HP iLO 2 Skript- und Befehlszeilen-Handbuch

HP Teilenummer: 382328-049
Ausgabedatum: Juni 2012
Ausgabe: 1

Mitteilungen

Inhaltliche Änderungen dieses Dokuments behalten wir uns ohne Ankündigung vor. Die Informationen in dieser Veröffentlichung werden ohne Gewähr für ihre Richtigkeit zur Verfügung gestellt. Insbesondere enthalten diese Informationen keinerlei zugesicherte Eigenschaften. Alle sich aus der Verwendung dieser Informationen ergebenden Risiken trägt der Benutzer. Die Garantien für HP Produkte und Services werden ausschließlich in der entsprechenden, zum Produkt bzw. Service gehörigen Garantieerklärung beschrieben. Aus dem vorliegenden Dokument sind keine weiter reichenden Garantieansprüche abzuleiten. Hewlett-Packard („HP") haftet – ausgenommen für die Verletzung des Lebens, des Körpers, der Gesundheit oder nach dem Produkthaftungsgesetz – nicht für Schäden, die fahrlässig von HP, einem gesetzlichen Vertreter oder einem Erfüllungsgehilfen verursacht wurden. Die Haftung für grobe Fahrlässigkeit und Vorsatz bleibt hiervon unberührt.

Vertrauliche Computersoftware. Für Besitz, Nutzung und Kopieren ist eine gültige Lizenz von HP erforderlich. In Übereinstimmung mit FAR 12.211 und 12.212 sind kommerzielle Computersoftware, Computersoftware-Dokumentation und technische Daten für kommerzielle Komponenten für die US-Regierung mit der Standardlizenz des Herstellers lizenziert.

Microsoft, Windows, Windows Server, Windows Vista, Windows NT und Windows XP sind in den USA eingetragene Marken der Microsoft Corporation. AMD ist eine Marke von Advanced Micro Devices, Inc. Intel ist eine Marke der Intel Corporation in den USA und anderen Ländern. Java ist eine US-Marke von Oracle und/oder seiner Tochtergesellschaften. UNIX ist eine Marke der The Open Group.

Zielgruppe

Dieses Dokument wendet sich an Personen, die für die Installation, Verwaltung und Fehlerbeseitigung von Servern und Speichersystemen zuständig sind. HP setzt voraus, dass Sie über die erforderliche Ausbildung für Wartungsarbeiten an Computersystemen verfügen und sich der Risiken bewusst sind, die beim Betrieb von Geräten mit gefährlichen Spannungen auftreten können.

Inhalt

1 Einführung

Übersicht

Mit HP iLO 2 können HP ProLiant Server auf mehrere Arten remote konfiguriert, aktualisiert und in Betrieb genommen werden. Das *HP Integrated Lights-Out 2 Benutzerhandbuch* beschreibt die einzelnen Funktionen und deren Verwendung über die Browser-basierten Benutzeroberfläche und RBSU.

Im *HP Integrated Lights-Out Managementprozessor Skript- und Befehlszeilen-Ressourcenhandbuch* werden die Syntax und die Tools ausführlich behandelt, die für die Verwendung von iLO 2 über eine Befehlszeilenschnittstelle oder eine Skriptoberfläche zur Verfügung stehen.

XML-Beispielskripts mit Befehlen für iLo, iLO 2 und RILOE II Firmware stehen auf der HP Website zur Verfügung. Sofern nicht anderweitig angegeben, gelten die Beispiele im vorliegenden Handbuch speziell für iLO 2 Firmwareversion 2.09 und höher. Vor der Verwendung von XML-Beispielskripts, die von der HP Website unter http://www.hp.com/servers/lights-out heruntergeladen wurden, lesen Sie bitte die Firmware-Supportinformationen zu den einzelnen Skripts, um das betreffende Skript auf die jeweilige Firmware und Version abzustimmen.

Neuerungen in dieser Version

Dieses Handbuch berücksichtigt Änderungen, die an der iLO 2 Firmware vorgenommen wurden. Es bezieht sich auf iLO 2 Version 2.09.

Die folgenden Funktionen wurden hinzugefügt oder aktualisiert:

- Enhanced CLI Prompt (Erweiterte CLI-Eingabeaufforderung)
- Virtual Serial Port Log (Protokoll für virtuellen seriellen Port)

HP Insight Control Server Deployment

HP Insight Control Server Deployment wird so in iLO integriert, dass die Verwaltung von Remote-Servern und die Überwachung der Leistung von Remote Console-Vorgängen unabhängig vom Status des Betriebssystems oder der Hardware möglich ist.

Der Bereitstellungsserver ermöglicht die Nutzung der Energiesparfunktionen von iLO zum Einschalten, Ausschalten bzw. zum Aus- und anschließenden Einschalten des Zielservers. Wenn ein Server eine Verbindung zum Bereitstellungsserver herstellt, fragt der Bereitstellungsserver den Zielserver ab, um zu ermitteln, ob ein LOM Management-Gerät vorhanden ist. Ist ein solches Gerät installiert, erfasst der Server Informationen wie DNS-Name, IP-Adresse und Benutzeranmeldename. Sicherheit wird durch die Eingabe des richtigen Kennworts für den Benutzernamen gewährleistet.

Weitere Informationen zu HP Insight Control Server Deployment finden Sie in der Dokumentation auf der HP Insight Software DVD oder auf der HP Webseite unter http://www.hp.com/go/insightcontrol.

Serververwaltung mit IPMI 2.0-kompatiblen Anwendungen

Die Serververwaltung mittels IPMI stellt ein Standardverfahren für die Steuerung und Überwachung von Servern dar. iLO 2 ermöglicht die Serververwaltung auf Grundlage der Spezifikation der IPMI Version 2.0.

Die IPMI-Spezifikation stellt eine standardisierte Schnittstelle für die Plattformverwaltung zur Verfügung. Die IPMI-Spezifikation enthält Vorgaben für die folgenden Plattform-Verwaltungsaufgaben:

- Überwachung von Systemdaten wie Lüfter, Temperatur und Stromversorgung
- Wiederherstellungsfunktionen wie Systemzurücksetzung und Ein-/Ausschalten

- Protokollfunktionen für problematische Ereignisse wie Systemüberhitzung oder Lüfterausfall
- Funktionen für die Bestandsüberwachung wie beispielsweise die Identifizierung ausgefallener Hardwarekomponenten

Die IPMI-Kommunikationsvorgänge sind abhängig von BMC und SMS. Dabei verwaltet der BMC die Schnittstelle zwischen dem SMS und der Hardware für das Plattform-Management. iLO 2 emuliert die BMC-Funktionalität, während die SMS-Funktionalität von diversen Standard-Tools bereitgestellt werden kann. Zusätzliche Informationen finden Sie in der IPMI-Spezifikation auf der Intel Website unter http://www.intel.com/design/servers/ipmi/tools.htm.

iLO 2 stellt die KCS- bzw. die offene Schnittstelle für die SMS-Kommunikationsvorgänge zur Verfügung. Die KCS-Schnittstelle bietet eine Reihe von Kommunikationsregisterkarten mit isolierter Adressierung (I/O Mapping). Die standardmäßige Systembasisadresse für die SMS-Schnittstelle mit I/O Mapping lautet 0xCA2 und ist durch das Byte-Alignment mit dieser Systemadresse gekennzeichnet.

Der Zugriff auf die KCS-Schnittstelle erfolgt mittels der auf dem lokalen System ausgeführten SMS-Software. Es folgen Beispiele zweier kompatibler SMS-Softwareanwendungen:

- IPMI Version 2.0 Command Test Tool ist ein einfach strukturiertes MS-DOS-Befehlszeilentool, mit dem IPMI-Befehle im Hexadezimalformat an einen IPMI-BMC gesendet werden können, der die KCS-Schnittstelle implementiert. Sie finden dieses Tool auf der Intel Website unter http://www.intel.com/design/servers/ipmi/tools.htm.
- IPMItool ist ein Dienstprogramm für die Verwaltung und Konfiguration von Geräten, die die Spezifikationen der IPMI-Versionen 1.5 und 2.0 unterstützen. Es kann in Linux-Umgebungen eingesetzt werden Sie finden dieses Tool auf der IPMItool Website unter http://ipmitool.sourceforge.net/index.html.

Die IPMI-Funktionalität von iLO 2

Bei der Emulation eines BMC für die IPMI-Schnittstelle unterstützt iLO 2 sämtliche obligatorischen Befehle der IPMI 2.0-Spezifikation. Eine Übersicht über diese Befehle kann der IPMI 2.0-Spezifikation entnommen werden. Darüber hinaus muss der SMS die in der Spezifikation genannten Verfahren unterstützen, mit denen ermittelt wird, welche IPMI-Funktionen für den BMC aktiviert bzw. deaktiviert sind (z. B. der Befehl `Get Device ID`).

Wenn das Serverbetriebssystem ausgeführt wird und der Health Driver aktiviert ist, kann sich IPMI-Datenverkehr über die KCS-Schnittstelle negativ auf die Leistung des Health Driver und die Gesamtperformance des Systems auswirken. Aus diesem Grund sollten Sie keine IPMI-Befehle über die KCS-Schnittstelle eingeben, die einen nachteiligen Effekt auf die Systemüberwachung durch den Health Driver haben könnten. Dies betrifft Befehle für das Einstellen oder Ändern von IPMI-Parametern wie `Set Watchdog Timer` und `Set BMC Global Enabled`. IPMI-Befehle, mit denen lediglich Daten zurückgegeben werden (z. B. `Get Device ID` und `Get Sensor Reading`), stellen dagegen kein Problem dar.

Übersicht über die WS-Management-Kompatibilität

Die iLO 2 Firmware-Implementierung des WS-Management erfolgt in Übereinstimmung mit der Spezifikation *Web Services for Management* 1.0.0a (DTMF Webdienste für Management 1.0.0a).

Authentifizierung

- iLO 2 verwendet grundlegende Authentifizierung über SSL, konform mit dem Profil:

  `wsman:secprofile/https/basic`

- Authentifizierte Benutzer sind zur Ausführung von WS-Management-Befehlen in Übereinstimmung mit festgelegten Berechtigungen in ihren lokalen oder Verzeichniskonten berechtigt.
- Um die grundlegende Authentifizierung auf Windows Vista zu aktivieren, geben Sie an der Eingabeaufforderung `gpedit.msc` ein. Dadurch wird der Gruppenrichtlinienobjekt-Editor

aufgerufen. Wählen Sie **Computerkonfiguration>Administrative Vorlagen>Windows-Komponenten>Windows Remote Management (WinRM)>WinRM Client**. Stellen Sie „Allow Basic Authentification“ (Grundlegende Authentifizierung zulassen) auf **Enabled** (Aktiviert) ein.

Kompatibilität

- WS-Management in iLO 2 ist mit dem Windows Vista Dienstprogramm WinRM, Microsoft Operations Manager 3 und dem von HP bereitgestellten Management Pack kompatibel.
- Ein vollständiger Satz von WS-Management-Befehlen ist auf iLO 2 Servern mit integrierter System Health-Unterstützung zur Überwachung des Systemstatus verfügbar. Ein stark reduzierter Teilsatz dieser Befehle ist auf Servern ohne integrierte System Health-Unterstützung verfügbar.

Es sind folgende Befehle für den Remote-Aufruf von Geräten verfügbar:

- Server Power (Server-Stromversorgung)
- UID

Zustand

Das WS-Management in iLO 2 gibt Statusinformationen für Lüfter, Temperaturfühler, Netzteile und Spannungsregler zurück.

2 Befehlszeile

Übersicht über die Befehlszeilenschnittstelle

HP hat in Zusammenarbeit mit wichtigen Branchenpartnern im Rahmen der Distributed Management Task Force (DMTF), Inc. einen Satz von Befehlen nach Industriestandard entwickelt. DMTF arbeitet derzeit an einer Suite von Spezifikationen, „Systems Management Architecture for Server“, zur Standardisierung Management-fähiger Schnittstellen für Server. iLO 2 verwendet den im Dokument *Server Management Command Line Protocol Specification, 1.00 Draft* (Spezifikation des Server-Management-Befehlszeilenprotokolls, 1.00 Entwurf) definierten Befehlssatz. Das CLP soll die einfache CLI ersetzen.

Zugriff über die Befehlszeile

Mit iLO 2 können Sie die unterstützten Befehle von einer Befehlszeile aus ausführen. Auf die Befehlszeilenoption können Sie über zwei Schnittstellen zugreifen:

- Serieller Port mit einer Verbindung
- Netzwerk mittels:
  - SSH, wodurch drei gleichzeitige Verbindungen ermöglicht werden. IP-Name oder DNS-Name, Anmeldename und Kennwort werden zum Start einer Sitzung mit SSH benötigt.
  - Telnet-Protokoll mit drei gleichzeitigen Verbindungen.

Alle vier Netzwerkverbindungen können gleichzeitig aktiv sein. Nachdem die serielle CLI auf dem Bildschirm „Global Settings“ (Globale Einstellungen) aktiviert wurde, kann die iLO 2 CLI durch Drücken der Taste `ESC` und `ESC` aktiviert werden. Die SSH- und Telnet-Sitzungen starten nach der Authentifizierung.

Verwenden der Befehlszeile

Nach dem Starten einer Befehlszeilensitzung erscheint die iLO CLI-Eingabeaufforderung. Bei jedem Ausführen eines Befehls (oder beim Beenden der Remote Console oder von VSP) kehren Sie, wie im folgenden Beispiel gezeigt, zur CLI-Eingabeaufforderung zurück:

```
hpiLO->
```

Nach Ausführung eines CLI-Befehls wird eine Ausgabe im folgenden allgemeinen Format zurückgegeben:

```
hpiLO-> CLI command
status=0
status_tag=COMMAND COMPLETED
… output returned…
hpiLO->
```

Bei Eingabe eines ungültigen Befehls wird der Fehler in den Werten `status` and `status_tag` in folgender Weise wiedergegeben:

```
hpiLO-> boguscommand
status=2
status_tag=COMMAND PROCESSING FAILED
error_tag=COMMAND NOT RECOGNIZED
```

Wenn für einen gültigen Befehl ein ungültiger Parameter eingegeben wird, so ist die Reaktion geringfügig unterschiedlich:

```
hpiLO-> show /bad
status=2
status_tag=COMMAND PROCESSING FAILED
error_tag=COMMAND ERROR-UNSPECIFIED
Invalid property.
hpiLO->
```

Die folgenden Befehle werden in dieser CLP-Version unterstützt. Derselbe Befehlssatz wird bei den Verbindungen über den seriellen Port sowie bei den SSH- und Telnet-Verbindungen unterstützt.

Die folgenden Befehle werden in dieser CLP-Version unterstützt. Derselbe Befehlssatz wird bei den Verbindungen über den seriellen Port sowie bei den SSH-Verbindungen unterstützt.

Die Berechtigungsebene des angemeldeten Benutzers wird mit der für den Befehl benötigten Berechtigung verglichen. Der Befehl wird nur ausgeführt, wenn die Berechtigungen übereinstimmen. Wenn für den Status einer seriellen Befehlszeilensitzung `Enabled-No Authentication` festgelegt ist, werden alle Befehle ausgeführt, ohne die Berechtigungsebene zu prüfen.

Der CLP-Befehl hat folgende allgemeine Syntax:

```
<Verb> <Ziel> <Option> <Eigenschaft>
```

- **Verben**: Die folgenden Verben werden unterstützt:
  - `cd`
  - `create`
  - `delete`
  - `help`
  - `load`
  - `reset`
  - `set`
  - `show`
  - `start`
  - `stop`
  - `exit`
  - `version`
- **Ziel**: Das Standardziel ist `/`. Sie können das Ziel mit dem Befehl `cd` oder durch Angabe eines Ziels in der Befehlszeile ändern.
- **Optionen**: Gültige Optionen sind:
  - `-help/-h`
  - `-all/-a`
- **Eigenschaften**: Sind die Attribute des Ziels, die geändert werden können.
- **Ausgabe**: Die Ausgabesyntax sieht folgendermaßen aus:
  - `status`
  - `status_tag`

- `status_msg`

Gültige boolesche Werte für die einzelnen Befehle sind `yes`, `no`, `true`, `false`, `y`, `n`, `t`, `f`, `1` und `0`.

HINWEIS: Wenn ein CLP-Befehl sich über mehr als eine Zeile erstreckt, kann nicht zwischen den verschiedenen Zeilen navigiert werden.

Der Windows 2000 Telnet-Client unterstützt die Funktionstasten F1 bis F12 und die Tasten „Einfügen“, „Pos1“ und „Ende“ nicht. Diese Tasten funktionieren nicht in einer iLO 2 Befehlszeilensitzung.

Der **Rücktaste** ist in der CLP-Implementierung von iLO 2 der Wert 0x8 zugewiesen. In einigen Client-Betriebssystemen, wie z. B. Novell Linux Desktop und Red Hat Enterprise Linux 4 Desktop, wird der Rücktaste der Wert 0x7f zugewiesen. Dieser Wert wird im Windows Telnet-Client für die Taste „Entf“ verwendet. Die Rücktaste funktioniert nicht über einen Client, auf dem ihr der Wert 0x7f zugewiesen ist. Für Linux-Clients kann mit der Taste „Pos1“ oder „Ende“ festgelegt werden, dass der iLO 2 CLP-Dienst der Rücktaste den Wert 0x7f zugeordnet, um diese Taste funktionsfähig zu machen.

Ordnen Sie im Windows PuTTy Client der Rücktaste den Wert 0x8 zu, indem Sie die Einstellung für „Terminal Keyboard“ (Terminal-Tastatur) in **Ctrl+H** ändern.

Escape-Befehle

Die Escape-Tastenbefehle sind Kurzbefehle für gängige Tasks.

`ESC (`	Ruft die serielle CLI-Verbindung auf. Für SSH-Sitzungen ist dies nicht erforderlich, da diese nach einer erfolgreichen Anmeldung automatisch eine CLI-Sitzung starten.
`ESC Q`	Stoppt die CLI-Sitzung und beendet die SSH- und Telnet-Verbindung.
`ESC R ESC r ESC R`	Setzt das System zurück.
`ESC ^`	Schaltet das System ein.
`ESC ESC`	Löscht die aktuelle Zeile.

Für die Eingabe der Escape-Sequenzzeichen steht ein Timeout von einer Sekunde zur Verfügung.

Basisbefehle

Es folgen die Basisbefehle zur Verwendung in der Befehlszeile:

`help`	Zeigt kontextspezifische Onlinehilfe und alle unterstützten Befehle an.
`command help/?`	Zeigt die für den betreffenden Befehl spezifische Hilfemeldung an.
`exit`	Beendet die CLP-Sitzung.
`cd`	Der Befehl legt das aktuelle Standardziel fest. Der Kontext arbeitet wie ein Verzeichnispfad. Der Stammkontext für den Server ist ein Schrägstrich (/) und bildet den Ausgangspunkt für ein CLP-System. Sie können Befehle durch eine Änderung des Kontextes verkürzen. Geben Sie zur Suche nach der aktuellen iLO Firmwareversion z. B. den folgenden Befehl ein: `show /map1/firmware1`
`show`	Mit dem Befehl werden die Werte einer Eigenschaft oder der Inhalt eines Sammelziels angezeigt. Beispiel: `hpiLO-> show`

```
status=0
status_tag=COMMAND COMPLETED
/
Targets
system1
map1
Properties
Verbs
cd version exit show
```

In der ersten Zeile mit Informationen, die durch den Befehl `show` ausgegeben wird, steht der aktuelle Kontext. In dem Beispiel ist `/` der aktuelle Inhalt. Im Anschluss an den Kontext wird eine Liste der Unterziele (Targets) und Eigenschaften (Properties) angezeigt, die auf den aktuellen Kontext angewendet werden. Im Abschnitt Verben (Verbs) wird angezeigt, welche Befehle auf diesen Kontext anwendbar sind.

Geben Sie den Befehl `show` mit einem expliziten oder impliziten Kontext sowie mit einer bestimmten Eigenschaft an. Beispiel: Ein expliziter Kontext ist `/map1/firmware1` und ist nicht vom aktuellen Kontext abhängig. Ein impliziter Kontext geht dagegen davon aus, dass der angegebene Kontext dem aktuellen Kontext untergeordnet ist. Wenn der aktuelle Kontext `/map1` ist, dann werden mit dem Befehl `show firmware` die Daten `/map1/firmware1` angezeigt.

Wenn Sie keine Eigenschaft angeben, werden alle Eigenschaften angezeigt. Im Falle des Kontexts `/map1/firmware1` sind zwei Eigenschaften verfügbar: `version` und `date`. Wenn Sie `show /map1/firmware1 date` ausführen, wird nur das Datum angezeigt.

`create` Erstellt eine neue Instanz von MAP im Namespace.

`delete` Entfernt Instanzen von MAP aus dem Namespace.

`load` Verschiebt eine Binärgrafik von einem URL zum MAP.

`reset` Bewirkt, dass ein Ziel die Zustände „Aktiviert“, „Deaktiviert“ und danach wieder „Aktiviert“ schleifenförmig durchläuft.

`set` Legt für eine Eigenschaft oder einen Satz von Eigenschaften einen bestimmten Wert fest und setzt iLO zur Implementierung der Änderungen zurück.

`start` Bewirkt, dass der Zustand eines Ziels auf eine höhere Ausführungsebene geändert wird.

`stop` Bewirkt, dass der Zustand eines Ziels auf eine niedrigere Ausführungsebene geändert wird.

`version` Der Befehl fragt die Version der CLP-Implementierung oder anderer CLP-Elemente ab.

Beispiel:

```
hpiLO-> version
status=0
status_tag=COMMAND COMPLETED
SM-CLP Version 1.0
```

`oemhp_ping` Der Befehl bestimmt, ob eine IP-Adresse mit der aktuellen iLO Sitzung erreichbar ist.

Beispiel:

```
oemhp_ping 192.168.1.1
```

wobei `192.168.1.1` die getestete IP-Adresse ist.

Spezifische Befehle

Die folgenden Abschnitte gehen auf iLO 2 spezifische Befehle ein, die bei Verwendung der Befehlszeile verfügbar sind:

Benutzerbefehle

Benutzerbefehle ermöglichen es Ihnen, die Benutzereinstellungen anzuzeigen und zu ändern. Benutzereinstellungen sind verfügbar unter /map1/accounts1.

Ziele

Alle lokalen Benutzer sind gültige Ziele. Wenn beispielsweise drei lokale Benutzer mit den Anmeldenamen `Administrator`, `admin` und `test` vorhanden sind, so wären folgende Angaben gültige Ziele:

- `Administrator`
- `admin`
- `test`

Eigenschaften

Eigenschaft	Zugriff	Beschreibung
`Benutzername`	Read / Write (Lese-/Schreibzugriff)	Entspricht dem iLO 2 Anmeldenamen.
`Kennwort`	Read / Write (Lese-/Schreibzugriff)	Entspricht dem Kennwort für den aktuellen Benutzer.

Eigenschaft	Zugriff	Beschreibung
name	Read / Write (Lese-/Schreibzugriff)	Zeigt den Namen des Benutzers an. Wird kein Name angegeben, verwendet der Parameter den gleichen Wert wie für den Anmeldenamen (username) Dieser Wert entspricht der iLO 2 Benutzernamen-Eigenschaft.
group	Read / Write (Lese-/Schreibzugriff)	Gibt die Berechtigungsebene an. Folgende Werte sind gültig: • admin • config • oemhp_power • oemhp_rc • oemhp_vm Wenn keine Gruppe angegeben wird, werden dem Benutzer keine Berechtigungen zugewiesen.

Beispiele

Der aktuelle Pfad ist `/map1/accounts1`.

- `create username=lname1 password=password`

  In diesem Beispiel entspricht *username* dem Anmeldenamen.

- `set lname1 username=lname2 password=password1 name=name2 group=admin,configure,oemhp_power,oemhp_vm,oemhp_rc`

  In dem Beispiel ist *`lname1`* der Anmeldename des Benutzers.

HP SIM SSO-Einstellungen

Der Zugriff auf Befehle für HP SIM SSO-Einstellungen erfolgt mit `/map1/oemhp_ssocfg1`. Diese Einstellungen können nur von Benutzern mit der Berechtigung „Configure iLO 2 Settings“ (iLO Einstellungen konfigurieren) geändert werden. SSO wird nur für Browser-Zugriff über vertrauenswürdige HP SIM Server unterstützt. SSO ist eine lizenzierte Funktion. Weitere Informationen sind im *HP Integrated Lights-Out 2 Benutzerhandbuch* zu finden.

Ziele

Keine

Eigenschaften

Eigenschaft	Zugriff	Beschreibung
oemhp_ssotrust	Read / Write (Lese-/Schreibzugriff)	Die für Single Sign-On erforderliche Vertrauensstufe. Gültige Werte sind disabled, all, name und certificate.
oemhp_ssouser	Read / Write (Lese-/Schreibzugriff)	Die mit der Benutzerrolle verknüpften Berechtigungen. Gültige Werte sind login, oemhp_rc, oemhp_power, oemhp_vm, config, admin
oemhp_ssooperator	Read / Write (Lese-/Schreibzugriff)	Die mit der Bedienerrolle verknüpften Berechtigungen. Gültige Werte sind login, oemhp_rc, oemhp_power, oemhp_vm, config, admin.
oemhp_ssoadministrator	Read / Write (Lese-/Schreibzugriff)	Die mit der Administratorrolle verknüpften Berechtigungen. Gültige Werte sind login, oemhp_rc, oemhp_power, oemhp_vm, config, admin.
oemhp_ssoserver	Read (Lesen)	Enthält 0 oder mehr Datensätze für HP SIM Trusted Server. Jeder Datensatz kann einen Servernamen oder ein Serverzertifikat enthalten.

Beispiele

- Um die SSO-Vertrauensstufe auf Vertrauen nach Zertifikat einzustellen:

  ```
  set oemhp_ssocfg/ oemhp_ssotrust = certificate
  ```

- Um Benutzerrollen die Anmeldeberechtigung zuzuweisen:

  ```
  set oemhp_ssocfg/ oemhp_ssouser = login
  ```

- Um der Bedienerrolle Berechtigungen für Anmeldung, Remote Console, virtuelle Energiesteuerung und virtuelle Medien zuzuweisen:

  ```
  set oemhp_ssocfg/ oemhp_ssooperator = login,oemhp_rc,oemhp_power,oemhp_vm
  ```

- Um einen Datensatz für einen HP SIM Trusted Servernamen hinzuzufügen:

  ```
  cd map1/oemhp_ssocfg
  </map1/oemhp_ssocfg>hpiLO-> create = hpsim1.corp.net
  ```

- Um ein Zertifikat dynamisch von dem angegebenen Server (`hpsim2.corp.net`) zu importieren:

  ```
  </map1/oemhp_ssocfg>hpiLO-> load = hpsim2.corp.net
  ```

- Um `oemhp_ssoserver` mit Index 5 zu löschen.

  ```
  </map1/oemhp_ssocfg>hpiLO-> delete = 5
  ```

- Um die vollständige iLO 2 SSO-Konfiguration anzuzeigen:

  ```
  cd map1/oemhp_ssocfg
  </map1/oemhp_ssocfg>hpiLO->show
  ```

Netzwerkbefehle

Die Netzwerk-Subsysteme befinden sich unter:

- `/map1/enetport1`
- `/map1/dhcpendpt1`
- `/map1/dnsendpt1`
- `/map1/gateway1`
- `/map1/dnsserver1`
- `/map1/dnsserver2`
- `/map1/dnsserver3`
- `/map1/dhcpserver1`
- `/map1/settings1`
- `/map1/vlan1`

Eigenschaften, Ziele und Verben:

- `dhcpendpt1`

  Eigenschaften

  — `EnabledState`

  — `OtherTypeDescription`

- `dnsendpt1`

  Eigenschaften

  — `EnabledState`

- HostName
- DomainName
- OtherTypeDescription

- gateway1

  Eigenschaften
  - AccessInfo
  - AccessContext

- dnsserver1

  Eigenschaften
  - AccessInfo
  - AccessContext

  Verben
  - cd
  - version
  - exit
  - show
  - set

- dnsserver2

  Eigenschaften
  - AccessInfo
  - AccessContext

- dnsserver3

  Eigenschaften
  - AccessInfo
  - AccessContext

- dhcpserver1

  Eigenschaften
  - AccessInfo
  - AccessContext

- settings1

  Ziele
  - DNSSettings1

    Eigenschaften
    - DNSServerAddress
    - RegisterThisConnection

- DomainName
- DHCPOptionToUse

WINSSettingData1

Eigenschaften

- WINSServerAddress
- RegisterThisConnection
- DHCPOptionToUse

— Verben

- cd
- version
- exit
- show

- StaticIPSettings1

  Eigenschaften

  - oemhp_SRoute1Address
  - oemhp_Gateway1Address
  - oemhp_SRoute2Address
  - oemhp_Gateway2Address
  - oemhp_SRoute3Address
  - oemhp_Gateway3Address
  - DHCPOptionToUse

Beispiele

```
set /map1/enetport1 speed=100
set /map1/enetport1/lanendpt1 ipv4address=192.168.0.13 subnetmask=255.255.252
```

Sie können eine oder mehrere Eigenschaften in der Befehlszeile angeben. Wenn mehrere Eigenschaften in derselben Befehlszeile angegeben werden, müssen sie durch ein Leerzeichen voneinander getrennt werden.

iLO 2 wird zurückgesetzt, nachdem die Netzwerkeinstellungen angewendet wurden.

iLO 2 Einstellungen

Die iLO 2 Einstellungen lassen sich mit einer Reihe von iLO 2 Einstellungsbefehlen anzeigen bzw. ändern. iLO 2 Einstellungen befinden sich unter `/map1/config1`.

Ziele

Keine Ziele.

Eigenschaften

- oemhp_rawvspport=3002
- oemhp_console_capture_port=17990

- `oemhp_console_capture_enable=yes`
- `oemhp_interactive_console_replay_enable=yes`
- `oemhp_capture_auto_export_enable=no`
- `oemhp_capture_auto_export_location=http://192.168.1.1/folder/capture%t.ilo`
- `oemhp_capture_auto_export_username=0`
- `oemhp_capture_auto_export_password=0`
- `oemhp_console_capture_boot_buffer_enable=no`
- `oemhp_console_capture_fault_buffer_enable=no`
- `emhp_shared_console_enable=yes`
- `oemhp_shared_console_port=0`
- `oemhp_key_up_key_down_enable=yes`

Eigenschaft	Zugriff	Beschreibung
`oemhp_mapenable`	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert iLO 2. Boolesche Werte werden akzeptiert.
`oemhp_timeout`	Read/Write (Lese-/Schreibzugriff)	Legt das Sitzungs-Timeout in Minuten fest. Gültige Werte sind 15, 30, 60 und 120.
`oemhp_passthrough`	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert den PassThrough der Terminal Services. Boolesche Werte werden akzeptiert.
`oemhp_rbsuenable`	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert die Eingabeaufforderung des RBSU während POST. Boolesche Werte werden akzeptiert.
`oemhp_rbsulogin`	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert die Anmeldeanforderung für den Zugriff auf RBSU. Boolesche Werte werden akzeptiert.
`oemhp_rbsushowip`	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert die Anzeige der iLO 2 IP-Adresse während POST. Boolesche Werte werden akzeptiert.
`oemhp_telnetenable`	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert Telnet.
`oemhp_httpport`	Read/Write (Lese-/Schreibzugriff)	Legt den Wert für den HTTP-Port fest.
`oemhp_sslport`	Read/Write (Lese-/Schreibzugriff)	Legt den Wert für den SSL-Port fest.
`oemhp_rcport`	Read/Write (Lese-/Schreibzugriff)	Legt den Wert für den Remote Console Port fest.
`oemhp_vmport`	Read/Write (Lese-/Schreibzugriff)	Legt den Wert für den Port für virtuelle Medien fest.
`oemhp_tsport`	Read/Write (Lese-/Schreibzugriff)	Legt den Wert für den Terminal Services-Port fest.
`oemhp_sshport`	Read/Write (Lese-/Schreibzugriff)	Legt den Wert für den SSH-Port fest.
`oemhp_sshstatus`	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert SSH. Boolesche Werte werden akzeptiert.
`oemhp_serialclistatus`	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert eine CLP-Sitzung über seriellen Port. Boolesche Werte werden akzeptiert.

Eigenschaft	Zugriff	Beschreibung
oemhp_serialcliauth	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert die Autorisierungsanforderung für die CLPSitzung über seriellen Port. Boolesche Werte werden akzeptiert.
oemhp_serialclispeed	Read/Write (Lese-/Schreibzugriff)	Legt die Geschwindigkeit am seriellen Port während der CLP-Sitzung fest. Gültige Werte sind 9600, 19200, 38400, 57600 und 115200.
oemhp_minpwdlen	Read/Write (Lese-/Schreibzugriff)	Legt die Mindestanforderung an die Kennwortlänge fest.
oemhp_authfailurelogging	Read/Write (Lese-/Schreibzugriff)	Legt die Protokollierungskriterien für fehlgeschlagene Authentifizierungen fest.
oemhp_hotkey_t	Read/Write (Lese-/Schreibzugriff)	Legt den Wert für den Hotkey Strg+T fest.
oemhp_hotkey_u	Read/Write (Lese-/Schreibzugriff)	Legt den Wert für den Hotkey Strg+U fest.
oemhp_hotkey_v	Read/Write (Lese-/Schreibzugriff)	Legt den Wert für den Hotkey Strg+V fest.
oemhp_hotkey_w	Read/Write (Lese-/Schreibzugriff)	Legt den Wert für den Hotkey Strg+W fest.
oemhp_hotkey_x	Read/Write (Lese-/Schreibzugriff)	Legt den Wert für den Hotkey Strg+X fest.
oemhp_hotkey_y	Read/Write (Lese-/Schreibzugriff)	Legt den Wert für den Hotkey Strg+Y fest.
oemhp_high_perf_mouse	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert die Hochleistungsmaus.
oemhp_computer_lock	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert die Computersperre für Remote Console.
oemhp_enforce_aes	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert die Erzwingung der AES/3DES-Verschlüsselung.
oemhp_enhanced_cliprompt_enable	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert die erweiterte CLI-Eingabeaufforderung. Standardmäßig ist diese Funktion deaktiviert.
oemhp_vsp_log_enable	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert die Funktion „Virtual Serial Port Log“ (Protokoll für virtuellen seriellen Port). Standardmäßig ist diese Funktion deaktiviert.

Beispiele

```
set /map1/config1 oemhp_enable=yes oemhp_timeout=30
```

Sie können eine oder mehrere Eigenschaften in der Befehlszeile angeben. Wenn mehrere Eigenschaften in derselben Befehlszeile angegeben werden, müssen sie durch ein Leerzeichen voneinander getrennt werden.

