die IPv4- und IPv6-Warnungsziele, die E-Mail-Einstellungen und die SMTP-Server-Einstellungen konfigurieren und diese Einstellungen testen.

Vor der Konfiguration 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.

Verwandte Links

[IP-basierte Warnziele konfigurieren](#)



[Konfigurieren von E-Mail-Benachrichtigungen](#)

IP-basierte Warnziele konfigurieren

Sie können die IPv6- oder IPv4-Adressen für den Empfang von IPMI-Warnungen oder SNMP-Traps konfigurieren.

IP-basierte Warnziele über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die Warnungszieleinstellungen unter Verwendung der Web-Schnittstelle:

1. Gehen Sie zu **Übersicht** → **Server** → **Warnungen** → **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 Optionen finden Sie in der *iDRAC7-Online-Hilfe*.
3. Geben Sie die iDRAC7 SNMP-Communityzeichenfolge ein.
Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC7-Online-Hilfe*.
 **ANMERKUNG:** Der Wert für die Community-Zeichenkette zeigt die Community-Zeichenkette an, die für einen Warnungs-Trap der Art „Simple Network Management Protocol“ (SNMP) verwendet wird, der von iDRAC7 aus versendet wird. Stellen Sie sicher, dass die Ziel-Community-Zeichenkette mit der iDRAC7-Community-Zeichenkette übereinstimmt. Der Standardwert lautet „Öffentlich“.
4. 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.
5. Klicken Sie auf **Anwenden**.
Die Warnungsziele sind damit konfiguriert.
6. Wählen Sie im Abschnitt **SNMP Trap Format** die Protokollversion aus, die zum Senden der Traps an die Trap-Ziele – **SNMP v1** oder **SNMP v2** 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 Format SNMP v1 gesendet und basieren nicht auf der konfigurierten Option **SNMP Trap Format**.

Das SNMP-Trap-Format ist konfiguriert.

IP-Warnungsziele über RACADM konfigurieren

So konfigurieren Sie Trap-Warnungseinstellungen:

1. So aktivieren Sie Traps:
 - Bei einer IPv4-Adresse:

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i <Index> <0|1>
```
 - Bei einer IPv6-Adresse:

```
racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6AlertEnable -i <Index> <0|1>
```wobei „(index)“ für den Zielindex steht und 0 oder 1 den Trap deaktivieren bzw. aktivieren.  
Beispiel: Um Trap mit dem Index 4 zu aktivieren, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
```
2. So konfigurieren Sie die Adresse für das Trap-Ziel:

```
racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6AlertDestIPAddr -i <Index> <IP-Adresse>
```

wobei [Index] der Trap-Zielindex und [IP-Adresse] die Ziel-IP-Adresse des Systems ist, welches die Plattformereigniswarnungen empfängt.

3. Konfigurieren Sie die SNMP-Community-Namen-Zeichenkette.

```
racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName <Name>
```

wobei [Name] der PET-Community-Name ist.

4. So testen bei Bedarf Sie den Trap:

```
racadm testtrap -i <Index>
```

wobei [Index] der zu testende E-Mail-Zielindex ist.

Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.



IP-basierte Warnziele über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren

Sie können Warnungsziele (IPv4, IPv6 oder FQDN) unter Verwendung des Dienstprogramms für die iDRAC-Einstellungen konfigurieren. Gehen Sie wie folgt vor:

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 E-Mail-Adresse für den Empfang der E-Mail-Warnungen konfigurieren. Außerdem können Sie die Einstellungen für die SMTP-Server-Adresse konfigurieren.

-  **ANMERKUNG:** Wenn Ihr Mail-Server Microsoft Exchange Server 2007 ist, ist sicherzustellen, dass der iDRAC7-Domänenname so konfiguriert ist, dass der Mail-Server die E-Mail-Warnungen des iDRAC7 empfängt.
-  **ANMERKUNG:** E-Mail-Warnungen unterstützen sowohl IPv4- als auch IPv6-Adressen. Der DRAC DNS-Domänenname muss beim Nutzen von IPv6 festgelegt werden.

Verwandte Links

[Konfigurieren der Adresseneinstellungen des SMTP-E-Mail-Server](#)

E-Mail-Warnungseinstellungen über Web-Schnittstelle konfigurieren

So konfigurieren Sie die E-Mail-Warnungseinstellungen über die Web-Schnittstelle:

1. Gehen Sie zu **Übersicht** → **Server** → **Warnungen** → **SNMP- und E-Mail-Einstellungen**.
2. Wählen Sie die Option **Status** aus, um die E-Mail-Adresse für den Empfang der Warnungen zu aktivieren; geben Sie außerdem eine gültige E-Mail-Adresse ein. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC7-Online-Hilfe*.
3. Klicken Sie auf **Senden** bei **E-Mail testen**, um die konfigurierten E-Mail-Warnungseinstellungen zu testen.
4. Klicken Sie auf **Anwenden**.

E-Mail-Warnungseinstellungen mit RACADM konfigurieren

So konfigurieren Sie E-Mail-Warnungseinstellungen:

1. E-Mail-Warnung aktivieren:

- Verwenden des Befehls **config**:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i <Index> <0|1>
```

wobei [Index] der zu testende E-Mail-Zielindex ist. 0 deaktiviert die E-Mail-Warnung und 1 aktiviert die Warnung.

Der E-Mail-Zielindex kann ein Wert zwischen 1 und 4 sein. Wenn Sie beispielsweise eine E-Mail mit Index 4 aktivieren möchten, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
```

- Verwenden des Befehls **set**:

```
racadm set iDRAC.EmailAlert.Enable.[Index] 1
```

wobei [Index] der zu testende E-Mail-Zielindex ist. 0 deaktiviert die E-Mail-Warnung und 1 aktiviert die Warnung.

Der E-Mail-Zielindex kann ein Wert zwischen 1 und 4 sein. Wenn Sie beispielsweise eine E-Mail mit Index 4 aktivieren möchten, geben Sie den folgenden Befehl ein:

```
racadm set iDRAC.EmailAlert.Enable.4 1
```

2. Konfigurieren der E-Mail-Einstellungen:

- Verwenden des Befehls **config**:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <E-Mail-Adresse>
```

wobei 1 der E-Mail-Zielindex und [E-Mail-Adresse] die Ziel-E-Mail-Adresse ist, die die Plattformereigniswarnungen empfängt.

- Verwenden des Befehls **set**:

```
racadm set iDRAC.EmailAlert.Address.1 [E-Mail-Adresse]
```

wobei 1 der E-Mail-Zielindex und [E-Mail-Adresse] die Ziel-E-Mail-Adresse ist, die die Plattformereigniswarnungen empfängt.

3. So konfigurieren Sie eine benutzerdefinierte Meldung:

- Verwenden des Befehls **config**:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i <Index> <benutzerdefinierte Meldung>
```

wobei [Index] der E-Mail-Zielindex und [benutzerdefinierte Meldung] die benutzerdefinierte Meldung ist.

- Verwenden des Befehls **set**:

```
racadm set iDRAC.EmailAlert.CustomMsg.[Index] [benutzerdefinierte Meldung]
```

wobei [Index] der E-Mail-Zielindex und [benutzerdefinierte Meldung] die benutzerdefinierte Meldung ist.

4. So testen Sie bei Bedarf die konfigurierte E-Mail-Warnung:

```
racadm testemail -i <Index>
```

wobei [Index] der zu testende E-Mail-Zielindex ist.

Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.

Konfigurieren der Adresseneinstellungen des SMTP-E-Mail-Server

Sie müssen die SMTP-Server-Adresse für E-Mail-Warnungen konfigurieren, damit diese an bestimmte Ziele versendet werden können.

Adresseinstellungen für den SMTP-E-Mail-Server über die iDRAC7-Web-Schnittstelle konfigurieren

So konfigurieren Sie die SMTP-Server-Adresse:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Warnungen** → **SNMP- und E-Mail-Einstellungen**.
2. Wählen Sie die Option **Authentifizierung aktivieren** aus, geben Sie den Benutzernamen und das Kennwort (des Benutzers mit Zugriff auf den SMTP-Server) an, und geben Sie eine gültige IP-Adresse oder einen vollständig qualifizierten Domännennamen (FQDN) für den SMTP-Server ein, der im Rahmen der Konfiguration verwendet wird. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC7-Online-Hilfe*.
3. Klicken Sie auf **Anwenden**.
Die SMTP-Einstellungen sind damit konfiguriert.

Adresseinstellungen für den SMTP-E-Mail-Server über RACADM konfigurieren

Um den SMTP-E-Mail-Server zu konfigurieren, nutzen Sie einen der folgenden Befehle:

- Verwenden des Befehls **set**:

```
racadm set iDRAC.RemoteHosts.SMTPServerIPAddress <IP-Adresse des SMTP-E-Mail-Servers>
```
- Verwenden des Befehls **config**:

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr <SMTP-E-Mail-Server-IP-Adresse>
```

Konfigurieren von WS-Ereignisauslösung

Das WS-Ereignisauslösungsprotokoll wird verwendet, damit ein Client-Dienst (Abonnent) bei einem Server (Ereignisquelle) Interesse (Abonnement) daran registrieren kann, Meldungen mit den Serverereignissen (Benachrichtigungen oder Ereignismeldungen) zu empfangen. Clients, die am Empfang von WS-Ereignisauslösungsmeldungen interessiert sind, können iDRAC abonnieren und Ereignisse in Zusammenhang mit Jobs des Lifecycle-Controllers erhalten.

Die Schritte, die zur Konfiguration der WS-Ereignisauslösungsfunktion für den Empfang von WS-Ereignisauslösungsnachrichten zur Änderungen in Zusammenhang mit Lifecycle-Controller-Jobs erforderlich sind, werden im Spezifikationsdokument der Web-Dienst-Ereignisunterstützung für iDRAC7 1.30.30 beschrieben. Neben dieser Spezifikation finden Sie die vollständigen Informationen zum WS-Ereignisauslösungsprotokoll im Dokument DSP0226 (DMTF WS-Verwaltungsspezifikationen), Abschnitt 10 Benachrichtigungen (Ereignisauslösung). Die Jobs in Zusammenhang mit dem Lifecycle-Controller sind im Dokument DCIM-Job-Kontrollprofil beschrieben.

IDs für Warnungsmeldung

Die folgende Tabelle enthält eine Liste mit Meldungs-IDs, die bei Warnungen angezeigt werden.

Tabelle 22. IDs für Warnungsmeldungen

| Meldungs-ID | Beschreibung |
|-------------|--------------------------------|
| AMP | Stromstärke (A) |
| ASR | Automatische Systemrücksetzung |

| Meldungs-ID | Beschreibung |
|---------------------|---------------------------|
| BAR | Sichern/Wiederherstellen |
| BAT | Batterieereignis |
| BIOS | BIOS Management |
| Boot (Startvorgang) | Boot-Steuerung |
| CBL | Kabel |
| CPU | Prozessor |
| CPUA | Verfahren nicht vorhanden |
| CTL | Speicher-Controller |
| DH | Zertifikatverwaltung |
| DIS | Auto-Ermittlung |
| ENC | Speichergehäuse |
| Lüfter (FAN) | Lüfterereignis |
| FSD | debug |
| HWC | Hardware-Konfiguration |
| IPA | DRAC-IP-Änderung |
| ITR | Eingriff |
| JCP | Auftragssteuerung |
| LC | Lifecycle-Controller |
| LIC | Lizenzierung |
| Verbindung | Link-Status |
| Protokoll | Protokollereignis |
| MEM | Speicher |
| NDR | NIC-Betriebssystemtreiber |
| NIC | NIC-Konfiguration |
| OSD | BS-Bereitstellung |
| OSE | BS-Ereignis |
| PCI | PCI-Gerät |
| PDR | Physische Festplatte |
| PR | Teileaustausch |
| PST | BIOS-POST |
| Netzteilereinheit | Netzteil |
| PSUA | PSU nicht vorhanden |
| PWR | Stromverbrauch |
| RAC | RAC-Ereignis |
| RDU | Redundanz |
| Rot | FW-Download |
| RFL | IDSDM-Datenträger |

| Meldungs-ID | Beschreibung |
|-------------|---------------------------|
| RFLA | IDSDM nicht vorhanden |
| RFM | FlexAddress-SD |
| RRDU | IDSDM-Redundanz |
| RSI | Remote-Dienst |
| SEC | Sicherheitsereignis |
| SEL | System-Ereignisprotokoll |
| SRD | Software-RAID |
| SSD | PCIe SSD |
| STOR | Lagerung |
| SUP | FW-Aktualisierungsaufgabe |
| SWC | Software-Konfiguration |
| SWU | Software-Änderung |
| [SYS] | Systeminfo |
| tmp | Temperatur: |
| TST | Test-Warnung |
| UEFI | UEFI-Ereignis |
| usr | Benutzerverfolgung |
| VDR | Virtuelle Festplatte |
| VF | vFlash-SD-Karte |
| VFL | vFlash-Ereignis |
| VFLA | vFlash nicht vorhanden |
| VLT | Spannung |
| VME | Virtueller Datenträger |
| VRM | Virtuelle Konsole |
| WRK | Arbeitsanmerkung |

Protokolle verwalten

iDRAC7 bietet ein Lifecycle-Protokoll, das Ereignisse zum System, zu Speichergeräten, zu Netzwerkgeräten, zu Firmware-Aktualisierungen, zu Konfigurationsänderungen, zu Lizenzmeldungen, usw. enthält. Die Systemereignisse sind jedoch auch als separates Protokoll mit der Bezeichnung „Systemereignisprotokoll“ (SEL) verfügbar. Das Lifecycle-Protokoll ist über die iDRAC7-Web-Schnittstelle, über RACADM und die WS-MAN-Schnittstelle verfügbar.

Wenn das Lifecycle-Protokoll eine Größe von 800 KB erreicht, werden die Protokolle komprimiert und archiviert. Sie können nur die nicht archivierten Protokolleinträge anzeigen und Filter und Kommentare auf nicht archivierte Protokolle anwenden. Zum Anzeigen von archivierten Protokollen müssen Sie das gesamte Lifecycle-Protokoll auf einen Speicherort auf Ihrem System exportieren.

Verwandte Links

- [Systemereignisprotokoll anzeigen](#)
- [Lifecycle-Protokoll anzeigen](#)
- [Arbeitsanmerkungen hinzufügen](#)
- [Remote-Systemprotokollierung konfigurieren](#)

Systemereignisprotokoll anzeigen

Wenn ein Systemereignis auf einem Managed System auftritt, wird es im Systemereignisprotokoll (SEL) erfasst. Der gleiche SEL-Eintrag ist auch im LC-Protokoll verfügbar.

Systemereignisprotokoll über die Web-Schnittstelle anzeigen

Um das Systemereignisprotokoll (SEL) anzuzeigen, gehen Sie in der iDRAC7-Web-Schnittstelle auf die Registerkarte **Übersicht** → **Server** → **Protokolle**.

Auf der Seite **Systemereignisprotokoll** wird eine Systemzustandsanzeige, ein Zeitstempel und eine Beschreibung für jedes protokollierte Ereignis angezeigt. Weitere Informationen finden Sie in der *iDRAC7-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 auf ein Problem stoßen, laden Sie die kumulative Sicherheitsaktualisierung für Internet Explorer von der Support-Website von Microsoft unter support.microsoft.com herunter.

Systemereignisprotokoll über RACADM anzeigen

So zeigen Sie das Systemereignisprotokoll (SEL) an:

```
racadm getsel <Optionen>
```

Wenn keine Argumente vorgegeben werden, wird das gesamte Protokoll angezeigt.

So zeigen Sie die Anzahl der Einträge im SEL an:

```
racadm getsel-i
```

Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.

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. Dies geschieht so:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Systemereignisprotokoll**.
Das **iDRAC- Settings.System Event Log** zeigt die **Gesamtzahl der Einträge** an.
2. Um die Einträge zu löschen, wählen Sie **Ja**. Ansonsten wählen Sie **Nein**.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.

Lifecycle-Protokoll anzeigen

Die Lifecycle Controller-Protokolle enthalten die Änderungsverlaufsdaten in Bezug auf die Komponenten, die auf einem Managed System installiert sind. Sie enthalten Protokolle zu den folgenden Ereignissen:

- Speichergeräte
- Systemereignisse
- Netzwerkgerät
- Configuration (Konfiguration)
- Audit
- Updates
- Arbeitsnotizen

Sie können die Protokolle auf der Basis der Kategorie und des Schweregrads filtern sowie Arbeitsanmerkungen zu einem Protokollereignis anzeigen, exportieren und hinzufügen.

Verwandte Links

[Filtern der Lifecycle-Protokolle](#)

[Lifecycle-Protokollergebnisse exportieren](#)

[Anmerkungen zu Lifecycle-Protokollen hinzufügen](#)

Lifecycle-Protokoll über die Web-Schnittstelle anzeigen

Klicken Sie zum Anzeigen der Lifecycle-Protokolle auf **Übersicht** → **Server** → **Protokolle** → **Lifecycle-Protokoll**. Daraufhin wird die Seite **Lifecycle-Protokoll** angezeigt. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC7-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 **Protokoltyp** 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 daraufhin unter **Protokollergebnisse** angezeigt.

Lifecycle-Protokollergebnisse exportieren

Um die Ergebnisse des Lifecycle-Protokolls zu exportieren, klicken Sie auf der Seite **Lifecycle-Protokoll** im Abschnitt **Protokollergebnisse** auf **Exportieren**. Daraufhin wird ein Dialogfeld angezeigt, in dem Sie die Protokolleinträge in einem XML-Format auf einen Speicherort Ihrer Wahl speichern können.

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

Um die Lifecycle-Protokolle anzuzeigen, verwenden Sie den Befehl `lcllog`. Für weitere Informationen siehe *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Arbeitsanmerkungen hinzufügen


Jeder Benutzer, der sich bei iDRAC7 anmeldet, kann Arbeitsanmerkungen hinzufügen. Diese werden im Lifecycle-Protokoll als ein Ereignis gespeichert. Sie müssen über iDRAC7-Protokollberechtigungen verfügen, um Arbeitsanmerkungen hinzufügen zu können. Pro neuer Arbeitsanmerkung sind bis zu 255 Zeichen zulässig.

 **ANMERKUNG:** Sie können Arbeitsanmerkungen löschen.

So fügen Sie eine Arbeitsanmerkung hinzu:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Eigenschaften** → **Zusammenfassung**.
Die Seite **Systemzusammenfassung** wird angezeigt.

2. Geben Sie unter **Arbeitsanmerkungen** den gewünschten Text in das leere Textfeld ein.

 **ANMERKUNG:** Es wird empfohlen, nicht zu viele Sonderzeichen zu verwenden.

3. Klicken Sie auf **Hinzufügen**.
Die Arbeitsanmerkung wird zum Protokoll hinzugefügt. Weitere Informationen finden Sie in der *iDRAC7-Online-Hilfe*.

Remote-Systemprotokollierung konfigurieren

Sie können Lifecycle-Protokolle an ein Remote-System senden. Vor diesem Schritt müssen Sie Folgendes sicherstellen:

- Der iDRAC7 und das Remote-System sind über eine Netzwerkkonnektivität verbunden.
- Das Remote-System und iDRAC7 befinden sich auf dem gleichen Netzwerk.

Remote-System-Protokollierung über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die Remote-Syslog-Server-Einstellungen:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Protokolle** → **Einstellungen**.
Die Seite **Remote-Syslog-Einstellungen** wird angezeigt.
2. Aktivieren Sie die Remote-Syslog, und geben Sie die Server-Adresse und die Schnittstellenummer an. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC7-Online-Hilfe*.
3. Klicken Sie auf **Anwenden**.
Die Einstellungen werden gespeichert. Alle in das Lifecycle-Protokoll geschriebenen Protokolle werden gleichzeitig auf die konfigurierten Remote-Server geschrieben.

Remote-Systemanmeldung über RACADM konfigurieren

Um die Einstellungen für den Remote-Syslog-Server zu konfigurieren, verwenden Sie eines der Folgenden:

- Objekte in der Gruppe **cfgRemoteHosts** mit dem Befehl **config**.
- Objekte in der Gruppe **iDRAC.SysLog** mit dem Befehl **set**.

Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.

Stromversorgung überwachen und verwalten

Sie können iDRAC7 zum Überwachen und Verwalten der Stromversorgungsanforderungen auf dem Managed System verwenden. Diese Funktionen unterstützt Sie dabei, das System vor Stromausfällen zu schützen, da der Stromzufluss auf dem System entsprechend verteilt und der Stromverbrauch 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 Managed System an und legen Sie sie fest, einschließlich der Anzeige des geringsten und maximalen potenziellen Stromverbrauchs. Dies ist eine Lizenzfunktion.
- **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.

Verwandte Links

[Stromversorgung überwachen](#)

[Stromsteuerungsvorgänge ausführen](#)

[Strombegrenzung](#)

[Netzteiloptionen konfigurieren](#)

[Netzschalter aktivieren oder deaktivieren](#)

Stromversorgung überwachen

iDRAC7 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 unmittelbare Aussteuerungsreserve-Werte (für Rack- und Tower-Server).

Stromversorgung über die Web-Schnittstelle überwachen

Um die Stromüberwachungsinformationen anzuzeigen, gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Strom/Thermisch** → **Stromüberwachung**. Daraufhin wird die Seite **Stromüberwachung** angezeigt. Weitere Informationen finden Sie in der *iDRAC7-Online-Hilfe*.

Stromversorgung über RACADM überwachen

Um die Stromversorgungsinformationen zu überwachen, verwenden Sie die Gruppenobjekte **System.Power** mit dem Befehl **get** oder das Objekt **cfgServerPower** mit dem Befehl **getconfig**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Stromsteuerungsvorgänge ausführen

Der iDRAC7 ermöglicht, im Remote-Zugriff die Maßnahmen Einschalten, Ausschalten, Reset, ordentliches Herunterfahren, nicht maskierbarer Interrupt (NMI) oder Aus- und Einschalten mithilfe der Webschnittstelle oder RACADM auszuführen.

Sie können diese Vorgänge auch mithilfe der Remote-Dienste des Lifecycle-Controllers oder der WS-Verwaltung durchführen. Weitere Informationen finden Sie im *Lifecycle Controller Remote Services Quick Start Guide* (Lifecycle-Controller Remote-Dienste Schnellstarthandbuch) unter dell.com/support/manuals und im Profildokument *Dell Power State Management* (Dell Verwaltung des Energiezustands) unter delltechcenter.com.

Stromsteuerungsvorgänge über die Web-Schnittstelle ausführen

So führen Sie Stromsteuerungsvorgänge aus:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Strom/Thermisch** → **Stromkonfiguration** → **Stromsteuerung**. Daraufhin wird die Seite **Stromsteuerung** angezeigt.
2. Wählen Sie die erforderliche Stromsteuerungsmaßnahme aus:
 - System einschalten
 - System ausschalten
 - NMI (Non-Masking Interrupt, nicht-maskierbare Unterbrechung)
 - Ordentliches Herunterfahren
 - System Reset (Softwareneustart)
 - System aus- und wieder einschalten (Hardwareneustart)
3. Klicken Sie auf **Anwenden**. Weitere Informationen finden Sie in der *iDRAC7-Online-Hilfe*.

Stromsteuerungsvorgänge über RACADM ausführen

Zur Durchführung von Stromversorgungsmaßnahmen verwenden Sie den Befehl **serveraction**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Strombegrenzung

Sie können die Stromverbrauchs-Schwellenwerte anzeigen, die den Bereich des Gleich- und Drehstrom-Stromverbrauchs abdecken, den ein System unter schwerer Belastung gegenüber dem Rechenzentrum meldet. Hierbei handelt es sich um eine Lizenzfunktion.

Strombegrenzung bei Blade-Servern

Bevor ein Server hochfährt, teilt iDRAC7 dem CMC seine Stromanforderung mit. Sie liegt höher als der eigentliche Strom, den der Blade-Server verbrauchen kann und wird auf der Basis von eingeschränkten Hardware-Bestandsinformationen berechnet. Basierend auf der vom Server tatsächlich verbrauchten Energie kann ein kleinerer Strombereich angefordert werden, nachdem der Server hochgefahren wurde. Wenn sich der Stromverbrauch im Laufe der Zeit erhöht und sich der Stromverbrauch des Servers der maximalen Zuweisung nähert, kann der iDRAC7 eine Erhöhung des maximalen potenziellen Stromverbrauchs anfordern und erhöht auf diese Weise den Power-Envelope. iDRAC7 erhöht seine Anforderung hinsichtlich der maximalen potenziellen Leistungsaufnahme nur für den CMC. Fällt der Verbrauch ab, fordert er keine geringere potenzielle Mindestenergie an. iDRAC7 fordert mehr Strom an, wenn der Stromverbrauch über den vom CMC zugewiesenen Stromwert hinausgeht.

Nach dem Einschalten und Initialisieren des Systems berechnet iDRAC7 eine neue Stromanforderung, die auf der tatsächlichen Blade-Konfiguration basiert. Das Blade wird auch dann mit Strom versorgt, wenn der CMC keine neue Stromanforderung erfüllen kann.

CMC fordert sämtliche ungenutzte Energie von Servern niedrigerer Priorität zurück und ordnet die zurückgeforderte Energie einem Infrastrukturmodul höherer Priorität oder einem Server zu.

Wenn nicht genügend Energie zugewiesen ist, startet der Blade-Server nicht. Wenn dem Blade ausreichend Energie zugewiesen wurde, schaltet das iDRAC die Systemversorgung ein.

Strombegrenzungsrichtlinie anzeigen und konfigurieren

Wenn die Strombegrenzungsrichtlinie aktiviert ist, werden benutzerdefinierte Strombegrenzungen für das System durchgesetzt. Ist diese Option nicht aktiviert, wird die Hardware-Stromschutzrichtlinie verwendet, die standardmäßig implementiert ist. Diese Stromschutzrichtlinie ist unabhängig von der benutzerdefinierten Richtlinie. Die Systemleistung wird dynamisch angepasst, um die Leistungsaufnahme am festgelegten Schwellenwert zu halten.

Die tatsächliche Leistungsaufnahme kann bei niedriger Auslastung geringer sein und den Schwellenwert für einen Augenblick überschreiten, bis Leistungsanpassungen abgeschlossen sind. Beispiel: Eine gegebene Systemkonfiguration sieht 700 W für den höchsten potenziellen Stromverbrauch und 500 W für den geringsten potenziellen Stromverbrauch vor. Sie können einen Strombudgetschwellenwert festlegen und aktivieren, um den Verbrauch von derzeit 650 W auf 525 W zu senken. Ab diesem Punkt wird die Leistung des Systems dynamisch angepasst, um den Stromverbrauch unter dem benutzerspezifisierten Schwellenwert von 525 W zu halten.

Wenn der Wert für die Strombegrenzung auf einen Wert unterhalb des empfohlenen Schwellenwerts gesetzt ist, ist iDRAC7 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 Umrechnung in Watt auf die nächste Ganzzahl aufgerundet. Bei der Rückumwandlung der Stromobergrenze von Watt in BTU/h erfolgt die Aufrundung in gleicher Weise. Folglich kann sich der geschriebene Wert nominal vom angezeigten Wert unterscheiden. Beispiel: Ein auf 600 BTU/h eingestellter Schwellenwert wird als 601 BTU/h angezeigt.

Strombegrenzungsrichtlinie über die Web-Schnittstelle konfigurieren

So zeigen Sie die Stromrichtlinien an:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Strom/Thermisch** → **Stromkonfiguration** → **Stromkonfiguration**. Daraufhin wird die Seite **Stromkonfiguration** angezeigt.
Die Seite **Stromkonfiguration** wird angezeigt. Die aktuelle Strombegrenzungsrichtlinie wird im Abschnitt **Aktive Strombegrenzungsrichtlinie** angezeigt.
2. Wählen Sie die Option **Aktivieren** unter **iDRAC-Strombegrenzungsrichtlinie** aus.

3. Geben Sie im Abschnitt **Benutzerdefinierte Begrenzungen** die maximale Stromgrenze in Watt und BTU/h oder den maximalen Prozentsatz der empfohlenen Systembegrenzung an.
4. Klicken Sie auf **Übernehmen**, um die Werte zu übernehmen.

Strombegrenzungsrichtlinie über RACADM konfigurieren

So zeigen Sie die Werte für die aktuelle Strombegrenzung an und konfigurieren sie:

- Verwenden Sie die folgenden Objekte mit dem Unterbefehl **config**:
 - `cfgServerPowerCapWatts`
 - `cfgServerPowerCapBTUhr`
 - `cfgServerPowerCapPercent`
 - `cfgServerPowerCapEnable`
- Verwenden Sie die folgenden Objekte mit dem Unterbefehl **set**:
 - `System.Power.Cap.Enable`
 - `System.Power.Cap.Watts`
 - `System.Power.Cap.Btuhr`
 - `System.Power.Cap.Percent`

Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.

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 Netzteileneinheit des Servers die Stromüberwachung unterstützt.

Daraufhin wird die Seite **iDRAC-Einstellungen – Stromkonfiguration** angezeigt.

2. Wählen Sie **Aktiviert** aus, um die **iDRAC-Strombegrenzungsrichtlinie** zu aktivieren. Wählen Sie ansonsten **Deaktiviert** aus.
3. Verwenden Sie die empfohlenen Einstellungen, oder geben Sie unter **Benutzerdefinierte Grenzwerte** die gewünschten Grenzwerte ein.
Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.
4. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
Damit sind die Strombegrenzungswerte konfiguriert.

Netzteiloptionen konfigurieren

Sie können die Netzteiloptionen konfigurieren, so z. B. die Redundanzrichtlinie, das Austauschen von Laufwerken im laufenden Betrieb und die Korrektur des Leistungsfaktors.

Das Hotspare ist eine Netzteilfunktion, über die die redundanten Netzteilgeräte (PSUs) je nach Server-Belastung ausgeschaltet werden können. Auf diese Weise können die übrigen PSUs mit einer höheren Auslastung und Effizienz laufen. Die PSUs müssen diese Funktion jedoch unterstützen, damit gewährleistet ist, dass sie bei Bedarf schnell eingeschaltet werden können.

In einem System mit zwei Netzteilen kann entweder PSU 1 oder PSU 2 als primäres Netzteil konfiguriert werden. In einem System mit vier Netzteilen muss ein Netzteilpaar (1+1 oder 2+2) als primäres Netzteil festgelegt werden.

Nachdem die Hotspare-Funktion aktiviert wurde, können die PSUs je nach Auslastung aktiv werden oder in den Ruhemodus versetzt werden.

Der Leistungsfaktor ist das Verhältnis aus verbrauchter Wirkleistung und der 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 bereits aktiviert.

Netzteiloptionen über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die Netzteiloptionen:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Stromversorgung/Thermisch** → **Stromverbrauchskonfiguration** → **Stromverbrauchskonfiguration**. Daraufhin wird die Seite **Stromversorgungskonfiguration** angezeigt.
2. Wählen Sie unter **Netzteiloptionen** die erforderlichen Optionen aus. Weitere Informationen finden Sie in der *iDRAC7-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 Unterbefehl **set**:

- System.Power.RedundancyPolicy
- System.Power.Hotspare.Enable
- System.Power.Hotspare.PrimaryPSU
- System.Power.PFC.Enable

Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.

Netzteiloptionen über das Dienstprogramm für die iDRAC-Einstellungen konfigurieren

So konfigurieren Sie die Netzteiloptionen:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Stromkonfiguration**.
 **ANMERKUNG:** Der Link **Stromkonfiguration** ist nur verfügbar, wenn die Netzteileinheit des Servers die Stromüberwachung unterstützt.
Daraufhin wird die Seite **iDRAC-Einstellungen – Stromkonfiguration** angezeigt.
2. Führen Sie unter „Netzteiloptionen“ die folgenden Schritte aus:
 - Aktivieren oder deaktivieren Sie die Netzteilredundanz.
 - Aktivieren oder deaktivieren Sie das Hotspare.
 - Legen Sie das primäre Netzteilgerät fest.
 - Aktivieren oder deaktivieren Sie die Leistungsfaktorkorrektur. Weitere Informationen zu diesen Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**.
Die Netzteiloptionen sind damit konfiguriert.

Netzschalter aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie den Netzschalter auf dem Managed System:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Frontblendensicherheit**.
Die Seite **iDRAC-Einstellungen Frontblendensicherheit** wird angezeigt.
2. Wählen Sie die Option **Aktiviert** aus, um den Netzschalter zu aktivieren. Wählen Sie ansonsten **Deaktiviert** aus.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**. Die Einstellungen sind damit gespeichert.

Virtuelle Konsole konfigurieren und verwenden

Sie können die virtuelle Konsole dazu verwenden, das Remote-System zu verwalten, indem Sie Tastatur, Video und Maus auf der Management-Station verwenden, um die entsprechenden Geräte auf einem verwalteten Remote-Server zu steuern. Hierbei handelt es sich um eine Lizenzfunktion für Rack- und Tower-Server. Sie ist auf Blade-Servern standardmäßig verfügbar.

Die Hauptfunktionen sind:

- Es können maximal vier gleichzeitige Sitzungen einer virtuellen Konsole unterstützt werden. Alle Sitzungen zeigen dieselbe verwaltete Serverkonsole gleichzeitig an.
- Sie können die virtuelle Konsole in einem unterstützten Web-Browser über das Java- oder das ActiveX-Plugin starten. Sie müssen den Java-Viewer verwenden, wenn die Management Station auf einem Nicht-Windows-Betriebssystem ausgeführt wird.
- Wenn Sie die Sitzung einer virtuellen Konsole öffnen, zeigt der verwaltete Server nicht an, dass die Konsole umgeleitet wurde.
- Sie können mehrere Sitzungen für virtuelle Konsolen von einer einzelnen Management Station aus auf einem oder mehreren Managed Systems gleichzeitig öffnen.
- Es ist nicht möglich, zwei Sitzungen für virtuelle Konsolen von der Management Station aus über das gleiche Plugin auf dem verwalteten Server zu öffnen.
- Wenn ein zweiter Benutzer eine Virtuelle Konsole-Sitzung anfordert, wird der erste Benutzer benachrichtigt und erhält die Option, den Zugriff abzulehnen, den schreibgeschützten Zugriff zu erlauben oder vollständig freigegebenen Zugriff zu erlauben. Der zweite Benutzer wird benachrichtigt, dass ein anderer Benutzer die Steuerung übernommen hat. Wenn der erste Benutzer nicht innerhalb von 30 Sekunden antwortet, wird dem zweiten Benutzer je nach Standardeinstellung ein Zugriff gewährt. Wenn zwei Sitzungen gleichzeitig aktiv sind, sieht der erste Benutzer eine Meldung in der rechten oberen Ecke des Bildschirms, dass der zweite Benutzer eine aktive Sitzung hat. Wenn weder der erste noch der zweite Benutzer über Administratorberechtigungen verfügt, wird die Sitzung des zweiten Benutzers automatisch beendet, wenn der erste Benutzer seine aktive Sitzung beendet.

Verwandte Links

[Web-Browser für die Verwendung der virtuellen Konsole konfigurieren](#)

[Virtuelle Konsole konfigurieren](#)

[Virtuelle Konsole starten](#)

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 23. Unterstützte Bildschirmauflösungen und Bildwiederholfrequenzen

| Bildschirmauflösung | Bildwiederholfrequenz (Hz) |
|---------------------|----------------------------|
| 720x400 | 70 |
| 640x480 | 60, 72, 75, 85 |
| 800x600 | 60, 70, 72, 75, 85 |

| Bildschirmauflösung | Bildwiederholfrequenz (Hz) |
|---------------------|----------------------------|
| 1024x768 | 60, 70, 72, 75, 85 |
| 1280x1024 | 60 |

Es wird empfohlen, die Bildschirmauflösung auf 1280x1024 Pixel oder höher einzustellen.

 **ANMERKUNG:** Wenn eine aktive Virtuelle Konsole-Sitzung vorhanden ist und ein Monitor mit niedrigerer Auflösung an die virtuelle Konsole angeschlossen wird, dann wird die Serverkonsolenauflösung bei Auswahl des Servers auf der lokalen Konsole eventuell zurückgesetzt. Wenn das System ein Linux-Betriebssystem ausführt, kann eine X11-Konsole auf dem lokalen Monitor u. U. nicht angezeigt werden. Drücken Sie in der virtuellen iDRAC7-Konsole <Strg><Alt><F1>, um Linux auf eine Textkonsole umzuschalten.

Web-Browser für die Verwendung der virtuellen Konsole konfigurieren

So verwenden Sie die virtuelle Konsole auf Ihrer Management Station:

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

Weitere Informationen zu den unterstützten Browserversionen finden Sie in *Readme* unter **dell.com/support/manuals**.

2. Konfigurieren Sie den Web-Browser für die Verwendung des ActiveX- oder Java-Plugins.
Der ActiveX-Viewer wird nur unter Internet Explorer unterstützt. Der Java-Viewer wird auf jedem Browser unterstützt.
3. Importieren Sie die Stammzertifikate auf das Managed System, um Popup-Fenster zu unterbinden, die Sie zur Überprüfung der Zertifikate auffordern.
4. 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.

5. 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.

Verwandte Links


[Web-Browser für die Verwendung des Java-Plugin konfigurieren](#)

[IE für die Verwendung des ActiveX-Plugin konfigurieren](#)

[Zertifizierungsstellenzertifikate auf die Management Station importieren](#)

Web-Browser für die Verwendung des Java-Plugin konfigurieren

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

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

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

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

Verwandte Links


[Virtuelle Konsole konfigurieren](#)

IE für die Verwendung des ActiveX-Plugin konfigurieren


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

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

1. Leeren Sie den Browser-Cache.
2. Fügen Sie die iDRAC7-IP-Adresse oder den Hostnamen zur Liste **Vertrauenswürdige Sites** hinzu.
3. Setzen Sie die benutzerdefinierten Einstellungen auf **Mittelhoch (Standard)** zurück, oder ändern Sie die Einstellungen, um die Installation von signierten ActiveX-Plugins zu ermöglichen.
4. Aktivieren Sie den Browser für das Herunterladen von verschlüsselten Inhalten, und aktivieren Sie Drittanbieter-Browser-Erweiterungen. Gehen Sie dazu zu **Extras** → **Internetoptionen** → **Erweitert**, deaktivieren Sie die Option **Verschlüsselte Sites nicht auf dem Datenträger speichern**, und aktivieren Sie die Option **Browsererweiterungen von Drittanbietern aktivieren**.

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

5. Gehen Sie zu **Extras** → **Internetoptionen** → **Sicherheit**, und wählen Sie die Zone aus, in der Sie die Anwendung ausführen möchten.
6. Klicken Sie auf **Stufe anpassen**. Führen Sie im Fenster **Sicherheitseinstellungen** die folgenden Schritte aus:
 - Wählen Sie die Option **Aktivieren** für **Automatische Eingabeaufforderung für ActiveX-Steuerelemente** aus.
 - Wählen Sie die Option **Auffordern** für **Signierte ActiveX-Steuerelemente herunterladen** aus.
 - Wählen Sie die Option **Aktivieren** oder **Auffordern** für **ActiveX-Steuerelemente und -Plugins ausführen** aus.
 - Wählen Sie die Option **Aktivieren** oder **Auffordern** für **Script-ActiveX-Steuerelemente, die für das Scripting als sicher gekennzeichnet wurden** aus.
7. Klicken Sie auf **OK**, um das Fenster **Sicherheitseinstellungen** zu schließen.
8. Klicken Sie auf **OK**, um das Fenster **Internetoptionen** zu schließen.

 **ANMERKUNG:** Vor der Installation des ActiveX-Steuerelements kann Internet Explorer eventuell eine Sicherheitswarnung anzeigen. Akzeptieren Sie die ActiveX-Steuerung, um das Installationsverfahren abzuschließen, wenn der Internet Explorer Sie mit einer Sicherheitswarnung dazu auffordert.

Verwandte Links

[Browser-Cache leeren](#)

[Zusätzliche Einstellungen für Windows Vista oder neuere Microsoft-Betriebssysteme](#)

Zusätzliche Einstellungen für Windows Vista oder neuere Microsoft-Betriebssysteme

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


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

1. Führen Sie IE als Administrator aus.
2. Gehen Sie zu **Extras** → **Internetoptionen** → **Sicherheit** → **Vertrauenswürdige Sites**.
3. Stellen Sie sicher, dass die Option **Schutzmodus aktivieren** nicht als Zone für vertrauenswürdige Sites ausgewählt ist. Alternativ dazu können Sie die iDRAC7-Adresse den Sites in der Intranetzone hinzufügen. Standardmäßig ist der Schutzmodus für Sites in der Intranetzone und in der Zone vertrauenswürdiger Sites ausgeschaltet.
4. Klicken Sie auf **Sites**.

5. Geben Sie in das Feld **Diese Website zur Zone hinzufügen** die Adresse des iDRAC7 ein und klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **Schließen** und dann auf **OK**.
7. Schließen Sie den Browser und starten Sie ihn neu, damit die Einstellungen wirksam werden.

Browser-Cache leeren

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

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

Frühere Versionen von ActiveX in IE7 löschen

So löschen Sie frühere Versionen von Active-X Viewer für IE7:

1. Schließen Sie den Video Viewer und Internet Explorer.
2. Öffnen Sie nochmals den Internet Explorer-Browser, gehen Sie zu **Internet Explorer** → **Extras** → **Add-Ons verwalten**, und klicken Sie dort auf **Add-Ons aktivieren oder deaktivieren**. Daraufhin wird das Fenster **Add-Ons verwalten** angezeigt.
3. Wählen Sie im Dropdown-Menü **Anzeigen Von Internet Explorer verwendete Add-Ons** aus.
4. Löschen Sie das Add-On *Video Viewer*.

Frühere Versionen von ActiveX in IE8 löschen

So löschen Sie frühere Versionen von Active-X Viewer für IE8:

1. Schließen Sie den Video Viewer und Internet Explorer.
2. Öffnen Sie dann wieder den Internet Explorer und gehen Sie zu **Internet Explorer Extras Add-Ons verwalten** und klicken Sie auf **Add-Ons aktivieren/deaktivieren**. Das Fenster **Add-Ons verwalten** wird angezeigt.
3. Wählen Sie aus dem Dropdown-Menü **Anzeigen** die Option **Alle Add-ons** aus.
4. Wählen Sie das Add-On *Video Viewer* aus und klicken Sie auf den Link **Weitere Informationen**.
5. Wählen Sie im Fenster **Weitere Informationen Entfernen** aus.
6. Schließen Sie die Fenster **Weitere Informationen** und **Add-Ons verwalten**.

Frühere Java-Versionen löschen

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

1. Führen Sie bei der Eingabeaufforderung `javaws-viewer` oder `javaws-uninstall` aus.
Der **Java Cache-Viewer** wird angezeigt.
2. Löschen Sie die Elemente mit der Bezeichnung *Client der virtuellen iDRAC7-Konsole*.

Zertifizierungsstellenzertifikate auf die Management Station importieren

Wenn Sie die virtuelle Konsole oder den virtuellen Datenträger starten, werden Sie über Abfragen dazu aufgefordert, die Zertifikate zu überprüfen. Wenn Sie über Web Server-Zertifikate verfügen, können Sie diese Abfragen durch das Importieren der Zertifizierungsstellenzertifikate in den vertrauenswürdigen Java- oder ActiveX-Store umgehen.

Verwandte Links

[Zertifizierungsstellenzertifikat in den Speicher für vertrauenswürdige Java-Zertifikate importieren](#)

[Zertifizierungsstellenzertifikat in den Speicher für vertrauenswürdige ActiveX-Zertifikate importieren](#)

Zertifizierungsstellenzertifikat in den Speicher für vertrauenswürdige Java-Zertifikate importieren

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

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

Zertifizierungsstellenzertifikat in den Speicher für vertrauenswürdige ActiveX-Zertifikate importieren

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

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

1. Öffnen Sie die OpenSSL-Befehlseingabe.
2. Führen Sie einen 8-Byte-Hash auf dem Zertifizierungsstellenzertifikat aus, das derzeit auf der Management Station verwendet wird. Verwenden Sie dazu den folgenden Befehl: `openssl x509 -in (Name des Zertifizierungsstellenzertifikats) -noout -hash`
Daraufhin wird eine Ausgabedatei generiert. Wenn der Dateiname des Zertifizierungsstellenzertifikats beispielsweise **cacert.pem** lautet, lautet der Befehl wie folgt:
`openssl x509 -in cacert.pem -noout -hash`
Es wird eine Ausgabedatei generiert, die dem folgenden Beispiel ähnelt: „431db322“.
3. Nennen Sie die Datei für das Zertifizierungsstellenzertifikat in den Namen der Ausgabedatei um, und fügen Sie die Erweiterung „.0“ hinzu. Beispiel: 431db322.0.
4. Kopieren Sie das umbenannte Zertifizierungsstellenzertifikat in Ihr Home-Verzeichnis. Beispiel für das Verzeichnis: **C:\Dokument und Einstellungen\<Benutzer>**.

Virtuelle Konsole konfigurieren

Vor der Konfigurierung der virtuellen Konsole müssen Sie sicherstellen, dass die Management Station konfiguriert ist. Sie können die virtuelle Konsole über die iDRAC7-Web-Schnittstelle oder die RACADM-Befehlszeilenschnittstelle konfigurieren.

Verwandte Links

- [Web-Browser für die Verwendung der virtuellen Konsole konfigurieren](#)
- [Virtuelle Konsole starten](#)

Virtuelle Konsole über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die virtuelle Konsole über die iDRAC7-Web-Schnittstelle:

1. Gehen Sie zu **Übersicht** → **Server** → **Konsole**. Daraufhin wird die Seite **Virtuelle Konsole** aufgerufen.
2. Aktivieren Sie die virtuelle Konsole, und geben Sie die erforderlichen Werte ein. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC7-Online-Hilfe*.
3. Klicken Sie auf **Anwenden**. Die virtuelle Konsole ist damit konfiguriert.

Virtuelle Konsole über RACADM konfigurieren


Verwenden Sie zum Konfigurieren der virtuellen Konsole eines der folgenden Objekte:

- Verwenden Sie die Objekte in der Gruppe **iDRAC.VirtualConsole** mit dem Befehl **set**.
- Verwenden Sie die folgenden Objekte mit dem Befehl **config**:
 - `cfgRacTuneConRedirEnable`
 - `cfgRacTuneConRedirPort`
 - `cfgRacTuneConRedirEncryptEnable`
 - `cfgRacTunePluginType`
 - `cfgRacTuneVirtualConsoleAuthorizeMultipleSessions`

Weitere Informationen zu diesen Objekten finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.


Vorschau der virtuellen Konsole

Bevor Sie die virtuelle Konsole starten, können Sie eine Vorschau des Zustands der virtuellen Konsole auf der Seite **System** → **Eigenschaften** → **Systemzusammenfassung** anzeigen. Der Abschnitt Vorschau der virtuellen Konsole zeigt ein Image an, das über den Zustand der virtuellen Konsole Aufschluss gibt. Das Image wird automatisch alle 30 Sekunden aktualisiert. Dies ist 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 iDRAC7-Web-Schnittstelle oder eine URL starten.

 **ANMERKUNG:** Starten Sie die Sitzung für eine virtuelle Konsole nicht über einen Web-Browser auf dem Managed System.

Stellen Sie vor dem Starten der virtuellen Konsole Folgendes sicher:

- Sie über Administrator-Zugriffsrechte verfügen.
- Der Web-Browser wird für die Verwendung der Java- oder ActiveX-Plugins konfiguriert.
- Die Mindestnetzwerkbandbreite von 1 MB/s ist verfügbar.

Während des Starts der virtuellen Konsole über einen 32-Bit- oder 64-Bit-IE-Browser steht das erforderliche Plugin (Java oder ActiveX) im entsprechenden Browser zur Verfügung. Die Einstellungen in den Internetoptionen sind für beide Browser gleich.

Beim Starten der virtuellen Konsole über das Java-Plugin wird gelegentlich ein Java-Kompilierungsfehler angezeigt. Um dieses Problem zu lösen, gehen Sie zu **Java-Systemsteuerung** → **Allgemein** → **Netzwerkeinstellungen**, und wählen Sie **Direkte Verbindung** aus.

Wenn die virtuelle Konsole für die Verwendung des ActiveX-Plugins konfiguriert wurde, scheitert möglicherweise der erste Startversuch. Der Grund dafür liegt in einer langsamen Netzwerkverbindung und einer Zeitüberschreitung nach zwei Minuten bei den temporären Anmeldeinformationen (die von der virtuellen Konsole für den Verbindungsaufbau

verwendet werden). Beim Herunterladen des ActiveX-Client-Plugin wird diese Zeit möglicherweise überschritten. Nachdem Sie das Plugin erfolgreich heruntergeladen haben, können Sie die virtuelle Konsole wie gewohnt starten. Wenn Sie die virtuelle Konsole erstmals über IE8 unter Verwendung des ActiveX-Plugin starten, wird möglicherweise die Meldung `Zertifikatfehler: Navigation blockiert` angezeigt. Klicken Sie auf **Weiter zu dieser Website** und dann auf **Installieren**, um die ActiveX-Steuerungen im Fenster **Sicherheitswarnung** zu installieren. Daraufhin wird die Sitzung für die virtuelle Konsole gestartet.

Verwandte Links

- [Virtuelle Konsole über URL starten](#)
- [Web-Browser für die Verwendung des Java-Plugin konfigurieren](#)
- [IE für die Verwendung des ActiveX-Plugin konfigurieren](#)
- [Virtuelle Konsole über die Web-Schnittstelle starten](#)
- [Mauszeiger synchronisieren](#)

Virtuelle Konsole über die Web-Schnittstelle starten

Sie können die virtuelle Konsole wie folgt starten:

- Gehen Sie zu **Übersicht** → **Server** → **Konsole**. Daraufhin wird die Seite **Virtuelle Konsole** angezeigt. Klicken Sie auf **Virtuelle Konsole starten**. Daraufhin wird der **Viewer für die virtuelle Konsole** gestartet.
- Gehen Sie zu **Übersicht** → **Server** → **Eigenschaften**. Daraufhin wird die Seite **Systemzusammenfassung** angezeigt. Klicken Sie im Abschnitt **Vorschau auf virtuelle Konsole** auf **Starten**. Daraufhin wird der **Viewer für die virtuelle Konsole** gestartet.

Im **Viewer für die virtuelle Konsole** wird der Desktop des Remote-Systems angezeigt. Über diesen Viewer können Sie die Maus- und Tastaturfunktionen des Remote-Systems über Ihre Management Station steuern.

Es ist möglich, dass nach dem Starten der Anwendung mehrere Dialogfelder eingeblendet werden können. Um den unberechtigten 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 Sicherheitswarnungen 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 Management Station. Zur Synchronisierung der Zeiger siehe [Mauszeiger synchronisieren](#).

Das Starten einer virtuellen Konsole über eine Windows Vista-Management Station kann Neustartmeldungen der virtuellen Konsole verursachen. Sie können dies vermeiden, indem Sie die entsprechenden Zeitüberschreitungswerte an den folgenden Stellen einstellen:


- **Systemsteuerung** → **Energieoptionen** → **Energiesparmodus** → **Erweiterte Einstellungen** → **Festplatte** → **Festplatte ausschalten nach <Zeitüberschreitung>**
- **Systemsteuerung** → **Energieoptionen** → **Hochleistung** → **Erweiterte Einstellungen** → **Festplatte** → **Festplatte ausschalten nach <Zeitüberschreitung>**


Virtuelle Konsole über URL starten

So starten Sie die virtuelle Konsole über die URL:

1. Öffnen Sie einen unterstützten Web-Browser, und geben Sie in das Adressfeld die folgende URL in Kleinbuchstaben ein: **https://iDRAC7_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 die lokale, Active Directory-, LDAP-, Smart Card- und Einmalanmeldung. Firefox unterstützt die lokale, AD- und die Einmalanmeldung auf Windows-basierten Betriebssystemen und die lokale, Active Directory- und LDAP-Anmeldung 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.

Viewer für virtuelle Konsole verwenden

Der Viewer für die virtuelle Konsole verfügt über verschiedene Steuerungen wie Maussynchronisierung, virtuelle Konsolenskalierung, Chatoptionen, Tastaturmakros, Stromversorgungsmaßnahmen, weitere Bootgeräte und Zugriff auf virtuelle Datenträger. Für mehr Informationen zu diesen Funktionen siehe *iDRAC7 Online-Hilfe*.

 **ANMERKUNG:** Wenn der Remote-Server ausgeschaltet wird, wird die Meldung „Kein Signal“ angezeigt.

Die Titelleiste des Virtuelle Konsole-Viewers zeigt den DNS-Namen oder die IP-Adresse des iDRAC7 an, mit dem Sie über die Management Station verbunden sind. Wenn der iDRAC7 keinen DNS-Namen hat, wird die IP-Adresse angezeigt.

- Für Rack- und Tower-Server:
<DNS-Name / IPv6-Adresse / IPv4-Adresse>, <Modell>, Benutzer:
<Benutzername>, <fps>
- Für Blade-Server:
<DNS-Name / IPv6-Adresse / IPv4-Adresse>, <Modell>, <Steckplatznummer>,
User: <Benutzername>, <fps>

Gelegentlich zeigt der Viewer für die virtuelle Konsole möglicherweise Videos in geringer Qualität an. Der Grund dafür kann eine langsame Netzwerkverbindung sein, die dazu führt, dass ein oder zwei Video-Frames verloren gehen, wenn Sie die Sitzung für die virtuelle Konsole starten. Für die Übertragung aller Video-Frames und zur Verbesserung der nachfolgenden Video-Qualität müssen Sie eine der folgenden Maßnahmen ausführen:

- Klicken Sie auf der Seite **Systemzusammenfassung** unter **Vorschau für virtuelle Konsole** auf **Aktualisieren**.
- Schieben Sie im **Viewer für die virtuelle Konsole** auf der Registerkarte **Leistung** den Regler auf **Maximale Video-Qualität**.

Mauszeiger synchronisieren

Wenn Sie über die virtuelle Konsole eine Verbindung zu einem Managed System herstellen, wird die Mausbeschleunigungsgeschwindigkeit auf dem Managed System möglicherweise nicht mit dem Mauszeiger auf der Management Station synchronisiert, so dass möglicherweise zwei Mauszeiger im Fenster „Viewer“ angezeigt werden.

Stellen Sie bei der Verwendung von Red Hat Enterprise Linux oder Novell SUSE Linux sicher, dass der Mausmodus für Linux konfiguriert ist, bevor Sie den Viewer der virtuellen Konsole starten. Die Standardmauseinstellungen des Betriebssystems werden zum Steuern des Mausfeils auf dem Viewer der virtuellen Konsole verwendet.

Wenn auf dem Viewer für die virtuelle Konsole des Clients zwei Mauszeiger sichtbar sind, weist dies darauf hin, dass das Betriebssystem des Servers die relative Positionierung unterstützt. Dies ist typisch für Linux-Betriebssysteme oder den Lifecycle Controller und verursacht zwei Mauszeiger, wenn sich die Einstellungen für die Mausbeschleunigung von denen des virtuellen Konsolen-Clients unterscheiden. Um dieses Problem zu beheben, wechseln Sie auf einen einzelnen

Cursor oder passen Sie die Mausbeschleunigung des verwalteten Systems an die Beschleunigung der Management Station an:

- Um auf einen einzigen Cursor zu wechseln, wählen Sie im Menü **Hilfsprogramme Ein Cursor** aus.
- Um die Mausbeschleunigung einzustellen, gehen Sie zu **Hilfsprogramme** → **Sitzungsoptionen** → **Maus** . Wählen Sie in der Registerkarte **Mausbeschleunigung** je nach Betriebssystem **Windows** oder **Linux** aus.

Um den Modus mit nur einem Cursor zu beenden, drücken Sie <Esc> oder die konfigurierte Beendigungstaste.



ANMERKUNG: Dies gilt nicht für verwaltete Systeme, die auf Windows-Betriebssystemen ausgeführt werden, da diese die Absolutposition unterstützen.

Wenn Sie die virtuelle Konsole verwenden, um eine Verbindung zu einem verwalteten System mit einem kürzlich installierten Linux-Betriebssystem herzustellen, können Probleme bei der Maussynchronisierung auftreten. Grund dafür kann die Funktion der vorhersehbaren Zeigerbeschleunigung des GNOME-Desktops sein. Zur korrekten Maussynchronisierung in der virtuellen Konsole von iDRAC7 muss diese Funktion deaktiviert sein. Um die vorhersehbare Zeigerbeschleunigung zu deaktivieren, fügen Sie im Abschnitt „Maus“ der Datei `/etc/X11/xorg.conf` Folgendes hinzu:
Option "AccelerationScheme" "lightweight".

Treten die Synchronisierungsprobleme weiterhin auf, nehmen Sie zusätzlich in der Datei `<user_home>/gconf/desktop/gnome/peripherals/mouse/%gconf.xml` folgende Änderung vor:

Ändern Sie die Werte für `motion_threshold` und `motion_acceleration` in `-1`.

Wenn Sie die Mausbeschleunigung auf dem GNOME-Desktop ausschalten, gehen Sie im Viewer für die virtuelle Konsole zu **Extras** → **Sitzungsvorgänge** → **Maus** . Wählen Sie auf der Registerkarte **Mausbeschleunigung** die Option **Keine** aus.

Für exklusiven Zugriff auf die Konsole des verwalteten Servers müssen Sie die lokale Konsole deaktivieren **und** die **Max. Sitzungen** auf der Seite Konfiguration der virtuellen Konsole auf 1 neu konfigurieren.

Alle Tastenanschläge über die virtuelle Konsole führen

Sie können die Option **Alle Tastenanschläge an den Server senden** aktivieren und alle Tastenanschläge und Tastenkombinationen von der Management Station an das Managed System durch den Virtual Console Viewer senden. Wenn dieser nicht aktiviert ist, werden alle Tastenkombinationen an die Management Station gesendet, wo die Sitzung der virtuellen Konsole ausgeführt wird. Um alle Tastenanschläge an den Server zu senden, gehen Sie in dem Viewer für die virtuelle Konsole zu der Registerkarte **Extras** → **Sitzungsvorgänge** → **Allgemein** und wählen Sie die Option **Alle Tastenanschläge an den Server senden** aus, um die Tastenanschläge der Management Station an das Managed System zu leiten.

Das Verhalten der Funktion „Alle Tastenanschläge an den Server senden“ hängt von den folgenden Aspekten ab:

- Plugin-Typ (Java oder ActiveX), auf Basis dessen die Sitzung für die virtuelle Konsole gestartet wird.
Für den Java Client muss die systemeigene Bibliotheken geladen sein, damit die Modi „Alle Tastenanschläge an den Server senden“ und „Single Cursor“ funktionieren. Wenn die systemeigenen Bibliotheken nicht geladen sind, dann sind die Optionen **Alle Tastenanschläge an den Server senden** und **Single Cursor** nicht ausgewählt. Wenn Sie eine dieser Optionen dennoch auswählen, wird eine Fehlermeldung angezeigt, die darauf hinweist, dass die ausgewählten Optionen nicht unterstützt werden.
Für den ActiveX Client muss die systemeigene Bibliothek geladen sein, damit die Option „Alle Tastenanschläge an den Server senden“ funktioniert. Wenn die systemeigenen Bibliotheken nicht geladen sind, wird die Auswahl für die Option **Alle Tastenanschläge an den Server senden** aufgehoben. Wenn Sie die Option dennoch auswählen, wird eine Fehlermeldung angezeigt, die darauf hinweist, dass die ausgewählte Funktion nicht unterstützt wird.
Aktivieren Sie für Mac OS die Option **Zugriff für Hilfsgeräte aktivieren** im Fenster **Universeller Zugriff**, damit die Funktion „Alle Tastenanschläge an den Server senden“ aktiviert ist.

- Betriebssystem, das auf der Management Station und dem Managed System ausgeführt wird. Die Tastenkombinationen, die für das Betriebssystem auf der Management Station von Bedeutung sind, werden nicht an das Managed System weitergeleitet.
- Modus für den Viewer für die virtuelle Konsole – Fensteransicht oder Vollbildschirm.
Im Vollbildschirmmodus ist die Funktion **Alle Tastenanschläge an den Server senden** standardmäßig aktiviert.
Im Fenstermodus werden die Tastenanschläge nur weitergeleitet, wenn der Viewer für die virtuelle Konsole sichtbar und aktiv ist.
Wenn Sie vom Fenster- in den Vollbildschirmmodus wechseln, wird der vorherige Status der Funktion „Alle Tastenanschläge an den Server senden“ wieder aufgenommen.

Verwandte Links

[Java-basierte Sitzung für die virtuelle Konsole, die auf dem Windows-Betriebssystem ausgeführt wird](#)

[Java-basierte Sitzung für virtuelle Konsole, die auf dem Linux-Betriebssystem ausgeführt wird](#)

[ActiveX-basierte Sitzung für virtuelle Konsole, die auf dem Windows-Betriebssystem ausgeführt wird](#)

Java-basierte Sitzung für die virtuelle Konsole, die auf dem Windows-Betriebssystem ausgeführt wird

- Die Tastenkombination „Strg+Alt+Entf“ wird nicht an das Managed System gesendet, sie wird jedoch immer durch Management Station interpretiert.
- Wenn die Option „Alle Tastenanschläge an den Server senden“ aktiviert ist, werden die folgenden Tastenkombinationen nicht an das verwaltete System gesendet:
 - Zurück (Browser) - Taste
 - Vor (Browser) – Taste
 - Aktualisierung (Browser) – Taste
 - Stopp (Browser) – Taste
 - Suchen (Browser) – (Taste)
 - Favoriten (Browser) – Taste
 - Start- und Startseite (Browser) – Taste
 - Stumm – Taste
 - Leiser – Taste
 - Lauter – Taste
 - Nächster Titel – Taste
 - Vorheriger Titel – Taste
 - Datenträger anhalten – Taste
 - Datenträger abspielen/anhalten – Taste
 - E-Mail starten – Taste
 - Datenträger starten – Taste
 - Anwendung 1 starten – Taste
 - Anwendung 2 starten – Taste
- Es werden alle einzelnen Tastenanschläge (keine Kombination aus verschiedenen Tasten, sondern einzelne Tastenanschläge) an das Managed System gesendet. Dazu gehören auch alle Funktionstasten sowie die Umschalt-, Alt-, Strg- und Menütasten. Einige dieser Tasten wirken sich sowohl auf der Management Station als auch auf dem Managed System aus.
Wenn die Management Station und das Managed System beispielsweise unter einem Windows-Betriebssystem laufen und die Option „Alle Tastenanschläge weiterreichen“ deaktiviert ist, wenn Sie die Windows-Taste zum Öffnen des **Startmenüs** drücken, wird das **Startmenü** auf der Management Station und auf dem Managed System geöffnet. Wenn die Option „Alle Tastenanschläge weiterreichen“ allerdings aktiviert ist, wird das **Startmenü** nur auf dem Managed System geöffnet, nicht aber auf der Management Station.

- Wenn die Option „Alle Tastenanschläge weiterreichen“ deaktiviert ist, hängt das Verhalten von den gedrückten Tastenkombinationen und den speziellen Tastenkombinationen ab, die durch das Betriebssystem auf der Management Station interpretiert werden.

Java-basierte Sitzung für virtuelle Konsole, die auf dem Linux-Betriebssystem ausgeführt wird

Das für das Windows-Betriebssystem dargestellte Verhalten gilt auch für das Linux-Betriebssystem, jedoch mit den folgenden Ausnahmen:

- Wenn die Option „Alle Tastenanschläge an den Server senden“ aktiviert ist, wird die Tastenkombination „<Strg+Alt+Entf>“ an das Betriebssystem auf dem Managed System weitergeleitet.
- Die magischen S-Abf-Tasten sind Tastenkombinationen, die durch den Linux-Kernel interpretiert werden. Diese sind nützlich, wenn das Betriebssystem auf der Management Station oder dem Managed System nicht mehr reagiert und Sie das System daher wiederherstellen müssen. Sie können die magischen S-Abf-Tasten auf dem Linux-Betriebssystem über eines der folgenden Verfahren aktivieren:
 - Fügen Sie einen Eintrag zu „`/etc/sysctl.conf`“ hinzu.
 - `echo "1" > /proc/sys/kernel/sysrq`
- Wenn die Option „Alle Tastenanschläge an den Server senden“ aktiviert ist, werden die magischen S-Abf-Tasten an das Betriebssystem auf dem Managed System weitergeleitet. Das Tastensequenzverhalten in Bezug auf das Zurücksetzen des Betriebssystems, also ein Neustart ohne Un-Mounten oder Synchronisieren, hängt davon ab, ob die magische S-Abf-Taste auf der Management Station aktiviert sind:
 - Ist die magische S-Abf-Taste auf der Management Station aktiviert, wird die Management Station über die Tastenkombinationen „<Strg+Alt+S-Abf+b>“ oder „<Alt+S-Abf+b>“, ungeachtet vom Status des Systems, zurückgesetzt.
 - Ist die magische S-Abf-Taste auf der Management Station deaktiviert, wird das Betriebssystem auf dem Managed System über die Tastenkombinationen „<Strg+Alt+S-Abf+b>“ oder „<Alt+S-Abf+b>“ zurückgesetzt.
 - Weitere S-Abf-Tastenkombinationen (z. B. „<Alt+S-Abf+k>“, „<Strg+Alt+S-Abf+m>“, usw.) werden unabhängig davon, ob die S-Abf-Tasten auf der Management Station aktiviert sind, an das Managed System weitergeleitet.

ActiveX-basierte Sitzung für virtuelle Konsole, die auf dem Windows-Betriebssystem ausgeführt wird

Das Verhalten der Funktion „Alle Tastenanschläge an den Server senden“ in einer ActiveX-basierten Sitzung für die virtuelle Konsole, die unter dem Windows-Betriebssystem ausgeführt wird, ähnelt dem Verhalten, das in Bezug auf die Java-basierte Sitzung für die virtuelle Konsole erläutert wurde, die auf der Windows-Management Station ausgeführt wird. Es gelten allerdings die folgenden Ausnahmen:

- Wenn die Funktion „Alle Tastenanschläge an den Server senden“ deaktiviert ist, wird durch Drücken der Taste F1 die Hilfe-Anwendung auf der Management Station und auf dem Managed System gestartet, und es wird die folgende Meldung angezeigt:
Klicken Sie auf der Seite „Virtuelle Konsole“ auf „Hilfe“, um die Online-Hilfe anzuzeigen.
- Die Datenträger-Tasten sind möglicherweise nicht ausdrücklich blockiert.
- Die Tastenkombinationen <Alt + Leer>, <Strg + Alt + +> und <Strg + Alt + -> werden nicht an das Managed System gesendet und werden durch das Betriebssystem auf der Management Station interpretiert.

Virtuelle Datenträger verwalten

Der virtuelle Datenträger ermöglicht dem verwalteten Server, auf Datenträgergeräte der Management Station oder auf ISO-CD/DVD-Images einer Netzwerkfreigabe zuzugreifen, als wären sie Geräte auf dem verwalteten Server.

Über die Funktion für den virtuellen Datenträger können Sie die folgenden Schritte ausführen:

- Remote auf Datenträger zugreifen, die über das Netzwerk mit einem Remote-System verbunden sind
- Anwendungen installieren
- Treiber aktualisieren
- Ein Betriebssystem auf dem Managed System installieren

Hierbei handelt es sich um eine Lizenzfunktion für Rack- und Tower-Server. Sie ist standardmäßig für Blade-Server verfügbar.

Zentrale Funktionen:

- Der virtuelle Datenträger unterstützt virtuelle optische Laufwerke (CD/DVD), Floppy-Laufwerke (einschließlich USB-basierte Laufwerke) und USB-Flash-Laufwerke.
- Sie können nur ein Floppy-Laufwerk, ein USB-Flash-Laufwerk, ein Image oder einen Schlüssel und nur ein optisches Laufwerk auf der Management Station mit einem Managed System verbinden. Unterstützte Floppy-Laufwerke umfassen ein Floppy-Image oder ein verfügbares Floppy-Laufwerk. 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.
- Es ist nicht möglich, über virtuelle Computer auf den virtuellen Floppy-Datenträger von iDRAC7 zuzugreifen.
- 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.

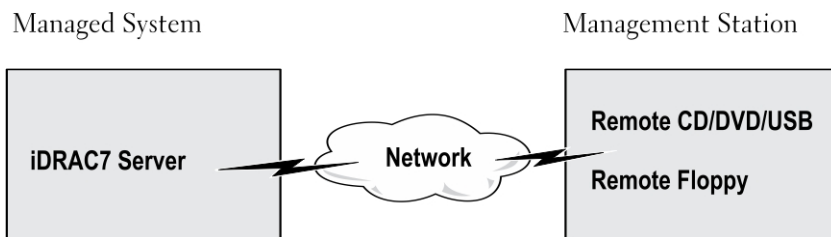


Abbildung 4. Setup für den virtuellen Datenträger

Unterstützte Laufwerke und Geräte

Die folgende Tabelle listet die Laufwerke auf, die durch den virtuellen Datenträger unterstützt werden.

Tabelle 24. Unterstützte Laufwerke und Geräte

| Laufwerk | Unterstützte Speichermedien |
|------------------------------|--|
| Virtuelle optische Laufwerke | <ul style="list-style-type: none"> • 1,44 Zoll Legacy-Diskettenlaufwerk mit 1,44 Zoll-Diskette • CD-ROM • DVD • CD-RW • Kombinationslaufwerk mit dem CD-ROM-Datenträger |
| Virtuelle Floppy-Laufwerke | <ul style="list-style-type: none"> • CD-ROM/DVD-Imagedatei im Format ISO9660 • Floppy-Imagedatei im ISO9660-Format |
| USB-Flash-Laufwerke | <ul style="list-style-type: none"> • USB-CD-ROM-Laufwerk mit CD-ROM-Datenträger • USB-Schlüssel-Image im ISO9660-Format |

Virtuellen Datenträger konfigurieren

Bevor Sie die Einstellungen für den virtuellen Datenträger konfigurieren, müssen Sie sicherstellen, dass Sie zuvor Ihren Web-Browser für die Verwendung des Java- oder ActiveX-Plugins konfigurieren.

Verwandte Links

[Web-Browser für die Verwendung der virtuellen Konsole konfigurieren](#)

Virtuelle Datenträger über die iDRAC7-Web-Schnittstelle konfigurieren

So konfigurieren Sie die Einstellungen für den virtuellen Datenträger:

△ VORSICHT: Setzen Sie iDRAC7 nicht zurück, während eine Sitzung für einen virtuellen Datenträger ausgeführt wird, da dieser Vorgang unerwünschte Folgen nach sich ziehen könnte, z. B. Datenverlust.

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Angehängter Datenträger**.
2. Nehmen Sie die gewünschten Einstellungen vor. Weitere Informationen finden Sie in der *iDRAC7-Online-Hilfe*.
3. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Virtuelle Datenträger über RACADM konfigurieren

So konfigurieren Sie den virtuellen Datenträger:

- Verwenden Sie die Objekte in der Gruppe **iDRAC.VirtualMedia** mit dem Befehl **set**.
- Verwenden Sie die Objekte in der Gruppe **cfgRacVirtual** mit dem Befehl **config**.

Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter dell.com/support/manuals verfügbar ist.

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 dazu wie folgt vor:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **Virtueller Datenträger**. Daraufhin wird die Seite **iDRAC-Einstellungen – Virtueller Datenträger** angezeigt.
2. Wählen Sie auf der Basis Ihrer Anforderungen entweder **Trennen**, **Verbinden** oder **Automatisch verbinden** aus. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**. Die 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 25. Status des verbundenen Datenträgers und Systemantwort

| Status des verbundenen Datenträgers | Systemreaktion |
|-------------------------------------|--|
| Trennen | Image konnte dem System nicht zugeordnet werden. |
| Verbinden | Der Datenträger wird verbunden, auch wenn die Client-Ansicht geschlossen wird. |
| Automatisch verbinden | Der Datenträger wird verbunden, wenn die Client-Ansicht geöffnet wird. Er wird getrennt, wenn die Client-Ansicht geschlossen wird. |

Auf virtuellen Datenträger zugreifen

Sie können auf den virtuellen Datenträger mit oder ohne Verwendung der virtuellen Konsole zugreifen. Bevor Sie auf den virtuellen Datenträger zugreifen, müssen Sie zuvor die Web-Browser konfigurieren.

Verwandte Links

[Web-Browser für die Verwendung der virtuellen Konsole konfigurieren](#)

[Virtuellen Datenträger konfigurieren](#)

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 dazu im Windows Explorer zu **Ordneroptionen**, deaktivieren Sie das Kontrollkästchen **Leere Laufwerke im Ordner „Computer“ ausblenden**, und klicken Sie auf **OK**.


So greifen Sie über die virtuelle Konsole auf den virtuellen Datenträger zu:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Konsole** .

Daraufhin wird die Seite **Virtuelle Konsole** angezeigt.

2. Klicken Sie auf **Virtuelle Konsole starten**.

Der **Virtuelle Konsole-Viewer** wird gestartet.

 **ANMERKUNG:** Unter Linux ist JAVA der Standard-Plugin-Typ für den Zugriff auf die virtuelle Konsole. Unter Windows öffnen Sie zum Zugreifen auf die virtuelle Konsole über die Datei **.jnlp**, um die virtuelle Konsole zu starten.

3. Klicken Sie auf **Virtueller Datenträger** → **Virtuellen Datenträger starten**.

Daraufhin wird das Fenster **Client-Ansicht** des virtuellen Datenträgers angezeigt und listet die Geräte auf, die zum Zuordnen verfügbar sind.

 **ANMERKUNG:** Das Fenster **Virtuelle Konsole-Viewer** muss während des Zugriffs auf den virtuellen Datenträger aktiviert bleiben.

Verwandte Links

[Web-Browser für die Verwendung der virtuellen Konsole konfigurieren](#)

[Virtuellen Datenträger konfigurieren](#)

Virtuellen Datenträger ohne virtuelle Konsole starten

Bevor Sie bei deaktivierter **virtueller Konsole** den virtuellen Datenträger starten, müssen Sie Folgenden sicherstellen:

- Der virtuelle Datenträger befindet sich im Status *Verbunden*.
- Das System ist so konfiguriert, dass leere Laufwerke eingeblendet werden. Gehen Sie dazu im Windows Explorer zu **Ordneroptionen**, deaktivieren Sie das Kontrollkästchen **Leere Laufwerke im Ordner „Computer“ ausblenden**, und klicken Sie auf **OK**.

So starten Sie den virtuellen Datenträger bei deaktivierter virtueller Konsole:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Konsole** .

Daraufhin wird die Seite **Virtuelle Konsole** angezeigt.


2. Klicken Sie auf **Virtuelle Konsole starten**.


Die folgende Meldung wird angezeigt:

Die virtuelle Konsole wurde deaktiviert. Möchten Sie die Umleitung des virtuellen Datenträgers weiterhin nutzen?

3. Klicken Sie auf **OK**, um eine Verbindung zum virtuellen Datenträger herzustellen.

Daraufhin wird das Fenster **Client-Ansicht** des virtuellen Datenträgers angezeigt und listet die Geräte auf, die für das Zuordnen zur Verfügung stehen.

 **ANMERKUNG:** Die Laufwerkbuchstaben der virtuellen Komponente auf dem verwalteten System entsprechen nicht den Buchstaben des physikalischen Laufwerks auf der Management Station.

 **ANMERKUNG:** Der virtuelle Datenträger funktioniert u. U. nicht ordnungsgemäß auf Clients des Windows-Betriebssystems, 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.

Verwandte Links

[Virtuellen Datenträger konfigurieren](#)

Images von virtuellen Datenträgern hinzufügen

Um Images von virtuellen Datenträgern hinzuzufügen, führen Sie im **Client-Ansicht** für den virtuellen Datenträger die folgenden Schritte aus:

- Klicken Sie zum Hinzufügen von Images auf **Image hinzufügen**, und wählen Sie dann die Image-Datei auf der Management Station oder auf Laufwerk C: des Managed System aus.

Das ISO- oder Floppy-Image wird damit zur Liste der verfügbaren Geräte hinzugefügt.

- Um einen Ordner als ISO- oder Floppy-Image hinzuzufügen, klicken Sie auf die Option **Ordner als Image hinzufügen**. Durch diese Funktion wird ein Datenträger-Image des Remote-Ordners erstellt und als über USB verbundenes Gerät auf das Betriebssystem des Servers gemountet.

Der Datenträger wird verbunden, und die Informationen im Fenster **Client-Ansicht** werden aktualisiert.

Wenn der Ordner als Image hinzugefügt wird, wird eine **.iso**-Datei auf dem Desktop der Management Station erstellt, über die diese Funktion verwendet wird. Wenn diese **.iso**-Datei verschoben oder gelöscht wird, kann der entsprechende Eintrag für diesen Ordner im Fenster **Client-Ansicht** des virtuellen Datenträgers nicht verwendet werden. Daher wird empfohlen, die **.iso**-Datei weder zu verschieben, noch zu löschen, während der *hinzugefügte Ordner* verwendet wird. Die **.iso**-Datei kann jedoch entfernt werden, nachdem die Auswahl für den entsprechenden Eintrag zunächst aufgehoben und der Eintrag anschließend über die Option **Image entfernen** entfernt wurde.

Images von virtuellen Datenträgern entfernen

Um das Image zu entfernen, wählen Sie im Fenster **Client-Ansicht** für den virtuellen Datenträger das erforderliche zugeordnete Image aus, und klicken Sie dann auf **Image entfernen**.

Das ausgewählte Image wird aus der Liste der Geräte im Fenster **Client-Ansicht** entfernt.

Details zum virtuellen Gerät anzeigen


Um die Details zu den virtuellen Geräten anzuzeigen, klicken Sie im Fenster **Client-Ansicht** des virtuellen Datenträgers auf **Details**. Daraufhin wird der Abschnitt **Details** mit den verfügbaren virtuellen Geräten und der Lesen-/Schreiben-Aktivität für jedes Gerät angezeigt.

USB-Gerät zurücksetzen

So setzen Sie das USB-Gerät zurück:


1. Klicken Sie im Fenster **Client-Ansicht** für den virtuellen Datenträger auf **Details** und anschließend auf **USB-Reset**. Es wird eine Meldung angezeigt, über die der Benutzer gewarnt wird, dass sich das Zurücksetzen der USB-Verbindung auf den gesamten Input für das Zielgerät auswirken kann, einschließlich des virtuellen Datenträgers und der Maus.
2. Klicken Sie auf **Ja**.

Das USB-Gerät wird zurückgesetzt.

 **ANMERKUNG:** Der virtuelle iDRAC7-Datenträger wird nicht beendet, auch wenn Sie sich von der Sitzung für die iDRAC7-Web-Schnittstelle abgemeldet haben.

Virtuelles Laufwerk zuordnen

So ordnen Sie das virtuelle Laufwerk zu:

 **ANMERKUNG:** Während Sie den ActiveX-basierten virtuellen Datenträger verwenden, benötigen Sie Administratorberechtigungen für das Zuordnen einer Betriebssystem-DVD oder eines USB-Flash-Laufwerks (das mit der Management Station) verbunden ist. Starten Sie zum Zuordnen der Laufwerke IE als Administrator, oder fügen Sie die iDRAC7-IP-Adresse zur Liste der vertrauenswürdigen Sites hinzu.

1. Trennen Sie alle vorhandenen zugeordneten Laufwerke, bevor Sie sie einer anderen Datenträgerquelle zuordnen.
2. Fügen Sie im Fenster **Client-Ansicht** für den virtuellen Datenträger das Image oder den Ordner mit dem Image hinzu.
3. Aktivieren Sie in der Spalte **Zugeordnet** das Kontrollkästchen, das sich auf das Laufwerk mit dem benötigten Image bezieht. Wählen Sie zum Zuordnen von beschreibbaren Geräten als schreibgeschützte Geräte die Option **Schreibgeschützt** für das Gerät aus, bevor Sie es zuordnen.

Das Gerät wird daraufhin dem Managed System zugeordnet.

Verwandte Links

[Korrekte virtuelle Laufwerke für die Zuordnung anzeigen](#)
[Images von virtuellen Datenträgern hinzufügen](#)

Korrekte virtuelle Laufwerke für die Zuordnung anzeigen

Auf einer Linux-basierten Management Station zeigt das Fenster **Client** für den virtuellen Datenträger möglicherweise entfernbare Festplatten und Floppy-Laufwerke an, die nicht Teil der Management Station sind. Um sicherzustellen, dass die korrekten virtuellen Laufwerke zum Zuordnen verfügbar sind, müssen Sie die Schnittstelleneinstellung für die verbundene SATA-Festplatte aktivieren. Gehen Sie dazu wie folgt vor:

1. Starten Sie das Betriebssystem auf der Management Station neu. Drücken Sie während des POST auf die Taste <F2> oder die Taste <F12>, um das System-Setup-Programm aufzurufen.
2. Gehen Sie zu **SATA-Einstellungen**. Dort werden die Schnittstellendetails angezeigt.
3. Aktivieren Sie die Schnittstellen, die derzeit tatsächlich vorhanden und mit der Festplatte verbunden sind.
4. Rufen Sie das Fenster **Client** für den virtuellen Datenträger auf. Es wird mit den Laufwerken angezeigt, die zugeordnet werden können.

Verwandte Links

[Virtuelles Laufwerk zuordnen](#)


Zuordnung für virtuelles Laufwerk aufheben

So heben Sie die Zuordnung für ein virtuelles Laufwerk auf:

1. Deaktivieren Sie im Fenster **Client-Ansicht** für den virtuellen Datenträger in der Spalte **Zugeordnet** das Kontrollkästchen für das Laufwerk.
Die Zuordnung des virtuellen Laufwerks zum Managed System wird aufgehoben.
2. Klicken Sie auf **Beenden**, um die **Sitzungen des virtuellen Datenträgers** zu beenden.
Das Fenster **Client-Ansicht** des virtuellen Datenträgers wird geschlossen.

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 Popup-Fenster werden die virtuellen optischen Laufwerke und virtuellen Diskettenlaufwerke mit den Standard-Startgeräten aufgeführt.
4. Stellen Sie sicher, dass das virtuelle Laufwerk aktiviert und als erstes Gerät mit startfähigem Datenträger aufgelistet wird. Falls erforderlich, folgen Sie den Bildschirmanleitungen zur Änderung der Startreihenfolge.
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 startfähigem Gerät zu starten. Wenn das virtuelle Gerät angeschlossen ist und es ist ein startfähiger Datenträger vorhanden, startet das System zum virtuellen Gerät. Ansonsten ignoriert das System das Gerät - ähnlich wie ein physisches Gerät ohne startfähigen Datenträger.

Einmalstart für virtuelle Datenträger aktivieren

Sie können die Startreihenfolge für den Start nur einmal ändern, nachdem Sie das virtuelle Remote-Datenträgergerät verbunden haben.

Bevor Sie die Einmalstart-Option aktivieren, müssen Sie Folgendes sicherstellen:

- Sie verfügen über die Berechtigung *Benutzer konfigurieren*.
- Ordnen Sie die lokalen oder virtuellen Laufwerke (CD/DVD, Floppy oder das USB-Flash-Gerät) dem startfähigen Datenträger oder dem Image über die Optionen für den virtuellen Datenträger zu.
- Der virtuelle Datenträger befindet sich im Status *Verbunden*, damit die virtuellen Laufwerke in der Startsequenz angezeigt werden.

So aktivieren Sie die Einmalstartoption und starten das Managed System über den virtuellen Datenträger:

1. Gehen Sie in der iDRAC7-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.

Verwandte Links

[Virtuelles Laufwerk zuordnen](#)

[Virtuellen Datenträger konfigurieren](#)


VMCLI-Dienstprogramm installieren und verwenden

Das Dienstprogramm Befehlszeilenoberfläche des virtuellen Datenträgers (VMCLI) ist eine Schnittstelle, die die Funktionen des virtuellen Datenträgers von der Management Station zum iDRAC7 auf dem verwalteten System bereitstellt. Mit diesem Dienstprogramm können Sie auf die Funktionen von virtuellen Datenträgern zugreifen, darunter Image-Dateien und physische Laufwerke, um ein Betriebssystem auf mehreren Remote-Systemen innerhalb eines Netzwerks bereitzustellen.

 **ANMERKUNG:** Sie können das VMCLI-Dienstprogramm nur auf der Management Station ausführen.

Das VMCLI-Dienstprogramm unterstützt folgende Funktionen:

- Austauschbare Geräte oder Images verwalten, auf die Sie über virtuelle Datenträger zugreifen können.
- Sitzungen automatisch beenden, wenn die iDRAC7-Firmware-Option **Einmalstart** aktiviert ist.
- Sichere Datenübertragung zum iDRAC7 mittels SSL-Verschlüsselung.
- Führen Sie die VMCLI-Befehle so lange aus, bis:
 - Die Verbindungen automatisch beendet werden.
 - Ein Betriebssystem den Prozess beendet.

 **ANMERKUNG:** Verwenden Sie zum Beenden des Prozesses unter Windows den Task Manager.

VMCLI installieren

Das VMCLI-Dienstprogramm ist auf der *Dell Systems Management Tools and Documentation*-DVD enthalten. So installieren Sie das VMCLI-Dienstprogramm:

1. Legen Sie die DVD *Dell Systems Management Tools and Documentation* in das DVD-Laufwerk der Verwaltungsstation ein.
 2. Folgen Sie zum Installieren der DRAC-Tools den Anweisungen auf dem Bildschirm.
 3. Überprüfen Sie nach der erfolgreichen Installation den Ordner `install\Del\SysMgt\trac5`, um sicherzustellen, dass die Datei `vmcli.exe` vorhanden ist. Überprüfen Sie in gleicher Weise den entsprechenden Pfad für UNIX.
- Das VMCLI-Dienstprogramm ist damit auf dem System installiert.

VMCLI-Dienstprogramm ausführen

- Wenn das Betriebssystem bestimmte Berechtigungen oder eine Gruppenmitgliedschaft benötigt, benötigen Sie ähnliche Berechtigungen für das Ausführen von VMCLI-Befehlen.
- Auf Windows-Systemen benötigen Nicht-Administratoren zum Ausführen des VMCLI-Dienstprogramms Berechtigungen als **Hauptbenutzer**.
- Auf Linux-Systemen müssen Nicht-Administratoren für den Zugriff auf iDRAC7, für das Ausführen des VMCLI-Dienstprogramms oder zum Protokollieren von Benutzerbefehlen den VMCLI-Befehlen das Präfix `sudo` voranstellen. Zum Hinzufügen oder Bearbeiten von Benutzern in der VMCLI-Administratorengruppe müssen Sie den Befehl `visudo` verwenden.


VMCLI-Syntax

Die VMCLI-Schnittstelle ist auf Windows- und Linux-Systemen identisch. Die VMCLI-Syntax lautet:

```
VMCLI [Parameter] [Betriebssystem_Shell-Optionen]
```

Beispiel: `vmcli -r iDRAC7-IP-Adresse:iDRAC7-SSL-Schnittstelle`

Der *Parameter* aktiviert VMCLI für den Verbindungsaufbau zum angegebenen Server, für den Zugriff auf iDRAC7 und für die Zuordnung zum angegebenen virtuellen Datenträger.

 **ANMERKUNG:** Bei der Eingabe der VMCLI-Syntax müssen Sie auf die Groß- und Kleinschreibung achten.

Zur Gewährleistung der Sicherheit wird empfohlen, die folgenden VMCLI-Parameter zu verwenden:

- `vmcli -i` – Aktiviert ein interaktives Verfahren für den Start von VMCLI. Mit diesem Verfahren ist sichergestellt, dass Benutzername und Kennwort nicht angezeigt werden, wenn Prozesse von anderen Benutzern überprüft werden.
- `vmcli -r <iDRAC7-IP-Adresse[:iDRAC7-SSL-Schnittstelle]> -S -u <iDRAC7-Benutzername> -p <iDRAC7-Benutzerkennwort> -c {<Gerätename> | <Imagedatei>}` – Zeigt an, ob das iDRAC7-Zertifizierungsstellenzertifikat gültig ist. Wenn das Zertifikat nicht gültig ist, wird bei Ausführung dieses Befehls eine Warnmeldung angezeigt. Der Befehl wird jedoch erfolgreich ausgeführt, und die VMCLI-Sitzung wird aufgebaut. Weitere Informationen zu VMCLI-Parametern finden Sie in der *VMCLI-Hilfe* oder auf den entsprechenden Seiten im *VMCLI-Benutzerhandbuch*.

Verwandte Links

[VMCLI-Befehle für den Zugriff auf virtuelle Datenträger](#)

[VMCLI: Betriebssystem-Shell-Optionen](#)

VMCLI-Befehle für den Zugriff auf virtuelle Datenträger

Die folgende Tabelle enthält die VMCLI-Befehle, die für den Zugriff auf verschiedene virtuelle Datenträger erforderlich sind.

Tabelle 26. VMCLI-Befehle

| Virtueller Datenträger | Befehl |
|---|---|
| Diskettenlaufwerk | <code>vmcli -r [iDRAC7-IP-Adresse oder Hostname] -u [iDRAC7-Benutzername] -p [iDRAC7-Benutzerkennwort] -f [Gerätename]</code> |
| Startfähiges Floppy- oder USB-Schlüssel-Image | <code>vmcli -r [iDRAC7-IP-Adresse] [iDRAC7-Benutzername] -p [iDRAC7-Kennwort] -f [floppy.img]</code> |
| CD-Laufwerk über die Option „-f“ | <code>vmcli -r [iDRAC7-IP-Adresse] -u [iDRAC7-Benutzername] -p [iDRAC7-Kennwort] -f [Gerätename] [Imagedatei] -f [CD-Rom - dev]</code> |
| Startfähiges CD/DVD-Image | <code>vmcli -r [iDRAC7-IP-Adresse] -u [iDRAC7-Benutzername] -p [iDRAC7-Kennwort] -c [DVD.img]</code> |

Wenn die Datei nicht schreibgeschützt ist, kann der virtuelle Datenträger in die Imagedatei schreiben. So stellen Sie sicher, dass der virtuelle Datenträger nicht auf den Datenträger schreibt:


- Konfigurieren Sie das Betriebssystem so, dass eine Disketten-Imagedatei, die nicht überschrieben werden darf, mit einem Schreibschutz versehen wird.
- Verwenden Sie Schreibschutzfunktion auf dem Gerät.

Beim Virtualisieren von schreibgeschützten Imagedateien können sich mehrere Sitzungen dieselben Imagedatenträger teilen.

Beim Virtualisieren von physischen Laufwerken kann zu einem bestimmten Zeitpunkt jeweils nur eine Sitzung auf ein gegebenes physisches Laufwerk zugreifen.

VMCLI: Betriebssystem-Shell-Optionen

VMCLI verwendet Shell-Optionen, um die folgenden Betriebssystemfunktionen zu aktivieren:


- **stderr/stdout-Umleitung** - leitet jede gedruckte Dienstprogrammausgabe zu einer Datei um.
Bei Verwendung des Größer-als-Zeichens (>), gefolgt von einem Dateinamen, wird die angegebene Datei mit der gedruckten Ausgabe des VMCLI-Dienstprogramms überschrieben.
-  **ANMERKUNG:** Das VMCLI-Dienstprogramm liest nicht von der Standardeingabe (stdin). Infolgedessen ist keine stdin-Umleitung erforderlich.
- **Ausführung im Hintergrund** – Standardmäßig wird das VMCLI-Dienstprogramm im Vordergrund ausgeführt. Verwenden Sie die Shell-Funktionen des Betriebssystems, um das Dienstprogramm im Hintergrund auszuführen. Unter einem Linux-Betriebssystem wird z. B. durch das auf den Befehl folgende Et-Zeichen (&) veranlasst, dass das Programm als neuer Hintergrundprozess gestartet wird. Diese Methode ist bei Skriptprogrammen nützlich, da dem Skript nach dem Starten eines neuen Vorgangs für den VMCLI-Befehl ermöglicht wird, fortzufahren (andernfalls würde das Skript blockieren, bis das VMCLI-Programm beendet ist).
Wenn mehrere VMCLI-Sitzungen gestartet werden, verwenden Sie die Betriebssystem-spezifischen Funktionen zum Auflisten oder Beenden von Prozessen.

vFlash SD-Karte verwalten

Die vFlash SD-Karte ist eine Secure Digital (SD)-Karte, die in den vFlash SD-Kartensteckplatz eines Systems eingeführt wird. Sie können Karten mit einer Speicherkapazität von bis zu 16 GB verwenden. Nachdem Sie die Karten eingeführt haben, müssen Sie die vFlash-Funktion aktivieren, um Partitionen erstellen und verwalten zu können. vFlash ist eine Lizenzfunktion.

Wenn die Karte im vFlash SD-Kartensteckplatz des Systems nicht erkannt wird, wird die folgende Fehlermeldung in der iDRAC7-Web-Schnittstelle unter **Übersicht** → **Server** → **vFlash** angezeigt:

Die SD-Karte wurde nicht erkannt. Bitte führen Sie eine SD-Karte mit einer Speicherkapazität von mindestens 256 MB ein.

 **ANMERKUNG:** Stellen Sie sicher, dass Sie ausschließlich eine vFlash-kompatible SD-Karte in den iDRAC7 vFlash-Kartensteckplatz einführen. Wenn Sie eine nicht-kompatible SD-Karten einführen, wird beim Initialisieren der Karte die folgende Fehlermeldung angezeigt: *Während der Initialisierung der SD-Karte ist ein Fehler aufgetreten.*


Zentrale Funktionen:

- Bereitstellung von Speicherplatz und Emulation von USB-Gerät(en).
- Erstellung von bis zu 16 Partitionen. Diese Partitionen werden dem System, wenn angeschlossen, je nach ausgewähltem Emulationsmodus als Floppy-Laufwerk, als Festplatte oder CD/DVD-Laufwerk bereitgestellt.
- Erstellung von Partitionen aus unterstützten Dateisystemtypen. Unterstützt das **.img**-Format für Floppy-Emulationstypen, das **.iso**-Format für CD/DVD-Emulationstypen und die **.iso**- und **.img**-Formate für Festplatten-Emulationstypen.
- Erstellung von startfähigen USB-Geräten
- Einmalstart auf ein emuliertes USB-Gerät

 **ANMERKUNG:** Es ist möglich, dass eine vFlash-Lizenz während eines vFlash-Vorgangs ausläuft. In diesem Fall werden die laufenden vFlash-Vorgänge vollständig abgeschlossen.

vFlash SD-Karten-Konfiguration

Stellen Sie vor der Konfiguration von vFlash sicher, dass die vFlash-SD-Karte auf dem System installiert ist. Informationen zur Installation und Entfernung der Karte aus Ihrem System finden Sie im *Hardware Owner's Manual* (Hardware-Benutzerhandbuch) des Systems unter dell.com/support/manuals.

 **ANMERKUNG:** Um vFlash-Funktion zu aktivieren oder deaktivieren und die Karte initialisieren zu können, müssen Sie über die Berechtigung zum Konfigurieren von iDRAC7 verfügen.

Verwandte Links

- [Eigenschaften der vFlash-SD-Karte anzeigen](#)
- [Aktivieren oder Deaktivieren der vFlash-Funktionalität](#)
- [vFlash SD-Karte initialisieren](#)

Eigenschaften der vFlash-SD-Karte anzeigen

Nachdem die vFlash-Funktion aktiviert wurde, können Sie die SD-Karteneigenschaften über die iDRAC7-Web-Schnittstelle oder über RACADM anzuzeigen.

vFlash SD-Karteneigenschaften über die Web-Schnittstelle anzeigen

Um die Eigenschaften der vFlash SD-Karte anzuzeigen, gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **vFlash**. Daraufhin wird die Seite **SD-Karteneigenschaften** angezeigt. Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der *iDRAC7-Online-Hilfe*.

vFlash SD-Karteneigenschaften über RACADM anzeigen

So zeigen Sie die Eigenschaften der vFlash SD-Karten über RACADM an:

1. Öffnen Sie eine Telnet-, SSH- oder serielle Konsole für das System, und melden Sie sich an.
2. Geben Sie den Befehl ein: `racadm getconfig -g cfgvFlashSD`

Die folgenden Nur-Lesen-Eigenschaften werden angezeigt:

- `cfgvFlashSDSize`
- `cfgVFlashSDLicensed`
- `cfgvFlashSDAvailableSize`
- `cfgvFlashSDHealth`
- `cfgVFlashSDEnable`
- `cfgVFlashSDWriteProtect`
- `cfgVFlashSDInitialized`

vFlash SD-Karteneigenschaften über das Dienstprogramm für die iDRAC-Einstellungen anzeigen


Um die vFlash SD-Karteneigenschaften anzuzeigen, gehen Sie im **Dienstprogramm für die iDRAC-Einstellungen** zu **vFlash-Datenträger**. Daraufhin werden die Eigenschaften auf der Seite **iDRAC-Einstellungen – vFlash-Datenträger** angezeigt. Weitere Informationen zu den angezeigten Eigenschaften finden Sie in der *Online-Hilfe des Dienstprogramms für die iDRAC-Einstellungen*.

Aktivieren oder Deaktivieren der vFlash-Funktionalität

Zum Ausführen der Partitionsverwaltung muss die vFlash-Funktionalität aktiviert sein.

vFlash-Funktionen über die Web-Schnittstelle aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die vFlash-Funktion:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **vFlash**. Die Seite **Eigenschaften der SD-Karte** wird angezeigt.
2. Wählen oder löschen Sie die Option **vFlash aktiviert**, um die vFlash-Medienkarte zu aktivieren. Wenn eine vFlash-Partition verbunden wird, ist es nicht möglich, vFlash zu deaktivieren, und es wird eine Fehlermeldung angezeigt.
 **ANMERKUNG:** Wenn die vFlash-Funktion deaktiviert ist, werden die SD-Karteneigenschaften nicht angezeigt.
3. Klicken Sie auf **Anwenden**. Die vFlash-Funktion wird entsprechend Ihrer Auswahl aktiviert oder deaktiviert.

vFlash-Funktionen über RACADM aktivieren oder deaktivieren


So aktivieren oder deaktivieren Sie die vFlash-Funktion über RACADM:

1. Öffnen Sie eine Telnet-, SSH- oder serielle Konsole für das System, und melden Sie sich an.
2. Geben Sie die folgenden Befehle ein:
 - Geben Sie für die Aktivierung von vFlash Folgendes ein:

```
racadm config -g cfgvFlashsd -o cfgvflashSDEnable 1
```

- Geben Sie für die Deaktivierung von vFlash Folgendes ein:

```
racadm config -g cfgvFlashsd -o cfgvflashSDEnable 0
```

 **ANMERKUNG:** Die RACADM-Befehlsfunktionen sind nur verfügbar, wenn eine vFlash SD-Karte vorhanden ist. Wenn keine solche Karte vorhanden ist, wird die folgende Meldung angezeigt: *FEHLER: SD-Karte nicht vorhanden.*

vFlash-Funktionen über das Dienstprogramm für die iDRAC-Einstellungen aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die vFlash-Funktion:

1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **vFlash-Datenträger**. Daraufhin wird die Seite **iDRAC-Einstellungen – vFlash-Datenträger** angezeigt.
2. Wählen Sie **Aktiviert**, um die vFlash-Funktion zu aktivieren, oder wählen Sie **Deaktiviert**, um die vFlash-Funktion zu deaktivieren.
3. Klicken Sie auf **Zurück**, dann auf **Fertigstellen** und schließlich auf **Ja**. Die vFlash-Funktion wird auf der Basis Ihrer Auswahl aktiviert oder deaktiviert.

vFlash SD-Karte initialisieren

Durch den Initialisierungsvorgang wird die SD-Karte neu formatiert, und die anfänglichen vFlash-Systeminformationen auf der Karte werden konfiguriert.

vFlash SD-Karte über die Web-Schnittstelle initialisieren

So initialisieren Sie die vFlash SD-Karte:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **vFlash**. Die Seite **Eigenschaften der SD-Karte** wird angezeigt.
2. Aktivieren Sie **vFLASH**, und klicken Sie auf **Initialisieren**. Alle vorhandenen Inhalte werden entfernt, und die Karte wird mit den neuen vFlash-Systeminformationen formatiert. Wenn eine vFlash-Partition verbunden wird, schlägt der Initialisierungsvorgang fehl, und es wird eine Fehlermeldung angezeigt.

Initialisieren der vFlash-SD-Karte mithilfe von RACADM

So initialisieren Sie die vFlash-SD-Karte mithilfe von RACADM:

1. Öffnen Sie eine Telnet-, SSH- oder serielle Konsole für das System, und melden Sie sich an.
2. Geben Sie den folgenden Befehl ein: `racadm vflashsd initialize`
Sämtliche vorhandenen Partitionen werden gelöscht, und die Karte wird erneut formatiert.

vFlash SD-Karte über das Dienstprogramm für die iDRAC-Einstellungen initialisieren

So initialisieren Sie die vFlash SD-Karte über das Dienstprogramm für die iDRAC-Einstellungen:


1. Gehen Sie im Dienstprogramm für die iDRAC-Einstellungen zu **vFlash-Datenträger**. Daraufhin wird die Seite **iDRAC-Einstellungen – vFlash-Datenträger** angezeigt.
2. Klicken Sie auf **vFlash initialisieren**.
3. Klicken Sie auf **Ja**. Daraufhin wird die Initialisierung gestartet.

4. Klicken Sie auf **Zurück**, und navigieren Sie erneut zur Seite **iDRAC-Einstellungen – vFlash-Datenträger**, um die Erfolgsmeldung anzuzeigen.
Alle vorhandenen Inhalt werden entfernt, und die Karte wird mit den neuen vFlash-Systeminformationen formatiert.

Aktuellen Status über RACADM abrufen

Sie rufen den Status des zuletzt an die vFlash SD-Karte gesendeten Initialisierungsbefehls ab:

1. Öffnen Sie eine Telnet-, SSH- oder serielle Konsole für das System, und melden Sie sich an.
2. Geben Sie den folgenden Befehl ein: `racadm vFlashsd status`
Daraufhin wird der Status der an die SD-Karte gesendeten Befehle angezeigt.
3. Verwenden Sie zum Abrufen des aktuellen Status für alle vflash-Partitionen den folgenden Befehl: `racadm vflashpartition status -a`
4. Verwenden Sie zum Abrufen des aktuellen Status für eine bestimmte Partition den folgenden Befehl: `racadm vflashpartition status -i (index)`


 **ANMERKUNG:** Wenn iDRAC7 zurückgesetzt wird, geht der Status des letzten Partitionsvorgangs verloren.

vFlash-Partitionen verwalten

Sie können die folgenden Schritte über die iDRAC7-Web-Schnittstelle oder RACADM ausführen:

 **ANMERKUNG:** Als Administrator können Sie alle Aufgaben auf den vFlash-Partitionen ausführen. Ansonsten benötigen Sie die Berechtigung **Auf virtuelle Datenträger zugreifen**, um die Inhalte auf der Partition erstellen, löschen, formatieren, verbinden, trennen oder kopieren zu können.

- [Leere Partition erstellen](#)
- [Partition unter Verwendung einer Imagedatei erstellen](#)
- [Partition formatieren](#)
- [Verfügbare Partitionen anzeigen](#)
- [Partition modifizieren](#)
- [Partitionen verbinden oder trennen](#)
- [Vorhandene Partitionen löschen](#)
- [Partitionsinhalte herunterladen](#)
- [Zu einer Partition starten](#)

 **ANMERKUNG:** Wenn Sie auf den vFlash-Seiten auf eine beliebige Option klicken, wenn eine Anwendung wie WS-MAN, das Dienstprogramm für die iDRAC-Einstellungen oder RACADM vFlash verwendet, oder wenn Sie zu einer anderen Seite in der GUI navigieren, zeigt iDRAC7 möglicherweise die folgende Meldung an: `vFlash wird derzeit durch einen anderen Prozess verwendet`. Versuchen Sie es später noch einmal.

vFlash ist in der Lage, eine schnelle Partitionserstellung auszuführen, wenn keine anderen laufenden vFlash-Vorgänge aktiv sind, z. B. Formatieren, Partitionen verbinden, usw. Daher wird empfohlen, zunächst alle Partitionen zu erstellen, bevor Sie andere einzelne Partitionsvorgänge durchführen.

Leere Partition erstellen

Eine leere Partition, die mit dem System verbunden ist, verhält sich ähnlich wie ein leeres USB-Flash-Laufwerk. Sie können leere Partitionen auf einer vFlash-SD-Karte erstellen. Sie können die Partitionen des Typs *Diskette* oder *Festplatte* erstellen. Die Partitionstyp-CD wird nur im Rahmen der Erstellung von Partitionen auf der Basis von Images unterstützt.

Stellen Sie vor dem Erstellen einer leeren Partition Folgendes sicher:

- dass Sie über die Berechtigung **Zugriff auf virtuellen Datenträger** verfügen.
- Die Karte ist initialisiert.
- Die Karte ist nicht schreibgeschützt.
- Auf der Karte wird kein Initialisierungsvorgang ausgeführt.

Leere Partition über die Web-Schnittstelle erstellen

So erstellen Sie eine leere vFlash-Partition:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **vFlash** → **Leere Partition erstellen**. Die Seite **Leere Partition erstellen** wird angezeigt.

2. Geben Sie die erforderlichen Informationen an, und klicken Sie auf **Anwenden**. Weitere Informationen zu diesen Optionen finden Sie in der *iDRAC7-Online-Hilfe*.

Es wird eine neue, unformatierte, leere Partition erstellt, die standardmäßig schreibgeschützt ist. Es wird eine Seite angezeigt, auf der der Verarbeitungsprozentsatz angezeigt wird. In den folgenden Fällen wird eine Fehlermeldung angezeigt:

- Die Karte ist schreibgeschützt.
- Der Kennzeichnungsname stimmt mit der Kennzeichnung einer vorhandenen Partition überein.
- Ein nicht ganzzahliger Wert wurde als Partitionsgröße eingegeben, der Wert übersteigt den auf der Karte verfügbaren Speicherplatz oder die Partition ist größer als 4 GB.
- Auf der Karte wird ein Initialisierungsvorgang ausgeführt.

Leere Partition über RACADM erstellen

So erstellen Sie eine leere 20-MB-Partition:

1. Öffnen Sie eine Telnet-, SSH- oder serielle Konsole für das System, und melden Sie sich an.
2. Geben Sie den Befehl ein: `racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s 20`

Es wird eine leere Partition mit 20 MB im FAT16-Format erstellt. Standardmäßig wird eine leere Partition als editierbare Partition erstellt.

Partition unter Verwendung einer Imagedatei erstellen

Sie können auf der vFlash SD-Karte mithilfe einer Imagedatei eine neue Partition erstellen. Dabei werden die folgenden Imagedateiformate unterstützt: **.img** oder **.iso**. Die Partitionen liegen in den folgenden Emulationstypen vor: Floppy (**.img**), Festplatte (**.img** oder **.iso**) oder CD (**.iso**). Die Größe der erstellen Partition entspricht der Größe der Imagedatei.

Vor der Erstellung einer Partition über eine Imagedatei müssen Sie Folgendes sicherstellen:

- Sie haben Berechtigungen für den Zugriff auf den virtuellen Datenträger.
- Die Karte ist initialisiert.
- Die Karte ist nicht schreibgeschützt.
- Auf der Karte wird kein Initialisierungsvorgang ausgeführt.
- Der Imagetyp und der Emulationstyp stimmen überein.



ANMERKUNG: Das hochgeladene Image und der Emulationstyp stimmen überein. Es werden Probleme auftreten, wenn iDRAC7 ein Gerät mit einem falschen Imagetyp emuliert. Beispiel: Wenn die Partition unter Verwendung eines ISO-Images erstellt wird und der Emulationstyp als Festplatte festgelegt ist, wird das BIOS nicht in der Lage sein, über dieses Image zu starten.

- Die Größe der Image-Datei ist geringer als der auf der Karte verfügbare Speicherplatz oder gleich diesem Speicherplatz.
- Die Imagedatei überschreitet nicht die Größe von 4 GB, da die maximal unterstützte Partitionsgröße 4 GB entspricht. Bei der Erstellung einer Partition über einen Web-Browser muss die Größe der Imagedatei jedoch unterhalb von 2 GB liegen.

Partition unter Verwendung einer Imagedatei mithilfe der Webschnittstelle erstellen


So erstellen Sie eine vFlash-Partition über eine Imagedatei:


1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **vFlash** → **Aus Image erstellen**. Die Seite **Partition über Imagedatei erstellen** wird angezeigt.
2. Geben Sie die angeforderten Informationen ein und klicken Sie auf **Anwenden**. Weitere Informationen über die Optionen finden Sie in der *iDRAC7-Online-Hilfe*.
Es wird eine neue Partition erstellt. Beim CD-Emulationstyp wird eine schreibgeschützte Partition erstellt. Bei den Floppy- oder Festplatten-Emulationstypen wird eine editierbare Partition erstellt. In den folgenden Fällen wird eine Fehlermeldung angezeigt:
 - Die Karte ist schreibgeschützt.
 - Der Kennzeichnungsname stimmt mit der Kennzeichnung einer vorhandenen Partition überein.
 - Die Imagedatei ist größer als 4 GB oder übersteigt den auf der Karte verfügbaren Speicherplatz.
 - Die Imagedatei existiert nicht oder die Erweiterung der Imagedatei ist weder .img noch .iso.
 - Auf der Karte wird bereits ein Initialisierungsvorgang ausgeführt.

Partition unter Verwendung einer Imagedatei mithilfe von RACADM erstellen

So erstellen Sie eine Partition aus einer Imagedatei über RACADM:

1. Öffnen Sie eine Telnet-, SSH- oder serielle Konsole für das System, und melden Sie sich an.
2. Geben Sie den Befehl ein: `racadm vflashpartition create -i 1 -o drive1 -e HDD -t image -l //myserver/sharedfolder/foo.iso -u root -p mypassword`
Es wird eine neue Partition erstellt. Die angelegte Partition ist schreibgeschützt. Dieser Befehl unterscheidet bei der Image-Dateinamenerweiterung zwischen Groß- und Kleinschreibung. Wird beispielsweise die Dateinamenerweiterung in Großbuchstaben (FOO.ISO) statt in Kleinbuchstaben (FOO.iso) angegeben, gibt der Befehl einen Syntaxfehler aus.

 **ANMERKUNG:** Diese Funktion wird im lokalen RACADM nicht unterstützt.

 **ANMERKUNG:** Die Erstellung einer vFlash-Partition aus einer Imagedatei, die sich auf dem CFS oder der für NFS IPv6 aktivierten Netzwerkfreigabe befindet, wird nicht unterstützt.

Partition formatieren

Sie können eine vorhandene Partition auf der vFlash-SD-Karte auf Grundlage des Dateisystemtyps formatieren. Die unterstützten Dateisystemtypen sind EXT2, EXT3, FAT16 und FAT32. Sie können nur eine Partition des Typs Festplatte oder Diskette, aber nicht CD, anlegen. Schreibgeschützte Partitionen können nicht formatiert werden.

Bevor Sie eine Partition aus einer Imagedatei erstellen, müssen Sie Folgendes sicherstellen:

- Sie haben Berechtigungen für den **Zugriff auf den virtuellen Datenträger**.
- Die Karte ist initialisiert.
- Die Karte ist nicht schreibgeschützt.
- Auf der Karte wird kein Initialisierungsvorgang ausgeführt.

So formatieren Sie eine vFlash-Partition:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **vFlash** → **Formatieren**. Die Seite **Partition formatieren** wird angezeigt.
2. Geben Sie die erforderlichen Informationen ein und klicken Sie auf **Übernehmen**. Weitere Informationen zu den verfügbaren Optionen finden Sie in der *iDRAC7-Online-Hilfe*. Es wird eine Warnungsmeldung angezeigt, die darauf hinweist, dass alle Daten auf der Partition gelöscht werden.
3. Klicken Sie auf **OK**. Die ausgewählte Partition wird gemäß dem festgelegten Dateisystemtyp formatiert. Es wird eine Fehlermeldung angezeigt, wenn Folgendes zutrifft:
 - Die Karte ist schreibgeschützt.
 - Auf der Karte wird bereits ein Initialisierungsvorgang ausgeführt.

Verfügbare Partitionen anzeigen

Stellen Sie sicher, dass die vFlash-Funktion aktiviert ist, damit die Liste der verfügbaren Partitionen angezeigt wird.


Verfügbare Partitionen über die Web-Schnittstelle anzeigen

Um die verfügbaren vFlash-Partitionen anzuzeigen, gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **vFlash** → **Verwalten**. Die Seite **Partitionen verwalten** wird angezeigt und zeigt die verfügbaren Partitionen und die verknüpften Informationen für jede einzelnen Partition an. Weitere Informationen zu den Partitionen finden Sie in der *iDRAC7-Online-Hilfe*.

Verfügbare Partitionen über RACADM anzeigen

So zeigen Sie die verfügbaren Partitionen und die dazugehörigen Eigenschaften über RACADM an:


1. Öffnen Sie eine Telnet-, SSH- oder serielle Konsole für das System, und melden Sie sich an.
2. Geben Sie die folgenden Befehle ein:
 - So listen Sie alle vorhandenen Partitionen und deren Eigenschaften auf:
`racadm vflashpartition list`
 - So rufen Sie den Status des Vorgangs auf Partition 1 ab:
`racadm vflashpartition status -i 1`
 - So rufen Sie den Status sämtlicher vorhandener Partitionen ab:
`racadm vflashpartition status -a`

 **ANMERKUNG:** Die Option „-a“ ist nur mit der Statusaktion gültig.

Partition modifizieren

Sie können den Schreibschutz für eine schreibgeschützte Partition aktivieren oder deaktivieren. Vor dem Ändern einer Partition müssen Sie Folgendes sicherstellen:


- Die vFlash-Funktion ist aktiviert.
- Sie haben Berechtigungen für den **Zugriff auf den virtuellen Datenträger**.

 **ANMERKUNG:** Standardmäßig wird eine schreibgeschützte Partition erstellt.

Partition über die Web-Schnittstelle ändern

So ändern Sie eine Partition:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **vFlash** → **Verwalten**. Die Seite **Partitionen verwalten** wird angezeigt.
2. Führen Sie in der Spalte **Nur-Lesen** die folgenden Schritte aus:
 - Aktivieren Sie das Kontrollkästchen für die Partition(en), und klicken Sie für den Wechsel in den schreibgeschützten Modus auf **Anwenden**.
 - Deaktivieren Sie das Kontrollkästchen für die Partition(en), und klicken Sie für den Wechsel des schreibgeschützten Modus auf **Anwenden**.Auf Grundlage der entsprechenden Auswahl werden die Partitionen zu Nur-Lesen oder Lesen-Schreiben geändert.

 **ANMERKUNG:** Handelt es sich um eine Partition des Typs CD, ist der Status schreibgeschützt. Sie können den Zustand nicht zu Lesen-Schreiben ändern. Wenn die Partition verbunden ist, ist das Kontrollkästchen grau unterlegt.

Partition über RACADM ändern

So zeigen Sie die verfügbaren Partitionen und Eigenschaften auf der Karte an:

1. Öffnen Sie eine Telnet-, SSH- oder serielle Konsole für das System, und melden Sie sich an.
2. Geben Sie die folgenden Befehle ein:
 - So ändern Sie eine schreibgeschützte Partition zu Lesen-Schreiben:

```
racadm config -g cfgvflashpartition -i 1 -o  
cfgvflashPartitionAccessType 1
```
 - So ändern Sie eine Lesen-Schreiben-Partition zu Nur-Lesen:

```
racadm config -g cfgvflashpartition -i 0 -o  
cfgvflashPartitionAccessType 1
```

Partitionen verbinden oder trennen

Wenn Sie eine oder mehrere Partitionen verbinden, werden diese gegenüber dem Betriebssystem und dem BIOS als USB-Massenspeichergeräte angezeigt. Wenn Sie mehrere Partitionen verbinden, werden diese auf der Basis des zugewiesenen Index in aufsteigender Reihenfolge im Betriebssystem und im BIOS-Startreihenfolgemenu angezeigt.

Wenn Sie eine Partition trennen, wird diese nicht mehr im Betriebssystem und im BIOS-Startreihenfolgemenu angezeigt.

Wenn Sie eine Partition verbinden oder trennen, wird der USB-Bus auf dem Managed System zurückgesetzt. Dies wirkt sich auch auf die Anwendungen aus, die vFlash verwenden. Außerdem werden die Sitzungen für die virtuellen iDRAC7-Datenträger getrennt.

Vor dem Verbinden und Trennen einer Partition müssen Sie Folgendes sicherstellen:

- Die vFlash-Funktion ist aktiviert.
- Es wird nicht bereits ein Initialisierungsvorgang auf der Karte ausgeführt.
- Sie haben Berechtigungen für den **Zugriff auf den virtuellen Datenträger**.

Partitionen über die Web-Schnittstelle verbinden

So werden Partitionen verbunden oder abgetrennt:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **vFlash** → **Verwalten**.

Die Seite **Partitionen verwalten** wird angezeigt.

2. Führen Sie in der Spalte **Verbunden** die folgenden Schritte aus:
 - Aktivieren Sie das Kontrollkästchen für die Partition(en), und klicken Sie zum Verbinden der Partition(en) auf **Anwenden**.
 - Aktivieren Sie das Kontrollkästchen für die Partition(en), und klicken Sie zum Trennen der Partition(en) auf **Anwenden**.Auf Grundlage der entsprechenden Auswahl werden die Partitionen verbunden oder abgetrennt.

Partitionen über RACADM verbinden oder trennen

So werden Partitionen verbunden oder abgetrennt:

1. Öffnen Sie eine Telnet-, SSH- oder serielle Konsole für das System, und melden Sie sich an.
2. Geben Sie die folgenden Befehle ein:
 - So verbinden Sie eine Partition:

```
racadm config -g cfgvflashpartition -i 1 -o  
cfgvflashPartitionAttachState 1
```
 - So trennen Sie eine Partition ab:

```
racadm config -g cfgvflashpartition -i 0 -o  
cfgvflashPartitionAttachState 1
```

Verhalten des Betriebssystems bei verbundenen Partitionen

Windows- und Linux-Betriebssysteme:

- Das Betriebssystem kontrolliert die Laufwerksbuchstaben und weist sie den angeschlossenen Partitionen zu.
- Schreibgeschützte Partitionen sind schreibgeschützte Laufwerke auf dem Betriebssystem.
- Das Betriebssystem muss das Dateisystem einer angeschlossenen Partition unterstützen. Ansonsten können Sie die Inhalte der Partition über das Betriebssystem weder lesen noch ändern. In einer Windows-Umgebung kann das Betriebssystem beispielsweise den Partitionstyp EXT2 nicht lesen, da es sich hierbei um einen Linux-eigenen Typ handelt. In einer Linux-Umgebung kann das Betriebssystem wiederum den Partitionstyp NTFS nicht lesen, da es sich hierbei um einen Windows-eigenen Typ handelt.
- Die Beschriftung der vFlash-Partition weicht vom Volume-Namen des Dateisystems auf dem emulierten USB-Gerät ab. Sie können den Volume-Namen des emulierten USB-Geräts von dem Namen auf dem Betriebssystem ändern. Auf den Namen der Partitionsbeschriftung, der in iDRAC7 gespeichert wird, hat dies jedoch keine Auswirkung.

Vorhandene Partitionen löschen

Stellen Sie vor dem Löschen vorhandener Partitionen Folgendes sicher:

- Die vFlash-Funktion ist aktiviert.
- Die Karte ist nicht schreibgeschützt.
- Die Partition ist nicht verbunden.
- Auf der Karte wird kein Initialisierungsvorgang ausgeführt.

Vorhandene Partitionen über die Web-Schnittstelle löschen

Löschen einer bestehenden Partition:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **vFlash** → **Verwalten**. Die Seite **Partitionen verwalten** wird angezeigt.
2. Klicken Sie in der Spalte **Löschen** auf das Symbol zum Löschen, um die gewünschte Partition zu löschen.

Es wird eine Meldung angezeigt, aus der hervorgeht, dass die Partition durch diese Maßnahme endgültig gelöscht wird.

3. Klicken Sie auf OK.

Die Partition ist damit gelöscht.

Vorhandene Partitionen über RACADM löschen

So löschen Sie Partitionen:

1. Öffnen Sie eine Telnet-, SSH- oder serielle Konsole für das System, und melden Sie sich an.

2. Geben Sie die folgenden Befehle ein:

- So löschen Sie eine Partition:

```
racadm vflashpartition delete -i 1
```

- Zum Löschen sämtlicher Partitionen ist die vFlash-SD-Karte erneut zu initialisieren.

Partitionsinhalte herunterladen

Sie können die Inhalte einer vFlash-Partition in den folgenden Formaten herunterladen: **.img** oder **.iso**:

- Managed System (über das iDRAC7 ausgeführt wird)
- Netzwerkstandort, der mit einer Management Station verknüpft ist.

Vor dem Herunterladen der Partitionsinhalte müssen Sie Folgendes sicherstellen:


- Sie haben Berechtigungen für den Zugriff auf den virtuellen Datenträger.
- Die vFlash-Funktion ist aktiviert.
- Auf der Karte wird kein Initialisierungsvorgang ausgeführt.
- Wenn eine Lesen-Schreiben-Partition vorliegt, darf diese nicht verbunden sein.

So laden Sie die Inhalte der vFlash-Partition herunter:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht → **Server** → **vFlash** → **Herunterladen**.**


Die Seite **Partition herunterladen** wird angezeigt.

2. Wählen Sie aus dem Drop-Down-Menü **Kennzeichnung eine Partition aus, die Sie herunterladen möchten, und klicken Sie auf **Herunterladen**.**

 **ANMERKUNG:** Alle vorhandenen Partitionen (mit Ausnahme der verbundenen Partitionen) werden in der Liste angezeigt. Es wird standardmäßig die erste Partition ausgewählt.

3. Legen Sie den Speicherort fest, an dem die Datei gespeichert werden soll.

Der Inhalt der ausgewählten Partition wird an den festgelegten Speicherort heruntergeladen.

 **ANMERKUNG:** Wenn nur der Ordnerspeicherort angegeben ist, wird die Partitionsbezeichnung mit dem Dateinamen und außerdem bei CD- und Festplattenpartitionen mit der Dateierweiterung **.iso** und bei Floppy- und Festplattenpartitionen mit der Dateierweiterung **.img** gekennzeichnet.

Zu einer Partition starten

Sie können eine verbundene vFlash-Partition als Startgerät für den nächsten Startvorgang einrichten.


Vor dem Starten einer Partition müssen Sie Folgendes sicherstellen:

- Die vFlash-Partition enthält ein startfähiges Image (in den Formaten **.img** oder **.iso**), um einen Start vom Gerät zu ermöglichen.

- Die vFlash-Funktion ist aktiviert.
- Sie haben Berechtigungen für den Zugriff auf den virtuellen Datenträger.


Über die Web-Schnittstelle auf eine Partition starten

Weitere Informationen zum Festlegen der vFlash-Partition als ein erstes Startlaufwerk finden Sie unter [Erstes Startlaufwerk einrichten](#).

 **ANMERKUNG:** Wenn die verbundene(n) vFlash-Partition(en) nicht im Drop-Down-Menü **Erstes Startlaufwerk** gelistet ist/sind, müssen Sie sicherstellen, dass das BIOS in der aktuellen Version vorliegt.


Über RACADM auf eine Partition starten

Um eine vFlash-Partition als erstes Startgerät einzustellen, verwenden Sie `cfgServerInfo`. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

 **ANMERKUNG:** Wenn Sie diesen Befehl ausführen, wird die Kennzeichnung der vFlash-Partition automatisch auf Einmalstart eingestellt, `cfgserverBootOnce` wird auf `1` eingestellt. Der Einmalstart startet das Gerät auf der Partition nur einmal und behält es nicht dauerhaft als erstes Gerät in der Startreihenfolge.


SMCLP verwenden

Die Server Management Command Line Protocol (SMCLP)-Spezifikation aktiviert die CLI-basierte Systemverwaltung. Es definiert ein Protokoll für die Verwaltungsbefehle, die über Standardzeichen-basierte Streams übertragen werden. Dieses Protokoll greift über einen von Hand eingegebenen Befehlssatz auf einen Common Information Model Object Manager (CIMOM) zu. SMCLP ist eine Unterkomponente der Distributed Management Task Force (DMTF)-Initiative, mit der die Systemverwaltung über mehrere Plattformen hinweg optimiert werden kann. In Verbindung mit der Spezifikation für verwaltete Elementadressierung und zahlreichen Profilen zu SMCLP-Zuordnungsspezifikationen beschreibt die SMCLP-Spezifikation die Standard-Verben und -Ziele zum Ausführen verschiedener Verwaltungsaufgaben.

 **ANMERKUNG:** Es wird angenommen, dass Sie mit der SMASH-Initiative (Systemverwaltungsarchitektur für Serverhardware) und den SMWG SMCLP-Angaben vertraut sind.

Das SM-CLP ist eine Unterkomponente der DMTF (Distributed Management Task Force) SMASH-Initiative zum Rationalisieren der Serververwaltung über mehrere Plattformen. In Verbindung mit der Spezifikation für verwaltete Elementadressierung und zahlreichen Profilen zu SM-CLP-Zuordnungsspezifikationen beschreibt die SM-CLP-Spezifikation die Standard-Verben und -Ziele zum Ausführen verschiedener Verwaltungsaufgaben.

Das SMCLP wird von der iDRAC7-Controller-Firmware aus gehostet und unterstützt Telnet, SSH und seriell-basierte Schnittstellen. Die iDRAC7-SMCLP-Schnittstelle basiert auf der SMCLP-Spezifikation Version 1.0, bereitgestellt von der DMTF-Organisation.

 **ANMERKUNG:** Informationen zu den Profilen, Erweiterungen und MOFs können unter delltechcenter.com abgerufen werden, und die gesamten DMTF-Informationen können von dmf.org/standards/profiles/ abgerufen werden.

SM-CLP-Befehle setzen einen Teilsatz der Befehle des lokalen RACADM um. Diese Befehle eignen sich gut für das Scripting, da sie über eine Befehlszeile der Management Station ausgeführt werden können. Sie können die Befehlsausgabe in eindeutigen Formaten, einschließlich XML, abrufen, wodurch das Scripting und die Integration mit vorhandenen Berichterstattungs- und Verwaltungshilfsprogrammen erleichtert wird.

System-Verwaltungsfunktionen über SMCLP

Mit iDRAC7 SMCLP können Sie die folgenden Funktionen ausführen:

- Serverenergieverwaltung – System einschalten, herunterfahren oder neu starten
- Verwaltung des Systemereignisprotokolls (SEL) – SEL-Datensätze anzeigen oder löschen
- iDRAC7-Benutzerkonto verwalten
- Systemeigenschaften anzeigen

SMCLP-Befehle ausführen


Sie können die SMCLP-Befehle über die SSH- oder Telnet-Schnittstelle ausführen. Öffnen Sie eine SSH- oder Telnet-Schnittstelle, und melden Sie sich als Administrator bei iDRAC7 an. Daraufhin wird die SMCLP-Befehlseingabe (admin ->) angezeigt.

SMCLP-Befehlseingaben:

- yx1x-Blade-Server verwenden –\$.

- yx1x-Rack- und Tower-Server verwenden `admin->`.
- yx2x-Blade-, Rack- und Tower-Server verwenden `admin->`.

Hier steht „y“ für ein alphanumerisches Zeichen wie „M“ (für Blade-Server), „R“ (für Rack-Server) und „T“ (für Tower-Server) und „x“ für eine Zahl. Diese Zahl dient der Kennzeichnung der Dell PowerEdge-Server-Generation.

 **ANMERKUNG:** Skripte, die `-$` verwenden, können diese für yx1x-Systeme verwenden, aber beginnend bei yx2x-Systemen kann ein Skript mit `admin->` für Blade-, Rack- und Tower-Server verwendet werden.

iDRAC7 SMCLP-Syntax

Das iDRAC7 SMCLP verwendet das Konzept von Verben und Zielen und stellt Systemverwaltungsfunktionen über die CLI bereit. Das Verb zeigt den auszuführenden Vorgang an, und das Ziel bestimmt die Einheit (oder das Objekt), die den Vorgang ausführt.

Die SMCLP Befehlszeilensyntax:

```
<Verb> [<Optionen>] [<Ziel>] [<Eigenschaften>]
```

Die folgende Tabelle zeigt die Verben sowie ihre Definitionen.

Tabelle 27. SMCLP-Verben

| Verb | Definition |
|----------------------|---|
| <code>cd</code> | Navigiert durch den MAP mittels der Shell. |
| <code>set</code> | Stellt eine Eigenschaft auf einen bestimmten Wert ein. |
| <code>help</code> | Zeigt die Hilfe für ein bestimmtes Ziel an. |
| <code>reset</code> | Setzt das Ziel zurück. |
| <code>show</code> | Zeigt die Zieleigenschaften, Verben und Unterziele an. |
| <code>start</code> | Schaltet ein Ziel ein. |
| <code>stop</code> | Führt ein Ziel herunter. |
| <code>exit</code> | Beendet die SMCLP-Shell-Sitzung |
| <code>version</code> | Zeigt die Versionsattribute eines Ziels an. |
| <code>load</code> | Lädt ein Binärbild von einer URL zu einer bestimmten Zieladresse. |

Die folgende Tabelle enthält eine Liste mit Zielen.

Tabelle 28. SMCLP-Ziele

| Ziel | Definitionen |
|---|---|
| <code>admin1</code> | admin domain |
| <code>admin1/profiles1</code> | Registrierte Profile in iDRAC7 |
| <code>admin1/hdwr1</code> | Hardware |
| <code>admin1/system1</code> | Ziel des verwalteten Systems |
| <code>admin1/system1/capabilities1</code> | SMASH-Erfassungsfunktionen des verwalteten Systems |
| <code>admin1/system1/capabilities1/pwrcap1</code> | Funktionen zur Energienutzung des verwalteten Systems |

| Ziel | Definitionen |
|---|---|
| admin1/system1/capabilities1/elecapi | Zielfunktionen des verwalteten Systems |
| admin1/system1/logs1 | Datensatzprotokoll-Erfassungsziel |
| admin1/system1/logs1/log1 | Systemereignisprotokoll (SEL) Datensatzeintrag |
| admin1/system1/logs1/log1/record* | Eine einzelne SEL-Datensatzinstanz auf dem verwalteten System |
| admin1/system1/settings1 | SMASH-Erfassungseinstellungen des verwalteten Systems |
| admin1/system1/capacities1 | SMASH-Erfassung der verwalteten Systemkapazitäten |
| admin1/system1/consoles1 | SMASH-Erfassung der verwalteten Systemkonsolen |
| admin1/system1/sp1 | Serviceprozessor |
| admin1/system1/sp1/timesvc1 | Zeitansage des Serviceprozessors |
| admin1/system1/sp1/capabilities1 | SMASH-Erfassung der Serviceprozessorfunktionen |
| admin1/system1/sp1/capabilities1/clpcap1 | CLP-Dienstfunktionen |
| admin1/system1/sp1/capabilities1/pwrmgtcap1 | Dienstfunktionen der Stromzustandsverwaltung auf dem System |
| admin1/system1/sp1/capabilities1/acctmgtcap* | Dienstfunktionen der Kontoverwaltung |
| admin1/system1/sp1/capabilities1/rolemgtcap* | Lokale rollenbasierte Verwaltungsfunktionen |
| admin1/system1/sp1/capabilities1/PwrutilmgTCap1 | Energienutzung-Verwaltungsfunktionen |
| admin1/system1/sp1/capabilities1/elecapi | Authentifizierungsfunktionen |
| admin1/system1/sp1/settings1 | Sammlung von Serviceprozessoreinstellungen |
| admin1/system1/sp1/settings1/clpsetting1 | CLP-Dienst-Einstellungsdaten |
| admin1/system1/sp1/clpsvc1 | CLP-Dienst-Protokolldienst |
| admin1/system1/sp1/clpsvc1/clpendpt* | CLP-Dienst-Protokollendpunkt |
| admin1/system1/sp1/clpsvc1/tcpndpt* | CLP-Dienst-Protokoll-TCP-Endpunkt |
| admin1/system1/sp1/jobq1 | Auftragswarteschlange des CLP-Dienst-Protokolls |
| admin1/system1/sp1/jobq1/job* | CLP-Dienst-Protokollaufgabe |
| admin1/system1/sp1/pwrmgtsvc1 | Stromzustandsverwaltungsdienst |
| admin1/system1/sp1/account1-16 | Lokales Benutzerkonto |

| Ziel | Definitionen |
|---|--|
| admin1/sysetm1/sp1/account1-16/identity1 | Identitätskonto des lokalen Benutzers |
| admin1/sysetm1/sp1/account1-16/identity2 | IPMI-Identitätskonto (LAN) |
| admin1/sysetm1/sp1/account1-16/identity3 | IPMI-Identitätskonto (seriell) |
| admin1/sysetm1/sp1/account1-16/identity4 | CLP-Identitätskonto |
| admin1/system1/sp1/acctsvc1 | Verwaltungsdienst für lokales Benutzerkonto |
| admin1/system1/sp1/acctsvc2 | IPMI-Kontoverwaltungsdienst |
| admin1/system1/sp1/acctsvc3 | CLP-Kontoverwaltungsdienst |
| admin1/system1/sp1/rolesvc1 | Lokaler rollenbasierter Authentifizierungsdienst (RBA) |
| admin1/system1/sp1/rolesvc1/Role1-16 | Lokale Rolle |
| admin1/system1/sp1/rolesvc1/Role1-16/privilege1 | Lokale Rollenberechtigung |
| admin1/system1/sp1/rolesvc2 | IPMI-RBA-Dienst |
| admin1/system1/sp1/rolesvc2/Role1-3 | IPMI-Rolle |
| admin1/system1/sp1/rolesvc2/Role4 | IPMI Seriell-über-LAN-Rolle (SOL) |
| admin1/system1/sp1/rolesvc3 | CLP-RBA-Dienst |
| admin1/system1/sp1/rolesvc3/Role1-3 | CLP-Rolle |
| admin1/system1/sp1/rolesvc3/Role1-3/privilege1 | CLP-Rollenberechtigung |

Verwandte Links

[SMCLP-Befehle ausführen](#)

[Anwendungsbeispiele](#)

MAP-Adressbereich navigieren

Objekte, die mit dem SM-CLP verwaltet werden können, werden durch Ziele repräsentiert, die in einem hierarchischen Bereich, Adressbereich des Verwaltungszugriffspunkts (Manageability Access Point = MAP) genannt, angeordnet sind. Ein Adresspfad legt den Pfad vom Adressbereichsstamm zu einem Objekt im Adressbereich fest.

Das root-Ziel wird durch einen Schrägstrich (/) oder einen umgekehrten Schrägstrich (\) dargestellt. Es ist der standardmäßige Ausgangspunkt, wenn Sie sich am iDRAC7 anmelden. Wechseln Sie von root abwärts, indem Sie das Verb `cd` verwenden.



ANMERKUNG: Auf SM-CLP-Adresspfaden sind der Schrägstrich (/) und der umgekehrte Schrägstrich (\) untereinander austauschbar. Mit einem umgekehrten Schrägstrich am Ende einer Befehlszeile wird jedoch der Befehl in der nächsten Zeile fortgesetzt und der Schrägstrich wird ignoriert, wenn der Befehl geparkt wird.

Wenn Sie z. B. zum dritten Eintrag des Systemereignisprotokolls (SEL) wechseln möchten, geben Sie den folgenden Befehl ein:

```
->cd /admin1/system1/logs1/log1/record3
```

Geben Sie das Verb `cd` ohne Ziel ein, um Ihren aktuellen Standort im Adressbereich zu finden. Die Abkürzungen `..` und `.` funktionieren auf dieselbe Weise wie unter Windows und Linux: `..` bezieht sich auf die übergeordnete Ebene und `.` bezieht sich auf die aktuelle Ebene.

Verb „show“ verwenden

Verwenden Sie zum Anzeigen weiterer Informationen zu einem Ziel das Verb `show`. Durch dieses Verb werden die Eigenschaften der Ziele, der Unterziele, der Verknüpfungen und eine Liste der SM-CLP-Verben angezeigt, die an einem bestimmten Standort zulässig sind.

Option `-display` verwenden

Anhand der Option `show -display` können Sie die Befehlsausgabe auf eines oder mehrere der folgenden Elemente einschränken: Eigenschaften, Ziele, Zuordnungen und Verben. Wenn Sie z. B. nur die Eigenschaften und Ziele des aktuellen Orts anzeigen möchten, verwenden Sie den folgenden Befehl:

```
show -display properties,targets
```

Wenn Sie nur bestimmte Eigenschaften aufführen möchten, qualifizieren Sie sie, wie im folgenden Befehl gezeigt wird:

```
show -d properties=(userid,name) /admin1/system1/sp1/account1
```

Wenn Sie nur eine Eigenschaft anzeigen möchten, können Sie die Klammern auslassen.

Option `-level` verwenden

Die Option `show -level` führt den Befehl `show` über weitere Ebenen neben dem angegebenen Ziel aus. Verwenden Sie zum Anzeigen aller Ziele und Eigenschaften im Adressbereich die Option `-l all`.

Option `-output` verwenden

Die Option `-output` legt eins von vier Formaten für die Ausgabe von SM-CLP-Verben fest: **text**, **clpcsv**, **keyword** und **clpxml**.

Das Standardformat ist **text**, die am einfachsten lesbare Ausgabe. Das Format **clpcsv** ist ein Format, bei dem Werte durch Kommas getrennt werden. Es eignet sich zum Laden in ein Tabellenkalkulationsprogramm. Das Format **keyword** gibt Informationen als Liste von **keyword=value**-Paaren (eins pro Zeile) aus. Das Format **clpxml** ist ein XML-Dokument, das ein **response-XML**-Element enthält. Die DMTF hat die Formate **clpcsv** und **clpxml** festgelegt, deren Spezifikationen auf der DMTF-Website unter www.dmtf.org verfügbar sind.

Das folgende Beispiel zeigt, wie der Inhalt des SEL in XML ausgegeben werden kann:

```
show -l all -output format=clpxml /admin1/system1/logs1/log1
```

Anwendungsbeispiele

In diesem Abschnitt werden die Fallbeispiele für SMCLP dargestellt:

- [Server-Energieverwaltung](#)
- [SEL-Verwaltung](#)
- [MAP-Zielnavigation](#)

Server-Energieverwaltung

Die folgenden Beispiele stellen die Verwendung von SMCLP für die Ausführung von Energieverwaltungsaufgaben auf einem Managed System dar.

Geben Sie die folgenden Befehle an der SMCLP-Befehlseingabe ein:

- **Ausschalten des Servers:**
->stop /system1
Die folgende Meldung wird angezeigt:
system1 wurde erfolgreich angehalten
- **Einschalten des Servers:**
->start /system1
Die folgende Meldung wird angezeigt:
system1 wurde erfolgreich gestartet
- **Neustart des Servers:**
->reset /system1
Die folgende Meldung wird angezeigt:
system1 wurde erfolgreich zurückgesetzt

SEL-Verwaltung

Die folgenden Beispiele zeigen die Verwendung von SMCLP für die Ausführung von SEL-bezogenen Vorgängen auf dem Managed System. Geben Sie die folgenden Befehle an der SMCLP-Eingabeaufforderung ein:

- **Zum Anzeigen von SEL:**
->show /system1/logs1/log1
Die folgende Ausgabe wird angezeigt.
/system1/logs1/log1
Ziele:
Record1
Record2
Record3
Record4
Record5
Eigenschaften:
InstanceID = IPMI:BMCI SEL Log
MaxNumberOfRecords = 512
CurrentNumberOfRecords = 5
Name = IPMI SEL
EnabledState = 2
OperationalState = 2
HealthState = 2
Caption = IPMI SEL
Description = IPMI SEL
ElementName = IPMI SEL

Befehle:

```
cd
show
help
exit
version
```

- Zum Anzeigen des SEL-Datensatzes:

```
->show /system1/logs1/log1
```

Die folgende Ausgabe wird angezeigt:

```
/system1/logs1/log1/record4
```

Eigenschaften:

```
LogCreationClassName = CIM_RecordLog
CreationClassName = CIM_LogRecord
LogName = IPMI SEL
RecordID = 1
MessageTimeStamp = 20050620100512,000000-000
Beschreibung = FAN 7 RPM: Lüftersensor, Fehler erkannt
ElementName = IPMI SEL Record
```

Befehle:

```
cd
show
help
exit
version
```

- Zum Löschen von SEL:

```
->delete /system1/logs1/log1/record*
```

Die folgende Ausgabe wird angezeigt:

```
Alle Einträge wurden erfolgreich gelöscht
```

MAP-Zielnavigation

Die folgenden Beispiele stellen die Verwendung des Befehls „cd verb“ für die Navigation des MAP dar. Bei allen Beispielen wird als anfängliches Ziel „/“ angenommen.

Geben Sie die folgenden Beispiele an der SMCLP-Befehlseingabe ein:

- Anhand des folgenden Befehls navigieren Sie für einen Neustart zum Systemziel:
cd system1 reset – Das aktuelle Ziel lautet „/“.
- So wechseln Sie zum SEL-Ziel und zeigen die Protokolldatensätze an:
->cd system1
->cd logs1/log1
Anzeigen
- So zeigen Sie das aktuelle Ziel an:
Geben Sie „cd “ ein.
- So gehen Sie eine Ebene nach oben:
Geben Sie „cd. . “ ein.

- So schließen Sie die Befehlseingabe:
Beenden

Betriebssysteme bereitstellen

Sie können die folgenden Dienstprogramme verwenden, um Betriebssysteme auf Managed Systemen bereitzustellen:

- Befehlszeilenoberfläche (CLI) des virtuellen Datenträgers
- Konsole für virtuelle Datenträger
- Remote-Dateifreigabe

Verwandte Links

[Betriebssystem mittels VMCLI bereitstellen](#)

[Betriebssystem über eine Remote-Dateifreigabe bereitstellen](#)

[Betriebssystem über virtuelle Datenträger bereitstellen](#)

Betriebssystem mittels VMCLI bereitstellen

Vor der Bereitstellung des Betriebssystems über das Skript „vmdeploy“ müssen Sie Folgendes sicherstellen:


- Das VMCLI-Dienstprogramm ist auf der Management Station installiert.
- Die iDRAC7-Berechtigungen **Benutzer konfigurieren** und **Auf virtuellen Datenträger zugreifen** sind für den Benutzer aktiviert.
- IPMItool ist auf der Management Station installiert.
 - ✎ **ANMERKUNG:** IPMItool kann nicht verwendet werden, wenn IPv6 auf dem Managed System oder auf der Management Station konfiguriert ist.
- iDRAC7 ist auf den Ziel-Remote-Systemen konfiguriert.
- System kann von der Imagedatei starten.
- IPMI über LAN ist in iDRAC7 aktiviert.
- Die Netzwerkfreigabe enthält Treiber und eine startfähige Imagedatei für das Betriebssystem in einem branchenüblichen Standardformat, wie z. B. **.img** oder **.iso**.
 - ✎ **ANMERKUNG:** Folgen Sie während der Erstellung der Imagedatei den standardmäßigen, netzwerkbasierten Installationsvorgängen, und markieren Sie das Bereitstellungsimage als schreibgeschütztes Image, um sicherzustellen, dass jedes Zielsystem gestartet werden kann und gemäß dem gleichen Bereitstellungsverfahren ausgeführt wird.
- Der Status des virtuellen Datenträgers lautet „Verbunden“.
- Das Skript **vmdeploy** ist auf der Management Station installiert. Überprüfen Sie das beispielhafte vmdeploy-Skript, das in der VMCLI enthalten ist. Dieses Skript beschreibt das Verfahren für die Bereitstellung des Betriebssystems auf Remote-Systemen innerhalb des Netzwerks. Intern werden VMCLI und IPMItool verwendet.
 - ✎ **ANMERKUNG:** Das Skript **vmdeploy** ist während der Installation davon abhängig, dass einige unterstützende Dateien im Verzeichnis vorhanden sind. Zur Verwendung des Skripts aus einem anderen Verzeichnis müssen Sie alle damit verknüpften Dateien kopieren. Wenn das IPMItool-Dienstprogramm nicht installiert ist, kopieren Sie das Dienstprogramm zusammen mit den anderen Dateien.

So stellen Sie das Betriebssystem auf Ziel-Remote-Systemen bereit:

1. Listen Sie die iDRAC7-IPv4-Adressen auf den Ziel-Remote-Systemen in der Textdatei **ip.txt** auf. Listen Sie eine IPv4-Adresse pro Zeile auf.
2. Legen Sie eine startfähige Betriebssystem-CD oder -DVD in das Laufwerk der Verwaltungsstation ein.
3. Öffnen Sie eine Befehlseingabe mit Administratorberechtigungen, und führen Sie das **vmdeploy**-Skript aus:

```
vmdeploy.bat -r <iDRAC7-IP-Adresse oder Datei> -u <iDRAC7-Benutzer> -p
<iDRAC7-Benutzerkennwort> [ -f {<Floppy-Image> | <Gerätename>} | -c
{ <Gerätename>|<Image-Datei>} ] [-i <Geräte-ID>]
```

 **ANMERKUNG:** IPv6 wird durch das vmdeploy-Skript nicht unterstützt, da IPv6 IPMItool nicht unterstützt.

 **ANMERKUNG:** Das vmdeploy-Skript verarbeitet die Option `-r` etwa anders als die Option `vmcli -r`. Wenn das Argument für die Option `-r` der Name einer vorhandenen Datei ist, liest das Skript iDRAC7 IPv4- oder -IPv6-Adressen aus der angegebenen Datei und führt das Dienstprogramm einmal für jede Zeile aus. Wenn das Argument für die Option `-r` kein Dateiname ist, sollte es eine einzelne iDRAC7-Adresse sein. In diesem Fall arbeitet die Option `-r` wie beschrieben für das VMCLI-Dienstprogramm.

In der folgenden Tabelle werden die vmdeploy-Befehlsparameter beschrieben.

Tabelle 29. vmdeploy-Befehlsparameter

| Parameter | Beschreibung |
|--|--|
| <code><iDRAC7-Benutzer></code> | iDRAC7-Benutzername. Dieser Name muss die folgenden Attribute aufweisen: <ul style="list-style-type: none"> – Gültiger Benutzername – iDRAC7 - Benutzerberechtigung für den virtuellen Datenträger <p>Wenn die iDRAC7-Authentifizierung fehlschlägt, wird eine Fehlermeldung angezeigt und der Befehl abgebrochen.</p> |
| <code><iDRAC7-IP-Adresse Datei></code> | iDRAC7-IP-Adresse oder die Datei, die die iDRAC7-IP-Adresse enthält. |
| <code><iDRAC7-Benutzer-Kennwort> oder <iDRAC7-Kennwort></code> | Kennwort für den iDRAC7-Benutzer.
<p>Wenn die iDRAC7-Authentifizierung fehlschlägt, wird eine Fehlermeldung angezeigt und der Befehl abgebrochen.</p> |
| <code>-c {<Gerätename> <Imagedatei>}</code> | Pfad zu einem ISO9660-Image auf der Betriebssysteminstallation-CD/DVD. |
| <code><Floppy-Gerät></code> | Pfad zu dem Gerät, das die Betriebssysteminstallations-CD/DVD oder das -Floppy-Laufwerk enthält. |
| <code><Floppy-Image></code> | Pfad zum gültigen Floppy-Image. |
| <code><Geräte-ID></code> | ID für das Gerät für den Einmalstart. |

Verwandte Links


[Virtuellen Datenträger konfigurieren](#)

[iDRAC7 konfigurieren](#)

Betriebssystem über eine Remote-Dateifreigabe bereitstellen

Bevor Sie das Betriebssystem über eine Remote-Datei-Freigabe bereitstellen, müssen Sie Folgendes sicherstellen:

- Der virtuelle Datenträger befindet sich im Status **Verbunden**, damit die virtuellen Laufwerke in der Startsequenz angezeigt werden.
- Die iDRAC7-Berechtigungen **Benutzer konfigurieren** und **Auf virtuellen Datenträger zugreifen** sind für den Benutzer aktiviert.
- Die Remote-Dateifreigabe ist aktiviert.
- Die Netzwerkfreigabe enthält Treiber und eine startfähige Imagedatei für das Betriebssystem in einem branchenüblichen Standardformat, wie z. B. **.img** oder **.iso**.

 **ANMERKUNG:** Folgen Sie während der Erstellung der Imagedatei den standardmäßigen, netzwerkbasierenden Installationsvorgängen, und markieren Sie das Bereitstellungsimagen als schreibgeschütztes Images. So stellen Sie sicher, dass jedes Zielsystem gestartet werden kann und gemäß dem gleichen Bereitstellungsverfahren ausgeführt wird.

So stellen Sie ein Betriebssystem über eine Remote-Dateifreigabe bereit:

1. Mounten die das ISO- oder IMG-Imagedatei über NFS oder CIFS auf das Managed System.
2. Gehen Sie zu **Übersicht** → **Einrichtung** → **Erstes Startgerät**.
3. Legen Sie die Startreihenfolge in der Drop-Down-Liste **Erstes Startgerät** auf **Remote-Dateifreigabe** fest.
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.

Verwandte Links


[Virtuellen Datenträger konfigurieren](#)

[Erstes Startlaufwerk einstellen](#)

[Verwalten der Remote-Dateifreigabe \(Remote File Share\)](#)


Verwalten der Remote-Dateifreigabe (Remote File Share)

Mit der Remote-Dateifreigabe (Remote File Share; RFS)-Funktion können Sie eine ISO- oder IMG-Imagedatei festzulegen, die sich auf einer Netzwerkfreigabe befindet, und sie dem Betriebssystem des verwalteten Servers als virtuelles Laufwerk zur Verfügung zu stellen, indem sie mithilfe von NFS oder CIFS als CD oder DVD geladen wird. Dies ist eine lizenzierte Funktion.


 **ANMERKUNG:** Die IPv4-Adresse wird sowohl für CIFS als auch für NFS unterstützt. Die IPv6-Adresse wird nur für CIFS unterstützt.

Die Remote-Dateifreigabe unterstützt nur die Image-Dateiformate **.img** und **.iso**. Eine **.img**-Datei wird als virtueller Floppy-Datenträger umgeleitet, und eine **.iso**-Datei wird als virtuelles CDROM-Laufwerk umgeleitet.

Sie müssen über Virtuelle Datenträger-Berechtigungen verfügen, um RFS-Mounting durchführen zu können.

 **ANMERKUNG:** Wenn ESXi auf dem Managed System ausgeführt wird und Sie ein Floppy-Image (**.img**) über die Remote-Dateifreigabe mounten, ist das verbundene Floppy-Image auf dem ESXi-Betriebssystem nicht verfügbar.


Der Verbindungsstatus für RFS ist im iDRAC7-Protokoll verfügbar. Nach einer Verbindung eines per RFS geladenen Laufwerks wird diese Verbindung selbst dann nicht getrennt, wenn Sie sich vom iDRAC7 abmelden. Die RFS-Verbindung wird beendet, wenn der iDRAC7 zurückgesetzt wird oder die Verbindung zum Netzwerk abbricht. Die Webschnittstelle und Befehlszeilenoptionen zum Schließen einer RFS-Verbindung sind für CMC und iDRAC7 ebenfalls verfügbar. Die RFS-Verbindung des CMC hebt immer ein bestehendes RFS-Mounting des iDRAC7 auf.

 **ANMERKUNG:** Zwischen der iDRAC7 vFlash-Funktion und RFS besteht kein Zusammenhang.

Remote-Dateifreigabe über die Web-Schnittstelle konfigurieren

So aktivieren Sie die Remote-Dateifreigabe:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Verbundener Datenträger**. Daraufhin wird die Seite **Verbundener Datenträger** angezeigt.
2. Wählen Sie unter **Remote Dateifreigabe** die Option „Verbinden“ oder „Automatisch verbinden“ und geben Sie Dateipfad, Domänenname, Benutzername und Kennwort an. Weitere Informationen zu den Feldern finden Sie in der *iDRAC7-Online-Hilfe*.
3. 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.

Bei Linux-Distributionen kann diese Funktion einen Befehl zum manuellen Bereitstellen erfordern, wenn es mit runlevel init 3 betrieben wird. Die Syntax für den Befehl lautet:

```
mount /dev/OS_specific_device / user_defined_mount_point
```

wobei `user_defined_mount_point` jedes Verzeichnis ist, das Sie für das Bereitstellen auswählen, ähnlich wie für jeden Bereitstellen-Befehl.

Für RHEL ist das CD-Gerät (virtuelles Gerät **.iso**) `/dev/scd0` und das Floppy-Gerät (virtuelles Gerät **.img**) `/dev/sdc`.

Für SLES ist das CD-Gerät `/dev/sr0` und das Floppy-Gerät `/dev/sdc`. Um sicherzustellen, dass das richtige Gerät verwendet wurde (entweder für SLES oder RHEL), muss auf dem Linux-Betriebssystem, unmittelbar nachdem Sie sich mit dem virtuellen Gerät verbunden haben, folgender Befehl ausgeführt werden:

```
tail /var/log/messages | grep SCSI
```

Hierbei wird der das Gerät identifizierende Text angezeigt (z. B. SCSI-Gerät `sdc`). Dieses Verfahren gilt auch für virtuelle Medien, wenn Sie Linux-Distributionen in runlevel init 3 verwenden. Standardmäßig werden die virtuellen Medien 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 <Optionen>
```

Optionen sind:

`-c`; Verbindung zu Image herstellen

`-d`; Verbindung zu Image abbrechen

`-u <Benutzername>`; Benutzername zum Zugriff auf die Netzwerkfreigabe

`-p <Kennwort>`; Kennwort zum Zugriff auf die Netzwerkfreigabe

`-l <image_location>`; Image-Speicherort auf der Netzwerkfreigabe; doppelte Anführungszeichen um den Speicherort setzen

`-s`; aktuellen Status anzeigen



ANMERKUNG: Alle Zeichen einschließlich alphanumerischer Zeichen und Sonderzeichen sind als Teil des Benutzernamens, des Kennworts und des Imagespeicherorts zulässig, außer den folgenden Zeichen: ' (Apostroph), "(Anführungszeichen), , (Komma), < (kleiner als) und > (größer als).

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 Vorgänge 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 iDRAC7-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.

Verwandte Links

[Virtuellen Datenträger konfigurieren](#)

[Erstes Startlaufwerk einstellen](#)

[iDRAC7 konfigurieren](#)

Betriebssystem über mehrere Festplatten bereitstellen

1. Lösen Sie die bestehende CD/DVD-Verbindung.
2. Legen Sie die nächste CD/DVD in das optische Remote-Laufwerk ein.
3. Weisen Sie das CD/DVD-Laufwerk neu zu.

Integriertes Betriebssystem auf SD-Karte bereitstellen

So installieren Sie einen eingebetteten Hypervisor auf eine SD-Karte:

1. Setzen Sie zwei SD-Karten in die Steckplätze für das interne Dual-SD-Modul (IDSMD) auf dem System ein.
2. Aktivieren Sie das SD-Modul und die Redundanz (falls erforderlich) im BIOS.

- Überprüfen Sie, ob die SD-Karte auf einem der Laufwerke verfügbar ist, indem Sie während des Startvorgangs auf die Taste <F11> drücken.
- Stellen Sie das eingebettete Betriebssystem bereit, und folgen Sie den Anweisungen zur Installation des Betriebssystems.

Verwandte Links

- [Über IDSDM](#)
- [SD-Modul und Redundanz im BIOS aktivieren](#)

SD-Modul und Redundanz im BIOS aktivieren

So aktivieren Sie das SD-Modul und die Redundanz im BIOS:

- Drücken Sie während des Startvorgangs auf <F2>.
- Gehen Sie zu **System-Setup** → **System-BIOS-Einstellungen** → **Integrierte Geräte**.
- Setzen Sie die **interne USB-Schnittstelle** auf **Ein**. Wenn sie auf **Aus** gesetzt ist, kann IDSDM nicht als Startgerät verwendet werden.
- Wenn Redundanz nicht benötigt wird (einzelne SD-Karte), setzen Sie die **interne SD-Kartenschnittstelle** auf **Ein** und die **interne SD-Kartenredundanz** auf **Deaktiviert**.
- Wenn Redundanz benötigt wird (zwei SD-Karten), setzen Sie die **interne SD-Kartenschnittstelle** auf **Ein** und die **interne SD-Kartenredundanz** auf **Spiegelung**.
- Klicken Sie auf **Weiter** und dann auf **Fertig stellen**.
- Klicken Sie zum Speichern der Einstellungen auf **Ja**, und drücken Sie auf <Esc>, um das **System-Setup** zu beenden.

Über IDSDM

Das interne zweifache SD-Modul (IDSDM) ist nur auf geeigneten Plattformen verfügbar. IDSDM bietet Redundanz auf der Hypervisor-SD-Karte, indem eine andere SD-Karte verwendet wird, die den Inhalt der ersten SD-Karte spiegelt.

Eine der beiden SD-Karten kann Master sein. Wenn z. B. zwei neue SD-Karten in das IDSDM eingesetzt werden, wird SD1 die aktive oder Master-Karte und SD2 die Standby-Karte. Die Daten werden auf den beiden Karten geschrieben, aber die Daten werden von SD1 gelesen. Immer wenn SD1 ausfällt oder entfernt wird, wird SD2 automatisch zur aktiven (Master-) Karte.

Unter Verwendung des iDRAC7 können Sie den Status, den Funktionszustand sowie die Verfügbarkeit von IDSDM anzeigen. Der Redundanzstatus der SD-Karte sowie Fehlerereignisse werden zum SEL protokolliert und auf der Frontblende angezeigt, und PET-Warnungen werden erstellt, wenn Warnungen aktiviert sind.

Verwandte Links

- [Sensorinformationen anzeigen](#)

Fehler auf Managed System über iDRAC7 beheben

Sie können Fehler auf einem Remote-Managed-System wie folgt analysieren und beheben:

- Diagnosekonsole
- POST-Code
- Videos zur Start- und Absturzerfassung
- Bildschirm zum letzten Absturz
- Systemereignisprotokolle
- Lifecycle-Protokolle
- Status auf der Frontblende
- Problemanzeigen
- Systemzustand

Verwandte Links

[Diagnosekonsole verwenden](#)

[POST-Codes anzeigen](#)

[Videos zum Startvorgang und zur Absturzerfassung anzeigen](#)

[Protokolle anzeigen](#)

[Bildschirm „Letzter Systemabsturz“ anzeigen](#)

[Status der Anzeige auf der Frontblende anzeigen](#)

[Anzeigen für Hardwareprobleme](#)

[Systemzustand anzeigen](#)

Diagnosekonsole verwenden

iDRAC7 bietet einen Standardsatz mit Netzwerkdiagnose-Tools, die den Tools auf Microsoft Windows- oder Linux-basierten Systemen ähneln. Über die iDRAC7-Web-Schnittstelle können Sie auf die Netzwerk-Debugging-Tools zugreifen.

So rufen Sie die Diagnosekonsole auf:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Fehlerbehebung** → **Diagnose**.
2. Geben Sie in das Textfeld **Befehl** einen Befehl ein, und klicken Sie dann auf **Senden**. Weitere Informationen zu den verfügbaren Befehlen finden Sie in der *iDRAC7-Online-Hilfe*.

Die Ergebnisse werden auf der gleichen Seite angezeigt.

POST-Codes anzeigen

POST-Codes zeigen den Fortschritt des System-BIOS an, kennzeichnen verschiedene Phasen der Startsequenz von Power-on-Reset und ermöglichen, Fehler bezüglich des Systemstarts zu diagnostizieren. Die Seite POST-Code zeigt den letzten **POST-Code** des Systems vor dem Start des Betriebssystems an.

Gehen Sie zum Anzeigen von POST-Codes zu **Übersicht** → **Server** → **Fehlerbehebung** → **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 Video zum Startzyklus 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.

Dies ist eine lizenzierte Funktion.

iDRAC7 zeichnet zum Zeitpunkt des Starts 50 Frames auf. Die Wiedergabe der Startbildschirme tritt mit einer Rate von 1 Frame pro Sekunde auf. Wenn iDRAC zurückgesetzt wird, ist das Systemstartvideo nicht mehr verfügbar, da dieses 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.

Um den Bildschirm **Systemstartprotokoll** anzuzeigen, klicken Sie auf **Übersicht** → **Server** → **Fehlerbehebung** → **Videoerfassung**.

Der Bildschirm **Videoerfassung** zeigt die Videoaufzeichnungen an. Weitere Informationen finden Sie in der *iDRAC7-Online-Hilfe*.

Protokolle anzeigen

Sie können die Systemereignisprotokolle (SEs) und die Lifecycle-Protokolle anzeigen. Weitere Informationen finden Sie unter [Systemereignisprotokoll anzeigen](#) und [Lifecycle-Protokoll anzeigen](#).

Bildschirm „Letzter Systemabsturz“ anzeigen

Die Funktion „Bildschirm Letzter Absturz“ erfasst einen Screenshot des letzten Systemabsturzes, speichert diesen und zeigt ihn in iDRAC7 an. Dies ist eine Lizenzfunktion.

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 iDRAC7-Web-Schnittstelle 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.

Verwandte Links

[Bildschirm „Letzter Absturz“ aktivieren](#)

Status der Anzeige auf der Frontblende anzeigen

Die Frontblende auf dem Managed System fasst den Status der folgenden Systemkomponenten zusammen:

- Batterien

- Lüfter
- Eingriff
- Netzteile
- Wechselbare Flash-Datenträger
- Temperaturen
- Spannungen

Sie können den Status der Frontblende auf dem Managed System wie folgt abrufen:

- Bei Rack- und Tower-Servern: Über den Status der LC-Anzeige auf der Frontblende und die System-ID-LED oder über den Status der LE-Anzeige auf der Frontblende und die System-ID-LED.
- Bei Blade-Servern: Nur über die System-ID-LEDs.

Status der LC-Anzeige auf der Frontblende des Systems anzeigen

Um den Status der LC-Anzeige auf der Frontblende für die jeweiligen Rack- und Tower-Server anzuzeigen, gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Hardware** → **Frontblende**. Daraufhin wird die Seite **Frontblende** angezeigt.

Der Abschnitt **Live-Status auf der Frontblende** zeigt den Live-Status der Meldungen an, die derzeit auf der LC-Anzeige auf der Frontblende angezeigt werden. Wenn das System normal ausgeführt wird (angezeigt durch eine dauerhaft blaue Anzeige auf der LC-Anzeige auf der Frontblende), werden **Fehler ausblenden** und **Fehler einblenden** ausgegraut dargestellt. Sie können die Fehler nur für Rack- und Tower-Server ein- und ausblenden.

Um den Status der LC-Anzeige auf der Frontblende über RACADM anzuzeigen, verwenden Sie die Objekte in der Gruppe `System.LCD`. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Verwandte Links

[LCD-Einstellung konfigurieren](#)

Status der LE-Anzeige auf der Frontblende des Systems anzeigen

Um den Status der aktuellen System-ID-LED anzuzeigen, gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Hardware** → **Frontblende**. Daraufhin wird der Abschnitt **Live-Status der Frontblende** mit dem aktuellen Status der Frontblende angezeigt:

- Dauerhaft blau – Auf dem Managed System liegen keine Probleme vor.
- Blau blinkend – Der Identifizierungsmodus ist aktiviert (unabhängig davon, ob ein Fehler auf dem Managed System vorhanden ist).
- Dauerhaft gelb – Das Managed System befindet sich im Failsafe-Modus.
- Gelb blinkend – Auf dem Managed System sind Fehler vorhanden.

Wenn das System normal ausgeführt wird (erkennbar am blauen Statussymbol auf der LE-Anzeige auf der Frontblende), werden die Optionen **Fehler ausblenden** und **Fehler einblenden** ausgegraut dargestellt. Sie können die Fehleranzeige nur auf Rack- und Tower-Servern ein- und ausblenden.

Um den Status der System-ID-LED über RACADM anzuzeigen, verwenden Sie den Befehl **getled**. Weitere Informationen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Verwandte Links

[LED-Einstellung für die System-ID konfigurieren](#)

Anzeigen für Hardwareprobleme


Die Hardware-bezogenen Probleme lauten:

- Gerät kann nicht hochgefahren werden
- Laute Lüfter
- Verlust der Netzwerkkonnektivität
- Festplattenfehler
- Fehler des USB-Datenträgers
- Physischer Schaden

Verwenden Sie auf der Basis des Problems die folgenden Verfahren, um das Problem zu beheben:

- Setzen Sie das Modul oder die Komponente neu ein, und starten Sie das System neu.
- Setzen Sie bei einem Blade-Server das Modul in einen anderen Schacht des Gehäuses ein.
- Tauschen Sie die Festplatten oder die USB-Flash-Laufwerke aus.
- Schließen Sie die Strom- und Netzkabel erneut an, oder tauschen Sie sie aus

Sollte das Problem fortbestehen, finden Sie weitere Informationen zum Beheben von spezifischen Fehlern auf dem Hardware-Gerät im *Hardware-Benutzerhandbuch*.

 **VORSICHT: Sie dürfen nur Fehlerbehebungsmaßnahmen ausführen und einfache Reparaturen vornehmen, wenn dies in Ihrer Produktdokumentation genehmigt ist oder wenn Sie online bzw. telefonisch von einem Service- und Support-Team entsprechende Anleitungen erhalten. Schäden durch nicht von Dell genehmigte Wartungsversuche werden nicht durch die Garantie abgedeckt. Lesen und befolgen Sie die zusammen mit dem Produkt gelieferten Sicherheitshinweise.**

Systemzustand anzeigen




Die Web-Schnittstellen für iDRAC7 und CMC (für Blade-Server) zeigen den Status für die folgenden Komponenten an:


- Batterien
- Lüfter
- Eingriff
- Netzteile
- Wechselbarer Flash-Datenträger
- Temperaturen
- Spannungen
- CPU

Gehen Sie in der iDRAC7-Web-Schnittstelle zum Abschnitt **Übersicht** → **Server** → **Systemzusammenfassung** → **Server-Zustand**.

Gehen Sie zum Abrufen des CPU-Zustands zu **Übersicht** → **Hardware** → **CPU**.

Die Anzeichen für den System-Zustand lauten wie folgt:

-  – Weist auf einen normalen Status hin.
-  – Weist auf einen Warnstatus hin.
-  – Weist auf einen Ausfallstatus hin.

-  – Weist auf einen unbekanntem Status hin.