Beispiele für den Befehl

```
oemhp_computer_lock
```

:

```
set /map1/config1 oemhp_computer_lock = windows
set /map1/config1 oemhp_computer_lock = custom,l_gui,l
set /map1/config1 oemhp_computer_lock = disabled
```

Eine vollständige Liste benutzerdefinierter Tastenfolgen für `oemhp_computer_lock` finden Sie im *HP Integrated Lights-Out 2 Benutzerhandbuch*. Bei allen Tastenfolgen mit einer Leerstelle muss die Leerstelle durch einen Unterstrich ersetzt werden. Beispiel:

```
set /map1/config1 oemhp_computer_lock = custom,SYS_RQ
set /map1/config1 oemhp_computer_lock = custom,SYS_RQ
```

Integrierte Health-Einstellungen von iLO 2

Mit integrierten iLO 2 Befehlen können Sie Informationen zum Systemzustand (Lüfter, Temperatur-/Spannungssensoren und Stromversorgung) abrufen.

In iLO 2 integrierte CLP-Health-Einstellungen befinden sich unter `/system1/fan*`, `/system1/sensor*` und `/system1/powersupply*`.

Ziele

- `Lüfter`
- `Sensor`
- `Netzteil`

Eigenschaften

Eigenschaft	Zugriff	Beschreibung
`DeviceID`	Read (Lesen)	Zeigt die Gerätenummer von Lüfter, Sensoren oder Stromversorgung an.
`ElementName`	Read (Lesen)	Zeigt die Position von Lüfter, Sensoren oder Stromversorgung an.
`Operationalstatus`	Read (Lesen)	Zeigt den Betriebszustand von Lüfter, Sensoren oder Stromversorgung an.
`VariableSpeed`	Read (Lesen)	Zeigt an, ob der Lüfter mit variabler Drehzahl arbeitet.
`Desired Speed`	Read (Lesen)	Zeigt die aktuelle Lüfterdrehzahl an.
`HealthState`	Read (Lesen)	Zeigt den Health-Zustand von Lüfter, Sensoren oder Stromversorgung an.
`RateUnits`	Read (Lesen)	Gibt die Einheit an, in der die Werte der Temperatur- und Spannungssensoren angezeigt werden.
`CurrentReading`	Read (Lesen)	Zeigt den aktuellen Sensorwert an.
`SensorType`	Read (Lesen)	Gibt den Sensortyp an.
`Oemhp_CautionValue`	Read (Lesen)	Zeigt den Warnwert für den Temperatursensor an.
`Oemhp_CriticalValue`	Read (Lesen)	Zeigt den Alarmwert für den Temperatursensor an.

Beispiele

Der Befehl `show system1/fan1` zeigt die Eigenschaften von Systemlüfter 1 an. Beispiel:

```
/system1/fan1
Ziele
Eigenschaften
DeviceID=Fan 1
ElementName=I/O Board
OperationalStatus=Ok
VariableSpeed=Yes
DesiredSpeed=40
```

```
HealthState=Ok
```

Die VRM-Stromversorgungen werden in der Regel den Sensorzielen zugeordnet. Der Befehl `show system1/sensor1` zeigt die Eigenschaften von VRM 1 an. Beispiel:

```
/system1/sensor1
Ziele
Eigenschaften
DeviceID=VRM 1
ElementName=CPU 1
OperationalStatus=Ok
RateUnits=Volts
CurrentReading=0
SensorType=Voltage
HealthState=Ok
oemhp_CautionValue=0
oemhp_CriticalValue=0
```

Andere Sensorziele zeigen Systemtemperaturwerte an. Der Befehl `show system1/sensor3` zeigt die Eigenschaften einer der Temperaturzonen an. Beispiel:

```
/system1/sensor3
Ziele
Eigenschaften
DeviceID=Temp 1
ElementName=I/O Board Zone
OperationalStatus=Ok
RateUnits=Celsius
CurrentReading=32
SensorType=Temperature
HealthState=Ok
oemhp_CautionValue=68
oemhp_CriticalValue=73
```

SNMP-Einstellungen

SNMP-Einstellungen ermöglichen es Ihnen, die SNMP-Einstellungen anzuzeigen und zu ändern. SNMP-Einstellungen sind verfügbar unter

```
/map1/snmp1
```

.

Ziele

Keine

Eigenschaften

Eigenschaft	Zugriff	Beschreibung
`accessinfo1`	Read/Write (Lese-/Schreibzugriff)	Legt die erste SNMP-Trap-Zieladresse fest.
`accessinfo2`	Read/Write (Lese-/Schreibzugriff)	Legt die zweite SNMP-Trap-Zieladresse fest.
`accessinfo3`	Read/Write (Lese-/Schreibzugriff)	Legt die dritte SNMP-Trap-Zieladresse fest.

Eigenschaft	Zugriff	Beschreibung
oemhp_iloalert	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert die iLO 2 SNMP-Alarmmeldungen. Boolesche Werte werden akzeptiert.
oemhp_agentalert	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert SNMP-Alarmmeldungen des Host-Agent. Boolesche Werte werden akzeptiert.
oemhp_snmppassthru	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert den iLO 2 SNMP-Pass-Through. Boolesche Werte werden akzeptiert.
oemhp_imagenturl	Read/Write (Lese-/Schreibzugriff)	Legt den URL für den Insight Manager Agent fest.
oemhp_imdatalevel	Read/Write (Lese-/Schreibzugriff)	Legt fest, ob das LOM-Gerät auf anonyme XML-Abfragen antwortet. Diese Eigenschaft kann aktiviert und deaktiviert werden.

Beispiele

Sie können eine oder mehrere Eigenschaften in der Befehlszeile angeben. Wenn mehrere Eigenschaften in derselben Befehlszeile angegeben werden, müssen sie durch ein Leerzeichen voneinander getrennt werden. Beispiel:

```
set /map1/snmp1 accessinfo1=192.168.0.50 oemhp_imdatalevel=Enabled
```

Lizenzbefehle

Mit Lizenzbefehlen können Sie die iLO 2 Lizenz anzeigen bzw. ändern. Lizenzbefehle sind verfügbar unter:

```
/map1/
```

Ziele

Keine

Befehle

Befehl	Beschreibung
cd	Ändert das aktuelle Verzeichnis.
show	Zeigt Lizenzinformationen an.
set	Ändert die aktuelle Lizenz.

Beispiele

- `set /map1 license=1234500000678910000000001`
- `show /map1 license`

Verzeichnisbefehle

Verzeichnisbefehle ermöglichen es Ihnen, die Verzeichniseinstellungen anzuzeigen und zu ändern. Verzeichniseinstellungen sind verfügbar unter:

```
/map1/oemhp_dircfg1
```

Ziele

Keine

Eigenschaften

Eigenschaft	Zugriff	Beschreibung
`oemhp_dirauth`	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert die Verzeichnisauthentifizierung. Gültige Einstellungen sind: • extended_schema: Verwendet HP-erweitertes Schema. • default_schema: Verwendet schemafreie Verzeichnisse. • disabled: Die verzeichnisbasierte Authentifizierung ist deaktiviert.
`oemhp_localacct`	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert die Authentifizierung des lokalen Kontos. Diese Eigenschaft kann nur deaktiviert werden, wenn die Verzeichnisauthentifizierung aktiviert ist. Boolesche Werte werden akzeptiert.
`oemhp_dirsrvaddr`	Read/Write (Lese-/Schreibzugriff)	Legt die IP-Adresse oder den DNS-Namen für den Verzeichnisserver fest. Für die Konfiguration schemafreier Verzeichnisse ist ein DNS-Name erforderlich.
`oemhp_ldapport`	Read/Write (Lese-/Schreibzugriff)	Legt den Verzeichnisserverport fest.
`oemhp_dirdn`	Read/Write (Lese-/Schreibzugriff)	Zeigt den DN (Distinguished Name) für das LOM-Objekt. Dieses Feld wird bei Einsatz der Konfiguration der schemafreien Verzeichnisse ignoriert.
`oemhp_dirpassword`	Read/Write (Lese-/Schreibzugriff)	Legt das Kennwort für das LOM-Objekt fest. Dieses Feld wird bei Einsatz der Konfiguration „default_schema“ ignoriert.
`oemhp_usercntxt1, 2 ...` (bis zu 15)	Read/Write (Lese-/Schreibzugriff)	Zeigt den Suchkontext der Verzeichnis-Benutzeranmeldung an. Dieses Feld wird bei Einsatz der Konfiguration der schemafreien Verzeichnisse nicht benötigt.

Beispiele

Mit zusätzlichen festgelegten Befehlen können weitere Gruppen definiert werden.

Sie können eine oder mehrere Eigenschaften in der Befehlszeile angeben. Wenn mehrere Eigenschaften in derselben Befehlszeile angegeben werden, müssen sie durch ein Leerzeichen voneinander getrennt werden. Beispiel:

- `set /map1/oemhp_dircfg1`
- `set /map1/oemhp_dircfg1 oemhp_dirauth=default_schema oemhp_dirsrvaddr=adserv.demo.com`

Befehle für virtuelle Medien

Das CLP unterstützt den Zugriff auf die virtuellen Medien in iLO 2. Das Subsystem der virtuellen Medien befindet sich unter:

`/map1/oemhp_vm1`

Ziele

Sie haben Zugriff auf die folgenden Unterkomponenten der virtuellen Medien:

Ziel	Beschreibung
`/map1/oemhp_vm1/floppydr1`	Virtuelles Disketten- oder Schlüssellaufwerkgerät
`/map1/oemhp_vm1/cddr1`	Virtuelles CD-ROM-Gerät

Eigenschaften

Eigenschaft	Zugriff	Beschreibung
`oemhp_image`	Read/Write (Lese-/Schreibzugriff)	Der Image-Pfad und -Name für den Zugriff auf virtuelle Medien. Der Wert ist ein URL mit einer maximalen Länge von 80 Zeichen.
`oemhp_connect`	Read (Lesen)	Zeigt an, ob ein virtuelles Mediengerät bereits über das CLP oder über ein Skript für virtuelle Medien verbunden ist.
`oemhp_boot`	Read/Write (Lese-/Schreibzugriff)	Stellt das Starten-Flag ein. Folgende Werte sind gültig: • Never (Nie): Es wird nicht über dieses Gerät gestartet. Der Wert wird als `No_Boot` angezeigt. • Once (Einmal): Es wird nur einmal über dieses Gerät gestartet. Der Wert wird als `Once` angezeigt. • Always (Immer): Es wird bei jedem Neustart des Servers über dieses Gerät gestartet. Der Wert wird als `Always` angezeigt. • Connect (Verbinden): Verbindet das virtuelle Medien-Gerät. Legt für oemhp_connect `Yes` und für oemhp_boot `Always` fest. • Disconnect (Verbindung aufheben): Trennt die Verbindung mit dem virtuellen Mediengerät und stellt für oemhp_boot den Wert `No_Boot` ein.
`oemhp_wp`	Read/Write (Lese-/Schreibzugriff)	Aktiviert oder deaktiviert das Schreibschutz-Flag. Boolesche Werte werden akzeptiert.
`oemhp_applet_connected`	Read (Lesen)	Zeigt an, ob das Java Applet verbunden ist.

Image-URL

Der Image-Wert für `oemhp` besteht aus einer URL. Der URL darf maximal 80 Zeichen lang sein und gibt den Ablageort der Image-Datei für die virtuellen Medien auf einem HTTP-Server an. Für diesen URL gilt dasselbe Format wie für den Ablageort von Medien, die über ein Skript für virtuelle Medien verbunden sind.

URL-Beispiel:

`Protokoll://Benutzername:Kennwort@Hostname:Port/Dateiname`

- Das Protokoll muss angegeben werden (entweder HTTP oder HTTPS).
- Die Angabe Benutzername:Kennwort ist optional.
- Der Hostname muss angegeben werden.
- Die Portangabe ist optional.
- Der Dateiname muss angegeben werden.

Die CLP führt nur eine oberflächliche Überprüfung der Syntax des Werts für die <URL> durch. Sie müssen selbst mit einer Sichtprüfung sicherstellen, dass der URL gültig ist.

Beispiele

- `set oemhp_image=http://imgserver.company.com/image/dosboot.bin`
- `set oemhp_image=http://john:abc123@imgserver.company.com/VMimage/installlDisk.iso`

iLO 2,00 CLI-Unterstützung

Die einfachen `vm`-CLI-Befehle werden für virtuelle Medien weiterhin unterstützt:

- `vm`*Gerät* `insert`*Pfad*: Fügt ein Image ein.
- `vm`*Gerät* `eject`: Wirft ein Image aus.
- `vm`*Gerät* `get`: Fordert den Status der virtuellen Medien an.

- `vm`*Gerät* `set boot`*Zugriff*: Legt den Status der virtuellen Medien fest.

  Befehlsoptionen:

  — Gültige Gerätenamen sind `floppy` oder `cdrom`

  HINWEIS: Es müssen USB-Schlüssellaufwerke mit der Disketten-Schlüsselwortsyntax verwendet werden.

  — Der Pfad ist der URL zum Medien-Image.

  — Startoptionen sind `boot_once`, `boot_always`, `no_boot`, `connect` und `disconnect`

  — Zugriffsoptionen sind `write_protect` und `write_allow`.

  Weitere Informationen zur Verwendung dieser Befehle finden Sie unter den Befehlen INSERT_VIRTUAL_MEDIA, EJECT_VIRTUAL_MEDIA, GET_VM_STATUS und SET_VM_STATUS unter Kapitel 9, „Verwenden von RIBCL“.

Tasks

- Legen Sie ein Disketten- oder USB-Schlüssel-Image in das virtuelle Disketten-/USB-Schlüssellaufwerk ein:

  ```
  cd /map1/oemhp_vm1/floppydr1
  show
  set oemhp_image=http://my.imageserver.com/floppyimg.bin
  set oemhp_boot=connect
  show
  ```

  Dieses Beispiel führt die folgenden Befehle aus:

  — Der aktuelle Kontext des Disketten- oder Schlüssellaufwerks wird geändert.

  — Der aktuelle Status wird angezeigt, um sicherzustellen, dass das Medium nicht in Verwendung ist.

  — Das gewünschte Image wird in das Laufwerk eingefügt.

  — Eine Verbindung zu dem Medium wird hergestellt. Mit der Start-Einstellung „always“ wird automatisch eine Verbindung hergestellt.

- Werfen Sie ein Disketten- oder USB-Schlüssel-Image aus dem virtuellen Disketten-/USB-Schlüssellaufwerk aus:

  ```
  cd /map1/oemhp_vm1/floppydr1
  set oemhp_boot=disconnect
  ```

  Dieses Beispiel führt die folgenden Befehle aus:

  — Der aktuelle Kontext des Disketten- oder Schlüssellaufwerks wird geändert.

  — Gibt den Befehl zum Trennen der Verbindung aus, der die Verbindung der Medien trennt und den Wert für oemhp_image löscht.

- Legen Sie ein CD-ROM-Image in das virtuelle CD-ROM-Laufwerk ein:

  ```
  cd /map1/oemhp_vm1/cddr1
  show
  set oemhp_image=http://my.imageserver.com/ISO/install_disk1.iso
  set oemhp_boot=connect
  show
  ```

  Dieses Beispiel führt die folgenden Befehle aus:

  — Ändert den aktuellen Kontext in den des CD-ROM-Laufwerks.

— Der aktuelle Status wird angezeigt, um sicherzustellen, dass das Medium nicht in Verwendung ist.

— Das gewünschte Image wird in das Laufwerk eingefügt.

— Eine Verbindung zu dem Medium wird hergestellt. Mit der Start-Einstellung „always“ wird automatisch eine Verbindung hergestellt.

- Werfen Sie ein CD-ROM-Image aus dem virtuellen CD-ROM-Laufwerk aus:

  ```
  cd /map1/oemhp_vm1/cddr1
  set oemhp_boot=disconnect
  ```

  Dieses Beispiel führt die folgenden Befehle aus:

  — Ändert den aktuellen Kontext in den des CD-ROM-Laufwerks.

  — Gibt den Befehl zum Trennen der Verbindung aus, der die Verbindung der Medien trennt und den Wert für oemhp_image löscht.

- Legen Sie ein CD-ROM-Image ein und stellen Sie einmaliges Starten ein:

  ```
  cd /map1/oemhp_vm1/cddr1
  set oemhp_image=http://my.imageserver.com/ISO/install_disk1.iso
  set oemhp_boot=connect
  set oemhp_boot=once
  show
  ```

  Dieses Beispiel führt die folgenden Befehle aus:

  — Ändert den aktuellen Kontext in den des CD-ROM-Laufwerks.

  — Der aktuelle Status wird angezeigt, um sicherzustellen, dass das Medium nicht in Verwendung ist.

  — Das gewünschte Image wird in das Laufwerk eingefügt.

  — Eine Verbindung zu dem Medium wird hergestellt. Mit der Start-Einstellung „always“ wird automatisch eine Verbindung hergestellt.

  — Übersteuert die Start-Einstellung durch „Once“.

- Werfen Sie ein CD-ROM-Image mit einem einzelnen Befehl aus dem virtuellen CD-ROM-Laufwerk aus:

  ```
  set /map1/oemhp_vm1/cddr1 oemhp_boot=disconnect
  ```

  Wenn Sie versuchen, die Verbindung zum Laufwerk zu trennen, während das Laufwerk nicht angeschlossen ist, wird eine Fehlermeldung ausgegeben.

Befehle zum Starten und Zurücksetzen

Mit den Befehlen zum Starten und Zurücksetzen können Sie den iLO 2 Server oder iLO 2 selbst zurücksetzen.

Befehl	Beschreibung
`start`	Schaltet den Server ein.
`stop`	Schaltet den Server aus.
`reset hard`	Schaltet den Server aus und wieder ein.
`reset soft`	Führt einen Warmstart des Servers durch.

Beispiele

Wenn das aktuelle Ziel `/system1` ist, werden die folgenden Befehle unterstützt:

- `start`
- `stop`
- `reset hard`
- `reset soft`

Wenn das aktuelle Ziel `/map1` ist, werden die folgenden Befehle unterstützt:

- `reset`
- `reset soft`

iLO 2,00 CLI-Unterstützung

- **Stromversorgung**

  Mit dem Befehl power kann der Energiezustand des Servers geändert werden. Diesen Befehl können nur Benutzer mit der Berechtigung Power und Reset verwenden.

  — `power`: Zeigt den aktuellen Stromversorgungszustand des Servers an.

  — `power on`: Schaltet den Server ein.

  — `power off`: Schaltet den Server aus.

  — `power reset`: Setzt den Server zurück (Aus- und anschließendes Einschalten des Servers)

  — `power warm`: Führt einen Warmstart des Servers durch.

  Anstatt der einfachen Befehle können auch die neuen Befehle im CLP-Format verwendet werden, die in den folgenden Beispielen aufgeführt sind:

  ◦ `start /system1`: Schaltet den Server ein.

  ◦ `stop /system1`: Schaltet den Server aus.

  ◦ `reset /system1`: Setzt den Server zurück.

  ◦ `reset /system1 hard`: Führt einen Kaltstart des Servers durch.

  ◦ `reset /system1 soft`: Führt einen Warmstart des Servers durch.

  ◦ `show /system1 enabledstate`: Zeigt den aktuellen Stromversorgungszustand an, für den „Aktiviert“ eingeschaltet und „Deaktiviert“ ausgeschaltet ist.

- **vsp**

  Der Befehl vsp ruft eine virtuelle serielle Port-Sitzung auf. Geben Sie in der Sitzung für den virtuellen seriellen Port `Esc(` ein, um zur CLI zurückzukehren.

  Anstatt des einfachen Befehls kann auch der neue Befehl im CLP-Format verwendet werden, der im folgenden Beispiel aufgeführt ist:

  ```
  start /system1/oemhp vsp1
  ```

- **textcons**

  Der Befehl `textcons` startet eine Remote Console-Sitzung und kann nur von den Benutzern verwendet werden, die die Berechtigung „Remote Console“ besitzen. Es wird nur eine textbasierte Remote Console unterstützt, ähnlich einer Telnet-Sitzung. Geben Sie in der Remote Console-Sitzung `Esc(` ein, um zur CLI zurückzukehren.

  Anstatt des einfachen Befehls kann auch der neue Befehl im CLP-Format verwendet werden, der im folgenden Beispiel aufgeführt ist:

```
start /system1/console1
```

Firmware-Aktualisierung

Mit den Firmware-Befehlen können Sie die Version der iLO 2 Firmware anzeigen und ändern. Firmware-Einstellungen sind verfügbar unter `/map1/firmware1`.

Ziele

Keine Ziele.

Eigenschaften

Eigenschaft	Zugriff	Beschreibung
`version`	Read (Lesen)	Zeigt die aktuelle Firmware-Version an.
`date`	Read (Lesen)	Zeigt das Freigabedatum der aktuellen Firmware-Version an.

Befehlsformat:

`load -source <URL> [<Ziel>]`

<URL> steht dabei für den URL der Image-Datei der Firmware-Aktualisierung auf dem Webserver. Der URL darf in der Version iLO 2.00 der Firmware maximal 80 Zeichen lang sein.

URL-Beispiel:

`Protokoll://Benutzername:Kennwort@Hostname:Port/Dateiname`

- Im Feld `protocol` muss eine Angabe gemacht werden (entweder HTTP oder HTTPS).
- Das Feld `username:password` ist optional.
- Das Feld `hostname` ist erforderlich.
- Das Feld `port` ist optional.
- Das Feld `filename` ist erforderlich.

Das CLP führt nur eine oberflächliche Überprüfung der Syntax des Werts für den <URL> durch. Sie müssen selbst mit einer Sichtprüfung sicherstellen, dass der URL gültig ist.

Beispiele

```
load -source http://imgserver.company.com/firmware/iloFWimage.bin
load -source http://john:abc123@imgserver.company.com/firmware/ilo.bin
```

Im Feld [<Ziel>] ist `/map1/firmware` angegeben. Die Wertangabe in diesem Feld ist optional, wenn es sich dabei bereits um das Standardziel handelt.

Ereignisprotokollbefehle

Mit den Ereignisprotokollbefehlen können Sie die Ereignisprotokolle des Systems und von iLO 2 anzeigen oder löschen. Die betreffenden Einstellungen sind verfügbar unter:

- `/system1/log1 for the system event log`
- `/map1/log1 for the iLO 2 event log`

Ziele

`record:1..n`

dabei ist *n* die Gesamtzahl der Datensätze.

Eigenschaften

Eigenschaft	Zugriff	Beschreibung
number	Read (Lesen)	Gibt die Datensatznummer für das Ereignis an.
Schweregrad	Read (Lesen)	Gibt den Schweregrad des Ereignisses an. Der Schweregrad kann informational (Information), noncritical (nicht kritisch), critical (kritisch) oder unknown (unbekannt) sein.
date	Read (Lesen)	Gibt das Ereignisdatum an.
time	Read (Lesen)	Gibt die Ereigniszeit an.
description	Read (Lesen)	Gibt eine Beschreibung des Ereignisses an.

Beispiele

- `show /system1/log1`: Zeigt das Systemereignisprotokoll an.
- `show /map1/log1`: Zeigt das iLO 2 Ereignisprotokoll an.
- `show /system1/log1/recordn`: Zeigt Datensatz n aus dem Systemereignis-Standardtext an.
- `show /map1/log1/recordn`: Zeigt das iLO 2 Ereignisprotokoll an.
- `delete /system1/log1`: Löscht das Systemereignisprotokoll.
- `delete /map1/log1`: Löscht das iLO 2 Ereignisprotokoll.

Blade-Befehle

Blade-Befehle ermöglichen es Ihnen, die Werte auf einem p-Class Server anzuzeigen und zu ändern. Diese Werte sind unter

`/system1/map1/blade1`

verfügbar.

p-Class Blades

Diese Befehle werden nur in iLO 2 Firmwareversion 1.82 und niedriger unterstützt.

Ziele

Sie können auf die folgenden Subkomponenten der Blade-Befehle zugreifen:

Ziel	Beschreibung
/map1/blade1/diagport	Zeigt die vorderen Diagnoseport-Einstellungen an und ermöglicht deren Änderung.
/map1/blade1/rack	Zeigt die Blade-Rack-Einstellungen an und ermöglicht deren Änderung.
/map1/blade1/rack1/enclosure1	Zeigt die Blade-Gehäuse-Einstellungen an und ermöglicht deren Änderung.

Eigenschaften

Eigenschaft	Zugriff	Beschreibung
bay_name	Read (Lesen)	Zeigt den Blade-Schachtnamen an und ermöglicht dessen Änderung.
bay_number	Read (Lesen)	Zeigt die Blade-Einschubsnummer an.

Eigenschaft	Zugriff	Beschreibung
facility_power	Read (Lesen)	Zeigt an, ob die 48-Volt-Stromversorgung für das Blade von der Einrichtung zur Verfügung gestellt wird, und ermöglicht das Ändern der Einstellung.
auto_power	Read / Write (Lese-/Schreibzugriff)	Zeigt an, ob für das Blade ein automatisches Einschalten eingestellt wurde und ermöglicht das Ändern der Einstellung.
log_alerts	Read / Write (Lese-/Schreibzugriff)	Zeigt an, ob die Protokollierung von Rack-Alarmmeldungen aktiviert ist und ermöglicht das Ändern der Einstellung.
autoselect	Read / Write (Lese-/Schreibzugriff)	Zeigt die automatisch ausgewählte Diagnoseport-Einstellung an und ermöglicht deren Änderung.
speed	Read / Write (Lese-/Schreibzugriff)	Zeigt die Diagnoseport-Geschwindigkeitseinstellung an und ermöglicht deren Änderung.
fullduplex	Read / Write (Lese-/Schreibzugriff)	Zeigt an, ob der Diagnoseport den Voll- oder Halbduplexmodus unterstützt und ermöglicht die Änderung dieser Einstellung.
ipaddress	Read / Write (Lese-/Schreibzugriff)	Zeigt die IP-Adresse für den Diagnoseport an und ermöglicht deren Änderung.
mask	Read / Write (Lese-/Schreibzugriff)	Zeigt die Subnetzmaske für den Diagnoseport an und ermöglicht deren Änderung.
rack_name	Read / Write (Lese-/Schreibzugriff)	Zeigt den Rack-Namen an und ermöglicht dessen Änderung.
rack_sn	Read (Lesen)	Zeigt die Rack-Seriennummer an.
encl_name	Read / Write (Lese-/Schreibzugriff)	Zeigt den Gehäusenamen an und ermöglicht dessen Änderung.
ser	Read (Lesen)	Zeigt die Gehäuseseriennummer an.
encl_type	Read (Lesen)	Zeigt den Gehäusetyp an.

Beispiele

- `set /map1/blade1/bay_name=BayOne`: Legt als Blade-Einschubnamen „BayOne“ fest.
- `show /map1/blade1/diagport1/ipaddress`: Zeigt die IP-Adresse des vorderseitigen Diagnose-Ports an.
- `show /map1/blade1/rack1/enclosure1(`*n*`)/encl_type`: Zeigt den Gehäusetyp für das Blade-Gehäuse *n* an.

c-Class Blades

Diese Befehle werden erst ab iLO 2 Firmwareversion 2.09 unterstützt.

Ziele

Sie können auf die folgenden Subkomponenten der Blade-Befehle zugreifen:

Ziel	Beschreibung
/map1/blade1/rack	Zeigt die Blade-Rack-Einstellungen an und ermöglicht deren Änderung.

Eigenschaften

Sie können auf die folgenden Subkomponenten der Blade-Befehle zugreifen:

Eigenschaft	Zugriff	Beschreibung
`bay_number`	Read (Lesen)	Zeigt die Blade-Einschubnummer an.
`autopower`	Read / Write (Lese-/Schreibzugriff)	Zeigt an, ob die 48-Volt-Stromversorgung für das Blade von der Einrichtung zur Verfügung gestellt wird, und ermöglicht das Ändern der Einstellung.
`rack_name`	Read / Write (Lese-/Schreibzugriff)	Zeigt den Rack-Namen an und ermöglicht dessen Änderung.
`rack_sn`	Read (Lesen)	Zeigt die Rack-Seriennummer an.

Beispiele

- `set /map1/blade1/auto_power=yes`: Ermöglicht das automatische Einschalten des Blades beim Einschieben in ein Gehäuse.
- `show map1/blade1/rack`: Zeigt den Rack-Namen und die Rack-Seriennummer an.

Startbefehle

Die Startbefehle ermöglichen es Ihnen, die Startquelle und die Startreihenfolge des Systems zu ändern. Start-Einstellungen sind verfügbar unter:

`/system1/bootconfig1`

Ziele

`bootsource1..`*n*,

dabei ist *n* ist die Gesamtzahl der Startquellen.

Legt die Startquelle für das System fest. Die folgenden Werte sind möglich:

- `BootFmCd : bootsource1`
- `BootFmFloppy : bootsource2`
- `BootFmDrive: bootsource3`
- `BootFmNetwork : bootsource4`

  oder

- `BootFmCd : bootsource1`
- `BootFmFloppy : bootsource2`
- `BootFmDrive: bootsource3`
- `BootFmUSBKey : bootsource4`
- `BootFmNetwork : bootsource5`

Eigenschaften

Eigenschaft	Zugriff	Beschreibung
`bootorder`	Read / Write (Lese-/Schreibzugriff)	Legt die Startreihenfolge für eine bestimmte Startquelle fest.

Beispiele

- `set /system1/bootconfig1/bootsource(n) bootorder=(num).`

- `show /system/bootconfig1`: Zeigt die vollständige Startkonfiguration an.
- `show /system1/bootconfig1/bootsource1`: Zeigt die Startreihenfolge für `bootsource1` an.

LED-Befehle

Mit LED-Befehlen kann der Zustand der UID-LED am Server geändert werden. Die LED-Einstellungen sind verfügbar unter:

`/system1/led1`

Eigenschaft	Beschreibung
`start`	Schaltet die LED ein.
`stop`	Schaltet die LED aus.
`show`	Zeigt den Status der LED an.

Beispiele

- `show /system1/led1`: Zeigt den Status der LED an.
- `start /system1/led1`: Schaltet die LED ein.
- `stop /system1/led1`: Schaltet die LED aus.

iLO 2.00 CLI-Unterstützung

Die einfachen UID-Befehle der CLI-Schnittstelle, die in iLO 1.60 eingeführt wurden, werden weiterhin unterstützt.

- `uid`: Zeigt den aktuellen UID-Zustand am Server an.
- `uid on`: Schaltet die UID-LED ein.
- `uid off`: Schaltet die UID-LED aus.

Anstatt der einfachen Befehle können auch die neuen Befehle im CLP-Format verwendet werden, die in den folgenden Beispielen aufgeführt sind:

- `show /system1/led1`: Überprüft den LED-Status.
- `start /system1/led1`: Schaltet die LED ein.
- `stop /system1/led1`: Schaltet die LED aus.

Systemziele und -eigenschaften

Die in diesem Abschnitt beschriebenen Ziele und Eigenschaften liefern Informationen zum Server.

Ziele

Ziel	Beschreibung
`oemhp_PresentPower`	Zeigt die durchschnittliche Strommessung der letzten Abtastung an.
`oemhp_AveragePower`	Zeigt die durchschnittliche Strommessung der letzten 24 Stunden an.
`oemhp_MaxPower`	Zeigt die maximale Stromspitzenmessung der letzten 24 Stunden an.
`oemhp_MinPower`	Zeigt die minimale durchschnittliche Strommessung der letzten 24 Stunden an.
`warning_type`	Zeigt den Warnungstyp an und ermöglicht dessen Änderung.

Ziel	Beschreibung
warning_threshold	Zeigt den Warnungsschwellenwert für den Stromverbrauch an und ermöglicht dessen Änderung.
warning_duration	Zeigt die Dauer an, die der Stromschwellenwert überschreiten muss, bevor eine Warnung erzeugt wird.

Die folgenden Eigenschaften sind in /system1 verfügbar.

Eigenschaft	Zugriff	Beschreibung
name	Read (Lesen)	Zeigt den Systemnamen an.
number	Read (Lesen)	Zeigt die Seriennummer des Systems an.
oemhp_server_name	Read (Lesen)	Zeigt die Zeichenfolge des Hostservernamens an. Diese Zeichenfolge kann bis zu 50 Zeichen lang sein und erfordert eine Änderung der Berechtigung zum Konfigurieren von iLO 2 Einstellungen.
enabledstate	Read (Lesen)	Wird angezeigt, wenn der Server eingeschaltet ist.
oemhp_powerreg	Read / Write (Lese-/Schreibzugriff)	Zeigt die Einstellung für den dynamischen Energiesparmodus an. Gültige Werte sind: dynamic, min, max, os.
processor_number	Read (Lesen)	Zeigt die Anzahl der logischen Prozessoren im System an.
pstate_number	Read (Lesen)	Zeigt die Anzahl der vom Server unterstützten p-Zustände an.
oemhp_pwrcap	Read / Write (Lese-/Schreibzugriff)	Zeigt die aktuelle Stromobergrenze des Servers an. Der Wert wird in Watt angegeben. Diese Eigenschaft kann nicht eingestellt werden, wenn für das Gehäuse eine dynamische Stromobergrenze festgelegt ist. Die dynamische Stromobergrenze des Gehäuses wird mit dem Onboard Administrator oder Insight Power Manager festgelegt und geändert.
oemhp_power_micro_ver	Read (Lesen)	Zeigt die Version und den aktuellen Zustand der optionalen Strom-Mikroprozessors an.

Beispiele

- show /system1
- show /system1 name
- set /system1 oemhp_powergov=auto

Die Eigenschaft cpu ist ein Ziel von /system1 und zeigt Informationen zum Systemprozessor an. Die folgenden Eigenschaften sind in /system1/cpu<*n*> verfügbar:

Eigenschaft	Zugriff	Beschreibung
speed	Read (Lesen)	Zeigt die Prozessorgeschwindigkeit an.
cachememory1	Read (Lesen)	Zeigt die Größe des Level -1 Cache des Prozessors an.
cachememory2	Read (Lesen)	Zeigt die Größe des Level -2 Cache des Prozessors an.
logical_processor<*n*>	Read (Lesen)	Zeigt den logischen Prozessor an.

`CPU power state`: Ermöglicht die Untersuchung der CPU-Stromzustände. Die CPU-Stromzustandswerte werden als Prozentsatz der CPU-Zielwerte angezeigt. Sie verwenden eine weitere Eigenschaft von `logical_processor<n>`.

Beispiel:

Der Befehl `show cpu1/logical_processor1` zeigt die p-Zustände des Prozessors an: Beispiel:

```
/system1/cpu1/logical_processor1
Ziele
Eigenschaften
current_pstate=1
pstate0_avg=0.0
pstate1_avg=100.0
pstate2_avg=0.0
pstate3_avg=0.0
pstate4_avg=0.0
pstate5_avg=0.0
pstate6_avg=0.0
pstate7_avg=0.0
```

`Memory`

: Zeigt Informationen über den Arbeitsspeicher des Systems an.

Die folgenden Eigenschaften sind in `/system1/memory<n>` verfügbar:

Eigenschaft	Zugriff	Beschreibung
`size`	Read (Lesen)	Zeigt die Größe des Arbeitsspeichers an.
`speed`	Read (Lesen)	Zeigt die Arbeitsspeichergeschwindigkeit an.
`location`	Read (Lesen)	Zeigt den Speicherort des Arbeitsspeichers an.

`Slot`

: Zeigt Informationen über die Systemsteckplätze an.

Die folgenden Eigenschaften sind in `/system1/slot<n>` verfügbar:

Eigenschaft	Zugriff	Beschreibung
`Typ`	Read (Lesen)	Zeigt den Steckplatztyp an.
`width`	Read (Lesen)	Zeigt die Steckplatzbreite an.

`Firmware`: Zeigt Informationen über den ROM-Speicher des Systems an.

Die folgenden Eigenschaften sind in `/system1/firmware` verfügbar:

Eigenschaft	Zugriff	Beschreibung
`version`	Read (Lesen)	Zeigt die Version des ROM-Speichers des Systems an.
`date`	Read (Lesen)	Zeigt das Datum des ROM-Speichers des Systems an.

Beispiele:

- `show /system1/cpu1`: Zeigt Informationen zu einer CPU an.
- `show /system1/memory1`: Zeigt Informationen zu einem Speichersteckplatz an.

- `show /system1/slot1`: Zeigt Informationen zu einem Steckplatz an.
- `show /system1/firmware1`: Zeigt Informationen zum ROM-Speicher des Systems an.

  Beispiel:

  ```
  /system1/firmware1 Targets Properties version=P56 date=01/05/2006
  ```

  HINWEIS: `system1/cpu`, `system1/memory` und `system1/slot` werden in iLO 1.81 nicht unterstützt.

Sonstige Befehle

- `start /system1/oemhp vsp1`: Startet eine Sitzung für den virtuellen seriellen Port. Drücken Sie `ESC(`, um zur CLI-Sitzung zurückzukehren.
- `nmi server`: Erzeugt einen NMI und sendet diesen an den Server. Diesen Befehl können nur Benutzer mit der Berechtigung „Power und Reset“ verwenden.

3 Telnet

Telnet-Unterstützung

iLO 2 unterstützt die Verwendung von Telnet für den Zugriff auf die iLO 2 Befehlszeilenschnittstelle. Der Telnet-Zugriff auf iLO 2 unterstützt CLI. CLI kann eine Remote Console Verbindung und eine Verbindung über den virtuellen seriellen Port aufrufen. Weitere Informationen finden Sie unter Kapitel 2, „Befehlszeile“.

Verwenden von Telnet

Wenn Sie Telnet verwenden möchten, müssen die iLO 2 Einstellungen „Remote Console Port Configuration“ (Konfiguration des Ports für Remote Console) und „Remote Console Data Encryption“ (Datenverschlüsselung für Remote Console) auf dem Bildschirm „Global Settings“ (Allgemeine Einstellungen) folgendermaßen konfiguriert werden:

1. Setzen Sie „Remote Console Port Configuration“ (Konfiguration des Remote Console-Ports) auf `Enabled` (Aktiviert).
2. Setzen Sie „Remote Console Data Encryption“ (Remote Console-Datenverschlüsselung) auf `No` (Nein).

Sie können entweder eine Telnet-basierte Remote Console Sitzung oder eine Browser-basierte Remote Console Sitzung öffnen. Sie können nicht beide gleichzeitig öffnen. Werden beide Sitzungen gleichzeitig geöffnet, wird eine Fehlermeldung angezeigt.

So greifen Sie mit Telnet auf iLO 2 zu:

1. Öffnen Sie ein Telnet-Fenster.
2. Geben Sie bei der entsprechenden Aufforderung die IP-Adresse oder den DNS-Namen sowie den Anmeldenamen und das Kennwort ein.

HINWEIS: Der Zugriff über Telnet ist deaktiviert, wenn die Konfiguration des Ports für Remote Console auf der Registerkarte „Global Settings“ (Allgemeine Einstellungen) auf „Disabled“ (Deaktiviert) oder „Automatic“ (Automatisch) eingestellt bzw. die Datenverschlüsselung für Remote Console aktiviert ist.

So beenden Sie eine Telnet-Sitzung:

1. Drücken Sie an der Eingabeaufforderung **Strg+]** und die **Eingabetaste**.
2. Wenn beim Betätigen der Eingabetaste ein Zeilenumbruch angezeigt wird, drücken Sie **Strg+]**, und geben Sie an der Eingabeaufforderung `set crlf off` ein.

   Eine vollständige Liste der Fehler finden Sie unter „iLO 2 VT100+ Tastenkombinationen“.

Einfacher Telnet-Befehlssatz

Die folgenden Tastenkombinationen für einfache Befehlssätze sind verfügbar und können in Telnet-Sitzungen verwendet werden. Diese Befehle stehen nur in einer Telnet-basierten Remote Console- oder einer Virtual Serial Port-Sitzung zur Verfügung.

Action	Tastenfolge	Bemerkung
EINSCHALTEN	STRG P 1	STRG P ist das Präfix der Befehle zum Ein-/Ausschalten. 1 bedeutet, dass EIN ausgewählt wurde.
AUSSCHALTEN	STRG P 0	STRG P ist das Präfix der Befehle zum Ein-/Ausschalten. 0 bedeutet, dass AUS ausgewählt wurde.
ACPI DRÜCKEN	STRG P 6	STRG P ist das Präfix der Befehle zum Ein-/Ausschalten. 6 zeigt einen ACPI Powerdruck an. Ein ACPI Powerdruck hat dieselbe

Action	Tastenfolge	Bemerkung
		Wirkung wie das Halten des Ein-/Aus-Schalters für ca. sechs Sekunden.
SYSTEM-REBOOT	STRG P !	STRG P ist das Präfix der Befehle zum Ein-/Ausschalten. Das ! zeigt einen sofortigen Neustart in einem Notfall an.
UID EIN	STRG U 1	STRG U ist das Präfix für UID-Befehle. 1 bedeutet, dass EIN ausgewählt wurde.
UID AUS	STRG U 0	STRG U ist das Präfix für UID-Befehle. 0 bedeutet, dass AUS ausgewählt wurde.

Vor der Authentifizierung sind die Tasten nicht funktionsfähig. Die Energiesteuerungsanforderungen werden ignoriert, wenn Sie nicht über die entsprechenden Berechtigungen verfügen.

Telnet-Sicherheit

Telnet ist kein gesichertes Netzwerkprotokoll. So vermindern Sie Sicherheitsrisiken:

- Verwenden Sie SSH anstelle von Telnet. SSH ist sicheres oder verschlüsseltes Telnet. CLI wird über Telnet und über SSH unterstützt.
- Verwenden Sie ein separates Management-Netzwerk. Verhindern Sie den Zugriff Unbefugter auf das Netzwerksegment. Dann sind nicht erlaubte Handlungen unmöglich.

Unterstützte Tastenkombinationen

iLO 2 unterstützt das Protokoll VT100+. Die folgenden Tabellen enthalten eine Aufstellung der unterstützten Tastenkombinationen.

iLO 2 VT100+ Tastenkombinationen

Nachfolgend sind VT100+ Tastencodes aufgeführt.

- Viele Terminalprogramme senden `CR-LF` anstelle von **Enter**.

  Code `"\r\n" = '\r'`
- Einige Terminals senden `ASCII 127` (ENTF) anstelle der Rücktaste. Die Entf-Taste sendet niemals ENTF. Sie sendet stattdessen `"\e[3~"`.
- Einige Programme verwenden für die Pos1- und Ende-Taste die folgenden Codes:

  Sequenz `"\e[H" = HOME_KEY`

  Sequenz `"\e[F" = END_KEY`
- `ALT_CAPITAL_O` und `ALT_LEFT_SQBRACKET` sind mehrdeutig.
- Beenden Sie längere Sequenzen, die mit `\eO and \e[)` starten, mit `\?`.

Taste	Sequenz	Taste	Sequenz
\010	\177	**ALT_AMPER**	\e&
UP_KEY	\e[A	**ALT_APOS**	\e'
DOWN_KEY	\e[B	**ALT_OPAREN**	\e(
RIGHT_KEY	\e[C	**ALT_CPAREN**	\e)
LEFT_KEY	\e[D	**ALT_STAR**	\e*
ALT_A	\eA	**ALT_PLUS**	\e+
ALT_B	\eB	**ALT_COMMA**	\e,

Taste	Sequenz	Taste	Sequenz
ALT_C	\eC	**ALT_MINUS**	\e-
ALT_D	\eD	**ALT_PERIOD**	\e.
ALT_E	\eE	**ALT_SLASH**	\e/
ALT_F	\eF	**ALT_COLON**	\e:
ALT_G	\eG	**ALT_SEMICO**	\e;
ALT_H	\eH	**ALT_LESS**	\e<
ALT_I	\eI	**ALT_EQUAL**	\e=
ALT_J	\eJ	**ALT_MORE**	\e>
ALT_K	\eK	**ALT_QUES**	\e?
ALT_L	\eL	**ALT_AT**	\e@
ALT_M	\eM	**ALT_OPENSQ**	\e[\?
ALT_N	\eN	**ALT_BSLASH**	\e\\
ALT_O	\eO\?	**ALT_CLOSESQ**	\e]
ALT_P	\eP	**ALT_CARAT**	\e^
ALT_Q	\eQ	**ALT_USCORE**	\e_
ALT_R	\eR	**ALT_ACCENT**	\e`
ALT_T	\eT	**ALT_PIPE**	\e|
ALT_U	\eU	**ALT_CBRACK**	\e}
ALT_V	\eV	**ALT_TILDE**	\e~
ALT_W	\eW	**ALT_TAB**	\e\t
ALT_X	\eX	**ALT_BS**	\e\010
ALT_Y	\eY	**ALT_CR**	\e\r
ALT_Z	\eZ	**ALT_ESC**	\e\e\?
ALT_LOWER_A	\ea	**ALT_F1**	\e\eOP
ALT_LOWER_B	\eb	**ALT_F2**	\e\eOQ
ALT_LOWER_C	\ec	**ALT_F3**	\e\eOR
ALT_LOWER_D	\ed	**ALT_F4**	\e\eOS
ALT_LOWER_E	\ee	**ALT_F5**	\e\eOT
ALT_LOWER_F	\ef	**ALT_F6**	\e\eOU
ALT_LOWER_G	\eg	**ALT_F7**	\e\eOV
ALT_LOWER_H	\eh	**ALT_F8**	\e\eOW
ALT_LOWER_I	\ei	**ALT_F9**	\e\eOX
ALT_LOWER_J	\ej	**ALT_F10**	\e\eOY
ALT_LOWER_K	\ek	**ALT_F11**	\e\eOZ
ALT_LOWER_L	\el	**ALT_F12**	\e\eO[
ALT_LOWER_M	\em	**ALT_F5**	\e\e[15~
ALT_LOWER_N	\en	**ALT_F6**	\e\e[17~

Taste	Sequenz	Taste	Sequenz
ALT_LOWER_O	\eo	**ALT_F7**	\e\e[18~
ALT_LOWER_P	\ep	**ALT_F8**	\e\e[19~
ALT_LOWER_Q	\eq	**ALT_F9**	\e\e[20~
ALT_LOWER_R	\er	**ALT_F10**	\e\e[21~
ALT_LOWER_S	\es	**ALT_F11**	\e\e[23~
ALT_LOWER_T	\et	**ALT_F12**	\e\e[24~
ALT_LOWER_U	\eu	**ALT_HOME**	\e\e[1~
ALT_LOWER_V	\ev	**ALT_INS**	\e\e[2~
ALT_LOWER_W	\ew	**ALT_DEL**	\e\e[3~
ALT_LOWER_X	\ex	**ALT_END**	\e\e[4~
ALT_LOWER_Y	\ey	**ALT_PGUP**	\e\e[5~
ALT_LOWER_Z	\ez	**ALT_PGDN**	\e\e[6~
ALT_SPACE	\e\040	**ALT_HOME**	\e\e[H
ALT_EXCL	\e!	**ALT_END**	\e\e[F
ALT_QUOTE	\e\"	**ALT_UP**	\e\e[A
ALT_POUND	\e#	**ALT_DOWN**	\e\e[B
ALT_DOLLAR	\e$	**ALT_RIGHT**	\e\e[C
ALT_PERCENT	\e%	**ALT_LEFT**	\e\e[D

VT100+ Codes für die F-Tasten

Taste	Sequenz
F1_KEY	\eOP
F2_KEY	\eOQ
F3_KEY	\eOR
F4_KEY	\eOS
F5_KEY	\eOT
F6_KEY	\eOU
F7_KEY	\eOV
F8_KEY	\eOW
F9_KEY	\eOX
F10_KEY	\eOY
F11_KEY	eOZ
F12_KEY	\eO[

Linux-Codes für die F-Tasten

Taste	Sequenz
F5_KEY	\e[15~
F6_KEY	\e[17~
F7_KEY	\e[18~
F8_KEY	\e[19~
F9_KEY	\e[20~
F10_KEY	\e[21~
F11_KEY	\e[23~
F12_KEY	\e[24~
HOME_KEY	\e[1~
INSERT_KEY	\e[2~
DELETE_KEY	\e[3~
END_KEY	\e[4~
BILD AUF	\e[5~
PG_DOWN	\e[6~

4 Secure Shell

Übersicht über SSH

SSH ist ein mit Telnet vergleichbares Programm zum Anmelden und Ausführen von Befehlen auf einem Remotecomputer. Es umfasst Authentifzierungs-, Verschlüsselungs- und Datenintegritätsfunktionen. Der iLO 2 Firmware kann den gleichzeitigen Zugriff von zwei SSH-Clients unterstützen. Nachdem SSH verbunden und authentifiziert wurde, ist die Befehlszeilenschnittstelle verfügbar.

iLO 2 unterstützt:

- SSH Protokoll Version 2
- PuTTY 0.58, eine kostenlose Version von Telnet und dem SSH Protokoll, die aus dem Internet heruntergeladen werden kann. Wenn Sie ältere Versionen von PuTTY (vor 0.54) verwenden, können zwei anstelle von einem Zeilenvorschub angezeigt werden, wenn Sie die Eingabetaste drücken. Um dieses Problem auszuschließen und die bestmöglichen Ergebnisse zu erzielen, empfiehlt HP, Version 0.54 oder höher einzusetzen.
- OpenSSH, eine kostenlose Version des SSH Protokolls, die aus dem Internet heruntergeladen werden kann.

Bei der Aktualisierung der Firmware kommt es zu einer einmaligen Verzögerung von 25 Minuten, bevor die SSH-Funktionalität zur Verfügung steht. Während dieser Zeit generiert iLO 2 die 1024-Bit-RSA- und DSA-Schlüssel. iLO 2 speichert diese Schlüssel zur späteren Wiederverwendung. Wenn Sie iLO 2 auf die Werkseinstellungen zurücksetzen, werden die RSA- und DSA-Schlüssel gelöscht und beim nächsten Start erneut generiert.

Von iLO 2 unterstützte SSH-Funktionen

Die iLO 2 Library unterstützt lediglich Version 2 (SSH-2) des Protokolls. Die unterstützten Funktionen werden in der folgenden Tabelle aufgeführt.

Merkmal	Unterstützter Algorithmus
Serverhostkey-Algorithmen	ssh-dsa , ssh-rsa
Verschlüsselung (gleicher Satz wird in beiden Richtungen unterstützt)	3des-cbc, aes128-cbc
Hashing-Algorithmen	hmac-sha1, hmac-md5
Public-Key-Algorithmen	ssh-dss, ssh-rsa
Schlüsselaustausch	Diffie-hellman-group1-sha1
Komprimierung	Keine
Language (Sprache)	Englisch
Client-/Benutzerauthentifizierungsmethode	Password (Kennwort)
Authentifizierungs-Timeout	2 Minuten
Authentifizierungsversuche	3
Standard-SSH Port	22

Verwenden von Secure Shell

Verwenden von SSH

So greifen Sie mit SSH auf iLO 2 zu:

1. Öffnen Sie ein SSH-Fenster.
2. Geben Sie bei der entsprechenden Aufforderung die IP-Adresse oder den DNS-Namen sowie den Anmeldenamen und das Kennwort ein.

Verwenden von OpenSSH

So starten Sie den OpenSSH Client in Linux:

```
ssh -l loginname ipaddress/dns name
```

Verwenden von PuTTY

- Starten Sie die PuTTY-Sitzung, indem Sie auf das PuTTY-Symbol in dem Verzeichnis doppelklicken, in dem Sie PuTTY installiert haben.
- So starten Sie eine PuTTY-Sitzung von der Befehlszeile:
  - So starten Sie eine Verbindung zu einem Server mit der Bezeichnung *host:*

    ```
    putty.exe [-ssh | -telnet | -rlogin | -raw] [user@]host
    ```

  - Für Telnet-Sitzungen wird die folgende alternative Syntax unterstützt:

    ```
    putty.exe telnet://host[:port]/
    ```

  - So starten Sie eine bestehende gespeicherte Sitzung mit der Bezeichnung *Sitzungsname*:

    ```
    putty.exe -load "Sitzungsname"
    ```

SSH-Schlüsselautorisierung

Die SSH-Schlüssel-basierte Authentifizierung ermöglicht HP SIM, über SSH eine Verbindung zu LOMGeräten herzustellen und zum Durchführen von Tasks auf administrativer Ebene authentifiziert und autorisiert zu werden. Zur Ausführung der Tasks wird das CLP verwendet. HP SIM kann diese Tasks praktisch gleichzeitig zu geplanten Zeiten auf mehreren LOM-Geräten ausführen. HP SIM bietet eine menügesteuerte Schnittstelle zur Verwaltung und Konfiguration mehrerer Ziele. Erweiterungen zu HP SIM werden über Tool-Definitionsdateien bereitgestellt.

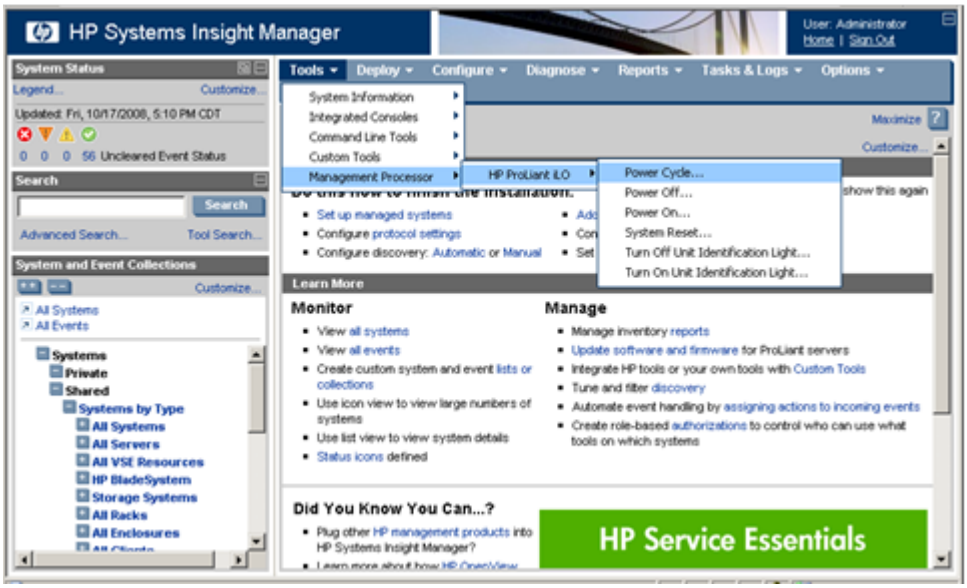
HP SIM kann über eine SSH-Schnittstelle, die eine Authentifizierung basierend auf privaten Schlüsseln erfordert, Aktionen auf Zielgeräten ausführen. Wenn HP SIM für eine engere Integration mit LOM-Geräten aktiviert ist, wird in iLO 2 eine SSH-Schlüssel-basierte Authentifizierung implementiert.

Dabei wird eine HP SIM-Instanz als vertrauenswürdiger SSH-Client erstellt, indem ihr öffentlicher Schlüssel in iLO 2 gespeichert wird. Dies erfolgt entweder manuell über eine webbasierte Benutzeroberfläche oder automatisch anhand des Dienstprogramms `mxagentconfig`. Weitere Informationen finden Sie unter „Mxagentconfig“.

Für die Verwendung von SSH im interaktiven Betriebsmodus müssen keine SSH-Schlüssel erzeugt werden. Informationen zum Verwenden von SSH im interaktiven Modus finden Sie unter „Übersicht über SSH“.

Tool-Definitionsdateien

TDEF-Dateien erweitern das Menüsystem von HP SIM und stellen somit die CLP-Befehle bereit, die HP SIM über eine SSH-Verbindung an iLO 2 sendet.



Mxagentconfig

Mxagentconfig ist ein Dienstprogramm zum Export und zur Installation von öffentlichen SSH-Schlüsseln des HP SIM in anderen Systemen. Dieses Dienstprogramm vereinfacht den Vorgang und kann den öffentlichen Schlüssel auf vielen Systemen gleichzeitig installieren. Mxagentconfig stellt eine SSHVerbindung zu iLO 2 her, führt die Authentifizierung mit einem Benutzernamen und einem Kennwort durch und überträgt den erforderlichen öffentlichen Schlüssel. iLO 2 speichert diesen Schlüssel als Schlüssel eines vertrauenswürdigen SSH-Clients.

Importieren von SSH-Schlüsseln von PuTTY

Das von PuTTY erzeugte Dateiformat des öffentlichen Schlüssels ist nicht mit iLO 2 kompatibel. Das folgende Beispiel veranschaulicht eine von PuTTY erzeugte Schlüsseldatei:

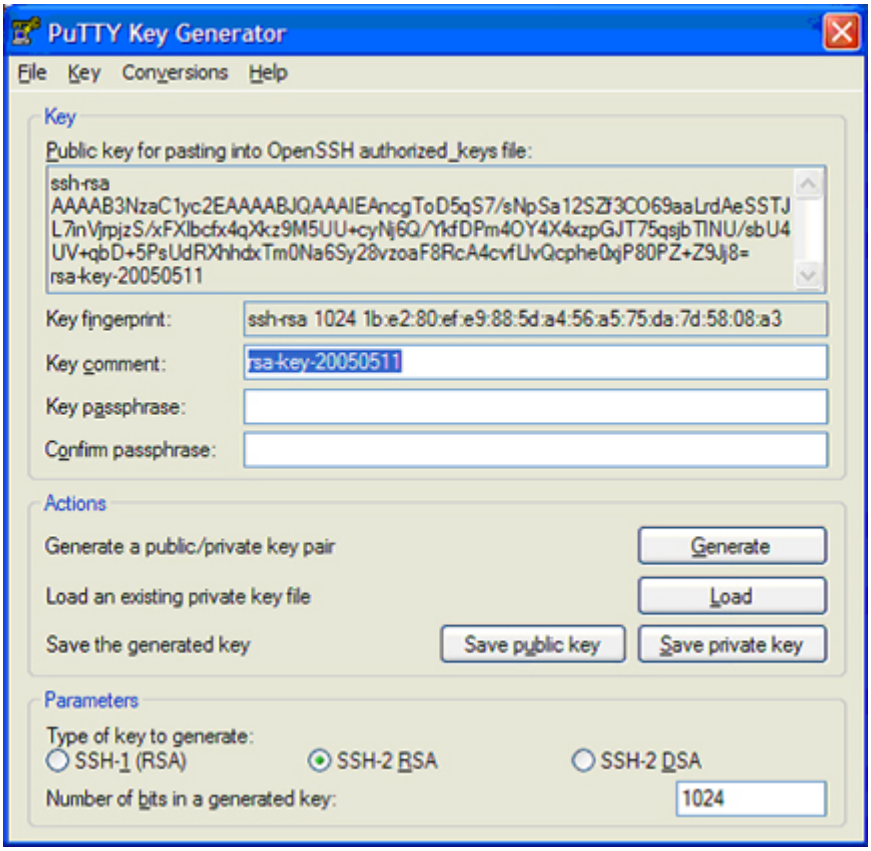
```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "Administrator"
AAAAB3NzaC1yc2EAAAABJQAAAIB0x0wVO9itQB11o+tHnY3VvmsGgwghCyLOVzJl
3A9F5yzKj+RXJVPxOGusAhmJwF8PBQ9wV5E0Rumm6gNOaPyvAMJCG/l0PW7Fhac1
VLt8i5F3Lossw+/LWa+6H0da13TF2vq3ZoYFUT4esC6YbAACM7kLuGwxF5XMNR2E
Foup3w==
---- END SSH2 PUBLIC KEY ----
```

iLO 2 erwartet Informationen zur Datei mit dem öffentlichen Schlüssel in einer Zeile. Aus diesem Grund müssen Sie mit dem PuTTY-Schlüsselerstellungsprogramm (puttygen.exe) einen korrekt formatierten SSH-Schlüssel importieren, um den Schlüssel in iLO 2 verwenden zu können.

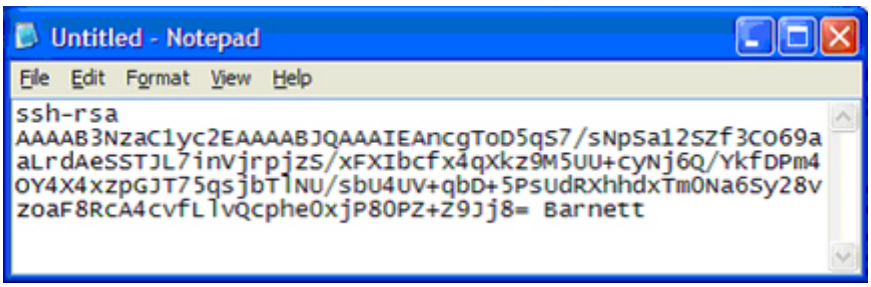
So importieren Sie SSH-Schlüssel von PuTTY zur Verwendung in iLO 2:

1. Doppelklicken Sie auf das Symbol des PuTTY-Schlüsselerstellungsprogramms, um das Dienstprogramm zu starten.
2. Wählen Sie **SSH-2 RSA**, und klicken Sie dann auf **Generate** (Erstellen).

   Bewegen Sie die Maus im Schlüsselbereich, um einen den Schlüssel zu erstellen. Sie müssen die Maus fortwährend bewegen, bis die Schlüsselerstellungsvorgang abgeschlossen ist.

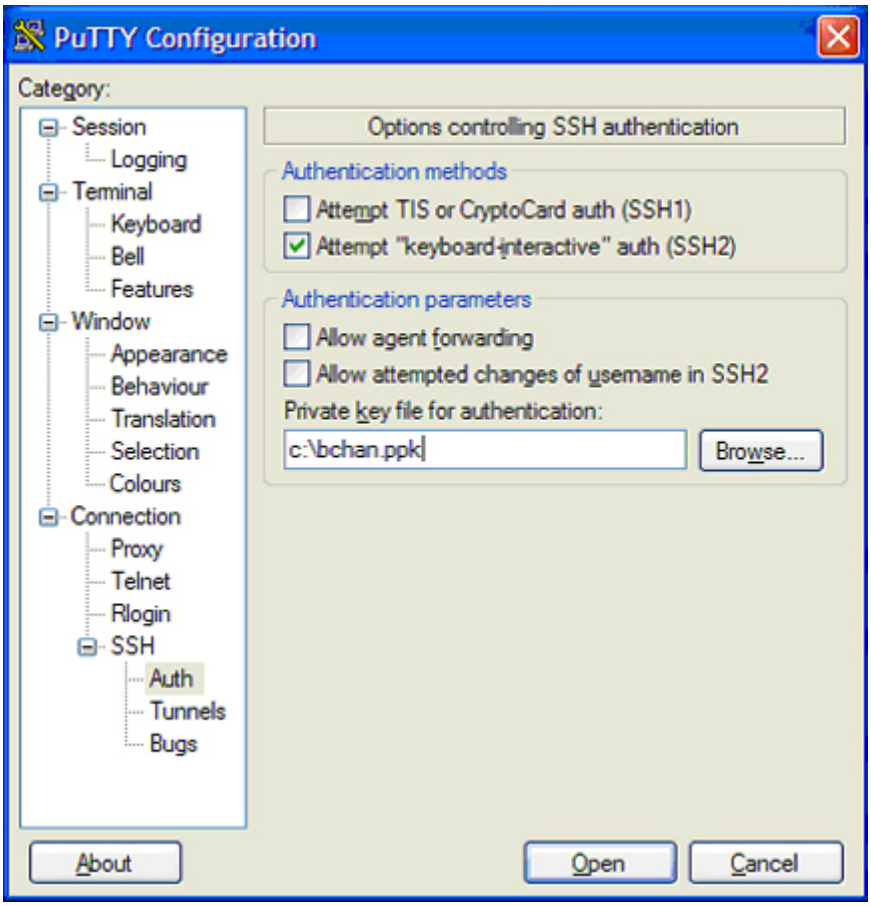


3. Nachdem der Schlüssel erstellt wurde, ersetzen Sie den Schlüsselbefehl durch Ihren iLO 2 Benutzernamen (bei dem Benutzername sind Groß-/Kleinschreibung bedeutsam).
4. Wählen Sie den gesamten Text im Bereich des öffentlichen Schlüssels aus. Kopieren Sie den Schlüssel, und fügen Sie ihn in eine Notepad-Sitzung ein.
5. Kehren Sie zum PuTTY-Schlüsselerstellungsprogramm zurück.
6. Klicken Sie auf **Save private key** (Privaten Schlüssel speichern), um den Schlüssel zu speichern und auf eine entsprechende Aufforderung hin einen Dateinamen einzugeben, z. B. c:\bchan.ppk.
7. Kehren Sie zu Notepad zurück.
8. Speichern Sie die Datei mit dem öffentlichen Schlüssel. Klicken Sie auf **Datei>Speichern unter**, und geben Sie auf eine entsprechende Aufforderung hin einen Dateinamen ein, z. B. c:\bchan.pub.



9. Melden Sie sich bei iLO 2 an (falls nicht bereits geschehen).
10. Klicken Sie auf der iLO 2 Seite „SSH Key Administration“ (SSH-Schlüsselverwaltung) auf **Browse** (Durchsuchen), und suchen Sie nach der Datei mit dem öffentlichen Schlüssel.
11. Klicken Sie auf **Authorize Key** (Schlüssel autorisieren). In der Liste erscheint ein neuer autorisierter SSH-Schlüssel.
12. Starten Sie PuTTY.

13. Wählen Sie **SSH>Auth.**.
14. Klicken Sie auf **Browse** (Durchsuchen), und suchen Sie die Datei mit dem privaten Schlüssel.
15. Konfigurieren Sie Ihre iLO 2 IP, und klicken Sie auf **Open** (Öffnen). iLO 2 fordert Sie zur Eingabe eines Benutzernamens auf.



16. Geben Sie den mit dem öffentlichen Schlüssel verknüpften Anmeldenamen ein. Der öffentliche Schlüssel in iLO 2 wird mit durch den privaten Schlüssel in PuTTY authentifiziert. Wenn die Schlüssel zueinander passen, können Sie sich ohne Eingabe eines Kennworts bei iLO 2 anmelden.

    Schlüssel können mit einer Schlüssel-Passphrase erstellt werden. Wenn beim Erstellen des öffentlichen Schlüssels eine Schlüssel-Passphrase verwendet wurde, werden Sie vor der Anmeldung bei iLO 2 zur Eingabe der Schlüssel-Passphrase aufgefordert.

Importieren von mit ssh-keygen erstellten SSH-Schlüsseln

Nachdem Sie mit ssh-keygen einen SSH-Schlüssel und die Datei key.pub erstellt haben, müssen Sie wie folgt verfahren:

1. Suchen Sie die Datei key.pub mit einem Textexditor, und öffnen Sie sie. Die Datei muss mit dem Text `ssh-dss` oder `ssh-rsa` beginnen.
2. Hängen Sie am Ende der Zeile eine Leerstelle („ “) und den Namen eines gültigen iLO 2 Benutzers an, der auf der Seite „Modify User“ (Benutzer ändern) angegeben wird. Beispiel:

    ```
    xxx_some_text_xxx ASmith
    ```

    Bei dem Benutzernamen wird zwischen Groß- und Kleinschreibung unterschieden. Er muss daher genauso wie der iLO 2 Benutzername geschrieben werden, damit der SSH-Schlüssel mit dem richtigen Benutzer verknüpft wird.
3. Speichern und schließen Sie die Datei.

Die Datei kann nun importiert und autorisiert werden.

5 Gruppenadministration und iLO 2 Scripting

CPQLOCFG Utility

CPQLOCFG.EXE ist ein Windows-Utility, das über eine sichere Netzwerkverbindung eine Verbindung zu iLO aufbaut. RIBCL-Skripts werden über die sichere Verbindung zu CPQLOCFG an iLO übergeben. Zur Verwendung dieses Dienstprogramms sind eine gültige Benutzer-ID und ein Kennwort mit den entsprechenden Berechtigungen erforderlich. Starten Sie CPQLOCFG zur Gruppenadministration über HP SIM, oder starten Sie es zur Stapelverarbeitung eigenständig über eine Befehlsaufforderung.

Laden Sie das Utility von der HP Website herunter: http://h20000.www2.hp.com/bizsupport/TechSupport/SoftwareDescription.jsp?lang=en&cc=US&swItem=MTX-UNITY-I16117&mode=4&idx=1&prodTypeId=329290&prodSeriesId=397206.

Zur Unterstützung aller Funktionen von iLO 3 v1.20 und iLO 4 v1.05 und höher wird Version 4.0 oder höher von CPQLOCFG benötigt.

HP SIM erkennt iLO Geräte als Managementprozessoren. CPQLOCFG sendet eine RIBCL-Datei an eine Gruppe von iLO Geräten, um die Benutzerkonten dieser iLO Geräte zu verwalten. Die iLO Geräte führen dann den durch die RIBCL-Datei festgelegten Vorgang aus und senden eine Antwort an die Protokolldatei.

Führen Sie mit CPQLOCFG RIBCL-Skripts auf iLO aus. CPQLOCFG muss sich auf demselben Server wie HP SIM befinden. CPQLOCFG erstellt zwei Arten von Fehlermeldungen: Laufzeitfehler und Syntaxfehler.

- Laufzeitfehler treten auf, wenn eine ungültige Aktion angefordert wird. Laufzeitfehler werden im folgenden Verzeichnis protokolliert:

  `C:\PROGRAM FILES\INSIGHT MANAGER\HP\SYSTEMS`

- Syntaxfehler treten auf, wenn ein ungültiger XML-Tag angetroffen wird. Wenn ein Syntaxfehler auftritt, stoppt CPQLOCFG die Ausführung und protokolliert den Fehler im Laufzeitskript und in der Ausgabeprotokolldatei.

  Syntaxfehler weisen das folgende Format auf:

  `Syntax error: expected X but found Y.`

  Beispiel:

  `Syntax error: expected USER_LOGIN=userlogin but found USER_NAME=username`

Eine vollständige Liste der Fehler finden Sie unter Kapitel 9, „Verwenden von RIBCL“.