Klicken Sie einen beliebigen Komponentennamen im Abschnitt **Server-Zustand**, um die Details zu den jeweiligen Komponenten anzuzeigen.

Serverstatusbildschirm auf Fehlermeldungen überprüfen

Wenn eine gelbe LED zu blinken beginnt und ein bestimmter Server einen Fehler aufweist, kennzeichnet der Hauptserverstatusbildschirm auf dem LCD den betroffenen Server in Orange. Verwenden Sie die Navigationsschaltflächen des LCD, um den betroffenen Server zu kennzeichnen, und klicken Sie dann auf die Schaltfläche in der Mitte. Fehler- und Warnmeldungen werden jetzt in der zweiten Zeile angezeigt. Im Server-Benutzerhandbuch finden Sie eine Liste der auf der LC-Anzeige angezeigten Fehlermeldungen.

iDRAC7 neu starten

Sie können einen harten oder weichen iDRAC7-Neustart ausführen, ohne den Server auszuschalten:

- Harter Neustart – Halten Sie auf dem Server die LED-Schaltfläche für 15 Sekunden gedrückt.
- Weicher Neustart – Mithilfe der iDRAC7-Web-Schnittstelle oder RACADM.

iDRAC7 über die iDRAC7-Web-Schnittstelle zurücksetzen

Führen Sie zum Zurücksetzen von iDRAC7 einen der folgenden Schritte über die iDRAC7-Web-Schnittstelle aus:

- Gehen Sie zu **Übersicht** → **Server** → **Zusammenfassung**. Klicken Sie unter **Schnellstart-Tasks** auf **iDRAC zurücksetzen**.
- Gehen Sie zu **Übersicht** → **Server** → **Fehlerbehebung** → **Diagnose**. Klicken Sie auf **iDRAC zurücksetzen**.

iDRAC7 über RACADM zurücksetzen

Zum Neustart von iDRAC7 verwenden Sie den Befehl **racreset**. Weitere Informationen finden Sie im *RACADM Reference Guide for iDRAC7 and CMC* (RACADM-Referenzhandbuch für iDRAC7 und CMC) unter dell.com/support/manuals.

Zurücksetzen des iDRAC7 auf die Werkseinstellungen

Sie können iDRAC7 mithilfe des Dienstprogramms für die iDRAC-Einstellungen oder der iDRAC7-Web-Schnittstelle auf die Werkseinstellungen zurücksetzen.

Zurücksetzen von iDRAC7 auf die Standardwerkseinstellungen unter Verwendung der iDRAC7-Web-Schnittstelle

So setzen Sie iDRAC7 mithilfe der iDRAC7-Web-Schnittstelle auf die Standardwerkseinstellungen zurück:

1. Gehen Sie zu **Übersicht** → **Server** → **Fehlerbehebung** → **Diagnose**. Daraufhin wird die Seite **Diagnoseprogramm Konsole** angezeigt.
2. Klicken Sie auf **iDRAC auf Standardeinstellungen zurücksetzen**. iDRAC7 startet neu und wird zurück auf die Werkseinstellungen gesetzt. Die iDRAC7-IP wird zurückgesetzt und es kann nicht darauf zugegriffen werden. Sie können die IP mithilfe der Frontblende oder des BIOS konfigurieren.

iDRAC7 mithilfe des Dienstprogramms für iDRAC-Einstellungen auf Werkseinstellungen zurücksetzen

So setzen Sie iDRAC7 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.**

Häufig gestellte Fragen (FAQs)

In diesem Abschnitt werden häufig gestellte Fragen zu den folgenden Themen aufgelistet:


- [System-Ereignisprotokoll](#)
- [Netzwerksicherheit](#)
- [Active Directory](#)
- [Einfache Anmeldung](#)
- [Smart Card-Anmeldung](#)
- [Virtuelle Konsole](#)
- [Virtueller Datenträger](#)
- [vFlash-SD-Karte](#)
- [SNMP-Authentifizierung](#)
- [Speichergeräte](#)
- [RACADM](#)
- [Verschiedenes](#)

System-Ereignisprotokoll

Warum verwendet SEL während der Verwendung der iDRAC7-Web-Schnittstelle über den Internet Explorer nicht die Option „Speichern unter“?

Der Grund dafür liegt in einer Browser-Einstellung. So beheben Sie diesen Fehler:

1. Wechseln Sie im Internet Explorer zu **Tools** → **Internetoptionen** → **Sicherheit** und wählen Sie die Zone, in die Sie versuchen herunterzuladen.
Wenn sich das iDRAC7-Gerät z. B. in Ihrem lokalen Intranet befindet, wählen Sie **Lokales Intranet** und klicken Sie auf **Stufe anpassen...**
2. Im Fenster **Sicherheitseinstellungen** müssen unter **Downloads** die folgenden Optionen aktiviert sein:
 - Automatische Eingabeaufforderung für Datei-Downloads (falls diese Option verfügbar ist)
 - Dateien herunterladen

 **VORSICHT: Um sicherzustellen, dass der Computer, der für den Zugriff auf iDRAC7 verwendet wird, sicher ist, aktivieren Sie unter Verschiedenes nicht die Option Anwendungen und unsichere Dateien starten.**

Netzwerksicherheit

Während des Zugriffs auf die iDRAC7-Web-Schnittstelle wird eine Sicherheitswarnung angezeigt, aus der hervorgeht, dass das durch die Zertifizierungsstelle ausgestellte SSL-Zertifikat nicht vertrauenswürdig ist.

iDRAC7 ist mit einem standardmäßigen iDRAC7-Server-Zertifikat ausgestattet, das die Netzwerksicherheit gewährleistet, während der Zugriff über die Web-Schnittstelle oder ein Remote-RACADM erfolgt. Dieses Zertifikat wurde durch eine nicht vertrauenswürdige Zertifizierungsstelle ausgestellt. Um dieses Problem zu beheben, laden Sie ein iDRAC7-Server-Zertifikat hoch, das durch eine vertrauenswürdige Zertifizierungsstelle ausgestellt wurde (z. B. Microsoft Certificate Authority, Thawte oder Verisign).

Warum führt der DNS-Server keine Registrierung von iDRAC7 durch?

Einige DNS-Server registrieren ausschließlich iDRAC7-Namen mit bis zu 31 Zeichen.

Wenn Sie auf die iDRAC7-Web-Schnittstelle zugreifen, wird eine Sicherheitswarnung angezeigt, aus der hervorgeht, dass der SSL-Zertifikat-Host-Name nicht mit dem iDRAC7-Host-Namen übereinstimmt.

iDRAC7 ist mit einem standardmäßigen iDRAC7-Server-Zertifikat ausgestattet, das die Netzwerksicherheit gewährleistet, während der Zugriff über die Web-Schnittstelle oder ein Remote-RACADM erfolgt. Wenn dieses Zertifikat verwendet wird, zeigt der Web-Browser eine Sicherheitswarnung an, da das für iDRAC7 ausgestellte Standardzertifikat nicht mit dem iDRAC7-Host-Namen übereinstimmt (z. B. mit der IP-Adresse).

Um dieses Problem zu lösen, laden Sie ein iDRAC7-Server-Zertifikat hoch, das auf die IP-Adresse oder den iDRAC7-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 iDRAC7-IP-Adresse (wenn auf die IP-Adresse ausgestellt) oder mit dem registrierten DNS-iDRAC7-Namen (wenn auf den registrierten iDRAC7-Namen ausgestellt) übereinstimmt.

So stellen Sie sicher, dass die Zertifikatsignierungsanforderung mit dem registrierten DNS-iDRAC7-Namen übereinstimmt:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **iDRAC-Einstellungen** → **Netzwerk**. Daraufhin wird die Seite **Netzwerk** angezeigt.
2. Im Abschnitt **Allgemeine Einstellungen**:
 - Wählen Sie die Option **iDRAC auf DNS registrieren** aus.
 - Geben Sie den iDRAC7-Namen in das Feld **DNS-iDRAC-Name** ein.
3. Klicken Sie auf **Anwenden**.

Active Directory

Meine Active Directory-Anmeldung ist gescheitert. Wie kann ich dieses Problem lösen?

Um das Problem zu diagnostizieren, klicken Sie auf der Seite **Active Directory-Konfiguration und -Verwaltung** auf die Option **Einstellungen testen**. Überprüfen Sie die Testergebnisse, und beheben Sie das Problem. Ändern Sie die Konfiguration, und führen Sie den Test aus, bis der Test den Autorisierungsschritt erfolgreich bestanden hat.

Überprüfen Sie allgemein die folgenden Aspekte:

- Stellen Sie während des Anmeldens sicher, dass Sie den richtigen Benutzerdomännennamen und nicht den NetBIOS-Namen verwenden. Wenn Sie ein lokales iDRAC7-Benutzerkonto haben, melden Sie sich auf dem iDRAC7 mit den lokalen Anmeldeinformationen an. Überprüfen Sie nach der Anmeldung Folgendes:
 - Die Option **Active Directory aktivieren** auf der iDRAC7-Seite **Active Directory-Konfiguration und -Verwaltung** markiert ist.
 - Die DNS-Einstellung auf der **iDRAC7-Netzwerkkonfigurationsseite** korrekt ist.
 - Sie das richtige Stamm-CA-Zertifikat des Active Directory auf den iDRAC7 hochgeladen haben, falls Überprüfung des Zertifikats aktiviert wurde.
 - Der iDRAC-Name und der iDRAC-Domänenname stimmen mit der Active Directory-Umgebungs-konfiguration überein, wenn Sie das erweiterte Schema verwenden.
 - Der Gruppenname und der Gruppendomänenname stimmen mit der Active Directory-Konfiguration überein, wenn Sie das Standardschema verwenden.
- Überprüfen Sie die SSL-Zertifikate des Domänen-Controllers, um sicherzustellen, dass die iDRAC7-Zeit innerhalb der Gültigkeitsdauer des Zertifikats liegt.

Die Anmeldung bei Active Directory schlägt selbst dann fehl, wenn die Zertifikatüberprüfung aktiviert ist. Die Testergebnisse zeigen die folgende Fehlermeldung an. Warum tritt dieses Verhalten auf, und wie kann es gelöst werden?

```
ERROR: Can't contact LDAP server, error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check
the correct Certificate Authority (CA) certificate has been uploaded to iDRAC7.
Please also check if the iDRAC7 date is within the valid period of the
certificates and if the Domain Controller Address configured in iDRAC7 matches
the subject of the Directory Server Certificate. (FEHLER: Kontakt zu LDAP-
Server nicht möglich, Fehler:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Überprüfen Sie,
dass das richtige Zertifizierungsstellenzertifikat in iDRAC7 hochgeladen wurde.
Überprüfen Sie außerdem, ob das iDRAC7-Datum innerhalb des Gültigkeitszeitraums
des Zertifikats liegt und ob die in iDRAC7 konfigurierte Domänen-Controller-
Adresse dem Betreff des Verzeichnisserverzertifikats entspricht.)
```

Wenn die Zertifikatsüberprüfung aktiviert ist, sobald der iDRAC7 die SSL-Verbindung zum Verzeichnisserver herstellt, verwendet iDRAC7 das hochgeladene Zertifizierungsstellenzertifikat, um das Zertifikat des Verzeichnisservers zu überprüfen. Die häufigsten Gründe für eine fehlgeschlagene Zertifikatsüberprüfung sind folgende:

- Das Gültigkeitsdatum des iDRAC7 liegt nicht innerhalb des Gültigkeitszeitraums des Serverzertifikats oder des Zertifizierungsstellenzertifikats. Überprüfen Sie die Gültigkeit des iDRAC7-Zertifikats und Ihres Zertifikats.
- Die in iDRAC7 konfigurierten Domänen-Controller-Adressen stimmen nicht mit dem Servernamen oder alternativen Servernamen im Directory-Server-Zertifikat überein. Falls Sie eine IP-Adresse verwenden, lesen Sie bitte die folgende Frage. Wenn Sie einen FQDN verwenden, stellen Sie bitte sicher, dass Sie den FQDN des Domänen-Controllers verwenden und nicht den der Domäne selbst, zum Beispiel **servername.example.com** anstelle von **example.com**.

Die Zertifikatüberprüfung schlägt fehl, auch wenn die IP-Adresse als Domänen-Controller-Adresse verwendet wird. Wie kann dieses Verhalten gelöst werden?

Prüfen Sie das Feld Servername oder alternativer Servername Ihres Domänen-Controller-Zertifikats. Normalerweise verwendet Active Directory den Host-Namen und nicht die IP-Adresse des Domänen-Controllers im Feld Servername oder alternativer Servername des Domänen-Controller-Zertifikats. Um das Problem zu lösen, führen Sie einen der folgenden Schritte aus:

- Konfigurieren Sie den Hostnamen (FQDN) des Domänen-Controllers als *Adresse(n) des Domänen-Controllers* auf dem iDRAC7, damit er mit dem Servernamen oder alternativen Servernamen des Server-Zertifikats übereinstimmt.
- Erstellen Sie das Server-Zertifikat erneut, damit im Feld "Servername" oder "Alternativer Servername" eine IP-Adresse verwendet wird, die auf dem iDRAC7 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 iDRAC7-Objekt befindet.

Wann muss ich Adressen des globalen Katalogs konfigurieren?

Wenn Sie das Standardschema verwenden und die Benutzer und Rollengruppen verschiedenen Domänen angehören, sind Adressen des globalen Katalogs erforderlich. In diesem Fall können Sie nur die Universalgruppe benutzen.

Wenn Sie das Standardschema verwenden und alle Benutzer und Rollengruppen derselben Domäne angehören, sind keine Adressen des globalen Katalogs erforderlich.

Wenn Sie ein erweitertes Schema verwenden, wird die Adresse des globalen Katalogs nicht verwendet.

Wie funktioniert die Abfrage im Standardschema?

iDRAC7 verbindet sich zuerst mit den konfigurierten Domänen-Controller-Adressen, wenn sich die Benutzer und Rollengruppen in dieser Domäne befinden. Die Berechtigungen werden gespeichert.

Wenn Adressen des globalen Katalogs konfiguriert sind, fragt iDRAC7 weiterhin den globalen Katalog ab. Wenn zusätzliche Berechtigungen vom Global Catalog erfasst werden, werden diese Berechtigungen aufgespeichert.

Verwendet iDRAC7 immer LDAP über SSL?

Ja. Der gesamte Transfer erfolgt über den geschützten Anschluss 636 und/oder 3269. Unter Einstellungen testen führt iDRAC7 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 iDRAC7 die Überprüfung des Zertifikats aktiviert?

iDRAC7 setzt eine hohe Sicherheit durch, um die Identität des Domänen-Controllers, mit dem iDRAC7 eine Verbindung herstellt, sicherzustellen. Ohne Überprüfung des Zertifikats kann ein Hacker über einen vorgetäuschten Domänen-Controller die SSL-Verbindung übernehmen. Wenn Sie allen Domänen-Controllern in Ihrem Sicherheitsbereich ohne Überprüfung des Zertifikats vertrauen, können Sie die Überprüfung durch die Web-Schnittstelle oder RACADM deaktivieren.

Unterstützt iDRAC7 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 iDRAC7 anzumelden?

Die Active Directory-Einmal- oder die Smart Card-Anmeldung dauert in der Regel weniger als 10 Sekunden; die Anmeldung kann allerdings bis zu vier Minuten dauern, wenn Sie den bevorzugten DNS-Server und den alternativen DNS-Server angegeben haben und der bevorzugte DNS-Server fehlschlägt. DNS-Zeitüberschreitungen werden erwartet, wenn ein DNS-Server heruntergefahren ist. iDRAC7 meldet Sie unter Verwendung des alternativen DNS-Servers an.

Das Active Directory für eine Domäne in Windows Server 2008 Active Directory konfiguriert. Eine untergeordnete Domäne bzw. Subdomäne ist für die Domäne vorhanden, der Benutzer und die Gruppe sind in derselben untergeordneten Domäne vorhanden und der Benutzer ist ein Mitglied dieser Gruppe. Bei dem Versuch, sich unter Verwendung des Benutzers, der sich in der untergeordneten Domäne befindet, am iDRAC7 anzumelden, schlägt das Einmalige Anmelden über Active Directory fehl.

Dies kann möglicherweise auf den falschen Gruppentyp zurückzuführen sein. Im Active Directory-Server gibt es zwei Arten von Gruppentypen:

- Sicherheit – Sicherheitsgruppen ermöglichen Ihnen, den Benutzer- und Computerzugriff auf freigegebene Ressourcen zu verwalten und Gruppenrichtlinieneinstellungen zu filtern.
- Verteilung – Verteilungsgruppen sind nur als E-Mail-Verteilerlisten vorgesehen.

Stellen Sie immer sicher, dass der Gruppentyp Sicherheit lautet. Sie können zum Zuweisen von Berechtigungen für Objekte keine Verteilergruppen verwenden, verwenden Sie diese jedoch zum Filtern von Gruppenrichtlinieneinstellungen.

Einfache Anmeldung

Die SSO-Anmeldung schlägt auf Windows Server 2008 R2 x64 fehl. Welche Einstellungen sind zum Lösen dieses Problems erforderlich?

1. Führen Sie [http://technet.microsoft.com/en-us/library/dd560670\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd560670(WS.10).aspx) für den Domänen-Controller und die Domänenregel aus.
2. Konfigurieren Sie die Computer zur Verwendung der DES-CBC-MD5-Cipher-Suite.
Diese Einstellungen haben möglicherweise Einfluss auf die Kompatibilität mit Client-Computern oder -Diensten und Anwendungen in Ihrer Umgebung. Die Regeleinstellung Für Kerberos zulässige Verschlüsselungstypen

konfigurieren ist unter **Computer Configuration** → **Security Settings** → **Local Policies** → **Security Options** (Computer-Konfiguration, Sicherheitseinstellungen, Lokale Richtlinien, Sicherheitsoptionen) gespeichert.

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 Befehl `klint purge`.
5. Nachdem das GPO aktualisiert wurde, erstellen Sie die neue Keytab.
6. Laden Sie die Keytab zu iDRAC7 hoch.

Sie können sich jetzt unter Verwendung der SSO am iDRAC7 anmelden.

Warum scheitert die SSO-Anmeldung bei Active Directory-Benutzern auf Windows 7 und Windows Server 2008 R2?

Sie müssen die Verschlüsselungstypen für Windows 7 und Windows Server 2008 R2 aktivieren. So aktivieren Sie die Verschlüsselungstypen:

1. Melden Sie sich als Administrator oder als Benutzer mit Administratorrechten an.
2. Wechseln Sie zu **Start** und führen Sie `gpedit.msc` aus. Das Fenster **Editor für lokale Gruppenrichtlinien** wird angezeigt.
3. Wechseln 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 iDRAC7 anmelden.

Führen Sie die folgenden zusätzlichen Einstellungen für das erweiterte Schema aus:

1. Navigieren Sie im Fenster **Editor für lokale Gruppenrichtlinien** zu **Einstellungen des lokalen Computers** → **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. Gehen Sie zu **Start**, und führen Sie den Befehl „cmd“ aus. Daraufhin wird das Fenster mit der Windows-Befehlseingabe angezeigt.
5. Führen Sie den Befehl `gpupdate /force` aus. Die Gruppenrichtlinien werden daraufhin aktualisiert. Schließen Sie das Fenster für die Befehlseingabe.
6. Gehen Sie zu **Start**, und führen Sie den Befehl „regedit“ aus. Daraufhin wird der **Registrierungs-Editor** aufgerufen.
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 **Wertdaten** die Zahl **1** ein und klicken Sie auf **OK**.
12. Schließen Sie das Fenster **Registrierungseditor**. Sie können sich jetzt unter Verwendung der SSO am iDRAC7 anmelden.

Wenn Sie die SSO für iDRAC7 aktiviert haben und Internet Explorer zum Anmelden an iDRAC7 verwenden, schlägt die SSO fehl, und Sie werden aufgefordert, Ihren Benutzernamen und Ihr Kennwort einzugeben. Wie beheben Sie das Problem?

Stellen Sie sicher, dass die iDRAC7-IP-Adresse unter **Extras** → **Internetoptionen** → **Sicherheit** → **Vertrauenswürdige Sites** aufgelistet ist. Wenn sie nicht aufgelistet ist, schlägt die SSO fehl, und Sie werden aufgefordert, Ihren Benutzernamen und Ihr Kennwort einzugeben. Klicken Sie auf **Abbrechen** und fahren Sie fort.

Smart Card-Anmeldung

Bei Verwendung der Active Directory Smart-Card-Anmeldung dauert es bis zu vier Minuten, um sich am iDRAC7 anzumelden.

Die normale Active Directory-Smart Card-Anmeldung dauert weniger als zehn Sekunden, es kann jedoch bis zu vier Minuten dauern, wenn Sie den bevorzugten DNS-Server und den alternativen DNS-Server auf der Seite **Netzwerk** angegeben haben und der bevorzugte DNS-Server ausgefallen ist. DNS-Zeitüberschreitungen sind zu erwarten, wenn ein DNS-Server ausgeschaltet ist. iDRAC7 meldet Sie unter Verwendung des alternativen DNS-Servers an.

Das ActiveX-Plugin kann das Smart Card-Laufwerk nicht erkennen.

Stellen Sie sicher, dass die Smart Card auf dem Microsoft Windows-Betriebssystem unterstützt wird. Windows unterstützt eine beschränkte Anzahl von Cryptographic Service Providers (CSP) für die Smart Card.

Sie können generell überprüfen, ob die Smart Card-CSPs auf einem bestimmten Client vorhanden sind, indem Sie die Smart Card beim Windows-Anmeldebildschirm (Strg-Alt-Entf) in das Laufwerk einlegen, um zu sehen, ob Windows die Smart Card erkennt und das PIN-Dialogfeld einblendet.

Falsche Smart Card-PIN

Prüfen Sie, ob die Smart Card aufgrund übermäßiger Versuche mit einer falschen PIN gesperrt wurde. In solchen Fällen kann Ihnen der Aussteller der Smart Card in der Organisation helfen, eine neue Smart Card zu beschaffen.

Virtuelle Konsole

Die Sitzung für die virtuelle Konsole ist aktiv, auch wenn Sie sich von der iDRAC7-Web-Schnittstelle abgemeldet haben. Ist dies das erwartete Verhalten?

Ja. Schließen Sie das Fenster mit dem Viewer für die virtuelle Konsole, um sich von der entsprechenden Sitzung abzumelden.

Kann eine neue Remote-Konsolensitzung gestartet werden, wenn das lokale Video auf dem Server ausgeschaltet ist?

Ja.

Warum dauert es 15 Sekunden, um das lokale Video auf dem Server auszuschalten, nachdem eine Aufforderung zum Ausschalten des lokalen Videos eingereicht wurde?

Hierdurch wird einem lokalen Benutzer die Gelegenheit gegeben, Maßnahmen durchzuführen, bevor das Video ausgeschaltet wird.

Tritt beim Einschalten des lokalen Videos eine Zeitverzögerung auf?

Nein. Sobald der iDRAC7 eine Anforderung zum Einschalten des lokalen Videos erhält, wird das Video sofort eingeschaltet.

Kann der lokale Benutzer das Video aus- oder einschalten?

Wenn die lokale Konsole deaktiviert ist, kann der lokale Benutzer das Video nicht aus- oder einschalten.

Werden beim Ausschalten des lokalen Videos auch die lokale Tastatur und Maus ausgeschaltet?

Nein.

Wird durch das Ausschalten der lokalen Konsole auch das Video der Remote-Konsolensitzung ausgeschaltet?

Nein, das Ein- oder Ausschalten des lokalen Videos ist von der Remote-Konsolensitzung unabhängig.

Welche Berechtigungen sind für einen iDRAC7-Benutzer erforderlich, um das lokale Server-Video ein- oder auszuschalten?

Sämtliche Benutzer mit iDRAC7-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 den RACADM-Befehl `racadm getconfig -g cfgRacTuning`, um den Status im Objekt `cfgRacTuneLocalServerVideo` anzuzeigen.

Verwenden Sie alternativ den folgenden RACADM-Befehl über eine Telnet-, SSH- oder eine Remote-Sitzung:

```
racadm -r (iDRAC-IP-Adresse) -u -p getconfig -g cfgRacTuning
```

Der Status kann außerdem über die Anzeige für die virtuelle Konsole OSCAR abgerufen werden. Wenn die lokale Konsole aktiviert ist, wird neben dem Servernamen eine grüne Statusanzeige angezeigt. Wenn diese deaktiviert ist, zeigt ein gelber Punkt an, dass iDRAC7 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 auf Linux wird ein UTF-8-Zeichensatz benötigt. Überprüfen Sie Ihr Gebietschema, 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 auf die Registerkarte **Extras** → **Sitzungsoptionen** → **Maus**. Wählen Sie unter **Mausbeschleunigung** die Option **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 Konsole unter iDRAC7 auf dem Client für die virtuelle Konsole unter iDRAC7 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 ein unterstütztes Microsoft-Betriebssystem remote auf ein System installieren, auf dem eine virtuelle Konsole im BIOS aktiviert ist, wird eine EMS-Verbindungsnachricht gesendet, die erfordert, dass Sie remote auf **OK** klicken. Sie müssen entweder auf dem lokalen System auf **OK** klicken, oder den Remote-Managed Server neu starten. Anschließend müssen Sie die virtuelle Konsole im BIOS ausschalten.

Diese Meldung wird von Microsoft generiert und informiert den Benutzer darüber, 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 iDRAC7 auf den Nummerblock zugreifen, gilt die Nummernblockanzeige auf der Management Station nicht unbedingt für den Status des Nummernblocks auf dem Remote-Server. Der Status des Nummernblocks hängt von der Einstellung auf dem Remote-Server ab, wenn die Remote-Sitzung verbunden ist. Dabei ist der Status des Nummernblocks auf der Management Station nicht von Belang.

Warum werden mehrere Session Viewer-Fenster eingeblendet, wenn vom lokalen Host aus eine Sitzung der virtuellen Konsole aufgebaut wird?

Sie konfigurieren eine virtuelle Konsole über das lokale System. Dieser Vorgang wird nicht unterstützt.

Wenn eine Sitzung für eine virtuelle Konsole aktiv ist und ein lokaler Benutzer auf den Managed Server zugreift, wird dem ersten Benutzer eine Warnmeldung angezeigt?

Nein. Wenn ein lokaler Benutzer auf das System zugreift, haben beide Kontrolle über das System.

Wie viel Bandbreite ist für die Ausführung einer Sitzung für eine virtuelle Konsole erforderlich?

Für eine gute Leistung wird eine Verbindung mit einer Bandbreite von 5 MB/s empfohlen. Eine Verbindung mit einer Bandbreite von 1 MB/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 iDRAC7-Plugin für die virtuelle Konsole das Remote-Server-Desktop-Video nicht empfängt. Im Allgemeinen kann dieses Verhalten auftreten, wenn der Remote-Server ausgeschaltet ist. Gelegentlich wird diese Meldung jedoch auch aufgrund einer Fehlfunktion beim Empfang 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, da sich ein Parameter, der für die Erfassung des Videos benötigt wird, außerhalb des Bereichs befindet, in dem iDRAC7 das Video erfassen kann. Wenn bestimmte Parameter, z. B. die Anzeigeauflösung oder die Aktualisierungsrate, zu hoch eingestellt sind, ist es möglich, dass die Meldung „Außerhalb des Bereichs“ angezeigt wird. In der Regel wird der maximale Bereich der Parameter durch physikalische Begrenzungen definiert, wie z. B. des Videospeichers oder der Bandbreite.