XML-Abfrage ohne Authentifizierung

Bei einer entsprechenden Konfiguration gibt das iLO Gerät als Antwort auf eine nicht authentifizierte XML-Abfrage Identifizierungsinformationen zurück. Das iLO Gerät ist standardmäßig so konfiguriert, dass diese Informationen zurückgegeben werden. Um nicht authentifizierte XML-Abfragen zu deaktivieren, aktivieren Sie CIM_SECURITY_MASK im Befehl MOD_SNMP_IM_SETTINGS.

Sie können nicht authentifizierte XML-Abfragen auch über die iLO Webseite deaktivieren:

1. Navigieren Sie zu **Administration→Management**.

   Die Webseite **Management** erscheint.

2. Klicken Sie unter der Überschrift **Insight Management Integration** (Insight Management-Integration) auf das Menü für die Option **Level of Data Returned** (Umfang der zurückgegebenen Daten).

   In dem Menü befinden sich zwei Optionen:

   - 1) Enabled (iLO+Server Association Data) (Aktiviert (iLO+Serververknüpfungsdaten))

- 2) Disabled (No Response to Request) (Deaktiviert (Keine Antwort auf Anfrage))

3. Wählen Sie „2) Disabled (No Response to Request)“ (Deaktiviert (Keine Antwort auf Anfrage)), um die Rückgabe von Informationen auf nicht authentifizierte XML-Abfragen zu deaktivieren.

HINWEIS: Die nicht authentifizierte XML-Abfrage muss aktiviert sein, wenn Geräteermittlungen mit HP SIM durchgeführt werden.

Wenn Sie nicht authentifizierte Identifizierungsinformationen erhalten möchten, senden Sie den folgenden Befehl zum iLO Webserver-Port (oder wählen Sie die Option „1) Enabled (iLO+Server Association Data)“ (1) Aktiviert (iLO+Serververknüpfungsdaten)) über iLO aus):

`https://iloaddress/xmldata?item=all`

Eine typische Antwort lautet:

```
<?xml version="1.0" ?>
<RIMP>
<HSI>
<SBSN>0004PBM158</SBSN>
<SPN>ProLiant DL380 G5</SPN>
<UUID>1226570004PBM158</UUID>
<SP>1</SP>
</HSI>
<MP>
<ST>1</ST>
<PN>Integrated Lights-Out 2 (iLO 2)</PN>
<FWRI>1.10</FWRI>
<HWRI>ASIC: 5</HWRI>
<SN>ILO0004PBM158</SN>
<UUID>ILO1226570004PBM158</UUID>
</MP>
</RIMP>


<RIMP>
<HSI>
<SBSN>ABC12345678</SBSN>
<SPN>ProLiant BL460c Gen8</SPN>
<UUID>BL4608CN71320ZNN</UUID>
<SP>0</SP>
<cUUID>36344C42-4E43-3830-3731-33305A4E4E32</cUUID>
<VIRTUAL>
<STATE>Inactive</STATE>
<VID>
<BSN/>
<cUUID/>
</VID>
</VIRTUAL>
<PRODUCTID>BL4608-101</PRODUCTID>
<NICS>
<NIC>
<PORT>1</PORT>
<MACADDR>00:17:a4:77:08:02</MACADDR>
</NIC>
<NIC>
<PORT>2</PORT>
<MACADDR>00:17:a4:77:08:04</MACADDR>
</NIC>
<NIC>
<PORT>3</PORT>
<MACADDR>00:17:a4:77:08:00</MACADDR>
</NIC>
<NIC>
```

```
<PORT>4</PORT>
<MACADDR>9c:8e:99:13:20:cd</MACADDR>
</NIC>
<NIC>
<PORT>5</PORT>
<MACADDR>9c:8e:99:13:20:ca</MACADDR>
</NIC>
<NIC>
<PORT>6</PORT>
<MACADDR>9c:8e:99:13:20:ce</MACADDR>
</NIC>
<NIC>
<PORT>7</PORT>
<MACADDR>9c:8e:99:13:20:cb</MACADDR>
</NIC>
<NIC>
<PORT>8</PORT>
<MACADDR>9c:8e:99:13:20:cf</MACADDR>
</NIC>
</NICS>
</HSI>
<MP>
<ST>1</ST>
<PN>Integrated Lights-Out 4 (iLO 4)</PN>
<FWRI>1.01</FWRI>
<BBLK>08/30/2011</BBLK>
<HWRI>ASIC: 16</HWRI>
<SN>ILOABC12345678</SN>
<UUID>ILOBL4608ABC12345678</UUID>
<IPM>1</IPM>
<SSO>0</SSO>
<PWRM>3.0</PWRM>
<ERS>0</ERS>
<EALERT>1</EALERT>
</MP>
<BLADESYSTEM>
<BAY>1</BAY>
<MANAGER>
<TYPE>Onboard Administrator</TYPE>
<MGMTIPADDR>123.456.78.90</MGMTIPADDR>
<RACK>TestRACK</RACK>
<ENCL>TestRACKEnc-C</ENCL>
<ST>2</ST>
</MANAGER>
</BLADESYSTEM>
</RIMP>
```

Abfragedefinition in HP SIM

Um alle iLO Geräte zu gruppieren, melden Sie sich bei HP SIM an und erstellen eine Abfrage.

So erstellen Sie die Abfrage:

1. Melden Sie sich bei HP SIM an.
2. Klicken Sie auf dem Bildschirm links oben in der Navigationsleiste auf **Device** (Gerät).
3. Klicken Sie auf **Queries (Abfragen)**→**Device (Gerät)**.
4. Suchen Sie im Hauptfenster nach dem Abschnitt **Personal Queries** (Persönliche Abfragen). Wenn eine Abfragekategorie vorhanden ist, fahren Sie mit Schritt 8 fort. Fahren Sie andernfalls mit Schritt 5 fort.
5. Klicken Sie auf **New** (Neu), um eine neue Kategorie zu erstellen. In diesem Beispiel hat die neue Kategorie den Namen **`RIB Cards`**.
6. Klicken Sie auf **Create Category** (Kategorie erstellen).

7. Klicken Sie auf **Queries** (Abfragen), um zum Bildschirm **Device Queries** (Geräteabfragen) zurückzukehren.
8. Klicken Sie in der entsprechenden Abfragekategorie auf **New** (Neu), um das Fenster **Create/Edit Query** (Abfrage erstellen/bearbeiten) zu öffnen, in dem die Abfragedefinition erstellt wird.
9. Geben Sie den Namen der Abfrage ein, z. B. **`Mgmtprozessoren`**.
10. Wählen Sie **Device(s) of type** (Gerät(e) vom Typ) und anschließend **Devices by product name** (Geräte nach Produktname) aus.

    Legen Sie im Kriterienfenster **HP iLO 3** als Produktnamen fest.
11. Wählen Sie **Device(s) of type** (Gerät(e) vom Typ) und anschließend **Devices by product name** (Geräte nach Produktname) aus.

    Legen Sie im Kriterienfenster **`HP iLO 2`** als Produktnamen fest.
12. Klicken Sie im Feld **Query Description** (Abfragebeschreibung) auf **Type** (Typ).

    Das Fenster **Device Types** (Gerätetypen) wird geöffnet.
13. Wählen Sie **Management Processor** (Managementprozessor), und klicken Sie auf **OK**.
14. Klicken Sie auf **Save** (Speichern), um zum Bildschirm **Device Query** (Geräteabfrage) zurückzukehren.
15. Suchen Sie in der entsprechenden Abfragekategorie nach der gerade erzeugten Abfrage, und klicken Sie auf den Abfragenamen, um die Abfrage zur Verifizierung zu starten.
16. Klicken Sie auf **Overview** (Übersicht) auf der linken Bildschirmseite, nachdem die Verifizierung erfolgt ist.

    Die Startseite für Geräte wird geöffnet.

Anwendungsstart unter Verwendung von HP SIM

Der Anwendungsstart kombiniert RIBCL, CPQLOCFG und Abfragedefinition zur Verwaltung der Gruppenadministration von iLO Geräten.

So erstellen Sie einen Anwendungsaufruf-Task:

1. Klicken Sie auf dem Bildschirm links oben in der Navigationsleiste auf **Device** (Gerät).
2. Klicken Sie auf **Tasks**, um das Fenster „Tasks“ zu öffnen.
3. Klicken Sie auf **New Control Task** (Neue Steuertask), und wählen Sie im Dropdown-Menü **Application Launch** (Anwendungsstart), um das Fenster **Create/Edit Task** (Task erstellen/bearbeiten) zu öffnen.
4. Geben Sie den vollständigen Pfad und Namen des Lights-Out Configuration Utility in das dafür vorgesehene Feld ein. Wenn sich die Datei CPQLOCFG.EXE im Stammverzeichnis des Laufwerks `C:\` befindet, lautet der Pfad:

   ```
   C:\cpqlocfg.exe.
   ```
5. Geben Sie die Parameter in das dafür vorgesehene Feld ein. HP SIM benötigt die folgenden Parameter für CPQLOCFG:

   `-F` Vollständiger Pfad des RIBCL-Dateinamens

   `-V` Ausführliche Meldung (optional)

   Wenn sich die RIBCL-Datei im Stammverzeichnis des Laufwerks `C:\` befindet, lauten die Parameter:

   ```
   -F C:\MANAGEUSERS.xml -V
   ```

HINWEIS: Der Parameter `L` kann keine Ausgabe-Protokolldatei angeben. Im gleichen Verzeichnis, in dem CPQLOCFG gestartet wird, wird eine Standard-Protokolldatei erstellt, die mit dem DNS-Namen oder der IP-Adresse benannt wird.

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

   In einem Bildschirm werden die Optionen zum Benennen des Task, zum Definieren der Abfrageverknüpfung und zum Einrichten eines Zeitplans für den Task angezeigt.
7. Geben Sie in das Feld **Enter a name for this task** (Namen für diese Task eingeben) einen Namen für die Task ein.
8. Wählen Sie die zuvor erstellte Abfrage, z. B. **Mgmtprozessoren**.
9. Klicken Sie auf **Schedule** (Zeitplan), um festzulegen, wann der Anwendungsstart-Task ausgeführt wird.

   Das Fenster „Schedule Configuration" (Zeitplan-Konfiguration) wird angezeigt.
10. Klicken Sie auf **OK**, um den Zeitplan festzulegen.

    HINWEIS: Die voreingestellte Zeit für einen Steuerungs-Task ist **Now** (Jetzt).
11. Klicken Sie auf **Finish** (Fertig stellen), um den Anwendungsstart-Task zu speichern.
12. Klicken Sie auf das Symbol **Execute a Task** (Task ausführen) (das grüne Dreieck), um die Gruppenadministration auszuführen.

Stapelverarbeitung mittels CPQLOCFG

Die Gruppenadministration wird ebenfalls über Stapelverarbeitung an iLO übergeben. Die im Rahmen der Stapelverarbeitung verwendeten Komponenten sind CPQLOCFG, eine RIBCL-Datei und eine Stapeldatei.

Das folgende Beispiel zeigt eine Musterstapeldatei, über die die Gruppenadministration für iLO durchgeführt wird:

```
REM Updating the HP Integrated Lights-Out 2 board
REM Repeat line for each board to be updated
REM
CPQLOCFG -S RIB1 -F C:\...SCRIPT.XML -L RIB1LOG.TXT -V
CPQLOCFG -S RIB2 -F C:\...SCRIPT.XML -L RIB2LOG.TXT -V
CPQLOCFG -S RIB3 -F C:\...SCRIPT.XML -L RIB3LOG.TXT -V
.
.
.
RIBNLOG -S RIBN -F C:\...SCRIPT.XML -L LOGFILE.TXT -V


REM Updating the HP Integrated Lights-Out 3 board
REM Repeat line for each board to be updated
REM
CPQLOCFG -S RIB1 -F C:\...SCRIPT.XML -L RIB1LOG.TXT -V
CPQLOCFG -S RIB2 -F C:\...SCRIPT.XML -L RIB2LOG.TXT -V
CPQLOCFG -S RIB3 -F C:\...SCRIPT.XML -L RIB3LOG.TXT -V
.
.
.
RIBNLOG -S RIBN -F C:\...SCRIPT.XML -L LOGFILE.TXT -V
```

CPQLOCFG überschreibt alle bestehenden Protokolldateien.

CPQLOCFG-Parameter

- Der Schalter `-S` bestimmt das zu aktualisierende iLO Modul. Dieser Schalter ist entweder der DNS-Name oder die IP-Adresse des Zielservers.

  HINWEIS: Verwenden Sie diesen Schalter nicht beim Starten über HP SIM. HP SIM stellt automatisch die Adresse des iLO Moduls bereit, wenn Sie CPQLOCFG starten.

- Der Schalter `-F` gibt den vollständigen Pfad und Namen der RIBCL-Datei an, in der die auf der Karte auszuführenden Aktionen enthalten sind.
- `-U` und `-P` geben den Benutzeranmeldenamen bzw. das Benutzerkennwort an. Mit diesen Optionen können die Anmeldeinformationen innerhalb der Skriptdatei überschrieben werden.

Stellen Sie sicher, dass sich CPQLOCFG in einem Verzeichnis befindet, auf das die Umgebungsvariable PATH verweist. Alle erstellten Protokolldateien werden im gleichen Verzeichnis platziert wie die CPQLOCFG-Programmdatei.

HINWEIS:

- Wenn Sie den Benutzernamen und das Kennwort nicht über die Befehlszeile, sondern über die XML-Datei eingeben, verwenden Sie Anführungszeichen ("). Wenn Sie jedoch " im Kennwort in der XML-Datei verwenden, dann müssen Apostrophe als umschließende Anführungszeichen verwendet werden.

  Beispiel:

  `'admin"admin'`

  Wenn Sie CPQLOCFG oder LOCFG verwenden und das Kennwort oder den Befehl mit der Option `-p` in der Befehlszeile angeben, kann das Anführungszeichen (") nicht verwendet werden. Es gibt zwei weitere spezielle Zeichen, das kaufmännische Und (`&`) und das Kleiner-als-Zeichen `(<)`, die anders gehandhabt werden müssen. Der Benutzer muss Kennwörter oder Befehle, die eines dieser Sonderzeichen enthalten, in Anführungszeichen setzen.

  Beispiel:

  `"admin&admin"` oder `"admin<admin"`

- Wenn Sie LOCFG verwenden und das Kennwort oder den Befehl mit der Option `-i` über die Befehlszeile eingeben, muss das Anführungszeichen (") nicht verwendet werden.

  Beispiel:

  `admin&admin` oder `admin<admin`

  Das Kennwort oder der Befehl funktioniert nicht mit dem Anführungszeichen, wenn Sie die Option `-i` verwenden.

Das Setzen der Schalter `-L` und `-V` liegt im Ermessen des IT-Administrators.

- Der Schalter `-L` definiert den Namen und den Speicherort der Protokolldatei. Wenn dieser Schalter nicht verwendet wird, wird eine Standard-Protokolldatei, die mit dem DNSNamen oder der IP-Adresse benannt ist, in dem Verzeichnis erstellt, aus dem CPQLOCFG gestartet wird.

  HINWEIS: Verwenden Sie diesen Schalter nicht beim Starten über HP SIM.

  Die Ausgabewerte müssen möglicherweise geändert werden, damit sie der RIBCL-Syntax entsprechen.

  Der Schalter `–L` kann keine Ausgabe-Protokolldatei angeben. Im gleichen Verzeichnis, in dem CPQLOCFG gestartet wird, wird eine Standard-Protokolldatei erstellt, die mit dem DNS-Namen oder der IP-Adresse benannt wird.

- `-V` ist der optionale Schalter, der die Rückgabe der ausführlichen Nachricht aktiviert. Die resultierende Protokolldatei enthält alle Befehle, die an die Remote Insight Karte gesendet wurden, alle Antworten der Remote Insight Karte sowie sämtliche Fehler. Wird der Schalter nicht verwendet, werden standardmäßig nur Fehler und Antworten von GET-Befehlen protokolliert.

- Der Schalter `-t Namen-Wertepaare` ersetzt die in der Eingabedatei vorhandenen Variablen (`%variable%`) durch die in der Namen-Wertepaare-Variablen angegebenen Werte. Trennen Sie mehrere Namen-Wertepaare durch ein Komma.

  Beispiel:

  ```
  <RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="%user%" PASSWORD="%password%">
  <USER_INFO MODE="read">
  <GET_ALL_USERS/>
  </USER_INFO>
  </LOGIN>
  </RIBCL>
  ```

  Geben Sie an der Befehlszeile Folgendes ein:

  ```
  cpqlocfg -f Dateiname -s Server-IP -t user=Admin,password=pass
  ```

  Wenn der Parameter mehrere Wörter enthält, müssen Sie den Satz in Anführungszeichen ("") setzen. In einer XML-Datei werden bis zu 25 Variablen unterstützt. Die maximale Länge des Variablennamen beträgt 48 Zeichen.

  Beispiel für Web Agent:

  ```
  <RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <RIB_INFO MODE="write">
  <MOD_SNMP_IM_SETTINGS>
  <WEB_AGENT_IP_ADDRESS value=%WebAgent%/>
  </MOD_SNMP_IM_SETTINGS>
  </RIB_INFO>
  </LOGIN>
  </RIBCL>
  ```

  Rufen Sie das Skript folgendermaßen auf:

  ```
  cpqlocfg -s iLO-ip-name -f mod_snmp_im_settings.xml -t
  WebAgent='"Your_Value_Here"'
  ```

  Wenn ein Token ersetzt wird, das in doppelten Anführungszeichen steht, setzen Sie das Token in einfache Anführungszeichen.

Weitere Informationen zur Syntax der XML-Datendateien finden Sie unter „Verwenden von RIBCL“ (Seite 78).

XML-Beispielsskripts sind auf der HP Website unter http://www.hp.com/servers/lights-out verfügbar.

Weitere Informationen zur Syntax der XML-Datendateien finden Sie unter „Verwenden von RIBCL“ (Seite 78).

XML-Beispielskripts sind auf der HP Website unter www.hp.com/go/iLO3 verfügbar.

Weitere Informationen zur Syntax der XML-Datendateien finden Sie unter „Verwenden von RIBCL“ (Seite 78). Sie können XML-Skripts von der HP Website unter http://www.hp.com/go/ilo herunterladen. Klicken Sie unter **iLO Support and Downloads** (iLO Support und Downloads) auf **iLO Sample Scripts** (iLO-Beispielskripts).

6 Perl-Skripts

Verwenden von Perl mit der Oberfläche zum Erstellen von XML-Skripts

Mithilfe der bereitgestellten Oberfläche zur Skripterstellung können Administratoren praktisch alle Aspekte des Geräts automatisch verwalten. Administratoren verwenden vorwiegend Tools wie `cpqlocfg.exe`, um die Bereitstellung zu vereinfachen. Administratoren, die mit einem Nicht-Windows-Client arbeiten, können Perl-Skripts verwenden, um XML-Skripts an die Lights-Out Geräte zu senden. Administratoren können außerdem mit Perl komplexere Aufgaben ausführen, als dies mit `cpqlocfg.exe` möglich ist.

In diesem Abschnitt wird erläutert, wie Perl-Skripts in Verbindung mit der Lights-Out XML-Skriptsprache eingesetzt werden. Für Perl-Skripts sind ein gültige Benutzer-ID und ein gültiges Kennwort mit den entsprechenden Berechtigungen erforderlich. XML-Beispielskripts für Lights-Out-Geräte und ein Perl-Beispielskript sind auf der HP Website unter http://www.hp.com/servers/lights-out im Bereich „Best Practices“ (Optimale Vorgehensweise) verfügbar.

XML-Erweiterungen

Ältere Versionen der iLO 2 Firmware geben keine korrekt formatierte XML-Syntax zurück. Wenn die iLO 2 Firmware feststellt, dass das Client-Dienstprogramm die Rückgabe korrekt formatierter XML-Syntax nicht unterstützt, wird die folgende Meldung angezeigt:

```
<INFORM>Scripting utility should be updated to the latest version.</INFORM>
```

Diese Meldung weist darauf hin, dass für das Skript-Dienstprogramm CPQLOCFG ein Update auf eine aktuellere Version notwendig ist. Die aktuellste Version von CPQLOCFG ist 2.28.

Wenn Sie ein anderes Dienstprogramm als `cpqlocfg.exe` verwenden (wie beispielsweise Perl), kann folgendermaßen sichergestellt werden, dass die iLO 2 Firmware korrekt formatierte XML-Syntax zurückgibt. In das an iLO 2 gesendete Skript muss `<LOCFG version="2.21">` eingefügt werden, wobei dieses Tag entweder im Perl- oder im XML-Skript enthalten sein kann. Allerdings ist die Position dieses Tags wichtig. In Perl-Skripts muss das Tag nach `<?xml version="1.0"?>`, jedoch vor dem XML-Skript gesendet werden. Wenn das Tag im XML-Skript platziert wird, muss es vor `<RIBCL version="2.0">.` eingefügt werden. Wenn Sie das von HP bereitgestellte Perl-Skript verwenden, können Sie die fettgedruckte Linie im folgenden Beispiel hinzufügen, damit korrekt formatierte XML-Syntax zurückgegeben wird.

- Änderung von Perl-Skripts:

```
…
# Open the SSL connection and the input file
my $client = new IO::Socket::SSL->new(PeerAddr => $host);
open(F, "<$file") || die "Can't open $file\n";
# Send the XML header and begin processing the file
print $client '<?xml version="1.0"?>' . "\r\n";
# Send tag to iLO firmware to insure properly formatted XML is returned.
print $client '<LOCFG version="2.21">' . "\r\n";
…
```

- Änderung von XML-Skripts:

```
<!-- The bold line could be added for the return of properly formatted XML. -->
<LOCFG version="2.21"/>
<RIBCL version="2.0">
<LOGIN USER_LOGIN="Adminname" PASSWORD = "password">
<!--
Hier XML-Skript einfügen
```

```
-->
</LOGIN>
</RIBCL>
</LOCFG>
```

Öffnen einer SSL-Verbindung

Perl-Skripts müssen eine SSL-Verbindung zum HTTPS-Port des Geräts öffnen, standardmäßig ist dies Port 443. Beispiel:

```
use Socket;
use Net::SSLeay qw(die_now die_if_ssl_error);
Net::SSLeay::load_error_strings();
Net::SSLeay::SSLeay_add_ssl_algorithms();
Net::SSLeay::randomize();
#
# opens an ssl connection to port 443 of the passed host
#
sub openSSLconnection($)
{
my $host = shift;
my ($ctx, $ssl, $sin, $ip, $nip);
if (not $ip = inet_aton($host))
{
print "$host is a DNS Name, performing lookup\n" if $debug;
$ip = gethostbyname($host) or die "ERROR: Host $hostname not found.\n";
}
$nip = inet_ntoa($ip);
print STDERR "Connecting to $nip:443\n";
$sin = sockaddr_in(443, $ip);
socket  (S, &AF_INET, &SOCK_STREAM, 0) or die "ERROR: socket: $!";
connect (S, $sin) or die "connect: $!";
$ctx = Net::SSLeay::CTX_new() or die_now("ERROR: Failed to create SSL_CTX $! ");
Net::SSLeay::CTX_set_options($ctx, &Net::SSLeay::OP_ALL);
die_if_ssl_error("ERROR: ssl ctx set options");
$ssl = Net::SSLeay::new($ctx) or die_now("ERROR: Failed to create SSL $!");
Net::SSLeay::set_fd($ssl, fileno(S));
Net::SSLeay::connect($ssl) and die_if_ssl_error("ERROR: ssl connect");
print STDERR 'SSL Connected ';
print 'Using Cipher: ' . Net::SSLeay::get_cipher($ssl) if $debug;
print STDERR "\n\n";
return $ssl;
}
```

Senden von XML-Kopfzeile und Skripttext

Nachdem die Verbindung hergestellt wurde, muss die erste gesendete Skriptzeile aus einer XML-Dokumentkopfzeile bestehen, die dem HTTPS-Webserver des Geräts mitteilt, dass es sich bei dem nachfolgenden Inhalt um ein XML-Skript handelt. Die Kopfzeile muss mit der Beispiel-Kopfzeile absolut identisch sein. Nachdem die Kopfzeile vollständig gesendet wurde, kann der Rest des Skripts gesendet werden. In diesem Beispiel wird das gesamte Skript auf einmal gesendet. Beispiel:

```
# usage: sendscript(host, script)
# sends the xmlscript script to host, returns reply
sub sendscript($$)
{
my $host = shift;
my $script = shift;
my ($ssl, $reply, $lastreply, $res, $n);
$ssl = openSSLconnection($host);
# write header
$n = Net::SSLeay::ssl_write_all($ssl, '<?xml version="1.0"?>'."\r\n");
 print "Wrote $n\n" if $debug;
# write script
$n = Net::SSLeay::ssl_write_all($ssl, $script);
print "Wrote $n\n$script\n" if $debug;
$reply = "";
$lastreply = "";
READLOOP:
while(1)
{
$n++;
$reply .= $lastreply;
$lastreply = Net::SSLeay::read($ssl);
die_if_ssl_error("ERROR: ssl read");
if($lastreply eq "")
{
sleep(2); # 2 wait 2 sec for more text.
$lastreply = Net::SSLeay::read($ssl);
last READLOOP if($lastreply eq "");
}
sleep(2); # 2 wait 2 sec for more text.
$lastreply = Net::SSLeay::read($ssl);
last READLOOP if($lastreply eq "");
}
print "READ: $lastreply\n" if $debug;
if($lastreply =~ m/STATUS="(0x[0-9A-F]+)"[\s]+MESSAGE='(.*)'[\s]+\/>[\s]*(([\s]|.)*?)<\/RIBCL>/)
{
if($1 eq "0x0000")
{
print STDERR "$3\n" if $3;
}
else
{
print STDERR "ERROR: STATUS: $1, MESSAGE: $2\n";
}
}
}
$reply .= $lastreply;
closeSSLconnection($ssl);
```

```
return $reply;
}
```

PERL-Skripts können auch einen Teil des XML-Skripts senden, auf die Antwort warten und später weiteren XML-Code senden. Bei Verwendung dieser Technik kann eine Antwort, die für einen früheren Befehl erzeugt wurde, als Eingabe für einen späteren Fehler verwendet werden. Das PERL-Skript muss jedoch innerhalb einige weniger Sekunden Daten senden, da andernfalls eine Zeitüberschreitung eintritt und das Gerät getrennt wird.

Bei Verwendung der Oberfläche zur Erstellung von XML-Skripts mit PERL-Skripts gelten die folgenden Einschränkungen:

- PERL-Skripts müssen die XML-Kopfzeile senden, bevor der eigentliche Skripttext gesendet wird.
- PERL-Skripts müssen Skriptdaten so schnell bereitstellen, dass keine Zeitüberschreitung des Geräts eintritt.
- Pro Verbindung ist nur ein XML-Dokument zulässig, das heißt ein RIBCL-Tag-Paar.
- Das Gerät akzeptiert keine zusätzlichen XML-Tags, nachdem ein Syntaxfehler eingetreten ist. Um weiteren XML-Code zu senden, muss eine neue Verbindung hergestellt werden.

7 Skripts für virtuelle Medien

Webserveranforderungen an Skripts

Skripts für virtuelle Medien verwenden ein Medien-Image, das auf einem Webserver gespeichert ist und von dort abgerufen wird. Auf den Webserver kann vom Managementnetzwerk aus zugegriffen werden. Der Webserver muss mit HTTP 1.1 kompatibel sein und den Range-Header unterstützen. Außerdem sollte der Webserver für den Schreibzugriff DAV unterstützen. Für DAV Transaktionen muss er den Content-Range-Header unterstützen. Wenn der Webserver die Anforderungen für DAV nicht unterstützt, kann als Alternative ein CGI-Helper-Programm verwendet werden. Der Webserver kann optional für die grundlegende HTTP-Authentifizierung, SSL-Unterstützung oder beides konfiguriert werden.

Webserver	Lese-Unterstützung	Schreib-Unterstützung	Autorisierung	SSL-Unterstützung
Microsoft IIS 5.0	Ja	Ja*	Nicht getestet	Nicht getestet
Apache	Ja	Ja	Ja	Ja
Apache/Win32	Ja	Ja	Ja	Ja

*IIS bietet keine Unterstützung von Content-Range für DAV Transaktionen. Für die Schreib-Unterstützung wird ein CGI-Helper-Programm benötigt.

Verwenden von Skripts für virtuelle Medien

Mit Skripts für virtuelle Medien können virtuelle Mediengeräte ohne Browser gesteuert werden. Skripts für virtuelle Medien unterstützen Befehle zum Einlegen, Auswerfen und Anzeigen des Status von Disketten-, USB-Schlüssel- und CD-/DVD-ROM-Laufwerk-Images.

Mit Skripts für virtuelle Medien können Sie iLO 2 auch auf andere Art und Weise als über einen Browser für die Verwendung von virtuellen Medien konfigurieren. iLO 2 kann remote mit `CPQLOCFG`-XML-Befehlen, lokal mit `HPONCFG`-XML-Befehlen oder auch lokal mit dem `HPLOVM`-Dienstprogramm konfiguriert werden. Dieses Dienstprogramm ersetzt das Utility `VFLOP`, das Bestandteil des SmartStart Scripting Toolkits ist.

HINWEIS: Skripts für virtuelle Medien setzen das Applet Virtual Media nicht über den Browser ein. Umgekehrt gilt, dass der Browser keine Skript-Funktionen unterstützt. So kann beispielsweise die Einrichtung eines Diskettenlaufwerks, das zuvor mit dem Browser eingerichtet wurde, anschließend nicht über die Skriptoberfläche wieder aufgehoben werden.

Mit den XML-Befehlen können Sie virtuelle Medien genauso wie mit dem Applet Virtual Media konfigurieren. Das eigentliche Image befindet sich jedoch auf einem Webserver innerhalb desselben Netzwerks wie iLO 2. Nachdem der Image-Speicherort konfiguriert wurde, ruft iLO 2 die virtuellen Mediendaten direkt von dem betreffenden Webserver ab.

HINWEIS: Es müssen USB-Schlüssellaufwerke mit der Disketten-Schlüsselwortsyntax verwendet werden.

`HPLOVM.EXE` ist ein neues Skript-Utility, mit dem Sie ein Skript zum Einlegen und Auswerfen virtueller Medien sowie zum Festlegen von Startoptionen für virtuelle Medien schreiben können. `HPLOVM` ist zur Verwendung anstelle des Utility `VFLOP.exe` bestimmt, das Bestandteil des SmartStart Scripting Toolkit ist.

Befehlszeilensyntax:

```
HPLOVM [-device <floppy | cdrom>] [-insert <url>] [-eject] [-wp <y | n>]
```

```
[-boot <once | always | never>] [-mgmt <ilo | riloe>] [-ver] [-?]
```

Eingabe auf der Befehlszeile	Ergebnis
`[-device <floppy | cdrom>]`	Definiert, welches virtuelle Mediengerät aktiv ist.
`[-insert <url>]`	Definiert den Ort der Image-Datei für virtuelle Medien, zu der eine Verbindung hergestellt wird.
`[-eject]`	Wirft das derzeit über das virtuelle Medienlaufwerk verbundene Medium aus. Das virtuelle Medienlaufwerk ist noch immer verbunden, aber es befindet sich kein Medium mehr im Laufwerk.
`[-wp <y | n>]`	Definiert den Status „Schreibgeschützt“ des virtuellen Diskettenlaufwerks/USB-Schlüssellaufwerks. Dieses Argument hat keine Auswirkungen auf das virtuelle CD-ROM-Laufwerk.
`[-boot <once | always | never>]`	Definiert, wie das Laufwerk für virtuelle Medien den Zielserver bootet.
`[-mgmt <ilo | riloe>]`	Definiert, welcher Managementprozessor mit dem LOVM Utility verwendet wird. Bei Angabe von RILOE wird das VFLOP.EXE Utility verwendet. Die Standardeinstellung des Arguments ist iLO 2.
`[-ver]`	Zeigt die Version des HPLOVM Utilitys an.
`[-?]`	Zeigt Hilfeinformationen an.

Verwenden von virtuellen Medien auf Linux-Servern über eine SSH-Verbindung

1. Melden Sie sich bei iLO 2 über SSH an (SSH-Verbindung von einem anderen Linux-System aus und unter Verwendung von PuTTY von Windows).
2. Geben Sie `vm` ein, um eine Liste der für virtuelle Medien verfügbaren Befehle anzuzeigen.
3. Geben Sie `vm floppy insert http://<address>/<image-name>` ein.

   Das Image ist zum Starten verfügbar, wird jedoch vom Betriebssystem nicht gesehen. Startoptionen können mit `vm floppy set <`*Option*`>` konfiguriert werden. Die Optionen sind `boot_once`, `boot_always` und `no_boot`). Startoptionen von einem USB-Schlüssellaufwerk sind nur auf Servern mit Unterstützung für das ProLiant USB-Schlüssellaufwerk gültig.
4. Geben Sie `vm floppy set connect` ein, um das Disketten- oder USB-Laufwerk für das Betriebssystem verfügbar zu machen.
5. Geben Sie `vm floppy get` ein, um den aktuellen Status anzuzeigen. Beispiel:

   ```
   VM Applet = Disconnected
   Boot Option = BOOT_ONCE
   Write Protect = Yes
   Image Inserted = Connected
   ```

   Der Status des Applets Virtual Media lautet grundsätzlich „getrennt“, sofern über die grafische iLO 2 Oberfläche keine Verbindung zu einem virtuellen Disketten-/USB-Schlüssellaufwerk oder CD-ROM-Laufwerk besteht.

   Das virtuelle Disketten-/USB-Laufwerk kann mit den Befehlen `vm floppy set disconnect` oder `vm floppy eject` getrennt werden. Verwenden Sie zum Verbinden oder Trennen eines virtuellen CD-ROM-Laufwerks `cdrom` anstelle von `floppy`.

Bei dem Link zum Image des virtuellen Disketten-/USB-Schlüssellaufwerks oder CD-ROM-Laufwerks muss es sich um einen URL handeln. Sie können keinen Laufwerksbuchstaben angeben. Das CD-ROM-Image muss im Format `.iso` vorliegen. Das Diskettenlaufwerks-Image kann von einem physischen Diskettenlaufwerk unter Verwendung von `rawrite` oder mit dem Tool zur

Image-Erstellung erstellt werden, das im Virtual Media Applet in der grafischen iLO 2 Oberfläche enthalten ist.

Einrichten von virtuellen Medien auf dem Linux-Server:

1. Überprüfen Sie mit `lsmod`, ob die folgenden Module geladen sind:
   - `usbcore`
   - `usb-storage`
   - `usb-ohci`
   - `sd_mod`

   Wenn eines dieser Module fehlt, laden Sie es mithilfe von `modprobe <Modul>`.
2. Richten Sie das Laufwerk mit einem der folgenden Befehle ein:
   - `mount /dev/sda /mnt/floppy -t vfat`: Stellt ein virtuelles Diskettenlaufwerk bereit.
   - `mount /dev/sda1 /mnt/keydrive`: Stellt ein virtuelles USB-Laufwerk bereit.
   - `mount /dev/cdrom1 /mnt/cdrom`: Stellt ein virtuelles CD-ROM-Laufwerk auf einem Red Hat-System bereit. Verwenden Sie `/dev/cdrom`, wenn kein CD-ROM-Laufwerk lokal an den Server angeschlossen ist.
   - `mount /dev/scd0 /mnt/cdrom`: Stellt ein virtuelles CD-ROM-Laufwerk auf einem SUSE-System bereit.

Image-Dateien für virtuelle Medien

Gültige Disketten-Images mit dem Applet iLO 2 Virtual Media, UNIX-Utility dd oder DOS-Utility rawrite erzeugte können Raw-Disk-Images sein bzw. mit `CPQIMAGE` erstellte Images sein. CD-ROM-Images müssen Dateisystem-Images nach ISO-9660 sein. Andere Typen von CD-ROM-Images werden nicht unterstützt.

Mit dem Applet Virtual Media erstellte Images sind im Falle von Disketten Raw-Disk-Images und im Falle von CD-ROMs ISO-9660-Images. Viele Utilities zum Brennen von CD-ROMs können ISO-9660-Images erstellen. Lesen Sie die Begleitdokumentation Ihres Utilitys.

CGI-Helper-Anwendung

Das folgende Perl-Skript ist ein Beispiel einer CGI-Helper-Anwendung, mit der Disketten auf Webservern geschrieben werden können, die keine partiellen Schreibvorgänge durchführen können. Wenn die Helper-Anwendung verwendet wird, sendet die iLO 2 Firmware eine Anforderung mit drei Parametern an diese Anwendung:

- Das Parameter File enthält den Namen der Datei, die im Original-URL bereitgestellt wird.
- Der Parameter Range enthält einen eingeschlossenen Bereich (Hexadezimal), der angibt, wo die Daten geschrieben werden sollen.
- Der Parameter Data enthält eine Hexadezimalzeichenfolge, die die Daten darstellt, die geschrieben werden sollen.

Das Helper-Skript muss den Parameter File in einen relativen Pfad zum Arbeitsverzeichnis umwandeln. Eventuell setzt die Datei ein Präfix „../“ voraus, oder ein Alias-URL-Pfad muss in den richtigen Pfad auf dem Dateisystem umgewandelt werden. Das Helper-Skript setzt Schreibzugriff auf die Zieldatei voraus. Disketten-Image-Dateien benötigen die geeigneten Berechtigungen.

Beispiel:

```
#!/usr/bin/perl
use CGI;
use Fcntl;
```

```
#
# The prefix is used to get from the current working
# directory to the location of the image file#
my ($prefix) = "..";
my ($start, $end, $len, $decode);
# Get CGI data
my $q = new CGI();
# Get file to be written
my $file = $q->param('file');
# Byte range
$range = $q->param('range');
# And the data
my $data = $q->param('data');
#
# Change the filename appropriately
#
$file = $prefix . "/" . $file;
#
# Decode the range
#
if ($range =~ m/([0-9A-Fa-f]+)-([0-9A-Fa-f]+)/) {
 $start = hex($1);
 $end = hex($2);
 $len = $end - $start + 1;
}
#
# Decode the data (it's a big hex string)
#
$decode = pack("H*", $data);
#
# Write it to the target file
#
sysopen(F, $file, O_RDWR);
binmode(F);
sysseek(F, $start, SEEK_SET);
syswrite(F, $decode, $len);
close(F);
```

Einrichten von IIS für skriptgestützte virtuelle Medien

Vor der Einrichtung für skriptgestützte Medien muss sichergestellt werden, dass die IIS-Dienste (Internet Information Services) funktionsfähig sind. Erstellen Sie mit dem Internet Information Services Manager (Internetdienste-Manager) eine einfache Website und überprüfen Sie ihre Funktionsfähigkeit, indem Sie die Seite aufrufen.

1. Konfigurieren Sie IIS zur Bereitstellung von Disketten- oder ISO-9660-CD-ROM-Images für schreibgeschützten Zugriff.
   a. Fügen Sie der erstellten Website ein Verzeichnis hinzu, und stellen Sie die Images in das Verzeichnis.

b. Vergewissern Sie sich, dass die IIS-Dienste den MIME-Typ der betreffenden Dateien unterstützen. Wenn die Disketten-Images z. B. die Erweiterung .img haben, muss ein MIME-Typ für diese Erweiterung hinzugefügt werden. Öffnen Sie mit dem IIS Manager das Dialogfeld „Eigenschaften" der Website. Klicken Sie im Register „HTTP Headers" (HTTP-Kopfzeilen) auf **MIME Types** (MIME-Typen), um weitere MIME-Typen hinzuzufügen.

HP empfiehlt die Aufnahme der folgenden MIME-Typen:

`.imgapplication/octet-stream`

`.isoapplication/octet-stream`

2. Konfigurieren Sie IIS für den Lese-/Schreib-Zugriff.
   a. Installieren Sie Perl (sofern erforderlich).
   b. Erstellen Sie ein Website-Verzeichnis für das Helper-Skript der virtuellen Medien, und kopieren Sie das Skript in dieses Verzeichnis.
   c. Klicken Sie auf der Eigenschaftenseite des Verzeichnisses unter „Application Settings" (Anwendungseinstellungen) auf **Create** (Erstellen), um ein Anwendungsverzeichnis anzulegen.

   Das Symbol für das Verzeichnis im IIS Manager muss anstelle eines Ordners nun ein Zahnrad anzeigen.
   d. Setzen Sie „Execute Permissions" (Ausführberechtigungen) auf **Scripts Only** (Nur Skripts).
   e. Stellen Sie sicher, dass Perl als Skript-Interpreter festgelegt wurde. Klicken Sie hierfür auf der Eigenschaftenseite auf **Configuration** (Konfiguration), um die Anwendungszuordnungen anzuzeigen. Perl sollte als

   `pl c:\perl\bin\perl.exe "%s" %s GET,HEAD,POST`

   konfiguriert sein.
   f. Vergewissern Sie sich, dass Web Service Extensions die Ausführung von Perl-Skripts zulässt. Falls dies nicht der Fall ist, klicken Sie auf **Web Service Extensions** und setzen „Perl CGI Extension" auf **Allowed** (Zulässig).
   g. Stellen Sie sicher, dass die Präfixvariable im Helper-Skript korrekt gewählt wurde.

Weitere Informationen

Das Basisformat für den XML-Einfügebefehl lautet:

```
<INSERT_VIRTUAL_MEDIA DEVICE="device" IMAGE_URL="http://Servername/Pfad/zur/Datei"/>
```

- Dabei kann der Eintrag unter device entweder FLOPPY oder CDROM lauten.
- IMAGE_URL kann entweder eine http- oder einen https-URL für ein Disketten- oder ein CD_ROM-Image sein.

Das grundlegende Format des URL lautet:

`Protokoll://Benutzer:Kennwort@Servername:Port/Pfad,Helper-Skript`

, wobei gilt:

- `protocol`: Erforderlich. Kann entweder http oder https sein.
- `user:password`: Optional. Falls ein Eintrag vorhanden ist, wird eine http-Basisautorisierung verwendet.
- `servername`: Erforderlich. Entweder der Hostname oder die IP-Adresse des Webservers.
- `port`: Optional. Gibt einen Webserver auf einem nichtstandardmäßigen Port an.
- `path`: Erforderlich. Bezieht sich auf die Image-Datei, auf die zugegriffen wird.
- `helper-script`: Optional. Bezieht sich auf den Speicherort des Helper-Skripts auf IIS Webservern.

Helper-Skript:

Das folgende Perl-Skript ist ein Beispiel für ein CGI-Helper-Skript:

```
#!/usr/bin/perl
use CGI;
use Fcntl;
#
# The prefix is used to get from the current working directory
# to the location of the image file you are writing
#
my ($prefix) = "c:/inetpub/wwwroot";
my ($start, $end, $len, $decode);
my $q = new CGI();      # Get CGI data
my $file =  $q->param('file'); # File to be written
my $range = $q->param('range'); # Byte range to be written
my $data =  $q->param('data'); # Data to be written
#
# Merges the filename correctly
#
$file = $prefix . "/" . $file;
#
# Decode the range
#
if ($range =~ m/([0-9A-Fa-f]+)-([0-9A-Fa-f]+)/) {
$start = hex($1);
$end = hex($2);
$len = $end - $start + 1;
}
#
# Decode the data (a large hex string)
#
$decode = pack("H*", $data);
#
# Write it to the target file
#
sysopen(F, $file, O_RDWR);
binmode(F);
sysseek(F, $start, SEEK_SET);
syswrite(F, $decode, $len);
close(F);
print "Content-Length: 0\r\n";
print "\r\n";
```

8 HPONCFG Online Configuration Utility

HPONCFG

HPONCFG ist ein Online-Konfigurationstool zum Einrichten und Konfigurieren von iLO über Windows- und Linux-Betriebssysteme, ohne einen Neustart des Server-Betriebssystems erforderlich zu machen. HPONCFG wird im Befehlszeilenmodus ausgeführt und muss mit Administrator- oder Stammzugriff in einer Betriebssystem-Befehlszeile ausgeführt werden. HPONCFG stellt eine eingeschränkte grafische Oberfläche für Server zur Verfügung, die von Windows-Betriebssystemen Gebrauch machen.

Von HPONCFG unterstützte Betriebssysteme

- Windows
  - Windows Server 2008 R1 und R2
  - Windows Server 2011
  - Windows Vista (für Blade Server)
  - Windows 7 (für Blase Server)
- Red Hat Linux
  - Red Hat Linux Enterprise Linux 3
  - Red Hat Linux Enterprise Linux 4
  - Red Hat Linux Enterprise Linux 5
  - Red Hat Linux Enterprise Linux 6
- SUSE Linux
  - SUSE Linux Enterprise Server 9
  - SUSE Linux Enterprise Server 10
  - SUSE Linux Enterprise Server 11
- VMware
  - VMware 5

HPONCFG-Anforderungen

- Windows-basierte Server: Auf dem Server muss der iLO Management Interface Driver geladen sein. Dieser Treiber wird in der Regel während des SmartStart Installationsvorgangs des Betriebssystems installiert. Während der Ausführung gibt HPONCFG eine Warnmeldung aus, wenn der Treiber nicht gefunden wird. Wenn der Treiber nicht installiert ist, muss er heruntergeladen und auf dem Server installiert werden. Laden Sie den Treiber von der HP Website herunter:

  http://h20000.www2.hp.com/bizsupport/TechSupport/DriverDownload.jsp?prodNameId=1135772&lang=en&cc=us&taskId=135&prodTypeId=18964&prodSeriesId=1146658.
- Windows-basierte Server: Auf dem Server muss der iLO Management Interface Driver geladen sein.

- Linux-basierte Server: Auf dem Server muss der iLO Management Interface Driver (`hpilo`) geladen und das Healt Driver Package (`hp-health rpm`) installiert sein. Dieser Treiber wird in der Regel im Rahmen der Intelligent Provision-Betriebssysteminstallation installiert. Wenn der Treiber nicht installiert ist, muss er heruntergeladen und auf dem Server installiert werden. Laden Sie den Treiber von der HP Website herunter:

  http://h20000.www2.hp.com/bizsupport/TechSupport/DriverDownload.jsp?prodNameId=4154847&lang=en&cc=us&taskId=135&prodSeriesId=4154735&prodTypeId=18964

Installieren von HPONCFG

Das Utility HPONCFG wird in gesonderten Paketen für Windows- und Linux-Betriebssysteme geliefert. Für Windows-Betriebssysteme wird es als Smart Component geliefert.
Für Linux-Betriebssysteme wird es als RPM-Paketdatei geliefert. HPONCFG Pakete sind im ProLiant Support Pack enthalten.

Installation auf einem Windows-Server

HPONCFG wird automatisch zusammen mit dem ProLiant Support Pack installiert. Wenn Sie HPONCFG manuell installieren möchten, führen Sie die selbstextrahierende ausführbare Datei aus.

HPONCFG erstellt ein Verzeichnis unter:

`%Program files%\HP\hponcfg`.

Installation auf einem Linux-Server

HPONCFG wird automatisch zusammen mit dem ProLiant Support Pack installiert. Laden Sie das HPONCFG RPM-Paket für Linux-Distributionen von der HP Website herunter. Installieren Sie das entsprechende Paket mithilfe des RPM-Installationsprogramms.

Beispiel: Installieren Sie das HPONCFG RPM-Paket unter Red Hat Enterprise Linux 5 mit folgendem Befehl:

```
rpm -ivh hponcfg-4.0.0-2.linux.rpm
```

Wenn auf dem System eine ältere Version des HPONCFG RPM-Pakets installiert ist, führen Sie den folgenden Befehl aus, um die ältere Version zu entfernen, bevor die neue Version von HPONCFG installiert wird:

```
rpm –e hponcfg
```

Das rpm-Paket `hp-ilo` und das Paket `hp-health rpm` müssen vor dem Paket `hponcfg rpm` installiert werden.

Nach der Installation befindet sich die HPONCFG-Programmdatei im Verzeichnis `/sbin`. Vergewissern Sie sich, dass der richtige Management Interface Driver installiert ist. Einzelheiten zum Beziehen dieses Treibers finden Sie unter „HPONCFG-Anforderungen“ (Seite 68).

HPONCFG Utility

Das Konfigurationsdienstprogramm HPONCFG liest eine XML-Eingabedatei, die gemäß den Regeln der RIBCL-Sprache formatiert ist, und erstellt eine Protokolldatei, die die angeforderte Ausgabe enthält. Das HPONCFG-Lieferpaket enthält außerdem einige HPONCFG-Beispielskripts. Ein Paket mit verschiedenen umfassenden Beispielskripts ist als Download auf der folgenden HP Website verfügbar: http://www.hp.com/go/ilo. Klicken Sie unter **iLO Support and Downloads** (iLO Support und Downloads) auf **iLO Sample Scripts** (iLO-Beispielskripts).

Typischerweise wählen Sie ein Skript, das der gewünschten Funktionalität ähnlich ist, und ändern es Ihren Anforderungen gemäß ab. Obwohl keine Authentifizierung bei iLO erforderlich ist, setzt die XML-Syntax voraus, dass die Tags USER_LOGIN und PASSWORD im LOGIN-Tag vorhanden

sind und Daten enthalten. In diesem Feldern werden beliebige Daten akzeptiert. Um HPONCFG erfolgreich auszuführen, muss das Dienstprogramm von einem Administrator auf Windows-Servern und von einem root auf Linux-Servern ausgeführt werden. HPONCFG gibt eine Fehlermeldung zurück, wenn Ihre Berechtigung nicht ausreicht.

HPONCFG-Befehlszeilenparameter

HPONCFG akzeptiert die folgenden Befehlszeilenparameter:

`/help` oder `?`:	Zeigt die Hilfeseite an.
`/reset`	Setzt iLO auf die Werkseinstellungen zurück.
`/f` *`Dateiname`*	Dient zum Festlegen und Empfangen der iLO Konfiguration aus den Informationen in der XML-Eingabedatei namens *`Dateiname`*.
`/i` *`Dateiname`*	Dient zum Festlegen und Empfangen der iLO Konfiguration aus der über den Standardeingabestrom empfangenen XML-Eingabe.
`/w` *`Dateiname`*	Schreibt die vom Gerät bezogene iLO Konfiguration in die XML-Ausgabedatei namens *`Dateiname`*.
`/l` *`Dateiname`*	Protokolliert Antworten in der Textprotokolldatei namens *`Dateiname`*.
`/s` *`Namen-Wertepaare`* oder `/substitute` *`Namen-Wertepaare`*	Ersetzt die in der Eingabekonfigurationsdatei vorhandenen Variablen durch die in *`Namen-Wertepaare`* angegebenen Werte.
`/get_hostinfo`	Empfängt die Hostinformationen. Gibt Name und Seriennummer des Servers zurück.
`/m`	Gibt die Firmwareversion an, die mindestens auf dem Managementgerät installiert sein muss, damit das RIBCL-Skript ausgeführt werden kann. Ist diese Firmwareversion nicht vorhanden, wird von HPONCFG lediglich eine Fehlermeldung ausgegeben; es erfolgt keine weitere Aktion.
`/mouse`	Konfiguriert den Server für eine optimierte Verarbeitung von Maussignalen, um die Leistung der grafischen Remote-Konsole zu verbessern. Standardmäßig ist die Remote Console auf eine optimale Verwendung des Einzelzeiger-Modus durch den aktuellen Benutzer ausgelegt. Wenn die Befehlszeilenoption `dualcursor` zusammen mit der Option „Maus“ angegeben wird, wird die Handhabung der Maus als für den Dualcursor-Modus der Remote-Konsole geeignet optimiert. Mit der Befehlszeilenoption `allusers` wird die Verarbeitung der Maussignale für alle Benutzer im System optimiert. Diese Option ist nur unter Windows verfügbar.
`/display`	Konfiguriert die Windows-Anzeigeparameter zur Optimierung der Leistung der grafischen Remote Console-Anzeige.

Diesen Optionen muss unter Windows und Linux wie gezeigt ein Schrägstrich (`/`) vorangestellt werden.

Beispiel:

```
hponcfg /f add_user.xml /l log.txt > output.txt
```

Verwenden von HPONCFG auf Windows-Servern

Das Konfigurationsdienstprogramm HPONCFG wird über die Befehlszeile ausgeführt. Bei Verwendung von Windows ist `cmd.exe` durch Auswahl von **Start→Ausführen→cmd** verfügbar. Bei Eingabe von HPONCFG ohne Parameter wird eine Seite mit Verwendungshinweisen angezeigt. HPONCFG akzeptiert korrekt formatierte XML-Skripts. Das HPONCFG-Paket enthält außerdem HPONCFG-Beispielskripts.

Weitere Informationen über das Formatieren von XML-Skripts finden Sie unter Kapitel 9, „Verwenden von RIBCL“.

Die Befehlszeilensyntax lautet wie folgt:

```
hponcfg [ /help | /? | /m firmwarelevel | /reset [/m firmwarelevel]
| /f filename [/l filename] [/s namevaluepairs]
    [/xmlverbose or /v][/m firmwarelevel]
| /i [/l filename] [/s namevaluepairs]
[/xmlverbose or /v] [/m firmwarelevel]
| /w filename [/m firmwarelevel]
| /get_hostinfo [/m firmwarelevel]
| /mouse [/dualcursor][/allusers]  ]
```

Weitere Informationen zu diesen Parametern finden Sie unter „HPONCFG-Befehlszeilenparameter“ (Seite 70).

Verwenden von HPONCFG auf Linux-Servern

Rufen Sie das Konfigurationsdienstprogramm HPONCFG über die Befehlszeile auf. Bei Eingabe von HPONCFG in der Befehlszeile ohne irgendwelche Parameter wird eine Seite mit Verwendungshinweisen angezeigt.

Die Befehlszeilensyntax lautet wie folgt:

```
hponcfg  -?
hponcfg  -h
hponcfg  -m minFw
hponcfg  -r  [-m minFw ]
hponcfg  -w filename  [-m minFw]
hponcfg  -g  [-m minFw]
hponcfg  -f filename [-l filename] [-s namevaluepairs] [-v]  [-m minFw]
hponcfg -i [-l filename] [-s namevaluepairs] [-v] [-m minFw]
```

Weitere Informationen zu diesen Parametern finden Sie unter „HPONCFG-Befehlszeilenparameter“ (Seite 70).

Anfordern einer einfachen Konfiguration

Mit HPONCFG können Sie eine einfache Konfiguration von iLO 2,iLO 3 und iLO 4 beziehen. Dazu führen Sie das Utility über die Befehlszeile aus, ohne eine Eingabedatei anzugeben. Sie müssen auf der Befehlszeile den Namen der Ausgabedatei angeben.

Beispiel:

```
hponcfg /w config.xml
```

In diesem Beispiel zeigt das Dienstprogramm an, dass die Daten erfolgreich ermittelt und in die Ausgabedatei geschrieben wurden.

Es folgt ein Beispiel für eine typische Ausgabedatei:

```
<!-- HPONCFG VERSION = "1.2" -->
<!-- Generated 07/06/05 09:06:51 -->
<RIBCL VERSION="2.1">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
```

```
<DIR_INFO MODE="write">
<MOD_DIR_CONFIG>
<DIR_AUTHENTICATION_ENABLED VALUE = "N"/>
<DIR_LOCAL_USER_ACCT VALUE = "Y"/>
<DIR_SERVER_ADDRESS VALUE = ""/>
<DIR_SERVER_PORT VALUE = "636"/>
<DIR_OBJECT_DN VALUE = ""/>
<DIR_OBJECT_PASSWORD VALUE = ""/>
<DIR_USER_CONTEXT_1 VALUE = ""/>
<DIR_USER_CONTEXT_2 VALUE = ""/>
<DIR_USER_CONTEXT_3 VALUE = ""/>
</MOD_DIR_CONFIG>
</DIR_INFO>
<RIB_INFO MODE="write">
<MOD_NETWORK_SETTINGS>
<SPEED_AUTOSELECT VALUE = "Y"/>
<NIC_SPEED VALUE = "100"/>
<FULL_DUPLEX VALUE = "Y"/>
<DHCP_ENABLE VALUE = "Y"/>
<DHCP_GATEWAY VALUE = "Y"/>
<DHCP_DNS_SERVER VALUE = "Y"/>
<DHCP_STATIC_ROUTE VALUE = "Y"/>
<DHCP_WINS_SERVER VALUE = "Y"/>
<REG_WINS_SERVER VALUE = "N"/>
<IP_ADDRESS VALUE = "16.100.241.229"/>
<SUBNET_MASK VALUE = "255.255.252.0"/>
<GATEWAY_IP_ADDRESS VALUE = "16.100.240.1"/>
<DNS_NAME VALUE = "ILOD234KJ44D002"/>
<DOMAIN_NAME VALUE = "americas.cpqcorp.net"/>
<PRIM_DNS_SERVER value = "16.81.3.242"/>
<SEC_DNS_SERVER value = "0.0.0.0"/>
<TER_DNS_SERVER value = "0.0.0.0"/>
<PRIM_WINS_SERVER value = "16.81.3.247"/>
<SEC_WINS_SERVER value = "0.0.0.0"/>
<STATIC_ROUTE_1 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
<STATIC_ROUTE_2 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
<STATIC_ROUTE_3 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
</MOD_NETWORK_SETTINGS>
<USER_INFO MODE="write">
<ADD_USER
USER_NAME = "Username1"
USER_LOGIN = "User1"
PASSWORD = "%user_password%">
<ADMIN_PRIV value = "N"/>
<REMOTE_CONS_PRIV value = "Y"/>
<RESET_SERVER_PRIV value = "N"/>
<VIRTUAL_MEDIA_PRIV value = "N"/>
<CONFIG_ILO_PRIV value = "N"/>
</ADD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>
```

HINWEIS: Aus Sicherheitsgründen werden die Benutzerkennwörter nicht zurückgegeben.

Anfordern einer spezifischen Konfiguration

Sie können eine bestimmte Konfiguration über die entsprechende XML-Eingabedatei beziehen. Es folgt ein Beispiel für den Inhalt einer typischen XML-Eingabedatei:

```
get_global.xml
:
<!-- Sample file for Get Global command -->
```

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="x" PASSWORD="x">
<RIB_INFO MODE="read">
<GET_GLOBAL_SETTINGS />
</RIB_INFO>
</LOGIN>
</RIBCL>
```

Die XML-Befehle werden aus der Eingabedatei `get_global.xml` gelesen und vom Gerät verarbeitet:

```
hponcfg /f get_global.xml /l log.txt > output.txt
```

Die abgefragten Informationen werden in der Protokolldatei zurückgegeben, die in diesem Beispiel `log.txt` genannt wird.

```
<GET_GLOBAL_SETTINGS>
<SESSION_TIMEOUT VALUE="15"/>
<ILO_FUNCT_ENABLED VALUE="Y"/>
<F8_PROMPT_ENABLED VALUE="Y"/>
<F8_LOGIN_REQUIRED VALUE="N"/>
<TELNET_ENABLE VALUE="N"/>
<PASSTHROUGH_CONFIG VALUE="1"/>
<HTTPS_PORT VALUE="443"/>
<HTTP_PORT VALUE="80"/>
<REMOTE_CONSOLE_PORT VALUE="23"/>
<TERMINAL_SERVICES_PORT VALUE="3389"/>
<VIRTUAL_MEDIA_PORT VALUE="17988"/>
<SSH_PORT VALUE="22"/>
<SSH_STATUS VALUE="Y"/>
<SERIAL_CLI_STATUS VALUE="Enabled-Authentication Required"/>
<SERIAL_CLI_SPEED VALUE="9600"/>
<MIN_PASSWORD VALUE="8"/>
<AUTHENTICATION_FAILURE_LOGGING VALUE="Enabled-every 3rd failure"/>
<REMOTE_KEYBOARD_MODEL VALUE="US"/>
<RBSU_POST_IP VALUE="Y"/>
<HIGH_PERFORMANCE_MOUSE VALUE="Automatic">
<REMOTE_CONSOLE_ACQUIRE VALUE="N"/>
</GET_GLOBAL_SETTINGS>


<GET_GLOBAL_SETTINGS>
<SESSION_TIMEOUT VALUE="15"/>
<ILO_FUNCT_ENABLED VALUE="Y"/>
<F8_PROMPT_ENABLED VALUE="Y"/>
<F8_LOGIN_REQUIRED VALUE="N"/>
<TELNET_ENABLE VALUE="N"/>
<PASSTHROUGH_CONFIG VALUE="1"/>
<HTTPS_PORT VALUE="443"/>
<HTTP_PORT VALUE="80"/>
<REMOTE_CONSOLE_PORT VALUE="17990"/>
<TERMINAL_SERVICES_PORT VALUE="3389"/>
<VIRTUAL_MEDIA_PORT VALUE="17988"/>
<SSH_PORT VALUE="22"/>
<SSH_STATUS VALUE="Y"/>
<SERIAL_CLI_STATUS VALUE="Enabled-Authentication Required"/>
<SERIAL_CLI_SPEED VALUE="9600"/>
<MIN_PASSWORD VALUE="8"/>
<AUTHENTICATION_FAILURE_LOGGING VALUE="Enabled-every 3rd failure"/>
<REMOTE_KEYBOARD_MODEL VALUE="US"/>
<RBSU_POST_IP VALUE="Y"/>
<HIGH_PERFORMANCE_MOUSE VALUE="Automatic">
<REMOTE_CONSOLE_ACQUIRE VALUE="N"/>
```

```
</GET_GLOBAL_SETTINGS>
```

Einstellen einer Konfiguration

Verwenden Sie zum Einstellen einer bestimmten Konfiguration das folgende Befehlsformat:

```
hponcfg /f add_user.xml /l log.txt
```

In diesem Beispiel hat die Eingabedatei folgenden Inhalt:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="x" PASSWORD="x">
<USER_INFO MODE="write">
<ADD_USER
USER_NAME="Landy9"
USER_LOGIN="mandy8"
PASSWORD="floppyshoes">
<ADMIN_PRIV value ="No"/>
<REMOTE_CONS_PRIV value ="Yes"/>
<RESET_SERVER_PRIV value ="No"/>
<VIRTUAL_MEDIA_PRIV value ="No"/>
<CONFIG_ILO_PRIV value="Yes"/>
</ADD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>
```

Der angegebene Benutzer wird zum Gerät hinzugefügt.

Verwenden der Substitution von Variablen

Mit HPONCFG Version 1.2 und höher können Sie Variablen im XML-RIBCL-Skript angeben und ihnen bei der Ausführung von HPONCFG Werte zuweisen. Mit dieser Funktion muss die XML-Skriptdatei nicht immer wieder mit anderen Werten umgeschrieben werden. Alles, was in der XML-Datei zwischen zwei Prozentzeichen (%) steht, wird als Variable angesehen.

In diesem Beispiel sind `%username%`, `%loginname%` und `%password%` Variablen:

```
<!-- Add user with minimal privileges to test default setting of
     assigned privileges to 'N' -->
<RIBCL version="1.2">
<LOGIN USER_LOGIN="x" PASSWORD="x">
<USER_INFO MODE="write">
<ADD_USER USER_NAME="%username%" USER_LOGIN="%loginname%"  PASSWORD="%password%">
<RESET_SERVER_PRIV value="Y" />
<ADMIN_PRIV value="Y" />
</ADD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>
```

Sie können für diese Variablen mit der Ersetzungsoption Werte für die Ausführung von HPONCFG angeben. Das Argument muss eine Zeichenfolge aus dem Variablennamen und den Wertepaaren sein, getrennt durch Kommas (,). Der Variablenname und sein Wert müssen durch ein Gleichheitszeichen (=) voneinander getrennt sein.

```
hponcfg /f add_user.xml /s username=test
user,login=testlogin,password=testpasswd
```

In diesem Beispiel ist `%host_power%` eine Variable:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="write">
```

```
<!-- Modify the HOST_POWER attribute to toggle power on the host server -->
<!-- HOST_POWER="No" (Turns host server power off) -->
<!-- A graceful shutdown will be attempted for ACPI-aware -->
<!-- operating systems configured to support graceful shutdown. -->
<!-- HOST_POWER="Yes" (Turns host server power on) -->
<SET_HOST_POWER HOST_POWER="%host_power%"/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

- Geben Sie zum Einschalten des Systems Folgendes ein:

  ```
  hponcfg /f Set_Host_Power.xml /s host_power=YES
  ```

- Geben Sie zum Ausschalten des Systems Folgendes ein:

  ```
  hponcfg /f Set_Host_Power.xml /s host_power=NO
  ```

Erfassen und Wiederherstellen einer Konfiguration

Mit HPONCFG können Sie die Daten einer einfachen Konfiguration in einem lesbaren XML-Dateiformat erfassen. Anhand dieser Datei können Sie die iLO Konfiguration einstellen oder wiederherstellen. Diese Funktion ist ab HPONCFG Version 1.2 verfügbar. HPONCFG schreibt die Konfigurationsdaten im HP RIBCL-Format.

- Zum Erfassen einer Konfiguration müssen Sie den Namen und Ort der Ausgabedatei in der Befehlszeile angeben.

  Beispiel:

  ```
  hponcfg /w config.xml
  ```

  HPONCFG zeigt eine Meldung an, wenn die Konfigurationsdaten wie angefordert erfolgreich in die Ausgabedatei geschrieben wurden. Hier ein typisches Beispiel für den Inhalt einer Ausgabedatei:

```
<!-- HPONCFG VERSION = "1.2" -->
<!-- Generated 07/06/05 09:06:51 -->
<RIBCL VERSION="2.1">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
<DIR_INFO MODE="write">
<MOD_DIR_CONFIG>
<DIR_AUTHENTICATION_ENABLED VALUE = "N"/>
<DIR_LOCAL_USER_ACCT VALUE = "Y"/>
<DIR_SERVER_ADDRESS VALUE = ""/>
<DIR_SERVER_PORT VALUE = "636"/>
<DIR_OBJECT_DN VALUE = ""/>
<DIR_OBJECT_PASSWORD VALUE = ""/>
<DIR_USER_CONTEXT_1 VALUE = ""/>
<DIR_USER_CONTEXT_2 VALUE = ""/>
<DIR_USER_CONTEXT_3 VALUE = ""/>
</MOD_DIR_CONFIG>
</DIR_INFO>
<RIB_INFO MODE="write">
<MOD_NETWORK_SETTINGS>
<SPEED_AUTOSELECT VALUE = "Y"/>
<NIC_SPEED VALUE = "100"/>
<FULL_DUPLEX VALUE = "Y"/>
<DHCP_ENABLE VALUE = "Y"/>
<DHCP_GATEWAY VALUE = "Y"/>
<DHCP_DNS_SERVER VALUE = "Y"/>
<DHCP_STATIC_ROUTE VALUE = "Y"/>
<DHCP_WINS_SERVER VALUE = "Y"/>
<REG_WINS_SERVER VALUE = "N"/>
<IP_ADDRESS VALUE = "16.100.241.229"/>
```

```
<SUBNET_MASK VALUE = "255.255.252.0"/>
<GATEWAY_IP_ADDRESS VALUE = "16.100.240.1"/>
<DNS_NAME VALUE = "ILOD234KJ44D002"/>
<DOMAIN_NAME VALUE = "americas.cpqcorp.net"/>
<PRIM_DNS_SERVER value = "16.81.3.242"/>
<SEC_DNS_SERVER value = "0.0.0.0"/>
<TER_DNS_SERVER value = "0.0.0.0"/>
<PRIM_WINS_SERVER value = "16.81.3.247"/>
<SEC_WINS_SERVER value = "0.0.0.0"/>
<STATIC_ROUTE_1 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
<STATIC_ROUTE_2 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
<STATIC_ROUTE_3 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
</MOD_NETWORK_SETTINGS>
<USER_INFO MODE="write">
<ADD_USER
USER_NAME = "Username1"
USER_LOGIN = "User1"
PASSWORD = "%user_password%">
<ADMIN_PRIV value = "N"/>
<REMOTE_CONS_PRIV value = "Y"/>
<RESET_SERVER_PRIV value = "N"/>
<VIRTUAL_MEDIA_PRIV value = "N"/>
<CONFIG_ILO_PRIV value = "N"/>
</ADD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>
```

Aus Sicherheitsgründen werden die standardmäßigen Administrator- und Benutzerkennwörter nicht in der Konfigurationsdatei erfasst oder in der Antwort zurückgegeben. Es wird stattdessen eine Variable zur Verwendung mit der Option `substitute` bereitgestellt, mit der ein Standardkennwort für alle Benutzer zum Wiederherstellen einer Konfiguration angegeben werden kann. Ändern Sie das Kennwort manuell, bevor die Konfiguration aus der Datei wiederhergestellt wird.

- Zum Wiederherstellen einer Konfiguration muss die Datei als Eingabe für die Option `/f` oder `-f` an HPONCFG übergeben werden. Fügen Sie mit der Ersetzungsoption oder `s` ein Standardkennwort für alle Benutzer hinzu.

  Beispiel:

  ```
  hponcfg /f config.xml /s user_password=password
  ```

Benutzerbefehle

Mit Benutzerbefehlen können Sie Benutzereinstellungen anzeigen und ändern.
Tabelle 1, „Eigenschaften der Benutzerbefehle“ zeigt die Eigenschaften der Benutzerbefehle.
Benutzereinstellungen befinden sich unter:

`/map1/accounts1`.