Warum wird, wenn eine Sitzung für eine virtuelle Konsole von der iDRAC7-Web-Schnittstelle aus gestartet wird, ein ActiveX-Sicherheits-Popup-Fenster angezeigt?

iDRAC7 ist möglicherweise nicht in der Liste der vertrauenswürdigen Sites enthalten. Um zu verhindern, dass das Sicherheits-Popup-Fenster bei jedem Start einer Sitzung einer virtuellen Konsole aufgerufen wird, fügen Sie iDRAC7 wie folgt zur Liste der vertrauenswürdigen Sites im Client-Browser hinzu:

1. Klicken Sie auf **Extras** → **Internetoptionen** → **Sicherheit** → **Vertrauenswürdige Sites**.
2. Klicken Sie auf **Sites**, und geben Sie die IP-Adresse oder den DNS-Namen des iDRAC7 ein.
3. Klicken Sie auf **Hinzufügen**.
4. Klicken Sie auf **Stufe anpassen**.
5. Wählen Sie im Fenster **Sicherheitseinstellungen** die Option **Bestätigen** unter **Unsignierte ActiveX-Steuerelemente herunterladen** aus.

Warum ist das Fenster für den Viewer der virtuellen Konsole leer?

Wenn Sie über Berechtigungen für virtuelle Datenträger verfügen, nicht aber für die virtuelle Konsole, können Sie den Viewer für den Zugriff auf die Funktion für virtuelle Datenträger starten, die Konsole des verwalteten Servers wird jedoch nicht angezeigt.

Warum wird die Maus nicht unter DOS synchronisiert, wenn die virtuelle Konsole ausgeführt wird?

Das Dell-BIOS emuliert den Maustreiber als eine PS/2-Maus. Gemäß Konstruktion verwendet die PS/2-Maus eine relative Position für den Mauszeiger, dies bewirkt die Verzögerung bei der Synchronisierung. iDRAC7 verfügt über einen USB-Maustreiber, mit dem eine absolute Position und damit eine engere Verfolgung des Mauszeigers möglich ist. Selbst wenn iDRAC7 die absolute USB-Mausposition 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, müssen Sie den Mausmodus auf dem Bildschirm „Konfiguration“ auf „USC/Diags“ festlegen.

Nach dem Start der virtuellen Konsole ist der Maustreiber auf der virtuellen Konsole aktiv, jedoch nicht auf dem lokalen System. Warum tritt dieses Verhalten auf, und wie kann es gelöst werden?

Dieses Verhalten tritt auf, wenn der **Mausmodus** auf **USC/Diags** gesetzt ist. Drücken Sie auf die Tastenkombination **Alt + M**, um die Maus auf dem lokalen System zu verwenden. Drücken Sie nochmals auf **Alt + M**, um die Maus auf der virtuellen Konsole zu verwenden.

Warum tritt eine Zeitüberschreitung auf der GUI-Sitzung auf, wenn die iDRAC7-Web-Schnittstelle kurz nach dem Start der virtuellen Konsole über die CMC-Web-Schnittstelle gestartet wird?

Wenn die virtuelle Konsole über die CMC-Web-Schnittstelle für iDRAC7 gestartet wird, wird ein Popup-Fenster geöffnet, um die virtuelle Konsole zu starten. Dieses Popup-Fenster wird kurz nach dem Öffnen der virtuellen Konsole wieder geschlossen.


Wenn sowohl die GUI als auch die virtuelle Konsole auf das gleiche iDRAC7-System auf einer Management Station gestartet werden, tritt eine Sitzungszeitüberschreitung für die iDRAC7-GUI auf, wenn die GUI vor dem Schließen des Popup-Fensters gestartet wird. Wenn die iDRAC7-GUI über die CMC-Web-Schnittstelle gestartet wird, nachdem das Popup-Fenster für die virtuelle Konsole geschlossen wurde, tritt dieses Problem nicht auf.

Warum kann der Linux S-Abf-Schlüssel nicht mit Internet Explorer verwendet werden?

Das Verhalten des Linux S-Abf-Schlüssels weicht ab, wenn Sie die virtuelle Konsole über Internet Explorer verwenden. Drücken Sie zum Senden des S-Abf-Schlüssels die Taste **Druck**, und lassen Sie sie los, während Sie die Tastenkombination **Strg + Alt** drücken. So senden Sie den S-Abf-Schlüssel an einen Remote-Linux-Server über iDRAC7, während Sie Internet Explorer verwenden:

1. Aktivieren Sie die Funktion für den magischen Schlüssel auf dem Remote-Linux-Server. Sie können den folgenden Befehl verwenden, um diesen Schlüssel auf dem Linux-Terminal zu aktivieren:

```
echo 1 > /proc/sys/kernel/sysrq
```
2. Aktivieren Sie den Tastaturdurchgangsmodus von Active X Viewer.
3. Drücken Sie auf **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 die freigegebene Netzwerkschnittstelle verwenden, wird iDRAC getrennt, während das BIOS die Netzwerkkarte zurücksetzt. Dieser Vorgang dauert auf Karten mit 10 GB länger und dauert außerdem außergewöhnlich lange, wenn auf dem angeschlossenen Netzwerk-Switch Spanning Tree Protocol (STP) aktiviert ist. In diesem Fall wird empfohlen, die Option „portfast“ für die Switch-Schnittstelle zu verwenden, die 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 eine Netzwerk-Zeitüberschreitung eintritt, trennt die iDRAC7-Firmware die Verbindung und unterbricht die Verbindung zwischen dem Server und dem virtuellen Datenträger.

Wenn Sie die CD im Client-System wechseln, weist die neue CD eventuell eine Autostart-Funktion auf. Wenn dies der Fall ist, kann für die Firmware eine Zeitüberschreitung eintreten und die Verbindung wird unterbrochen, wenn es zu lange dauert, bis das Client-System die CD liest. Wenn eine Verbindung verloren geht, können Sie sie über die GUI wieder herstellen und mit dem vorherigen Vorgang fortfahren.

Wenn die Konfigurationseinstellungen des virtuellen Datenträgers in der iDRAC7-Webschnittstelle 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 iDRAC7-Webschnittstelle mehr Zeit erfordert. Das Installationsfenster zeigt den Installationsfortschritt nicht an.

Wie kann das virtuelle Gerät als Startlaufwerk konfiguriert werden?

Greifen Sie auf dem verwalteten System auf das BIOS-Setup zu, und wechseln Sie zum Startmenü. Lokalisieren Sie die virtuelle CD, die virtuelle Diskette oder VFlash, und ändern Sie die Geräte-Startreihenfolge nach Bedarf. Machen Sie außerdem den virtuellen Datenträger startfähig, indem Sie im CMOS-Setup während der Startsequenz die Leertaste drücken. Um z. B. von einem CD-Laufwerk aus zu starten, konfigurieren Sie das CD-Laufwerk als erstes Laufwerk in der Startreihenfolge.

Welche Datenträgertypen können als Startlaufwerk festgelegt werden?

Mit dem iDRAC7 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?

Suchen Sie auf support.dell.com nach dem Startdienstprogramm von Dell.

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 angeschlossen und mit der Remote-Diskette verbunden. Ich kann mein virtuelles Disketten-/CD-Laufwerk auf einem System mit dem Betriebssystem Red Hat Enterprise Linux oder SUSE® Linux nicht finden. Wie kann ich dieses Problem lösen?

Bei einigen Linux-Versionen werden virtuelle Diskettenlaufwerke und virtuelle CD-Laufwerke nicht in gleicher Weise automatisch geladen. Machen Sie zum Laden des virtuellen Diskettenlaufwerks den Geräteknoten ausfindig, den Linux dem virtuellen Diskettenlaufwerk zuweist. Um das virtuelle Diskettenlaufwerk zu laden:

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 Laufwerksnamen steht und /mnt/floppy der Mount-Punkt 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 Laufwerksnamen steht und /mnt/floppy der Mount-Punkt ist.

Warum werden die mit dem Server verbundenen virtuellen Laufwerke nach einer Remote-Firmware-Aktualisierung über die iDRAC7-Web-Schnittstelle entfernt?

Firmware-Aktualisierungen bewirken, dass der iDRAC7 eine Rücksetzung durchführt, die Remote-Verbindungen verwirft und die virtuellen Laufwerke aufhebt. Die Laufwerke werden wieder angezeigt, wenn der iDRAC7-Reset abgeschlossen ist.

Warum werden nach dem Anschließen eines USB-Geräts alle USB-Geräte abgetrennt?

Virtuelle Datenträgergeräte und vFlash-Geräte werden als Verbund-USB-Gerät am Host-USB-BUS angeschlossen und verwenden einen gemeinsamen USB-Anschluss. Immer wenn ein virtuelles Datenträgergerät oder vFlash-USB-Gerät an den Host-USB-BUS angeschlossen oder davon abgetrennt wird, werden alle virtuellen Datenträger- und vFlash-Geräte vorübergehend vom Host-USB-Bus abgetrennt und danach wieder verbunden. Wenn ein virtuelles Datenträgergerät vom Host-Betriebssystem verwendet wird, müssen Sie das Verbinden bzw. Abtrennen eines oder mehrerer virtueller Datenträger- oder vFlash-Geräte vermeiden. Es wird empfohlen, zuerst alle erforderlichen USB-Geräte anzuschließen, 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 iDRAC7 für den virtuellen Datenträger und für die virtuelle Konsole nicht gesichert.

- Wenn Sie ein Windows-Server-Betriebssystem verwenden, halten Sie bitte den Windows-Dienst mit der Bezeichnung Windows Event Collector an. Rufen Sie hierzu **Start** → **Verwaltungshilfsprogramme** → **Dienste** auf. Klicken Sie mit der rechten Maustaste auf **Windows Event Collector** und klicken Sie auf **Stopp**.

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?

Ein gleichzeitiger Zugriff auf virtuelle Diskettenlaufwerke ist nicht erlaubt. Vor dem Versuch, das Laufwerk zu virtualisieren, ist die Anwendung zum Anzeigen des Laufwerkinhalts zu schließen.

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?

Diese Fehlermeldung wird angezeigt, wenn zusätzlich eine Remote-Dateifreigabe (RFS) verwendet wird. Die Funktionen für die RFS und den virtuellen Datenträger können nicht gleichzeitig verwendet werden.

vFlash-SD-Karte

Wann ist die vFlash SD-Karte gesperrt?

Die vFlash SD-Karte ist gesperrt, wenn ein Vorgang läuft, z. B. während der Initialisierung eines Vorgangs.

SNMP-Authentifizierung

Warum wird die Meldung „Remote-Zugriff: SNMP-Authentifizierungsfehler“ angezeigt?

Als ein Teil der Ermittlung versucht IT Assistant, die Community-Namen get und set des Geräts zu überprüfen. Im IT Assistant ist der Get-Community-Name = public und der Set-Community-Name = private. Standardmäßig ist der Community-Name für den iDRAC67-Agenten public. Wenn IT Assistant eine Set-Anforderung sendet, erstellt der iDRAC7-Agent den SNMP-Authentifizierungsfehler, weil er nur Anforderungen von Community = public akzeptiert.

Um zu verhindern, dass SNMP-Authentifizierungsfehler erstellt werden, müssen Sie Community-Namen eingeben, die vom Agenten akzeptiert werden. Da der iDRAC7 nur einen einzigen Community-Namen zulässt, müssen Sie den gleichen Get- und Set-Community-Namen für das IT Assistant-Ermittlungs-Setup eingeben.

Speichergeräte

Es werden nicht alle Informationen zu allen Speichergeräten angezeigt, die mit dem System verbunden sind, und OpenManage Storage Management zeigt mehr Speichergeräte an, als auf iDRAC7 vorhanden sind. Warum?

iDRAC7 zeigt Informationen nur für die von Comprehensive Embedded Management (CEM) unterstützten Geräte an.

RACADM

Wenn nach dem Zurücksetzen eines iDRAC7 (über den Befehl „racadm racreset“) ein Befehl eingegeben wird, wird die folgende Meldung angezeigt. Wofür steht diese Meldung?

```
FEHLER: Verbindung zum RAC konnte unter angegebener IP-Adresse nicht hergestellt werden.
```

Die Meldung gibt an, dass Sie warten müssen, bis der iDRAC7-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 und -Unterbefehlen 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 iDRAC7 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 iDRAC7 über SUSE Linux Enterprise Server (SLES) 11 SP1 herzustellen.

Stellen Sie sicher, dass Sie die offiziellen openssl- und libopenssl-Versionen installiert haben. Führen Sie den folgenden Befehl aus, um die RPM-Pakete zu installieren:

```
rpm -ivh --force < Dateiname >
```

Hierbei ist <Dateiname> die openssl- oder libopenssl rpm-Paketdatei.

Zum Beispiel:

```
rpm -ivh --force openssl-0.9.8h-30.22.21.1.x86_64.rpm
```

```
rpm -ivh --force libopenssl0_9_8-0.9.8h-30.22.21.1.x86_64.rpm
```

Warum sind die Remote-RACADM- und webbasierten Dienste nach einer Eigenschaftsänderung nicht verfügbar?

Es kann eine Weile dauern, bis die Remote-RACADM-Dienste und die webbasierte Schnittstelle nach einem Reset des iDRAC7-Web Servers verfügbar sind.

Der iDRAC7 Web-Server wird zurückgesetzt, wenn:

- Die Netzwerkconfiguration oder Netzwerk-Sicherheitseigenschaften mittels der webbasierten iDRAC7-Benutzeroberfläche geändert werden
- Die Eigenschaft `cfgRacTuneHttpsPort` geändert wird (einschließlich der Änderung durch eine `config -f-` (Konfigurationsdatei)).
- Es wird der Befehl „`racresetcfg`“ verwendet.
- iDRAC7 zurückgesetzt wird.
- Ein neues SSL-Serverzertifikat hochgeladen wird.

Warum wird eine Fehlermeldung angezeigt, wenn Sie versuchen, eine Partition zu löschen, nachdem Sie sie über den lokalen RACADM erstellt haben?

Dies tritt auf, da der Partitionserstellungsvorgang noch nicht abgeschlossen ist. Die Partition wird jedoch nach einer Weile gelöscht und der Löschvorgang durch eine entsprechende Meldung bestätigt. Falls nicht, warten Sie, bis der Partitionserstellungsvorgang abgeschlossen ist, und löschen Sie die Partition anschließend.

Verschiedenes

Wie kann man eine iDRAC-IP-Adresse für einen Blade-Server ausfindig machen?

Sie können die iDRAC-IP-Adresse über eines der folgenden Verfahren ausfindig machen:

Über die CMC-Web-Schnittstelle: Gehen Sie zu **Gehäuse** → **Server** → **Setup** → **Bereitstellen**, und betrachten Sie in der angezeigten Tabelle die IP-Adresse für den Server.

Über die virtuelle Konsole: Starten Sie den Server neu, um die iDRAC-IP-Adresse im Rahmen eines POST zu betrachten. Wählen Sie im OSCAR die „Dell CMC“-Konsole aus, um sich über eine lokale serielle Verbindung am CMC anzumelden. CMC-RACADM-Befehle können über diese Verbindung gesendet werden. Eine vollständige Liste der CMC RACADM-Unterbefehle finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.

Über den lokalen RACADM: Verwenden Sie den folgenden Befehl: `racadm getsysinfo` Beispiel:

```
$ racadm getniccfg -m server-1 DHCP aktiviert = 1 IP-Adresse = 192.168.0.1  
Subnetzmaske = 255.255.255.0 Gateway = 192.168.0.1
```


Über die LC-Anzeige: Markieren Sie im Hauptmenü den Server, klicken Sie auf die Schaltfläche zum Markieren, wählen Sie den gewünschten Server aus, und klicken Sie auf die Schaltfläche zum Markieren.

Wie kann man die CMC-IP-Adresse ausfindig machen, die sich auf den Blade-Server bezieht?

Über die iDRAC7-Web-Schnittstelle: Klicken Sie auf **Übersicht** → **iDRAC-Einstellungen** → **CMC**. Daraufhin wird die Seite **CMC-Zusammenfassung** mit der CMC-IP-Adresse angezeigt.

Von der virtuellen Konsole: Wählen Sie im OSCAR die "Dell CMC"-Konsole aus, um sich über eine lokale serielle Verbindung am CMC anzumelden. CMC-RACADM-Befehle können über diese Verbindung ausgegeben werden. Eine vollständige Liste der CMC RACADM-Unterbefehle finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.

```
$ racadm getniccfg -m Gehäuse-NIC aktiviert = 1 DHCP aktiviert = 1 Statische IP-Adresse = 192.168.0.120 Statische Subnetzmaske = 255.255.255.0 Statisches Gateway = 192.168.0.1 Aktuelle IP-Adresse = 10.35.155.151 Aktuelle Subnetzmaske = 255.255.255.0 Aktuelles Gateway = 10.35.155.1 Geschwindigkeit = Automatische Verhandlung Duplex = Autonegotiate
```

 **ANMERKUNG:** Sie können diesen Vorgang außerdem über den Remote-RACADM ausführen.

Wie kann man die iDRAC-IP-Adresse für Rack- und Tower-Server ausfindig machen?

Über die iDRAC7-Web-Schnittstelle: Gehen Sie zu **Übersicht** → **Server** → **Eigenschaften** → **Zusammenfassung**.

Daraufhin wird auf der Seite **Systemzusammenfassung** die iDRAC7-IP-Adresse angezeigt.

Über den lokalen RACADM: Verwenden Sie den Befehl `racadm getsysinfo`.

Über die LC-Anzeige: Verwenden Sie auf dem physikalischen Server zum Anzeigen der iDRAC7-IP-Adresse die Navigationsschaltflächen auf dem Bedienfeld für die LC-Anzeige. Gehen Sie dazu zu **Setup-Ansicht** → **Anzeigen** → **iDRAC** → **IPv4-IP-Adresse** oder **IPv6** → **-IP-Adresse**.

Über OpenManage Server Administrator: Gehen Sie in der Server Administrator-Web-Schnittstelle zu **Modulares Gehäuse** → **System-/Server-Modul** → **Hauptsystemgehäuse/Hauptsystem** → **Remote-Zugriff**.

Die iDRAC7-Netzwerkverbindung funktioniert nicht.

Für Blade-Server:

- Stellen Sie sicher, dass das LAN-Kabel am CMC angeschlossen ist.
- Stellen Sie sicher, dass NIC-Einstellungen, IPv4- oder IPv6-Einstellungen und entweder Statisch oder DHCP für das Netzwerk aktiviert sind.

Für Rack- und Tower-Server:

- Stellen Sie im freigegebenen Modus sicher, dass das LAN-Kabel mit der NIC-Schnittstelle verbunden ist, die mit einem Schraubenschlüsselsymbol gekennzeichnet ist.
- Stellen Sie im dedizierten Modus sicher, dass das LAN-Kabel mit der iDRAC-LAN-Schnittstelle verbunden ist.
- Stellen Sie sicher, dass NIC-Einstellungen, IPv4- und IPv6-Einstellungen und entweder Statisch oder DHCP für das Netzwerk aktiviert sind.

Der Blade-Server wurde in das Gehäuse eingesetzt, der EIN-/AUS-Schalter wurde gedrückt, der Server konnte jedoch nicht eingeschaltet werden.

- Der iDRAC7 benötigt bis zu 2 Minuten zum Initialisieren, bevor der Server hochgefahren werden kann.
- Überprüfen Sie das Energiebudget des CMC. Das Energiebudget für das Gehäuse könnte möglicherweise überschritten sein.

Wie ruft man einen iDRAC7-Administrator-Benutzernamen und das zugehörige Kennwort ab?

Sie müssen die Standardeinstellungen des iDRAC7 wiederherstellen. Weitere Informationen finden Sie unter [iDRAC7 auf die Standardeinstellungen zurücksetzen](#).

Wie kann man den Namen des Steckplatzes für das System in einem Gehäuse ändern?

1. Melden Sie sich bei der CMC-Web-Schnittstelle an, und gehen Sie zu **Gehäuse** → **Server** → **Setup**.
2. Geben Sie den neuen Namen für den Steckplatz in die Zeile für den Server ein und klicken Sie auf **Übernehmen**.

Der iDRAC7 auf Blade-Server reagiert während des Startvorgangs nicht.

Entfernen Sie den Server und setzen Sie ihn erneut ein.

Überprüfen Sie die CMC-Webschnittstelle, um zu sehen, ob der iDRAC7 als aktualisierbare Komponente angezeigt wird. Ist dies der Fall, folgen Sie den Anweisungen unter [Firmware über die CMC-Web-Schnittstelle aktualisieren](#).

Falls das Problem weiterhin besteht, kontaktieren Sie den technischen Support.

Beim Versuch, den verwalteten Server zu starten, ist die Betriebsanzeige grün, aber es ist kein POST bzw. kein Video vorhanden.

Dies kann eintreten, wenn einer oder mehrere der folgenden Zustände zutreffen:

- Speicher ist nicht installiert oder ist unzugänglich.
- Die CPU ist nicht installiert oder ist unzugänglich.
- Die Video-Riser-Karte fehlt oder ist falsch eingesteckt.

Weitere Informationen finden Sie, wenn Sie über die iDRAC7-Web-Schnittstelle oder die Server-LC-Anzeige die Fehlermeldungen im iDRAC7-Protokoll aufrufen.

Anwendungsszenarien

In diesem Abschnitt erhalten Sie Erläuterungen zum Navigieren zu bestimmten Abschnitten innerhalb des Handbuchs, um typische Anwendungsszenarien auszuführen.


Fehler auf einem nicht zugreifbaren Managed System beheben

Nach dem Eingang von Warnungen aus OpenManage Essentials, Dell Management Console oder einem lokalen Trap-Kollektor sind fünf Server in einem Rechenzentrum aufgrund von Problemen wie einem nicht mehr reagierenden Betriebssystem oder Server nicht mehr zugänglich. Es ist daher erforderlich, den Grund für diesen Fehler zu ermitteln, um den Fehler zu beheben und den Server über iDRAC7 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 iDRAC7 sind aktiviert

Um den Grund für den Fehler zu identifizieren, müssen Sie Folgendes auf der iDRAC-Web-Schnittstelle überprüfen und die Verbindung zum System wiederherstellen:

 **ANMERKUNG:** Wenn Sie nicht auf die iDRAC-Web-Schnittstelle zugreifen können: Gehen Sie zum Server, rufen Sie das LCD-Bedienfeld auf, notieren Sie die IP-Adresse oder den Host-Namen, und führen Sie von Ihrer Management Station aus die folgenden Vorgänge über die iDRAC-Web-Schnittstelle aus:

- Server-LED-Status – Blinkt gelb oder leuchtet dauerhaft gelb.
- LCD-Bedienfeld auf der Frontblende oder Fehlermeldung – Gelbe LC-Anzeige oder Fehlermeldung.
- Betriebssystem-Image wird in der virtuellen Konsole angezeigt. Wenn das Image angezeigt wird, starten Sie das System über einen Warmstart neu, und melden Sie sich wieder an. Wenn die Anmeldung erfolgreich war, ist der Fehler behoben.
- Bildschirm „Letzter Absturz“
- Capture-Video beim Startvorgang
- Absturzvideo-Capture
- Serverzustand – Rote x-Symbole für die Systemkomponenten, bei denen Fehler vorliegen.
- Speicher-Array-Status – Array möglicherweise offline oder ausgefallen
- Lifecycle-Protokoll für kritische Ereignisse in Bezug auf die Hardware und die Firmware auf dem System und die Protokolleinträge, die beim Systemabsturz erfasst wurden.

Systeminformationen abrufen und Systemzustand bewerten

So rufen Sie Systeminformationen ab und bewerten den Systemzustand:

- Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Systemzusammenfassung**, um die Systeminformationen anzuzeigen und um auf bestimmte Links auf dieser Seite zuzugreifen, um den Systemstatus zu bewerten. Sie können beispielsweise den Zustand des Gehäuselüfters überprüfen.
- Sie können außerdem die Gehäuseortungs-LED konfigurieren und auf der Basis der Farbe den Systemzustand bewerten.


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.

Lifecycle-Protokoll und Systemereignisprotokoll anzeigen und exportieren

So zeigen Sie das Lifecycle-Protokoll und das Systemereignisprotokoll (SEL) an und exportieren diese:

1. Gehen Sie in der iDRAC7-Web-Schnittstelle zu **Übersicht** → **Server** → **Protokolle**, um das SEL anzuzeigen. Gehen Sie zu **Übersicht** → **Server** → **Protokolle** → **Lifecycle-Protokoll**, um das Lifecycle-Protokoll anzuzeigen.
 **ANMERKUNG:** Das SEL wird außerdem im Lifecycle-Protokoll angezeigt. Über die Filteroptionen können Sie das SEL anzeigen.
2. Exportieren Sie das SEL oder das Lifecycle-Protokoll im XML-Format an einen externen Speicherort (Management Station, USB-Schlüssel, Netzwerkfreigabe, usw.). Alternativ können Sie die Remote-System-Protokollierung aktivieren, so dass alle Protokolle, die in das Lifecycle-Protokoll geschrieben werden, gleichzeitig auch auf die konfigurierten Remote-Server geschrieben werden.

Schnittstellen zum Aktualisieren der iDRAC-Firmware

Verwenden Sie zum Aktualisieren der iDRAC-Firmware die folgenden Schnittstellen:

- iDRAC7-Web-Schnittstelle
- RACADM-Befehlszeilenschnittstelle (iDRAC7 und CMC)
- Dell Update Package (DUP)
- CMC-Webschnittstelle
- Lifecycle-Controller-Remote-Dienste
- Lifecycle-Controller
- Dell Remote Access Configuration Tool (DRACT)

Ordnungsgemäßes Herunterfahren durchführen

Um ein ordnungsgemäßes Herunterfahren durchzuführen, gehen Sie in der iDRAC7-Web-Schnittstelle zu einem der folgenden Standorte:

- **Übersicht** → **Server** → **Stromversorgung/Thermisch** → **Stromversorgungsconfiguration** → **Stromsteuerung**. Daraufhin wird die Seite **Stromsteuerung** angezeigt. Wählen Sie **Ordnungsgemäßes Herunterfahren** aus, und klicken Sie auf **Anwenden**.
- **Übersicht** → **Server** → **Stromversorgung/Thermisch** → **Stromversorgungsüberwachung**. Wählen Sie aus dem Drop-Down-Menü **Stromsteuerung** die Option **Ordnungsgemäßes Herunterfahren** aus, und klicken Sie dann auf **Anwenden**.

Weitere Informationen finden Sie in der *iDRAC7-Online-Hilfe*.

Neues Administratorbenutzerkonto erstellen

Sie können das standardmäßige lokale Administratorbenutzerkonto ändern oder ein neues Administratorbenutzerkonto erstellen. Weitere Informationen zum Ändern des lokalen Administratorbenutzerkontos finden Sie unter [Lokale Administratorkontoeinstellungen ändern](#).

Weitere Informationen zum Erstellen eines neuen Administratorkontos finden Sie in den folgenden Abschnitten:

- [Lokale Benutzer konfigurieren](#)
- [Konfigurieren von Active Directory-Benutzern](#)
- [Generische LDAP-Benutzer konfigurieren](#)

Server-Remote-Konsole starten und ein USB-Laufwerk mounten

So starten Sie die Remote-Konsole und mounten ein USB-Laufwerk:

1. Schließen Sie ein USB-Flash-Laufwerk (mit dem erforderlichen Image) an die Management Station an.
2. Starten Sie die virtuelle Konsole über eine der folgenden Möglichkeiten über die iDRAC7-Web-Schnittstelle:
 - Gehen Sie zu **Übersicht** → **Server** → **Konsole**, und klicken Sie auf **Virtuelle Konsole starten**.
 - Gehen Sie zu **Übersicht** → **Server** → **Eigenschaften**, und klicken Sie auf die Option **Starten**, die sich unter **Virtuelle Konsole – Vorschau** befindet.

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 Managed System zugeordnet.

Bare Metal-Betriebssystem über verbundenen virtuellen Datenträger und Remote-Dateifreigabe installieren

Weitere Informationen zu diesem Schritt finden Sie unter [Betriebssystem über eine Remote-Dateifreigabe bereitstellen](#).

Rack-Dichte verwalten

Derzeit sind die beiden Server in einem Rack installiert. Um zwei weitere Server hinzuzufügen, müssen Sie bestimmen, wie viel Kapazität im Rack noch verfügbar ist.

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](#).