Ziele

Alle lokalen Benutzer sind gültige Ziele. Wenn beispielsweise drei lokale Benutzer mit den Anmeldenamen `Administrator`, `admin` und `test` vorhanden sind, so wären folgende Angaben gültige Ziele:

- `Administrator`
- `admin`
- `test`

Tabelle 1 Eigenschaften der Benutzerbefehle

Eigenschaft	Zugriff	Beschreibung
`username`	Read / Write (Lese-/Schreibzugriff)	Entspricht dem Anmeldenamen für iLO 2, iLO 3 und iLO 4.
`password`	Read / Write (Lese-/Schreibzugriff)	Entspricht dem Kennwort für den aktuellen Benutzer.
`name`	Read / Write (Lese-/Schreibzugriff)	Zeigt den Namen des Benutzers an. Wird kein Name angegeben, verwendet der Parameter den gleichen Wert wie für den Anmeldenamen (username) Dieser Wert entspricht der Benutzernamenseigenschaft für iLO 2iLO 3iLO 4.
`group`	Read / Write (Lese-/Schreibzugriff)	Gibt die Berechtigungsebene an. Folgende Werte sind gültig: • `admin` • `config` • `oemhp_power` • `oemhp_rc` • `oemhp_vm` Wenn Sie keine Gruppe angeben, werden dem Benutzer keine Berechtigungen zugewiesen.

Beispiel:

Der aktuelle Pfad ist:

`/map1/accounts1`.

- `create` *`username`*`=lname1 password=password`

  In diesem Beispiel entspricht `username` dem Anmeldenamen.

- `set` *`lname1`* `username=lname2 password=password1 name=name2 group=admin,configure,oemhp_power,oemhp_vm,oemhp_rc`

  In diesem Beispiel ist `lname1` der Anmeldename des Benutzers.

9 Verwenden von RIBCL

Überblick über RIBCL

Mit RIBCL können Sie XML-Skripts zur Konfiguration und Verwaltung der iLO 2 Konfigurationseinstellungen, Benutzerkonten, Verzeichniseinstellungen, Servereinstellungen und HP SIM SSO-Einstellungen schreiben. Sie können für alle in diesem Abschnitt beschriebenen iLO 2 Befehle Beispielskripts von der HP Website unter http://www.hp.com/servers/lights-out herunterladen. Vor der Verwendung von XML-Beispielskripts, die von der HP Website heruntergeladen wurden, lesen Sie bitte die Firmware-Supportinformationen zu den einzelnen Skripts, um das betreffende Skript auf die jeweilige Firmware und Version abzustimmen.

Fügen Sie beim Schreiben Ihrer XML-Skripts Kommentare in den Befehl ein. Als Teil der Befehlszeile lösen Kommentare Fehlermeldungen aus. Sofern nicht anderweitig angegeben, gelten die Beispiele im vorliegenden Handbuch speziell für die iLO 2 Firmwareversion 1.10 und höher.

Im Abschnitt „Verwenden von RIBCL“ werden die XML-Befehle und ihre Parameter beschrieben, die für die meisten LOM Produkte und Server gelten. Weitere Informationen über die ProLiant BL p-class Server und Rack XML-Befehle finden Sie im *HP Integrated Lights-Out 2 Benutzerhandbuch*.

XML-Kopfzeile

Die XML-Kopfzeile stellt sicher, dass es sich um eine XML-Verbindung und keine HTTP-Verbindung handelt. Die XML-Kopfzeile ist in das Dienstprogramm cpqlocfg integriert und hat folgendes Format:

```
<?xml version="1.0" ?>
```

Datentypen

Es gibt drei verschiedene für einen Parameter zulässige Datentypen.

- Zeichenfolge
- Spezifische Zeichenfolge
- Boolesche Zeichenfolge

Zeichenfolge

Eine Zeichenfolge ist ein in Anführungszeichen stehender Text. Sie kann Leerstellen, Zahlen und beliebige druckbare Zeichen enthalten. Eine Zeichenfolge kann entweder mit doppelten oder einfachen Anführungszeichen beginnen und muss mit demselben Anführungszeichentyp enden. Die Zeichenfolge kann ein Anführungszeichen enthalten, wenn es sich dabei um ein Anführungszeichen handelt, das sich von dem zur Begrenzung der Zeichenfolge verwendeten Anführungszeichen unterscheidet.

Wenn eine Zeichenfolge beispielsweise mit einem doppelten Anführungszeichen beginnt, kann innerhalb dieser Zeichenfolge ein einfaches Anführungszeichen verwendet werden, die Zeichenfolge muss jedoch mit einem doppelten Anführungszeichen enden.

Spezifische Zeichenfolge

Eine spezifische Zeichenfolge ist eine Zeichenfolge, die bestimmte Zeichen enthalten muss. Im Allgemeinen steht Ihnen eine Auswahl an Begriffen zur Verfügung, die als korrekte Syntax akzeptiert werden, während alle anderen Begriffe einen Fehler verursachen.

Boolesche Zeichenfolge

Eine boolesche Zeichenfolge ist eine Zeichenfolge, die `yes` oder `no` repräsentiert. Akzeptable boolesche Zeichenfolgen sind `yes`, `y`, `no`, `n`, `true`, `t`, `false` und `f`. Bei diesen Zeichenfolgen werden Groß-/Kleinschreibung nicht beachtet.

Antwortdefinitionen

Jeder an iLO 2 gesendete Befehl generiert eine Antwort. Anhand dieser Antwort lässt sich erkennen, ob der jeweilige Befehl erfolgreich ausgeführt wurde oder fehlgeschlagen ist. Einige Befehle erzeugen zusätzliche Informationen. Diese zusätzlichen Informationen werden in der Reihenfolge der Ausführung angezeigt, vorausgesetzt, es sind keine Fehler aufgetreten.

Beispiel:

```
<RESPONSE
STATUS="0x0001"
MSG="There has been a severe error."
/>
```

- RESPONSE

  Dieser Tag-Name zeigt an, dass iLO 2 eine Antwort auf die vorherigen Befehle an die Client-Anwendung sendet, um anzugeben, ob die an iLO 2 gesendeten Befehle erfolgreich ausgeführt wurden oder fehlgeschlagen sind.

- STATUS

  Dieser Parameter enthält eine Fehlernummer. Die Nummer „0x0000“ zeigt an, dass kein Fehler aufgetreten ist.

- MSG

  Dieses Element enthält eine Meldung mit einer Beschreibung des/der aufgetretenen Fehler(s). Wenn kein Fehler auftritt, wird die Meldung `No error` ausgegeben.

RIBCL

Dieser Befehl wird zum Starten und Beenden einer RIBCL-Sitzung verwendet. Sie können ihn in einer RIBCL-Sitzung nur einmal verwenden, und es muss der erste Befehl sein, der im Skript angezeigt wird. Die RIBCL-Tags sind erforderlich, um den Anfang und das Ende des RIBCL-Dokuments zu kennzeichnen.

Beispiel:

```
<RIBCL VERSION="2.0">
</RIBCL>
```

RIBCL-Parameter

VERSION ist ein String, der die Version von RIBCL angibt, die die Client-Anwendung zur Verwendung erwartet. Der String VERSION wird mit der RIBCL-Version verglichen, die erwartet wird, und es wird ein Fehler zurückgegeben, wenn der String und die Version nicht übereinstimmen. Der bevorzugte Wert für den Parameter VERSION ist „2.0“. Der VERSION Parameter wird nicht mehr auf genaue Übereinstimmung überprüft. Dieser Parameter darf allerdings nicht leer sein.

RIBCL-Laufzeitfehler

Eine mögliche RIBCL-Fehlermeldung ist:

```
Version must not be blank. (Version darf nicht leer sein.)
```

LOGIN

Der Befehl LOGIN liefert die Informationen, die zur Authentifizierung des Benutzers verwendet werden, dessen Berechtigungsstufe bei der Ausführung von RIBCL-Aktionen verwendet wird. Der angegebene Benutzer muss über ein gültiges Konto auf dem jeweiligen iLO 2 verfügen, um RIBCL-Befehle ausführen zu können. Die Berechtigungen des Benutzers werden mit der erforderlichen Berechtigung für einen bestimmten Befehl verglichen. Bei nicht übereinstimmender Berechtigungsstufe wird ein Fehler zurückgegeben.

Beispiel:

```
<LOGIN USER_LOGIN="username" PASSWORD="password">
</LOGIN>
```

Alternativ kann das Dienstprogramm CPQLOCFG die Anmeldeinformationen auch in Form von Parametern in der Befehlszeile angeben.

```
cpqlocfg -u <Benutzername> -p <Kennwort>
```

Bei Verwendung dieses Formats gibt das Utility die Warnmeldung `Overriding credentials` zurück, zeigt jedoch weiterhin den Meldungseintrag im Fehlerprotokoll als `Login name must not be blank` an.

LOGIN-Parameter

USER_LOGIN ist der Anmeldename des Benutzerkontos. Bei diesem Parameter wird zwischen Groß- und Kleinschreibung unterschieden, und er darf nie leer sein.

PASSWORD ist das Kennwort, das dem Benutzer zugeordnet ist. Bei diesem Parameter wird zwischen Groß- und Kleinschreibung unterschieden. Er kann eine beliebige Kombination druckbarer Zeichen enthalten.

LOGIN-Laufzeitfehler

Die folgenden Laufzeit-Fehlermeldungen können angezeigt werden:

- User login name was not found. (Anmeldename des Benutzers konnte nicht gefunden werden.)
- Version must not be blank. (Version darf nicht leer sein.)
- Logged-in user does not have required privilege for this command. (Der angemeldete Benutzer verfügt nicht über die erforderliche Berechtigung für diesen Befehl).

USER_INFO

Der Befehl USER_INFO darf nur innerhalb eines LOGIN-Befehlsblocks stehen. Beim Übersetzen dieses Befehls wird die Datenbank mit den Benutzerinformationen in den Speicher gelesen und deren Bearbeitung vorbereitet. Nur Befehle des Typs USER_INFO sind innerhalb des USER_INFO-Befehlsblocks gültig. Der Befehl USER_INFO erzeugt eine Antwort, die die Host-Anwendung darüber informiert, ob die Datenbank erfolgreich gelesen wurde oder nicht. Wenn die Datenbank von einer anderen Anwendung überschrieben werden kann, schlägt dieser Aufruf fehl.

USER_INFO erfordert einen MODE-Parameter mit einem Wert „read“ oder „write“. MODE ist ein spezifischer Zeichenfolgeparameter mit einer maximalen Länge von 10 Zeichen, der die beabsichtigte Verarbeitung der Informationen angibt.

Im Schreibmodus können iLO 2 Informationen sowohl gelesen als auch geschrieben werden. Im Lesemodus ist ein Ändern der iLO 2 Informationen nicht möglich.

Beispiel:

```
<USER_INFO MODE="write">
…… USER_INFO Befehle ……
</USER_INFO>
```

ADD_USER

Der Befehl ADD_USER wird verwendet, um ein lokales Benutzerkonto hinzuzufügen. Die Parameter USER_NAME und USER_LOGIN dürfen nicht in der aktuellen Benutzerdatenbank enthalten sein. Verwenden Sie den Befehl MOD_USER, um die Informationen eines vorhandenen Benutzers zu ändern. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines USER_INFO-Befehlsblocks stehen, und USER_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über Administratorrechte verfügen.

Alle den Benutzer betreffenden Attribute werden mithilfe der folgenden Parameter festgelegt.

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="loginname" PASSWORD="password">
<USER_INFO MODE="write">
<ADD_USER
USER_NAME="User"
USER_LOGIN="username" PASSWORD="password">
<ADMIN_PRIV value ="No"/>
<REMOTE_CONS_PRIV value ="Yes"/>
<RESET_SERVER_PRIV value ="No"/>
<VIRTUAL_MEDIA_PRIV value ="No"/>
<CONFIG_ILO_PRIV value ="No"/>
</ADD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>
```

ADD_USER-Parameter

USER_NAME: Der tatsächliche Name des Benutzers. Dieser Parameter kann eine beliebige Kombination druckbarer Zeichen enthalten und darf maximal 39 Zeichen umfassen. Bei diesem Parameter wird zwischen Groß- und Kleinschreibung unterschieden, und er darf nie leer sein.

USER_LOGIN: Der Name, unter dem der Zugriff auf den betreffenden iLO 2 erfolgt. Dieser Parameter kann eine Kombination aus beliebigen druckbaren Zeichen enthalten und darf eine Länge von 39 Zeichen nicht überschreiten. Bei diesem Parameter wird zwischen Groß- und Kleinschreibung unterschieden, und er darf nie leer sein.

PASSWORD: Das mit dem Benutzer verknüpfte Kennwort. Bei diesem Parameter wird zwischen Groß- und Kleinschreibung unterschieden. Er kann eine beliebige Kombination druckbarer Zeichen enthalten. Die Länge ist benutzerdefiniert und kann zwischen mindestens null Zeichen und höchstens 39 Zeichen betragen. Die Mindestlänge wird unter „Global Settings“ (Allgemeine Einstellungen) von iLO 2 festgelegt und beträgt standardmäßig acht Zeichen.

ADMIN_PRIV: Ein boolescher Parameter, der es dem Benutzer erlaubt, Benutzerkonten zu verwalten. Der Benutzer kann eigene Kontoeinstellungen und Kontoeinstellungen anderer Benutzerkonten ändern sowie Benutzer hinzufügen oder löschen. Wenn dieser Parameter ausgelassen wird, kann der Benutzer keine Konten hinzufügen, löschen oder konfigurieren.

REMOTE_CONS_PRIV: Ein boolescher Parameter, der dem Benutzer den Zugriff auf die Remote Console-Funktionalität ermöglicht. Dieser Parameter ist optional. Die boolesche Zeichenfolge muss auf `yes` gesetzt sein, wenn der Benutzer diese Berechtigung benötigt. Bei Verwendung dieses Parameters darf die boolesche Zeichenfolge niemals leer sein. Wenn dieser Parameter ausgelassen wird, kann der Benutzer nicht auf die Remote Console Funktionalität zugreifen.

RESET_SERVER_PRIV: Ein boolescher Parameter, der dem Benutzer die Berechtigung erteilt, die Einstellung zum Ein-/Ausschalten des Servers remote zu bearbeiten. Dieser Parameter ist optional. Die boolesche Zeichenfolge muss auf `yes` gesetzt sein, wenn der Benutzer diese Berechtigung benötigt. Bei Verwendung dieses Parameters darf die boolesche Zeichenfolge niemals leer sein. Wenn dieser Parameter ausgelassen wird, kann der Benutzer die Einstellung zum Ein-/Ausschalten des Servers nicht bearbeiten.

VIRTUAL_MEDIA_PRIV: Ein boolescher Parameter, der dem Benutzer den Zugriff auf die Funktionalität für virtuelle Medien ermöglicht. Dieser Parameter ist optional. Die boolesche Zeichenfolge muss auf `yes` gesetzt sein, wenn der Benutzer diese Berechtigung benötigt. Bei Verwendung dieses Parameters darf die boolesche Zeichenfolge niemals leer sein. Wenn dieser Parameter ausgelassen wird, verfügt der Benutzer nicht über Berechtigungen für die Funktionalität für virtuelle Medien.

CONFIG_ILO_PRIV: Ein boolescher Parameter, der den Benutzer zum Konfigurieren von iLO Einstellungen berechtigt. Diese Berechtigung beinhaltet Netzwerkeinstellungen, allgemeine Einstellungen, Einstellungen von Insight Manager und SNMP-Einstellungen. Dieser Parameter ist optional. Die boolesche Zeichenfolge muss auf `yes` gesetzt sein, wenn der Benutzer diese Berechtigung benötigt. Bei Verwendung dieses Parameters darf die boolesche Zeichenfolge niemals leer sein. Wenn dieser Parameter ausgelassen wird, kann der Benutzer die aktuelle iLO 2 Konfiguration nicht bearbeiten.

Die folgenden Parameter gelten nicht für die Benutzerberechtigungen unter den iLO Firmwareversionen 1.40 und höher sowie den iLO 2 Firmwareversionen 1.1x und höher. Die Parameter werden ordnungsgemäß übersetzt, haben aber keine Auswirkung auf die Benutzerberechtigungen.

VIEW_LOGS_PRIV: Ein boolescher Parameter, der den Benutzer zur Anzeige von iLO 2 Systemprotokollen berechtigt. Dieser Parameter ist optional. Die boolesche Zeichenfolge muss auf `yes` gesetzt sein, wenn der Benutzer die Berechtigung zum Anzeigen von Protokollen benötigt. Bei Verwendung dieses Parameters darf die boolesche Zeichenfolge niemals leer sein.

CLEAR_LOGS_PRIV: Ein boolescher Parameter, der den Benutzer zum Löschen des Ereignisprotokolls berechtigt. Dieser Parameter ist optional. Die boolesche Zeichenfolge muss auf `yes` gesetzt sein, wenn der Benutzer die Berechtigung zum Löschen des iLO 2 Ereignisprotokolls benötigt. Bei Verwendung dieses Parameters darf die boolesche Zeichenfolge niemals leer sein.

EMS_PRIV: Ein boolescher Parameter, der den Benutzer zur Nutzung des Windows Server 2003 EMS-Dienstes berechtigt. Dieser Parameter ist optional. Die boolesche Zeichenfolge muss auf `yes` gesetzt sein, wenn der Benutzer die Berechtigung zum Anzeigen von EMS-Diensten benötigt. Bei Verwendung dieses Parameters darf die boolesche Zeichenfolge niemals leer sein.

UPDATE_ILO_PRIV: Ein boolescher Parameter, der den Benutzer berechtigt, ein neues Firmware-Image in das System-ROM von iLO 2 zu kopieren. Dieser Parameter ist optional. Die boolesche Zeichenfolge muss auf `Yes` gesetzt sein, wenn der Benutzer die Berechtigung zum Konfigurieren von iLO 2 benötigt. Bei Verwendung dieses Parameters darf die boolesche Zeichenfolge niemals leer sein.

CONFIG_RACK_PRIV: Ein boolescher Parameter, der den Benutzer zur Konfiguration und zum Management der Server-Rack-Ressourcen berechtigt. Dieser Parameter gilt nur für ProLiant BL p-Class Server. Dieser Parameter ist optional. Die boolesche Zeichenfolge muss auf `Yes` gesetzt sein, wenn der Benutzer die Berechtigung zum Verwalten oder Konfigurieren von Rack-Ressourcen benötigt. Bei Verwendung dieses Parameters darf die boolesche Zeichenfolge niemals leer sein.

DIAG_PRIV: Ein boolescher Parameter, mit dem der Benutzer Diagnoseinformationen zu iLO 2 anzeigen kann. Dieser Parameter ist optional. Die boolesche Zeichenfolge muss auf `Yes` gesetzt sein, wenn der Benutzer die Berechtigung zur Anzeige von Diagnoseinformationen benötigt. Bei Verwendung dieses Parameters darf die boolesche Zeichenfolge niemals leer sein.

ADD_USER-Laufzeitfehler

Zu den möglichen ADD_USER-Laufzeitfehlern gehören folgende Meldungen:

- `Login name is too long.`
- `Password is too short.`
- `Password is too long.`
- `User table is full. No room for new user.`
- `Cannot add user. The user name already exists.`
- `User information is open for read-only access. Write access is required for this operation.`
- `User name cannot be blank.`
- `User login ID cannot be blank.`

- `Boolean value not specified.`
- `User does not have correct privilege for action. ADMIN_PRIV required.`

DELETE_USER

Der Befehl DELETE_USER wird verwendet, um das Konto eines vorhandenen lokalen Benutzers zu löschen. Der Parameter USER_LOGIN muss in der aktuellen Benutzerdatenbank vorhanden sein. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines USER_INFO-Befehlsblocks stehen, und USER_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über Administratorrechte verfügen.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname"
PASSWORD=
"password">
<USER_INFO MODE="write">
<DELETE_USER USER_LOGIN="username"/>
</USER_INFO>
</LOGIN>
</RIBCL>
```

DELETE_USER-Parameter

USER_LOGIN ist der Anmeldename des Benutzerkontos. Bei diesem Parameter wird zwischen Groß- und Kleinschreibung unterschieden, und er darf nie leer sein.

DELETE_USER-Laufzeitfehler

Zu den möglichen DELETE_USER-Fehlern gehören folgende Meldungen:

- User information is open for read-only access. (Benutzerinformationen werden für Lesezugriff geöffnet.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- Cannot delete user information for currently logged in user. (Benutzerinformationen des aktuell angemeldeten Benutzers können nicht gelöscht werden.)
- User login name was not found. (Anmeldename des Benutzers konnte nicht gefunden werden.)
- User login name must not be blank. (Anmeldename darf nicht leer sein.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) ADMIN_PRIV required. (ADMIN_PRIV erforderlich.)

DELETE_CURRENT_USER

Der Befehl DELETE_CURRENT_USER wird verwendet, um das Benutzerkonto zu löschen, das über das Attribut USER_LOGIN definiert wird. Der Parameter USER_LOGIN muss in der aktuellen Benutzerdatenbank vorhanden sein. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines USER_INFO-Befehlsblocks stehen, und USER_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über Administratorrechte verfügen.

Dieser Befehl ist für Kunden gedacht, die alle Benutzerkonten auf iLO 2 löschen möchten.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname"
PASSWORD="password">
<USER_INFO MODE="write">
```

```
<DELETE_CURRENT_USER/>
</USER_INFO>
</LOGIN>
</RIBCL>
```

DELETE_CURRENT_USER-Parameter

Keine

DELETE_CURRENT_USER-Laufzeitfehler

Zu den möglichen DELETE_CURRENT_USER-Fehlern gehören folgende Meldungen:

User information is open for read-only access. (Benutzerinformationen werden für Lesezugriff geöffnet.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)

DELETE_SSH_KEY

Der Befehl DELETE_SSH_KEY löscht alle SSH-Schlüssel, die mit dem USER_LOGIN von iLO 2 verknüpft sind. Der Befehl DELETE_SSH_KEY wird als Unterbefehl implementiert und muss innerhalb eines MOD_USER-Befehlsblocks erscheinen.

Für diesen Befehl wird Version 2.27 oder höher von CPQLOCFG.EXE benötigt.

Beispiel:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="admin" PASSWORD="admin123">
      <USER_INFO MODE="write">
         <MOD_USER USER_LOGIN="admin">
            <DEL_USERS_SSH_KEY/>
         </MOD_USER>
      </USER_INFO>
   </LOGIN>
</RIBCL>
```

DELETE_SSH_KEY-Parameter

Dieser Befehl verfügt über keine Parameter.

DELETE_SSH_KEY-Laufzeitfehler

Folgende DELETE_USER-Laufzeitfehlermeldungen können angezeigt werden:

- `User login name must not be blank.`
- `User does not have correct privilege for action. ADMIN_PRIV required.`

GET_USER

Der Befehl GET_USER gibt die Informationen eines lokalen Benutzers mit Ausnahme des Kennworts zurück. Der Parameter USER_LOGIN muss in der aktuellen Benutzerdatenbank vorhanden sein. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines USER_INFO-Befehlsblocks stehen; USER_INFO MODE kann auf „read“ oder „write“ gesetzt sein. Der Benutzer muss über Administratorrechte verfügen, um andere Benutzerkonten abrufen zu können. Andernfalls kann der Benutzer nur seine eigenen Konto-Informationen anzeigen.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<USER_INFO MODE="read">
<GET_USER USER_LOGIN="username"/>
</USER_INFO>
```

```
</LOGIN>
</RIBCL>
```

GET_USER-Parameter

USER_LOGIN ist der Anmeldename des Benutzerkontos. Bei diesem Parameter wird zwischen Groß- und Kleinschreibung unterschieden, und er darf nie leer sein.

GET_USER-Laufzeitfehler

Zu den möglichen GET_USER-Laufzeitfehlern gehören folgende Meldungen:

- `User login name must not be blank.`
- `User login name was not found.`
- `User does not have correct privilege for action. ADMIN_PRIV required.`

GET_USER-Rückmeldungen

Eine mögliche GET_USER-Rückmeldung ist:

```
<RESPONSE
STATUS="0x0000"
MSG="No Errors"
/>
<GET_USER
USER_NAME="Administrator"
USER_LOGIN = “Benutzername”
ADMIN_PRIV="N"
REMOTE_CONS_PRIV="Y"
RESET_SERVER_PRIV="N"
VIRTUAL_MEDIA_PRIV="N"
CONFIG_ILO_PRIV value ="No"
/>
```

MOD_USER

Der Befehl MOD_USER wird verwendet, um das Konto eines vorhandenen lokalen Benutzers zu ändern. Der Parameter USER_LOGIN muss in der aktuellen Benutzerdatenbank vorhanden sein. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines USER_INFO-Befehlsblocks stehen, und USER_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über Administratorrechte verfügen. Benutzer ohne Administratorrechte können lediglich ihr eigenes Kennwort ändern.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<USER_INFO MODE="write">
<MOD_USER USER_LOGIN="loginname">
<USER_NAME value="username"/>
<USER_LOGIN value="newloginname"/>
<PASSWORD value="password"/>
<ADMIN_PRIV value="No"/>
<REMOTE_CONS_PRIV value="Yes"/>
<RESET_SERVER_PRIV value="No"/>
<VIRTUAL_MEDIA_PRIV value="No"/>
<CONFIG_ILO_PRIV value="Yes"/>
```

```
</MOD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>
```

Beispiel für das Zurücksetzen des Administratorkennworts:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<USER_INFO MODE="write">
<MOD_USER USER_LOGIN="Administrator">
<PASSWORD value="password"/>
</MOD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>
```

Beispiel für die Kennwortänderung:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<USER_INFO MODE="write">
<MOD_USER USER_LOGIN="username">
<PASSWORD value="newpassword"/>
</MOD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>
```

MOD_USER-Parameter

USER_LOGIN: Der Anmeldename des Benutzerkontos. Bei diesem Parameter wird zwischen Groß- und Kleinschreibung unterschieden, und er darf nie leer sein.

Wenn die folgenden Parameter nicht angegeben werden, wird der Parameterwert für den angegebenen Benutzer beibehalten.

USER_NAME: Der tatsächliche Name des Benutzers, der hinzugefügt werden soll. Bei diesem Parameter wird zwischen Groß- und Kleinschreibung unterschieden, er kann eine beliebige gültige Zeichenfolge sein und eine maximale Länge von 39 Zeichen haben. Dieser String wird nur zur Anzeige verwendet und darf nie leer sein.

USER_LOGIN: Der Name, unter dem der Zugriff auf den betreffenden iLO 2 erfolgt. Dieser Parameter kann eine Kombination aus beliebigen druckbaren Zeichen enthalten und darf eine Länge von 39 Zeichen nicht überschreiten. Bei diesem Parameter wird zwischen Groß- und Kleinschreibung unterschieden, und er darf nie leer sein.

PASSWORD: Das mit dem Benutzer verknüpfte Kennwort. Bei diesem Parameter wird zwischen Groß- und Kleinschreibung unterschieden. Er kann eine beliebige Kombination druckbarer Zeichen enthalten. Die Länge ist benutzerdefiniert und kann zwischen mindestens null Zeichen und höchstens 39 Zeichen betragen. Die Mindestlänge wird unter „Global Settings“ (Allgemeine Einstellungen) von iLO 2 festgelegt und beträgt standardmäßig acht Zeichen.

ADMIN_PRIV: Ein boolescher Parameter, der es dem Benutzer erlaubt, Benutzerkonten zu verwalten. Der Benutzer kann eigene Kontoeinstellungen und Kontoeinstellungen anderer Benutzerkonten ändern sowie Benutzer hinzufügen oder löschen. Wenn dieser Parameter ausgelassen wird, kann der Benutzer keine Konten hinzufügen, löschen oder konfigurieren.

REMOTE_CONS_PRIV: Ein boolescher Parameter, der dem Benutzer den Zugriff auf die Remote Console-Funktionalität ermöglicht. Dieser Parameter ist optional. Die boolesche Zeichenfolge muss

auf `Yes` gesetzt sein, wenn der Benutzer diese Berechtigung benötigt. Bei Verwendung dieses Parameters darf die boolesche Zeichenfolge niemals leer sein. Wenn dieser Parameter ausgelassen wird, kann der Benutzer nicht auf die Remote Console Funktionalität zugreifen.

RESET_SERVER_PRIV: Ein boolescher Parameter, der dem Benutzer die Berechtigung erteilt, die Einstellung zum Ein-/Ausschalten des Servers remote zu bearbeiten. Dieser Parameter ist optional. Die boolesche Zeichenfolge muss auf `Yes` gesetzt sein, wenn der Benutzer diese Berechtigung benötigt. Bei Verwendung dieses Parameters darf die boolesche Zeichenfolge niemals leer sein. Wenn dieser Parameter ausgelassen wird, kann der Benutzer die Einstellung zum Ein-/Ausschalten des Servers nicht bearbeiten.

VIRTUAL_MEDIA_PRIV: Ein boolescher Parameter, der dem Benutzer den Zugriff auf die Funktionalität für virtuelle Medien ermöglicht. Dieser Parameter ist optional. Die boolesche Zeichenfolge muss auf `Yes` gesetzt sein, wenn der Benutzer diese Berechtigung benötigt. Bei Verwendung dieses Parameters darf die boolesche Zeichenfolge niemals leer sein. Wenn dieser Parameter ausgelassen wird, verfügt der Benutzer nicht über Berechtigungen für die Funktionalität für virtuelle Medien.

CONFIG_ILO_PRIV: Ein boolescher Parameter, der den Benutzer zum Konfigurieren von iLO Einstellungen berechtigt. Diese Berechtigung beinhaltet Netzwerkeinstellungen, allgemeine Einstellungen, Einstellungen von Insight Manager und SNMP-Einstellungen. Dieser Parameter ist optional. Die boolesche Zeichenfolge muss auf `Yes` gesetzt sein, wenn der Benutzer diese Berechtigung benötigt. Bei Verwendung dieses Parameters darf die boolesche Zeichenfolge niemals leer sein. Wenn dieser Parameter ausgelassen wird, kann der Benutzer die aktuelle iLO 2 Konfiguration nicht bearbeiten.

MOD_USER-Laufzeitfehler

Zu den möglichen MOD_USER-Laufzeitfehlern gehören folgende Meldungen:

- `Login name is too long.`
- `Password is too short.`
- `Password is too long.`
- `User information is open for read-only access. Write access is required for this operation.`
- `User login name must not be blank.`
- `Cannot modify user information for currently logged user.`
- `User does not have correct privilege for action. ADMIN_PRIV required.`

GET_ALL_USERS

Der Befehl GET_ALL_USERS gibt alle USER_LOGIN-Parameter in der Benutzerdatenbank zurück. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines USER_INFO-Befehlsblocks stehen; USER_INFO MODE kann auf „read“ oder „write“ gesetzt sein. Der Benutzer muss über Administratorrechte verfügen, um alle Benutzerkonten abrufen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<USER_INFO MODE="read">
<GET_ALL_USERS/>
</USER_INFO>
</LOGIN>
</RIBCL>
```

GET_ALL_USERS-Parameter

Keine

GET_ALL_USERS-Laufzeitfehler

Folgende GET_ALL_USERS-Fehlermeldungen können angezeigt werden:

```
User does not have correct privilege for action. ADMIN_PRIV required.
```

GET_ALL_USERS-Rückmeldungen

Eine mögliche GET_ALL_USERS-Rückmeldung ist:

```
<RESPONSE
STATUS="0x0000"
MESSAGE='No error'
/>
<GET_ALL_USERS>
<USER_LOGIN VALUE="username"/>
<USER_LOGIN VALUE="user2"/>
<USER_LOGIN VALUE="user3"/>
<USER_LOGIN VALUE="user4"/>
<USER_LOGIN VALUE="user5"/>
<USER_LOGIN VALUE="user6"/>
<USER_LOGIN VALUE="user7"/>
<USER_LOGIN VALUE="user8"/>
<USER_LOGIN VALUE="user9"/>
<USER_LOGIN VALUE="user10"/>
<USER_LOGIN VALUE=""/>
<USER_LOGIN VALUE=""/>
</GET_ALL_USERS>
```

Eine mögliche, nicht erfolgreiche Anforderung ist:

```
<RESPONSE
STATUS="0x0023"
MESSAGE='User does NOT have correct privilege for action. ADMIN_PRIV required.'
/>
```

GET_ALL_USER_INFO

Der Befehl GET_ALL_USER_INFO gibt die Informationen aller lokalen Benutzer in der Benutzerdatenbank mit Ausnahme der Kennwörter zurück. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines USER_INFO-Befehlsblocks stehen; USER_INFO MODE kann auf „read“ oder „write“ gesetzt sein. Der Benutzer muss Administratorrechte besitzen, um diesen Befehl ausführen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<USER_INFO MODE="read">
<GET_ALL_USER_INFO/>
</USER_INFO>
</LOGIN>
</RIBCL>
```

GET_ALL_USER_INFO-Parameter

Keine

GET_ALL_USER_INFO-Laufzeitfehler

Folgende GET_ALL_USER_INFO-Fehlermeldungen können angezeigt werden:

```
User does not have correct privilege for action. ADMIN_PRIV required.
```

GET_ALL_USER_INFO-Rückmeldungen

Eine mögliche GET_ALL_USER_INFO-Rückmeldung ist:

```
<GET_ALL_USER_INFO/>
<GET_USER
USER_NAME="Admin"
USER_LOGIN="Admin"
ADMIN_PRIV="Y"
CONFIG_RILO_PRIV="Y"
LOGIN_PRIV="Y"
REMOTE_CONS_PRIV="Y"
RESET_SERVER_PRIV="Y"
VIRTUAL_MEDIA_PRIV="Y"
/> ......
Die gleichen Informationen werden für alle Benutzer wiederholt.
</GET_ALL_USER_INFO>
```

Eine mögliche, nicht erfolgreiche Anforderung ist:

```
<RESPONSE
STATUS="0x0023"
MESSAGE='User does NOT have correct privilege for action. ADMIN_PRIV required.'
/>
```

RIB_INFO

Der Befehl RIB_INFO darf nur innerhalb eines LOGIN-Befehlsblocks stehen. Beim Übersetzen dieses Befehls wird die Datenbank mit den iLO 2 Konfigurationsinformationen in den Speicher gelesen und ihre Bearbeitung vorbereitet. Nur Befehle des Typs RIB_INFO sind innerhalb des RIB_INFO-Befehlsblocks gültig. Der Befehl RIB_INFO erzeugt eine Antwort, die die Host-Anwendung darüber informiert, ob die Datenbank erfolgreich gelesen wurde oder nicht. Wenn die Datenbank von einer anderen Anwendung überschrieben werden kann, schlägt dieser Aufruf fehl.

RIB_INFO erfordert einen MODE-Parameter mit einem Wert „read“ oder „write“. MODE ist ein spezifischer Zeichenfolgeparameter mit einer maximalen Länge von 10 Zeichen, der die beabsichtigte Verarbeitung der Informationen angibt.

Im Schreibmodus können iLO 2 Informationen sowohl gelesen als auch geschrieben werden. Im Lesemodus ist ein Ändern der iLO 2 Informationen nicht möglich.

Beispiel:

```
<RIB_INFO MODE="write">
…… RIB_INFO Befehle ……
</RIB_INFO>
```

Beispiel für das Löschen des iLO 2 Ereignisprotokolls:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="write">
<CLEAR_EVENTLOG/>
</RIB_INFO>
</LOGIN>
```

```
</RIBCL>
```

CERT_SIGNATURE_ALGORITHM

Derzeit verwendet die iLO 2 Firmware standardmäßig den MD5-Nachrichtenhash-Algorithmus, wenn ein selbstsigniertes SSL-Zertifikat erstellt wird. Der MD5-Nachrichtenhash-Algorithmus wird aufgrund seiner Konfliktanfälligkeit von Sicherheitsexperten nicht mehr als sicherer Nachrichtenhash-Algorithmus angesehen. Folglich haben einige Kunden darum gebeten, dass iLO 2 beim Erstellen von selbstsignierten Zertifikaten von dem stärkeren Nachrichtenhash-Algorithmus namens SHA1 anstelle von MD5 Gebrauch macht. Der Befehl CERT_SIGNATURE_ALGORITHM wurde mit der iLO 2 2.00 Firmware eingeführt, um Kunden die Konfiguration von iLO 2 zum Erstellen eines selbstsignierten MD5- oder SHA1-Zertifikats zu gestatten.

HINWEIS: Die iLO 2 Firmware wird nach der erfolgreichen Ausführung des Befehls CERT_SIGNATURE_ALGORITHM zurückgesetzt.

Beispiele:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE = "write">
<CERT_SIGNATURE_ALGORITHM ="SHA1"/>
</RIB_INFO>
</LOGIN>
</RIBCL>
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE = "write">
<CERT_SIGNATURE_ALGORITHM ="MD5"/>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

CERT_SIGNATURE_ALGORITHM Parameter

CERT_SIGNATURE_ALGORITHM – „MD5“ zum Erstellen eines selbstsignierten MD5-Zertifikats. „SHA1“ zum Erstellen eines selbstsignierten SHA1-Zertifikats.

CERT_SIGNATURE_ALGORITHM-Laufzeitfehler

- RIB information is open for read-only access. (RIB-Informationen sind schreibgeschützt.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- Zum Ändern des Signatur-Algorithmus wird die Berechtigungsebene „Configure iLO 2 Settings“ (iLO 2 Einstellungen konfigurieren) benötigt.
- Der Parameter des Zertifikat-Signierungsalgorithmus muss „MD5“ oder „SHA1“ lauten.

RESET_RIB

Der Befehl RESET_RIB dient zum Zurücksetzen von iLO 2. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines RIB_INFO-Befehlsblocks stehen; RIB_INFO MODE kann dabei auf „read“ oder „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Admin" PASSWORD="Password">
```

```
<RIB_INFO MODE = "write">
<RESET_RIB/>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

RESET_RIB-Parameter

Keine

RESET_RIB-Laufzeitfehler

Folgende RESET_RIB-Fehlermeldungen können angezeigt werden:

```
User does not have correct privilege for action. CONFIG_ILO_PRIV
required.
```

GET_EVENT_LOG

Der Befehl GET_EVENT_LOG ruft je nach dem Befehlskontext das iLO 2 Ereignisprotokoll oder das integrierte Managementprotokoll ab. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines RIB_INFO- oder SERVER_INFO-Befehlsblocks stehen. Verwenden Sie zum Abruf des iLO 2 Ereignisprotokolls den Befehlsblock RIB_INFO. Verwenden Sie zum Abruf des integrierten Managementprotokolls den Befehlsblock SERVER_INFO.

Beispiele:

- Beispiel für das iLO 2 Ereignisprotokoll:

```
<RIBCL version="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="READ">
<GET_EVENT_LOG />
</RIB_INFO>
</LOGIN>
</RIBCL>
```

- Beispiel für das integrierte Managementprotokoll:

```
<RIBCL version="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="READ">
<GET_EVENT_LOG />
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

GET_EVENT_LOG-Parameter

Keine

GET_EVENT_LOG-Laufzeitfehler

GET_EVENT_LOG gibt einen Laufzeitfehler zurück, wenn es nicht aus dem Befehlsblock RIB_INFO oder SERVER_INFO heraus aufgerufen wird. Beispiel:

```
<RIBCL VERSION="2.21">
<RESPONSE
STATUS="0x0001"
MESSAGE='Syntax error: Line #3: syntax error near ">" in the line: " GET_EVENT_LOG >"'
```

```
/>
</RIBCL>
```

GET_EVENT_LOG-Rückmeldungen

Die Antwort umfasst alle aufgezeichneten Ereignisse in der Reihenfolge, in der sie aufgetreten sind. Die Ereignisse werden nicht nach Schweregrad oder anderen Kriterien sortiert. Jedes Ereignis enthält einen Satz gleicher Attribute:

- SEVERITY: Gibt den Schweregrad des Fehlers und seine mögliche Auswirkung auf die Server- oder iLO 2 Verfügbarkeit an.
  - FAILED: Weist auf ein Problem oder einen Komponentenfehler hin, der sich auf die Betriebsbereitschaft auswirken kann, wenn er nicht behoben wird.
  - CAUTION: Weist auf ein Ereignis hin, dass während des normalen Systembetriebs unerwartet auftrat. Dabei handelt es sich nicht unbedingt um einen Plattformfehler.
  - REPAIRED: Weist darauf hin, dass ein Ereignis oder ein Komponentenfehler behoben wurde.
  - INFORMATIONAL: Bedeutet, dass ein erwähnenswertes Ereignis aufgetreten ist, das jedoch nicht die Betriebsbereitschaft beeinträchtigt.
- CLASS: Gibt das Subsystem an, durch das das Ereignis generiert wurde, und kann unter anderem Informationen zu iLO 2, Umgebung, Stromversorgung, Systemfehler und Rack-Infrastruktur beinhalten.
- LAST_UPDATE: Gibt den Zeitpunkt an, an dem dieses Ereignis zuletzt geändert wurde.
- INITIAL_UPDATE: Gibt an, wann dieses Ereignis zuletzt aufgetreten ist.
- COUNT: Gibt an, wie oft ein doppeltes Ereignis aufgetreten ist.
- DESCRIPTION: Gibt die Art des Ereignisses und alle aufgezeichneten Details an.

Die folgende Antwort ist ein typisches Bespiel für die vom iLO 2 Ereignisprotokoll zurückgegebenen Daten:

```
<EVENT_LOG DESCRIPTION="iLO Event Log">
<EVENT
SEVERITY="Caution"
CLASS="iLO"
LAST_UPDATE="04/04/2004 12:34"
INITIAL_UPDATE="04/04/2004 12:34"
COUNT="1"
DESCRIPTION="Server reset."
/>
...
</EVENT_LOG>
```

Die folgende Antwort ist ein typisches Bespiel für die vom integrierten Managementprotokoll zurückgegebenen Daten:

```
<EVENT_LOG DESCRIPTION="Integrated Management Log">
<EVENT
SEVERITY="Caution"
CLASS="POST Message"
LAST_UPDATE="04/04/2004 12:34"
INITIAL_UPDATE="04/04/2004 12:34"
COUNT="1"
```

```
  DESCRIPTION="POST Error: 1775-Drive Array - ProLiant Storage System not Responding"
/>
...
</EVENT_LOG>
```

CLEAR_EVENTLOG

Mit dem Befehl CLEAR_EVENTLOG wird das iLO 2 Ereignisprotokoll gelöscht. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines RIB_INFO-Befehlsblocks stehen, und RIB_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="write">
<CLEAR_EVENTLOG/>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

CLEAR_EVENTLOG-Parameter

Keine

CLEAR_EVENTLOG-Laufzeitfehler

Folgende CLEAR_EVENTLOG Fehlermeldungen können angezeigt werden:

- RIB information is open for read-only access. (RIB-Informationen sind schreibgeschützt.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) CONFIG_ILO_PRIV required. (CONFIG_ILO_PRIV erforderlich.)

COMPUTER_LOCK_CONFIG

Mit dem Befehl COMPUTER_LOCK_CONFIG wird die Funktion „Remote Console Computer Lock“ (Computersperre von Remote Console) konfiguriert. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines RIB_INFO-Befehlsblocks stehen, und RIB_INFO MODE muss auf „write“ gesetzt sein. Sie müssen über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Großbuchstaben werden nicht unterstützt und automatisch in Kleinbuchstaben umgewandelt. Bei Verwendung doppelter oder einfacher Anführungszeichen müssen diese sich vom Begrenzungszeichen unterscheiden. Eine vollständige Liste der unterstützten benutzerdefinierten Tasten finden Sie im *HP Integrated Lights-Out 2 Benutzerhandbuch*.

Beispiel für Windows-Computersperre:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO_MODE="write">
<COMPUTER_LOCK_CONFIG>
<COMPUTER_LOCK value="windows"/>
</COMPUTER_LOCK_CONFIG>
</RIB_INFO_MODE="write">
</LOGIN>
```

```
</RIBCL>
```

Beispiel für benutzerdefinierte Computersperre:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO_MODE="write">
<COMPUTER_LOCK_CONFIG>
<COMPUTER_LOCK value="custom"/>
<COMPUTER_LOCK key="l_gui,l"/>
</COMPUTER_LOCK_CONFIG>
</RIB_INFO_MODE="write">
</LOGIN>
</RIBCL>
```

Beispiel für deaktivierte Computersperre:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO_MODE="write">
<COMPUTER_LOCK_CONFIG>
<COMPUTER_LOCK value="disabled"/>
</COMPUTER_LOCK_CONFIG>
</RIB_INFO_MODE="write">
</LOGIN>
</RIBCL>
```

COMPUTER_LOCK_CONFIG-Parameter

Für Computersperre wird auf Windows-basierten Betriebssystemen standardmäßig die Tastenkombination Windows Logo + **L** eingestellt. Linux- und andere Betriebssysteme können durch Setzen des Parameters `<COMPUTER_LOCK value="custom"/>` angepasst werden. Beispiel:

```
<COMPUTER_LOCK key="l_gui,l"/>
```

COMPUTER_LOCK_CONFIG- Laufzeitfehler

Folgende COMPUTER_LOCK_CONFIG-Fehlermeldungen können angezeigt werden:

- RIB information is open for read-only access. (RIB-Informationen sind schreibgeschützt.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- Invalid number of parameters. (Ungültige Anzahl Hotkeys.) The maximum allowed is five. (Die maximal zulässige Anzahl ist fünf.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) CONFIG_ILO_PRIV required. (CONFIG_ILO_PRIV erforderlich.)
- Invalid COMPUTER_LOCK option; value must be windows, custom or disabled. (Ungültige COMPUTER_LOCK-Option; Wert muss „windows“, „custom“ oder „disabled“ lauten.)
- COMPUTER_LOCK value must be set to custom to use the COMPUTER_LOCK_KEY tag. (COMPUTER_LOCK-Wert muss auf die Verwendung des Tags COMPUTER_LOCK_KEY eingestellt sein.)
- The COMPUTER_LOCK key command was used without a preceding COMPUTER_LOCK value command equal to custom. (Der Befehl COMPUTER_LOCK wurde ohne vorangehenden Befehl COMPUTER_LOCK mit dem Wert „custom“ verwendet.)
- The key parameter specified is not valid. (Der angegebene Schlüsselparameter ist ungültig.)

GET_NETWORK_SETTINGS

Mit dem Befehl GET_NETWORK_SETTINGS werden die betreffenden iLO 2 Netzwerkeinstellungen abgefragt. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines RIB_INFO-Befehlsblocks stehen; RIB_INFO MODE kann auf „read“ oder „write“ gesetzt sein.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="read">
<GET_NETWORK_SETTINGS/>
</RIB_INFO>
</LOGIN>
 </RIBCL>
```

GET_NETWORK_SETTINGS-Parameter

Keine

GET_NETWORK_SETTINGS-Laufzeitfehler

Keine

GET_NETWORK_SETTINGS-Rückmeldungen

Eine mögliche GET_NETWORK_SETTINGS-Rückmeldung ist:

```
<ENABLE_NIC VALUE="Y"/>
<SHARED_NETWORK_PORT VALUE="N" />
<VLAN ENABLED="N"/>
<VLAN_ID VALUE="0"/>
<SPEED_AUTOSELECT VALUE="Y"/>
<NIC_SPEED VALUE="10"/>
<FULL_DUPLEX VALUE="N"/>
<DHCP_ENABLE VALUE="Y"/>
<DHCP_GATEWAY VALUE="Y"/>
<DHCP_DNS_SERVER VALUE="Y"/>
<DHCP_WINS_SERVER VALUE="Y"/>
<DHCP_STATIC_ROUTE VALUE="Y"/>
<DHCP_DOMAIN_NAME VALUE="Y"/>
<REG_WINS_SERVER VALUE="Y"/>
<REG_DDNS_SERVER VALUE="Y"/>
<PING_GATEWAY VALUE="N"/>
<MAC_ADDRESS VALUE="00:12:79:a5:25:42"/>
<IP_ADDRESS VALUE="170.100.8.10"/>
<SUBNET_MASK VALUE="255.255.255.0"/>
<GATEWAY_IP_ADDRESS VALUE="170.100.8.254"/>
<DNS_NAME VALUE="ILO000FWDC451"/>
<DOMAIN_NAME VALUE="ferrari.com"/>
<PRIM_DNS_SERVER VALUE="172.25.163.199"/>
<SEC_DNS_SERVER VALUE="0.0.0.0"/>
<TER_DNS_SERVER VALUE="0.0.0.0"/>
<PRIM_WINS_SERVER VALUE="172.25.163.199"/>
<SEC_WINS_SERVER VALUE="0.0.0.0"/>
```

```
<STATIC_ROUTE_1 DEST="0.0.0.0"
GATEWAY="0.0.0.0"/>
<STATIC_ROUTE_2 DEST="0.0.0.0"
GATEWAY="0.0.0.0"/>
<STATIC_ROUTE_3 DEST="0.0.0.0"
GATEWAY="0.0.0.0"/>
</GET_NETWORK_SETTINGS>
```

Eine mögliche, nicht erfolgreiche Anforderung ist:

```
<RESPONSE
STATUS = "0x0001"
MSG = "Error message"/>
```

MOD_NETWORK_SETTINGS

Mit MOD_NETWORK_SETTINGS werden Netzwerkeinstellungen geändert. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines RIB_INFO-Befehlsblocks stehen, und RIB_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Die Skript-Firmware von iLO 2 versucht nicht festzustellen, ob die Netzwerkmodifizierungen für die Netzwerkumgebung geeignet sind. Beim Ändern der Netzwerkeinstellungen müssen Sie auf die Netzwerkbefehle an den Managementprozessor achten. In einigen Fällen ignoriert der Managementprozessor Befehle, ohne dass ein Fehler zurückgegeben wird. Wenn ein Skript beispielsweise den Befehl enthält, DHCP zu aktivieren, und einen Befehl, die IP-Adresse zu ändern, wird die IP-Adresse ignoriert. Wenn die Netzwerkeinstellungen auf Werte gesetzt werden, die für die Netzwerkumgebung nicht gültig sind, kann dies zu einer Trennung der Verbindung mit iLO 2 führen.

Nachdem das Skript erfolgreich ausgeführt wurde, wird der iLO 2 Managementprozessor neu gestartet, um die Änderungen zu übernehmen. Wenn die Verbindung mit iLO 2 getrennt wird, müssen Sie die Netzwerkeinstellungen mit dem RBSU so neu konfigurieren, dass die Werte mit der Netzwerkumgebung kompatibel sind.

Beispiel:

```
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="write">
<MOD_NETWORK_SETTINGS>
<ENABLE_NIC value="yes"/>
<REG_DDNS_SERVER value="yes"/>
<PING_GATEWAY value="no"/>
<DHCP_DOMAIN_NAME value="yes"/>
<SPEED_AUTOSELECT value="yes"/>
<NIC_SPEED value="100"/>
<FULL_DUPLEX value="yes"/>
<DHCP_ENABLE value="no"/>
<IP_ADDRESS value="172.20.60.152"/>
<SUBNET_MASK value="255.255.255.0"/>
<GATEWAY_IP_ADDRESS value="172.20.60.1"/>
<DNS_NAME value="demoilo"/>
<DOMAIN_NAME value="internal.com"/>
<DHCP_GATEWAY value="yes"/>
<DHCP_DNS_SERVER value="yes"/>
<DHCP_WINS_SERVER value="yes"/>
```

```
<DHCP_STATIC_ROUTE value="yes"/>
<REG_WINS_SERVER value="yes"/>
<PRIM_DNS_SERVER value="0.0.0.0"/>
<SEC_DNS_SERVER value="0.0.0.0"/>
<TER_DNS_SERVER value="0.0.0.0"/>
<PRIM_WINS_SERVER value="0.0.0.0"/>
<SEC_WINS_SERVER value="0.0.0.0"/>
<STATIC_ROUTE_1 DEST="0.0.0.0" GATEWAY="0.0.0.0"/>
<STATIC_ROUTE_2 DEST="0.0.0.0" GATEWAY="0.0.0.0"/>
<STATIC_ROUTE_3 DEST="0.0.0.0" GATEWAY="0.0.0.0"/>
<!-- This tag can be used on an iLO blade server to force iLO  -->
<!-- to attempt to get an IP address from the signal backplane -->
<!-- in a server enclosure. The IP address must be set prior -->
<!-- with Mod_Enc_Bay_IP_Settings.xml -->
<!-- <ENCLOSURE_IP_ENABLE VALUE="yes"/> -->
</MOD_NETWORK_SETTINGS>
</RIB_INFO>
</LOGIN>
```

Beispiel für die VLAN-Änderung:

```
<RIBCL version="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="WRITE">
<MOD_NETWORK_SETTINGS>
<SHARED_NETWORK_PORT VALUE="yes"/>
<VLAN_ENABLED VALUE="yes"/>
<VLAN_ID VALUE="1"/>
</MOD_NETWORK_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

Beispiel für ein RBSU POST-IP:

```
<RIBCL version="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="write">
<MOD_GLOBAL_SETTINGS>
<RBSU_POST_IP VALUE="Y"/>
</MOD_GLOBAL_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

Beispiel für einen gemeinsam genutzten Netzwerkport:

```
<RIBCL version="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="WRITE">
<MOD_NETWORK_SETTINGS>
<!-- Desired NIC: Substitute: -->
<!-- iLO NIC <SHARED_NETWORK_PORT VALUE="N"/> -->
```

```
<!-- Host NIC <SHARED_NETWORK_PORT VALUE="Y"/ -->
<SHARED_NETWORK_PORT VALUE="N" />
</MOD_NETWORK_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

MOD_NETWORK_SETTINGS-Parameter

Wenn die folgenden Parameter nicht angegeben werden, wird der Parameterwert für die angegebene Einstellung beibehalten. In einigen Feldern sind keine Nullwerte erlaubt. Daher werden in einigen Feldern die aktuellen Werte durch leere Zeichenfolgen überschrieben.

ENABLE_NIC: Ermöglicht dem Controller, den Zustand von iLO 2 widerzuspiegeln. Die Werte sind `Yes` oder `No`. Dabei wird nicht zwischen Groß- und Kleinschreibung unterschieden.

SHARED_NETWORK_PORT: Legt den Wert für „Shared Network Port“ (Gemeinsam genutzter Netzwerkport) fest. Mögliche Werte sind `Yes` und `No`. Die iLO Funktion für den gemeinsam genutzten Netzwerkport steht nur auf Servern mit Hardware, NIC-Firmware und iLO Firmware zur Verfügung, die diese Funktion unterstützen. Die iLO 2 Funktion für den gemeinsam genutzten Netzwerkport wird auf allen Firmwareversionen unterstützt und ist verfügbar, wenn die Hardware unterstützt wird.

ProLiant Server	iLO Firmwareversion (Minimum)
DL320 G3	1.64
DL360 G4	1.60
DL360 G4	1.64
DL380 G4	1.60
DL385 G1	1.64
DL580 G3	1.64
ML370 G4	1.60
ML570 G3	1.64

Bei der Verwendung des gemeinsam genutzten iLO 2 Netzwerkports dauert der iLO 2 Firmware-Flash über die XML-Schnittstelle ca. sieben Minuten. Der Firmware-Flash über den gemeinsam genutzten iLO 2 Netzwerkport dauert nicht länger als über einen dedizierten iLO 2 Management-Port.

VLAN_ENABLED VALUE: Aktiviert das VLAN-ID-Tagging des gemeinsam genutzten iLO 2 Netzwerkports. Mögliche Werte sind `yes` und `No`.

VLAN_ID VALUE: Legt den VLAN ID-Wert fest. Zulässige Werte liegen zwischen 1 und 4094.

REG_DDNS_SERVER VALUE: Weist iLO 2 an, den Management-Port bei einem DDNS-Server anzumelden. Die möglichen Werte sind `Yes` oder `No`.

SPEED_AUTOSELECT: Ein boolescher Parameter, mit dem festgelegt wird, ob der iLO 2 Transceiver die Geschwindigkeit und den Duplexmodus des Netzwerks automatisch erkennt. Dieser Parameter ist optional. Die boolesche Zeichenfolge muss auf `Yes` gesetzt sein, wenn dieses Verhalten erwünscht ist. Bei Verwendung dieses Parameters darf die boolesche Zeichenfolge niemals leer sein. Die möglichen Werte sind `Yes` oder `No`. Dabei wird nicht zwischen Groß- und Kleinschreibung unterschieden.

FULL_DUPLEX: Hiermit wird festgelegt, ob iLO 2 den Voll- oder Halbduplexmodus unterstützt. Dies trifft nur zu, wenn `SPEED_AUTOSELECT` auf `No` gesetzt wurde. Mögliche Werte sind `Yes` und `No`. Dabei wird nicht zwischen Groß- und Kleinschreibung unterschieden.

NIC_SPEED: Wird zum Einstellen der Transceiver-Geschwindigkeit verwendet, wenn SPEED_AUTOSELECT auf `No` gesetzt wurde. Mögliche Werte sind `10` und `100`. Alle anderen Werte verursachen einen Syntaxfehler.

DHCP_ENABLE: Wird verwendet, um DHCP zu aktivieren. Mögliche Werte sind `Yes` und `No`. Dabei wird nicht zwischen Groß- und Kleinschreibung unterschieden.

IP_ADDRESS: Wird zur Auswahl der IP-Adresse für iLO 2 verwendet, wenn DHCP nicht aktiviert ist. Bei Eingabe einer leeren Zeichenfolge wird der aktuelle Wert gelöscht.

SUBNET_MASK: Dient zur Auswahl der Subnetzmaske für iLO 2, wenn DHCP nicht aktiviert ist. Bei Eingabe einer leeren Zeichenfolge wird der aktuelle Wert gelöscht.

GATEWAY_IP_ADDRESS: Dient zur Auswahl der standardmäßigen Gateway-IP-Adresse für iLO 2, wenn DHCP nicht aktiviert ist. Bei Eingabe einer leeren Zeichenfolge wird der aktuelle Wert gelöscht.

DNS_NAME: Gibt den DNS-Namen für iLO 2 an. Bei Eingabe einer leeren Zeichenfolge wird der aktuelle Wert gelöscht.

DOMAIN_NAME: Wird zur Angabe des Domänennamens für das Netzwerk verwendet, in dem sich iLO 2 befindet. Bei Eingabe einer leeren Zeichenfolge wird der aktuelle Wert gelöscht.

DHCP_GATEWAY: Gibt an, ob die über DHCP zugewiesene Gateway-Adresse verwendet werden soll. Mögliche Werte sind `Yes` und `No`. Dabei wird nicht zwischen Groß- und Kleinschreibung unterschieden. Diese Auswahl ist nur dann gültig, wenn DHCP aktiviert ist.

DHCP_DNS_SERVER: Gibt an, ob der über DHCP zugewiesene DNS-Server verwendet werden soll. Mögliche Werte sind `Yes` und `No`. Dabei wird nicht zwischen Groß- und Kleinschreibung unterschieden. Diese Auswahl ist nur dann gültig, wenn DHCP aktiviert ist.

DHCP_WINS_SERVER: Gibt an, ob der über DHCP zugewiesene WINS-Server verwendet werden soll. Mögliche Werte sind `Yes` und `No`. Dabei wird nicht zwischen Groß- und Kleinschreibung unterschieden. Diese Auswahl ist nur dann gültig, wenn DHCP aktiviert ist.

DHCP_STATIC_ROUTE: Gibt an, ob die statischen über DHCP zugewiesenen Verbindungswege verwendet werden sollen. Mögliche Werte sind `Yes` und `No`. Dabei wird nicht zwischen Groß- und Kleinschreibung unterschieden. Diese Auswahl ist nur dann gültig, wenn DHCP aktiviert ist.

REG_WINS_SERVER: Gibt an, ob iLO 2 beim WINS-Server registriert werden muss. Mögliche Werte sind `Yes` und `No`. Dabei wird nicht zwischen Groß- und Kleinschreibung unterschieden. Diese Auswahl ist nur dann gültig, wenn DHCP aktiviert ist.

PRIM_DNS_SERVER: Gibt die IP-Adresse des primären DNS-Servers an. Dieser Parameter ist nur dann relevant, wenn die Funktion für die über DHCP zugewiesene DNS-Serveradresse deaktiviert ist. Bei Eingabe einer leeren Zeichenfolge wird der aktuelle Wert gelöscht.

SEC_DNS_SERVER: Gibt die IP-Adresse des sekundären DNS-Servers an. Dieser Parameter ist nur dann relevant, wenn die Funktion für die über DHCP zugewiesene DNS-Serveradresse deaktiviert ist. Bei Eingabe einer leeren Zeichenfolge wird der aktuelle Wert gelöscht.

TER_DNS_SERVER: Gibt die IP-Adresse des tertiären DNS-Servers an. Dieser Parameter ist nur dann relevant, wenn die Funktion für die über DHCP zugewiesene DNS-Serveradresse deaktiviert ist. Bei Eingabe einer leeren Zeichenfolge wird der aktuelle Wert gelöscht.

PRIM_WINS_SERVER: Gibt die IP-Adresse des primären WINS-Servers an. Dieser Parameter ist nur dann relevant, wenn die Funktion für die über DHCP zugewiesene WINS-Serveradresse deaktiviert ist. Bei Eingabe einer leeren Zeichenfolge wird der aktuelle Wert gelöscht.

SEC_WINS_SERVER gibt die IP-Adresse des sekundären WINS-Servers an. Dieser Parameter ist nur dann relevant, wenn die Funktion für die über DHCP zugewiesene WINS-Serveradresse deaktiviert ist. Bei Eingabe einer leeren Zeichenfolge wird der aktuelle Wert gelöscht.

STATIC_ROUTE_1, STATIC_ROUTE_2 und STATIC_ROUTE_3: Werden zur Angabe der Ziel- und Gateway-IP-Adresse der statischen Verbindungswege verwendet. Die beiden folgenden Parameter

werden innerhalb der Befehle für statische Verbindungswege verwendet. Bei Eingabe einer leeren Zeichenfolge wird der aktuelle Wert gelöscht.

- DEST: Gibt die Ziel-IP-Adresse des statischen Verbindungswegs an. Dieser Parameter ist nur dann relevant, wenn die Funktion für den über DHCP zugewiesenen statischen Verbindungsweg deaktiviert ist. Bei Eingabe einer leeren Zeichenfolge wird der aktuelle Wert gelöscht.
- GATEWAY: Gibt die Gateway-IP-Adressen des statischen Verbindungswegs an. Dieser Parameter ist nur dann relevant, wenn die Funktion für den über DHCP zugewiesenen statischen Verbindungsweg deaktiviert ist. Bei Eingabe einer leeren Zeichenfolge wird der aktuelle Wert gelöscht.

WEB_AGENT_IP_ADDRESS: Gibt die Adresse der Web-fähigen Agenten an. Bei Eingabe einer leeren Zeichenfolge wird der aktuelle Wert gelöscht.

MOD_NETWORK_SETTINGS-Laufzeitfehler

Zu den möglichen MOD_USER-Laufzeitfehlern gehören folgende Meldungen:

- RIB information is open for read-only access. (RIB-Informationen sind schreibgeschützt.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) CONFIG_ILO_PRIV required. (CONFIG_ILO_PRIV erforderlich.)

GET_GLOBAL_SETTINGS

Mit dem Befehl GET_GLOBAL_SETTINGS werden die allgemeinen iLO 2 Einstellungen abgefragt. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines RIB_INFO-Befehlsblocks stehen; RIB_INFO MODE kann auf `read` oder `write` gesetzt sein.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="read">
<GET_GLOBAL_SETTINGS />
</RIB_INFO>
</LOGIN>
</RIBCL>
```

GET_GLOBAL_SETTINGS-Parameter

Keine

GET_GLOBAL_SETTINGS-Laufzeitfehler

Keine

GET_GLOBAL_SETTINGS-Rückmeldungen

Eine mögliche GET_GLOBAL_SETTINGS-Rückmeldung ist:

```
<GET_GLOBAL_SETTINGS>
<SESSION_TIMEOUT="120">
<ILO_FUNCT_ENABLED VALUE="Y"/>
<F8_PROMPT_ENABLED="Y"/>
<F8_LOGIN_REQUIRED="Y"/>
<REMOTE_CONSOLE_PORT_STATUS VALUE="2"/>
<REMOTE_CONSOLE_ENCRYPTION VALUE="Y"/>
<REMOTE_CONSOLE_ACQUIRE VALUE="Y"/>
```

```
<PASSTHROUGH_CONFIG VALUE="3"/>
<HTTPS_PORT VALUE="443"/>
<HTTP_PORT VALUE="80"/>
<REMOTE_CONSOLE_PORT VALUE="23"/>
<TERMINAL_SERVICES_PORT VALUE="3389"/>
<VIRTUAL_MEDIA_PORT VALUE="17988"/>
<MIN_PASSWORD VALUE="8"/>
<AUTHENTICATION_FAILURE_LOGGING VALUE="Enabled-every 3rd failure"/>
<REMOTE_KEYBOARD_MODEL VALUE="US"/>
<SSH_PORT value="22"/>
<SSH_STATUS value="YES"/>
<SERIAL_CLI_STATUS value="3"/>
<SERIAL_CLI_SPEED value="1"/>
</GET_GLOBAL_SETTINGS>
```

Eine mögliche zurückgegebene Meldung für `GET_GLOBAL_SETTINGS` von der iLO 2 1.30 Firmware:

```
<GET_GLOBAL_SETTINGS>
<SESSION_TIMEOUT VALUE="0"/>
<ILO_FUNCT_ENABLED VALUE="Y"/>
<F8_PROMPT_ENABLED VALUE="Y"/>
<F8_LOGIN_REQUIRED VALUE="N"/>
<TELNET_ENABLE VALUE="Y"/>
<PASSTHROUGH_CONFIG VALUE="3"/>
<HTTPS_PORT VALUE="443"/>
<HTTP_PORT VALUE="80"/>
<REMOTE_CONSOLE_PORT VALUE="23"/>
<TERMINAL_SERVICES_PORT VALUE="3389"/>
<VIRTUAL_MEDIA_PORT VALUE="17988"/>
<SSH_PORT VALUE="22"/>
<CONSOLE_CAPTURE_PORT VALUE="17990"/>
<SHARED_CONSOLE_PORT VALUE="9300"/>
<SSH_STATUS VALUE="Y"/>
<SERIAL_CLI_STATUS VALUE="Enabled-Authentication Required"/>
<SERIAL_CLI_SPEED VALUE="9600"/>
<MIN_PASSWORD VALUE="8"/>
<AUTHENTICATION_FAILURE_LOGGING VALUE="Enabled-every 3rd failure"/>
<REMOTE_KEYBOARD_MODEL VALUE="US"/>
<RBSU_POST_IP VALUE="Y"/>
<HIGH_PERFORMANCE_MOUSE VALUE="Enabled"/>
<REMOTE_CONSOLE_ACQUIRE VALUE="Y"/>
<CONSOLE_CAPTURE_ENABLE VALUE="Disabled"/>
<CONSOLE_CAPTURE_BOOT_BUFFER_ENABLE VALUE="Disabled"/>
<CONSOLE_CAPTURE_FAULT_BUFFER_ENABLE VALUE="Disabled"/>
<INTERACTIVE_CONSOLE_REPLAY_ENABLE VALUE="Disabled"/>
<CAPTURE_AUTO_EXPORT_ENABLE VALUE="Disabled"/>
<CAPTURE_AUTO_EXPORT_LOCATION VALUE="http://192.168.1.1/folder/capture%h%t.ilo"/>
<CAPTURE_AUTO_EXPORT_USERNAME VALUE=""/>
<CAPTURE_AUTO_EXPORT_PASSWORD VALUE=""/>
```

```
<SHARED_CONSOLE_ENABLE VALUE="Enabled"/>
<ENFORCE_AES VALUE="N"/>
</GET_GLOBAL_SETTINGS>
```

MOD_GLOBAL_SETTINGS

Mit dem Befehl MOD_GLOBAL_SETTINGS werden globale Einstellungen geändert. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines RIB_INFO-Befehlsblocks stehen, und RIB_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Das Lights-Out Gerät (nicht der Server) wird automatisch zurückgesetzt, damit die Änderungen an den Porteinstellungen wirksam werden. Durch Festlegen von `No` für ILO_FUNCT_ENABLED werden die Managementfunktionen von iLO 2 und iLO deaktiviert. Wenn iLO 2/iLO deaktiviert wurden, müssen sie mit dem iLO Security Override-Schalter (dem Schalter zum Außerkraftsetzen der iLO Sicherheit) auf der Systemplatine des Servers und mit dem iLO 2/iLO RBSU (F8-Taste) wieder aktiviert werden.

Verwenden Sie mit den folgenden Skripts `CPQLOCFG.EXE`, Version 2.26 oder höher.

Beispiel 1:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="write">
<MOD_GLOBAL_SETTINGS>
<SESSION_TIMEOUT value="60"/>
<F8_PROMPT_ENABLED value="Yes"/>
<HTTP_PORT value="80"/>
<HTTPS_PORT value="443"/>
<REMOTE_CONSOLE_PORT value="23"/>
<REMOTE_CONSOLE_PORT_STATUS value="2"/>
<!-- Firmware support information for next 6 tags: -->
<!-- iLO 2 - All versions. -->
<!-- iLO - Version 1,50 and later. -->
<!-- RILOE II - None. -->
<REMOTE_CONSOLE_ENCRYPTION value="Yes"/>
<MIN_PASSWORD value="8"/>
<ILO_FUNCT_ENABLED value="Yes"/>
<VIRTUAL_MEDIA_PORT value="17988"/>
<F8_LOGIN_REQUIRED value="No"/>
<REMOTE_KEYBOARD_MODEL value="US"/>
<!-- Firmware support information for next 2 tags: -->
<!-- iLO 2 - All versions. -->
<!-- iLO - Version 1,50 and later. -->
<!-- RILOE II - Version 1.20 and later. -->
<PASSTHROUGH_CONFIG value="1"/>
<TERMINAL_SERVICES_PORT value="3389"/>
<!-- Firmware support information for next 5 tags: -->
<!-- iLO 2 - All versions. -->
<!-- iLO - Version 1.60 and later. -->
<!-- RILOE II - None. -->
<SSH_PORT value="22"/>
```

```
<SSH_STATUS value="Yes"/>
<SERIAL_CLI_STATUS value="3"/>
<SERIAL_CLI_SPEED value="1"/>
<RBSU_POST_IP value="Y"/>
<!-- Firmware support information for next tag: -->
<!-- iLO 2 - All versions. -->
<!-- iLO - None. -->
<!-- RILOE II - None. -->
<TELNET_ENABLE value="yes"/>
<!-- Firmware support information for next tag: -->
<!-- iLO 2 - All versions. -->
<!-- iLO - Version 1,75 and later. -->
<!-- RILOE II - None. -->
<!-- It can have the following three values -->
<!-- Disabled: Value = "No" -->
<!-- the mouse uses "relative" coordinates mode, -->
<!-- compatible with most host operating systems. -->
<!-- Enabled: Value = "Yes" -->
<!-- the mouse uses "absolute" coordinates mode, -->
<!-- eliminating synchronization issues -->
<!-- on supported operating systems -->
<!-- Automatic: Value = "Automatic" -->
<!-- iLO picks the appropriate mouse mode when -->
<!-- the iLO 2 driver is loaded on the host operating system.-->
<!-- The selected mode is persistent unless a different -->
<!-- mode is indicated when the OS driver is loaded or -->
<!-- if you choose another setting. -->
<HIGH_PERFORMANCE_MOUSE value="Automatic" />
<!-- Firmware support information for next 13 tags: -->
<!-- iLO 2 - Version 1.30 and later. -->
<!-- iLO - None. -->
<!-- RILOE II - None. -->
<ENFORCE_AES value="Y"/>
<AUTHENTICATION_FAILURE_LOGGING value="3"/>
<CONSOLE_CAPTURE_ENABLE value="Yes" />
<CONSOLE_CAPTURE_BOOT_BUFFER_ENABLE value="Yes" />
<CONSOLE_CAPTURE_FAULT_BUFFER_ENABLE value="Yes" />
<INTERACTIVE_CONSOLE_REPLAY_ENABLE value="Yes" />
<CONSOLE_CAPTURE_PORT value="17990" />
<CAPTURE_AUTO_EXPORT_ENABLE value="No" />
<CAPTURE_AUTO_EXPORT_LOCATION value="HTTP://1.1.1.1/folder/capture%h%t.ilo" />
<CAPTURE_AUTO_EXPORT_USERNAME value="username" />
<CAPTURE_AUTO_EXPORT_PASSWORD value="password" />
<SHARED_CONSOLE_ENABLE value="No" />
<SHARED_CONSOLE_PORT value="9300" />
<!-- Firmware support information for next two tags:-->
<!-- iLO 2 - Version 1.75 and later.-->
<!-- iLO - None. -->
```

```
<!-- RILOE II - None. -->
<KEY_UP_KEY_DOWN value="Yes"/>
<CAPTURE_MANUAL_EXPORT value="Yes"/>
<!-- Firmware support information for next tag: -->
<!-- iLO 2 - Version 1.30 and later. -->
<!-- iLO - Version 1,80 and later. -->
<!-- RILOE II - None. -->
<REMOTE_CONSOLE_ACQUIRE value="Yes" />
<!-- Firmware support information for next 13 tags: -->
<!-- iLO 2 - None. -->
<!-- iLO - None. -->
<!-- RILOE II - All versions. -->
<!--
<HOST_KEYBOARD_ENABLED value ="YES"/>
<REMOTE_KEYBOARD_MODEL value = "US"/>
<POCKETPC_ACCESS value = "YES"/>
<CIPHER_STRENGTH value = "128"/>
<SNMP_ADDRESS_1 value = "123.124.125.126"/>
<SNMP_ADDRESS_2 value = "test"/>
<SNMP_ADDRESS_3 value = "dest"/>
<OS_TRAPS value = "Y"/>
<RIB_TRAPS value = "N"/>
<CIM_SECURITY_MASK value = "3"/>
<EMS_STATUS value = "Y" />
<BYPASS_POWER_CABLE_REPORTING value = "N" />
<SNMP_PASSTHROUGH_STATUS value = "Y" />
-->
</MOD_GLOBAL_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

Ab Version 1.50 von iLO 2 unterstützt Virtual Serial Port die automatische Aktivierung und Deaktivierung der Software-Ablaufkontrolle. Standardmäßig ist diese Funktion deaktiviert. Sie können diese Konfigurationsoption nur mit RIBCL aktivieren. Um diese Option zu aktivieren, führen Sie folgendes Skript aus:

Beispiel 2:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
<RIB_INFO MODE="write">
<MOD_GLOBAL_SETTINGS>
<VSP_SOFTWARE_FLOW_CONTROL value="Yes"/>
</MOD_GLOBAL_SETTINGS>
<RESET_RIB />
</RIB_INFO>
</LOGIN>
</RIBCL>
```

Mit der Ausgabe von iLO 2 Version 2.06 kann der Virtual Media-Port über RIBCL aktiviert oder deaktiviert werden. Standardmäßig ist dieser Port „Enabled“ (Aktiviert). Um diesen Port zu deaktivieren, führen Sie folgendes Skript aus:

Beispiel 3:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="Administrator" PASSWORD="password">
  <RIB_INFO MODE="write">
    <MOD_GLOBAL_SETTINGS>
      <VMEDIA_DISABLE VALUE = "Yes"/>
    </MOD_GLOBAL_SETTINGS>
  </RIB_INFO>
  </LOGIN>
</RIBCL>
```

Ab iLO 2 Version 2.09 kann die Eingabeaufforderung `hpiLO` von SMASH CLP um den Servernamen erweitert werden. Diese erweiterte Eingabeaufforderung wird über RIBCL aktiviert oder deaktiviert. Standardmäßig ist diese Funktion deaktiviert. Um die erweiterte Eingabeaufforderung zu aktivieren, führen Sie folgendes Skript aus:

Beispiel 4:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="Administrator" PASSWORD="password">
  <RIB_INFO MODE="write">
    <MOD_GLOBAL_SETTINGS>
      <ENHANCED_CLI_PROMPT_ENABLE VALUE = "Yes"/>
    </MOD_GLOBAL_SETTINGS>
  </RIB_INFO>
  </LOGIN>
</RIBCL>
```

MOD_GLOBAL_SETTINGS-Parameter

Die folgenden Parameter sind optional. Wenn Sie keinen Parameter angeben, wird der Parameterwert für die angegebene Einstellung beibehalten.

SESSION_TIMEOUT: Legt das maximale Sitzungs-Timeout in Minuten fest. Die akzeptierten Werte sind 0, 15, 30, 60 und 120. Ein Wert von 0 gibt ein unbegrenztes Timeout an.

ILO_FUNCT_ENABLED: Legt fest, ob die Lights-Out Funktionalität für iLO 2 aktiviert oder deaktiviert ist. Mögliche Werte sind `yes` oder `No`. Bei diesem Parameter sind Groß- und Kleinschreibung bedeutsam.

F8_PROMPT_ENABLED: Legt fest, ob die F8-Eingabeaufforderung für die ROM-basierte Konfiguration während des POST angezeigt wird. Die möglichen Werte sind `Yes` oder `No`.

F8_LOGIN_REQUIRED: Legt fest, ob für den Zugriff auf das iLO 2 RBSU Anmeldeinformationen erforderlich sind. Die möglichen Werte sind `Yes` oder `No`.

REMOTE_CONSOLE_PORT_STATUS: Legt das Verhalten des Remote Console Dienstes fest. Die folgenden Werte sind möglich:

- 0: Keine Änderung
- 1: Deaktiviert (Der Remote Console Port ist deaktiviert. Dadurch wird verhindert, dass Remote Console- und Telnet-Sitzungen verwendet werden.)
- 2: Automatisch (Dies ist die Standardeinstellung. Der Remote Console Port wird erst geöffnet, wenn eine Remote Console-Sitzung gestartet wird.)
- 3: Aktiviert (Der Remote Console Port ist immer aktiviert. Dadurch wird ermöglicht, dass Remote Console- und Telnet-Sitzungen verwendet werden.)

REMOTE_CONSOLE_ENCRYPTION: Legt fest, ob Remote Console Daten verschlüsselt werden. Die möglichen Werte sind `Yes` oder `No`.

REMOTE_CONSOLE_ACQUIRE: Legt fest, ob die Remote Console Erfassungsoperation aktiviert oder deaktiviert ist. Die möglichen Werte sind `Yes` oder `No`.

PASSTHROUGH_CONFIG: Legt das Verhalten eines Microsoft Terminal Services-Client fest. Folgende Werte sind möglich:

- 0: Keine Änderung
- 1: Deaktiviert (Die Terminal Services-Funktion ist deaktiviert.)
- 2: Automatisch (Der Terminal Services-Client wird beim Starten von Remote Console gestartet.)
- 3: Aktiviert (Dies ist die Standardeinstellung. Die Terminal Services-Funktion ist aktiviert, wird jedoch beim Starten von Remote Console nicht automatisch gestartet.)

HTTPS_PORT: Gibt die HTTPS- (SSL) Portnummer an.

HTTP_PORT: Gibt die HTTP-Portnummer an.

REMOTE_CONSOLE_PORT: Gibt den für die Remote Console verwendeten Port an.

TERMINAL_SERVICES_PORT: Gibt den für Terminal Services verwendeten Port an.

VIRTUAL_MEDIA_PORT: Gibt den für virtuelle Medien verwendeten Port an.

HINWEIS: Wenn Port-Änderungen festgestellt werden, wird der iLO 2 Managementprozessor nach erfolgreicher Ausführung des Skripts neu gestartet, um die Änderungen anzuwenden.

`MIN_PASSWORD`: Gibt an, wie viele Zeichen für alle Benutzerkennwörter erforderlich sind. Der Wert kann zwischen 0 und 39 Zeichen liegen.

`AUTHENTICATION_FAILURE_LOGGING`: Legt die Protokollierungskriterien für fehlgeschlagene Authentifizierungen fest. Die folgenden Werte sind möglich:

- 0: Deaktiviert
- 1: Aktiviert (zeichnet jede fehlgeschlagene Authentifizierung auf)
- 2: Aktiviert (zeichnet jede zweite fehlgeschlagene Authentifizierung auf)
- 3: Aktiviert (zeichnet jede dritte fehlgeschlagene Authentifizierung auf, dies ist der Standardwert.)
- 5: Aktiviert (zeichnet jede fünfte fehlgeschlagene Authentifizierung auf)

REMOTE_KEYBOARD_MODEL: Legt das Remote-Tastaturmodell (die Tastatursprache) für den Remote Console Betrieb fest. Die folgenden Werte sind möglich:

US	Niederländisch (Belgien)	Englisch (GB)
Dänisch	Finnisch	French (Französisch)
Französisch (Kanada)	German (Deutsch)	Italian (Italienisch)
Japanese (Japanisch)	Spanisch (Lateinamerika)	Portugiesisch (Portugal)
Spanish (Spanisch)	Schwedisch	Französisch (Schweiz)
Deutsch (Schweiz)		

SSH_PORT: Gibt den Port an, der für die SSH-Verbindung auf dem iLO 2 verwendet wird. Wenn dieser Wert geändert wird, ist ein Neustart des Prozessors erforderlich.

SSH_STATUS: Legt fest, ob SSH aktiviert wird. Mögliche Werte sind `Yes` und `No`, um die SSH-Funktion zu aktivieren bzw. deaktivieren.

SERIAL_CLI_STATUS: Gibt den Status der Befehlszeilenschnittstelle (CLI) an. Die folgenden Werte sind möglich:

- 0: Keine Änderung
- 1: Deaktiviert
- 2: Aktiviert (Keine Authentifizierung erforderlich)

- 3: Aktiviert (Authentifizierung erforderlich)

SERIAL_CLI_SPEED: Gibt die CLI-Portgeschwindigkeit an. Die folgenden Werte sind möglich:

- 0: Keine Änderung
- 1: 9.600 Bit/s
- 2: 19.200 Bit/s
- 3: 38.400 Bit/s
- 4: 57.600 Bit/s
- 5: 115.200 Bit/s

ENFORCE_AES: Bestimmt, ob iLO 2 die Verwendung der AES/3DES-Verschlüsselungsstärke über die iLO 2 Benutzeroberfläche und SSH- und XML-Verbindungen erzwingt. Die möglichen Werte sind `Yes` oder `No`.

VSP_SOFTWARE_FLOW_CONTROL: Legt fest, ob Virtual Serial Port die Software-Ablaufkontrolle automatisch aktiviert und deaktiviert. Die möglichen Werte sind `Yes` oder `No`.

VMEDIA_DISABLE: Gibt an, ob der Virtual Media Port deaktiviert ist. Die möglichen Werte sind `Yes` oder `No`. Standardmäßig ist der Port auf `No` (Nein = aktiviert) eingestellt. Um den Port zu deaktivieren, stellen Sie den Wert auf `Yes` ein.

ENHANCED_CLP_PROMPT_ENABLE: Gibt an, ob die erweiterte CLI-Eingabeaufforderung aktiviert oder deaktiviert werden muss. Die möglichen Werte sind `Yes` und `No`. Die Funktion ist standardmäßig deaktiviert. Um die Funktion zu aktivieren, stellen Sie den Wert auf `Yes` ein.

ENHANCED_CLI_PROMPT_ENABLE: Gibt an, ob die erweiterte CLI-Eingabeaufforderung aktiviert oder deaktiviert werden muss. Die möglichen Werte sind „Yes“ oder „No“. Die Funktion ist standardmäßig deaktiviert. Um die Funktion zu aktivieren, stellen Sie den Wert auf `Yes` ein.

MOD_GLOBAL_SETTINGS-Laufzeitfehler

Folgende MOD_GLOBAL_SETTINGS-Fehlermeldungen können u. a. angezeigt werden:

- RIB information is open for read-only access. (RIB-Informationen sind schreibgeschützt.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- User does not have correct privilege for action. `CONFIG_ILO_PRIV` required. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion. CONFIG_ILO_PRIV erforderlich.)
- Unrecognized keyboard model. (Tastaturmodell nicht erkannt.)

GET_SNMP_IM_SETTINGS

Mit dem Befehl GET_SNMP_IM_SETTINGS werden die SNMP IM-Einstellungen des jeweiligen iLO 2 abgefragt. Damit der Befehl GET_SNMP_IM_SETTINGS richtig übersetzt wird, muss er innerhalb eines RIB_INFO-Befehlsblocks stehen; RIB_INFO MODE kann auf „read“ oder „write“ gesetzt sein.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="read">
<GET_SNMP_IM_SETTINGS/>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

GET_SNMP_IM_SETTINGS-Parameter

Keine

GET_SNMP_IM_SETTINGS-Laufzeitfehler

Keine

GET_SNMP_IM_SETTINGS-Rückmeldungen

Eine mögliche GET_SNMP_IM_SETTINGS-Rückmeldung lautet:

```
<GET_SNMP_IM_SETTINGS>
<SNMP_ADDRESS_1 VALUE="192.168.125.121"/>
<SNMP_ADDRESS_2 VALUE="192.168.125.122"/>
<SNMP_ADDRESS_3 VALUE="192.168.125.123"/>
<OS_TRAPS VALUE="Yes"/>
<RIB_TRAPS VALUE="No"/>
<SNMP_PASSTHROUGH_STATUS VALUE="No"/>
<WEB_AGENT_IP_ADDRESS VALUE="192.168.125.120"/>
<CIM_SECURITY_MASK VALUE="3"/>
</GET_SNMP_IM_SETTINGS>
```

MOD_SNMP_IM_SETTINGS

Mit dem Befehl MOD_SNMP_IM_SETTINGS werden Einstellungen für SNMP und Insight Manager geändert. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines RIB_INFO-Befehlsblocks stehen, und RIB_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="write">
<MOD_SNMP_IM_SETTINGS>
<WEB_AGENT_IP_ADDRESS value="192.168.125.120"/>
<SNMP_ADDRESS_1 value="192.168.125.121"/>
<SNMP_ADDRESS_2 value="192.168.125.122"/>
<SNMP_ADDRESS_3 value="192.168.125.123"/>
<OS_TRAPS value="Yes"/>
<RIB_TRAPS value="No"/>
<SNMP_PASSTHROUGH_STATUS value="No"/>
<CIM_SECURITY_MASK value="3"/>
</MOD_SNMP_IM_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

MOD_SNMP_IM_SETTINGS-Parameter

Alle nachfolgend genannten Parameter sind optional. Wenn ein Parameter nicht angegeben wird, wird der Parameterwert für die angegebene Einstellung beibehalten.

WEB_AGENT_IP_ADDRESS: Gibt die Adresse der Web-fähigen Agenten an. Der Wert für dieses Element hat eine maximale Länge von 50 Zeichen. Es darf nur eine gültige IP-Adresse angegeben werden. Bei Eingabe einer leeren Zeichenfolge wird der aktuelle Wert gelöscht.

SNMP_ADDRESS_1, SNMP_ADDRESS_2 und SNMP_ADDRESS_3: Die Adressen, die die an den Benutzer gesendeten Traps erhalten. Bei diesen Parametern kann es sich um beliebige gültige IP-Adressen mit max. 50 Zeichen handeln.

OS_TRAPS: Bestimmt, ob der Benutzer SNMP-Traps erhalten soll, die vom Betriebssystem erstellt werden. Die möglichen Werte sind Yes oder No. Standardmäßig ist der Wert auf No eingestellt.

RIB_TRAPS: Bestimmt, ob der Benutzer SNMP-Traps erhalten soll, die von RIB erzeugt werden. Die möglichen Werte sind Yes oder No. Standardmäßig ist der Wert auf No eingestellt.

SNMP_PASSTHROUGH_STATUS: Bestimmt, ob iLO SNMP-Anforderungen vom Betriebssystem empfangen bzw. an dieses senden kann. Standardmäßig ist der Wert auf Yes eingestellt.

CIM_SECURITY_MASK: Es kann eine ganze Zahl zwischen 0 und 4 angegeben werden. Mögliche Werte:

- 0: Keine Änderung
- 1: Keine (Es werden keine Daten zurückgegeben.)
- 2: Niedrig (Name und Statusdaten werden zurückgegeben.) Verknüpfungen sind vorhanden, falls SNMP-Pass-Through unterstützt wird. Andernfalls sind Server und Managementprozessor separate Elemente in der Geräteliste.
- 3: Mittel (iLO 2 und Serververknüpfungen werden angegeben, die Übersichtsseite ist jedoch weniger detailliert als bei hoher Sicherheit.)
- 4: Hoch (Verknüpfungen sind vorhanden, und die Zusammenfassungsseite enthält alle Daten.)

Die einzelnen Werte geben den Umfang der über den HTTP-Port zurückgegebenen Daten an.

MOD_SNMP_IM_SETTINGS-Laufzeitfehler

Folgende MOD_SNMP_IM_SETTINGS-Fehlermeldungen können angezeigt werden:

- RIB information is open for read-only access. (RIB-Informationen sind schreibgeschützt.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) CONFIG_ILO_PRIV required. (CONFIG_ILO_PRIV erforderlich.)

UPDATE_RIB_FIRMWARE

Der Befehl UPDATE_RIB_FIRMWARE kopiert eine bestimmte Datei auf iLO 2, startet den Aktualisierungsvorgang und führt nach der erfolgreichen Image-Aktualisierung einen Board-Neustart durch. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines RIB_INFO-Befehlsblocks stehen, und RIB_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Beispiel 1:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="write">
 <!-- Firmware support information for next tag:-->
 <!-- iLO 2 - 1.70 and later. For servers with TPM enabled.-->
 <!-- iLO - None -->
 <!-- Riloe II - None -->
<TPM_ENABLED VALUE="Yes"/>
<UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\firmware.bin"/>
</RIB_INFO>
</LOGIN>
```

```
</RIBCL>
```

Wenn Sie ein XML-Skript zum Aktualisieren der iLO 2 Firmware senden, überprüft die iLO 2 Firmware den TPM-Konfigurationsstatus der Options-ROM-Messung. Wenn der Befehl aktiviert ist, gibt die iLO 2 Firmware die gleiche Warnmeldung wie auf der Webbenutzeroberfläche zurück. Sie können den Befehl TPM_ENABLE in die Skriptdatei einfügen. HP empfiehlt, Firmwareaktualisierungen über die XML-Skriptsyntax auszuführen. Damit die Firmwareaktualisierung fortgesetzt werden kann, müssen Sie für TPM_ENABLE den Wert `Y` oder `Yes` festlegen.

Beispiel 2:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
<RIB_INFO MODE="write">
<TPM_ENABLE ="Yes"/>
<UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\xl170\iLO2_170D.bin"/>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

UPDATE_RIB_FIRMWARE-Parameter

IMAGE_LOCATION enthält den vollständigen Pfadnamen der Firmware-Aktualisierungsdatei.

TPM_ENABLE ermöglicht der Firmware, die Aktualisierung fortzusetzen, wenn die Options-ROM-Messung aktiviert ist. Damit die Firmwareaktualisierung fortgesetzt werden kann, müssen Sie für TPM_ENABLE den Wert `Y` oder `Yes` festlegen.

UPDATE_RIB_FIRMWARE-Laufzeitfehler

Folgende UPDATE_RIB_FIRMWARE-Fehlermeldungen können angezeigt werden:

- `RIB information is open for read-only access. Write access is required for this operation.`
- `Unable to open the firmware image update file.`
- `Unable to read the firmware image update file.`
- `The firmware upgrade file size is too big.`
- `The firmware image file is not valid.`
- `A valid firmware image has not been loaded.`
- `The flash process could not be started.`
- `IMAGE_LOCATION must not be blank.`
- `User does not have correct privilege for action. CONFIG_ILO_PRIV required.`

GET_FW_VERSION

Mit dem Befehl GET_FW_VERSION werden die jeweiligen iLO 2 Firmware-Informationen abgefragt. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines RIB_INFO-Befehlsblocks stehen; RIB_INFO MODE muss auf „read“ oder „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="read">
<GET_FW_VERSION/>
```

```
</RIB_INFO>
</LOGIN>
</RIBCL>
```

GET_FW_VERSION-Parameter

Keine

GET_FW_VERSION-Laufzeitfehler

Keine

GET_FW_VERSION-Rückmeldungen

In der Antwort werden die folgenden Informationen zurückgegeben:

```
<GET_FW_VERSION
FIRMWARE_VERSION = <Firmwareversion>
FIRMWARE_DATE = <Firmwaredatum>
MANAGEMENT_PROCESSOR = <Management-Prozessor-Typ>
/>
```

HOTKEY_CONFIG

Der Befehl HOTKEY_CONFIG konfiguriert die Remote Console Hotkey-Einstellungen in iLO 2. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines RIB_INFO-Befehlsblocks stehen; RIB_INFO MODE muss dabei auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Großbuchstaben werden nicht unterstützt und automatisch in Kleinbuchstaben umgewandelt. Wenn Sie doppelte oder einfache Anführungszeichen verwenden, müssen sie sich vom Begrenzungszeichen unterscheiden. Bei Angabe einer leeren Zeichenfolge wird der aktuelle Wert gelöscht.

Eine vollständige Liste der Fehler finden Sie unter „Unterstützte Hotkeys“.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="write">
<HOTKEY_CONFIG>
<CTRL_T value="CTRL,ALT,ESC"/>
<CTRL_U value="L_SHIFT,F10,F12"/>
<CTRL_V value=""/>
<CTRL_W value=""/>
<CTRL_X value=""/>
<CTRL_Y value=""/>
</HOTKEY_CONFIG>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

HOTKEY_CONFIG-Parameter

Alle nachfolgend genannten Parameter sind optional. Wenn ein Parameter nicht angegeben wird, wird der Parameterwert für die angegebene Einstellung beibehalten.

CTRL_T: Gibt die Einstellungen für den Hotkey CTRL_T an. Die Einstellungen müssen durch Kommata getrennt werden. Beispiel: `CTRL_T="CTRL,ALT,ESC."` Für jeden Hotkey können maximal fünf Tastatureingaben konfiguriert werden.

CTRL_U: Gibt die Einstellungen für den Hotkey CTRL_U an. Die Einstellungen müssen durch Kommata getrennt werden. Beispiel: `CTRL_U="CTRL,ALT,ESC."` Für jeden Hotkey können maximal fünf Tastatureingaben konfiguriert werden.

CTRL_V: Gibt die Einstellungen für den Hotkey CTRL_V an. Die Einstellungen müssen durch Kommata getrennt werden. Beispiel: `CTRL_V="CTRL,ALT,ESC.` Für jeden Hotkey können maximal fünf Tastatureingaben konfiguriert werden.

CTRL_W: Gibt die Einstellungen für den Hotkey CTRL_W an. Die Einstellungen müssen durch Kommata getrennt werden. Beispiel: `CTRL_W="CTRL,ALT,ESC."` Für jeden Hotkey können maximal fünf Tastatureingaben konfiguriert werden.

CTRL_X: Gibt die Einstellungen für den Hotkey CTRL_X an. Die Einstellungen müssen durch Kommata getrennt werden. Beispiel: `CTRL_X="CTRL,ALT,ESC."` Für jeden Hotkey können maximal fünf Tastatureingaben konfiguriert werden.

CTRL_Y: Gibt die Einstellungen für den Hotkey CTRL_Y an. Die Einstellungen müssen durch Kommata getrennt werden. Beispiel: `CTRL_Y="CTRL,ALT,ESC."` Für jeden Hotkey können maximal fünf Tastatureingaben konfiguriert werden.

HOTKEY_CONFIG-Laufzeitfehler

Folgende HOTKEY_CONFIG-Fehlermeldungen können angezeigt werden:

- `RIB information is open for read-only access. Write access is required for this operation.`
- `The hot key parameter specified is not valid.`
- `Invalid number of hot keys. The maximum allowed is five.`
- `User does not have correct privilege for action. CONFIG_ILO_PRIV required.`

Unterstützte Hotkeys

Im Bildschirm „Program Remote Console Hot Keys“ (Hotkeys für Remote Console programmieren) können Sie maximal sechs verschiedene Hotkey-Sätze für die Verwendung in einer Remote Console-Sitzung definieren. Jeder Hotkey stellt eine Kombination aus bis zu 5 verschiedenen Tasten dar, die an den Host-Computer gesendet werden, wenn während einer Remote Console-Sitzung der Hotkey gedrückt wird. Die gewählte Tastenkombination (alle Tasten gleichzeitig gedrückt) wird stattdessen übertragen. Eine vollständige Liste der Fehler finden Sie unter „Unterstützte Hotkeys“. In der folgenden Tabelle sind die Tasten aufgeführt, die in einer Remote Console Hotkey-Folge kombiniert werden können.

ESC	F12	:	o
L_ALT	" " (Leertaste)	<	p
R_ALT	!	>	q
L_UMSCHALT	#	=	r
R_UMSCHALT	$	?	s
EINFG	%	@	t
ENTF	&	[	u
POS1	~	]	v
ENDE	(	\	w
BILD-AUF	)	^	x
BILD-AB	*	_	J

EINGABE	+	a	z
TAB	-	b	{
BREAK	.	c	}
F1	/	d	|
F2	0	e	;
F3	1	f	'
F4	2	g	L_STRG
F5	3	h	R_STRG
F6	4	i	NUM PLUS
F7	5	j	NUM MINUS
F8	6	k	FESTSTELL
F9	7	l	RÜCKTASTE
F10	8	m	S-ABF
F11	9	n	

LICENSE

Mit dem Befehl LICENSE werden die erweiterten Funktionen von iLO aktiviert bzw. deaktiviert. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines RIB_INFO-Befehlsblocks stehen, und RIB_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Auf einem ProLiant BL Class Server ist kein Lizenzschlüssel erforderlich. Die erweiterten Funktionen werden automatisch aktiviert.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="write">
<LICENSE>
<ACTIVATE KEY="11111222223333344444455555"/>
</LICENSE>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

LICENSE-Parameter

Wenn auf ACTIVATE ein gültiger Wert für KEY folgt, wird die Lizenz für iLO 2 Advanced Pack aktiviert.

KEY gibt den Lizenzschlüsselwert an. Der Schlüssel muss als durchgehende Zeichenfolge eingegeben werden. Der Schlüsselwert darf nicht durch Kommata, Punkte oder sonstige Zeichen getrennt werden. Der Schlüssel muss 25 Zeichen lang sein. Sonstige zum Trennen des Schlüsselwerts eingegebene Zeichen werden als Teil des Schlüssels interpretiert, was zu einer falschen Schlüsseleingabe führt.

LICENSE-Laufzeitfehler

Folgende LICENSE-Fehlermeldungen können angezeigt werden:

- `License key error.`

- `License is already active.`
- `User does not have correct privilege for action. CONFIG_ILO_PRIV required.`

INSERT_VIRTUAL_MEDIA

Dieser Befehl meldet iLO 2 den Speicherort eines Disketten-Image. Der Befehl INSERT_VIRTUAL_MEDIA muss innerhalb eines RIB_INFO-Elements ausgegeben werden, und RIB_INFO muss sich im Schreibmodus befinden.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN = "adminname" PASSWORD = "password">
<RIB_INFO MODE = "write">
<INSERT_VIRTUAL_MEDIA DEVICE="FLOPPY" IMAGE_URL= "http://servername/path/to/file"/>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

INSERT_VIRTUAL_MEDIA-Parameter

DEVICE gibt das virtuelle Medienziellaufwerk an. Mögliche Werte sind FLOPPY und CDROM. Wird dieser Parameter nicht angegeben, wird FLOPPY übernommen. Bei diesem Wert wird zwischen Groß- und Kleinschreibung unterschieden.

IMAGE_URL gibt den URL des Disketten-Image an. Der URL muss folgendes Format haben:

`Protokoll://Benutzername:Kennwort@Hostname:Port/Dateiname,cgi-helper`

- Das Protokoll muss angegeben werden (entweder http oder https).
- Die Angabe Benutzername:Kennwort ist optional.
- Der Hostname muss angegeben werden.
- Die Portangabe ist optional.
- Der Dateiname muss angegeben werden.
- Die Angabe für CGI Helper ist optional.

Darüber hinaus kann der Dateiname Token enthalten, die in hostspezifische Zeichenfolgen aufgelöst werden:

- `%m`: Wird zur iLO 2 MAC-Adresse erweitert.
- `%i`: Wird zur vierteiligen iLO 2 IP-Adresse in Punktschreibweise erweitert.
- `%h`: Wird zum iLO 2 Hostnamen erweitert.

Beispiele:

```
http://john:abc123@imgserver.company.com/disk/win98dos.bin,/cgi-bin/hpvfhelp.pl
http://imgserver.company.com/disk/boot%m.bin
```

Dieser Befehl gibt nur den Pfad des Image an, das verwendet werden soll. Soll eine Verbindung zwischen Image und Server hergestellt werden, muss die entsprechende BOOT_OPTION über den Befehl SET_VM_STATUS angegeben werden. Wird BOOT_OPTION auf BOOT_ONCE gesetzt und der Server wird erneut gestartet, so wird das Image bei einem weitere Serverstart „ausgeworfen“.

INSERT_VIRTUAL_FLOPPY-Laufzeitfehler

Folgende INSERT_VIRTUAL_FLOPPY-Fehlermeldungen können angezeigt werden:

- `RIB information is open for read-only access. (RIB-Informationen sind schreibgeschützt.)`
  `Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)`

- IMAGE_URL must not be blank. (IMAGE_URL darf nicht leer sein.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.)
  VIRTUAL_MEDIA_PRIV required. (VIRTUAL_MEDIA_PRIV erforderlich.)
- Unable to parse Virtual Media URL (URL des virtuellen Mediums kann nicht übersetzt werden.)
- An invalid Virtual Floppy option has been given. (Ungültige Option für virtuelles Diskettenlaufwerk.)
- Virtua Media already connected through s script. (Virtuelles Medium bereits über ein Skript verbunden.)
  You must eject or disconnect before inserting new media. (Sie müssen das virtuelle Medium auswerfen oder die Verbindung unterbrechen, bevor ein neues Medium eingelegt werden kann.)

EJECT_VIRTUAL_MEDIA

Mit EJECT_VIRTUAL_MEDIA wird ein virtuelles Medien-Image ausgeworfen, falls eines eingelegt wurde. Der Befehl EJECT_VIRTUAL_MEDIA muss innerhalb eines RIB_INFO-Elements ausgegeben werden, und RIB_INFO muss sich im Schreibmodus befinden.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Admin" PASSWORD="Password">
<RIB_INFO MODE="write">
<EJECT_VIRTUAL_MEDIA DEVICE="FLOPPY"/>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

EJECT_VIRTUAL_MEDIA-Parameter

DEVICE gibt das virtuelle Medienziellaufwerk an. Mögliche Werte sind FLOPPY und CDROM. Wird dieser Parameter nicht angegeben, wird FLOPPY übernommen. Bei diesem Wert wird zwischen Groß- und Kleinschreibung unterschieden.

EJECT_VIRTUAL_MEDIA-Laufzeitfehler

Folgende EJECT_VIRTUAL_MEDIA-Fehler sind möglich:

- RIB information is open for read-only access. (RIB-Informationen sind schreibgeschützt.)
  Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.)
  VIRTUAL_MEDIA_PRIV required. (VIRTUAL_MEDIA_PRIV erforderlich.)
- No image present in the Virtual Floppy drive. (Kein Image im virtuellen Medienlaufwerk vorhanden.)
- An invalid Virtual Floppy option has been given. (Ungültige Option für virtuelles Diskettenlaufwerk.)

GET_VM_STATUS

GET_VM_STATUS gibt den Status des virtuellen Medienlaufwerks zurück. Dieser Befehl muss sich innerhalb eines RIB_INFO-Elements befinden.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN = "adminname" PASSWORD = "password">
<RIB_INFO MODE = "read">
<GET_VM_STATUS DEVICE="CDROM"/>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

GET_VM_STATUS-Parameter

DEVICE gibt das virtuelle Medienziellaufwerk an. Mögliche Werte sind FLOPPY und CDROM. Wird dieser Parameter nicht angegeben, wird FLOPPY übernommen. Bei diesem Wert wird zwischen Groß- und Kleinschreibung unterschieden.

GET_VM_STATUS-Laufzeitfehler

Folgende GET_VM_STATUS-Fehlermeldung kann angezeigt werden:

```
An invalid Virtual Floppy option has been given. (Ungültige Option für virtuelles Diskettenlaufwerk.)
```

GET_VM_STATUS-Rückmeldungen

In der Rückmeldung wird der aktuelle Status der virtuellen Medien angegeben. Der Parameter VM_APPLET zeigt an, ob ein virtuelles Mediengerät bereits über das Virtual Media-Applet verbunden ist. Gilt VM_APPLET = CONNECTED, so wird das virtuelle Mediengerät bereits verwendet und kann nicht über ein Skript für virtuelle Medien oder XML-Befehle für virtuelle Medien verbunden werden. Der Parameter DEVICE zeigt an, für welches Gerät diese Rückmeldung bestimmt ist. Mit BOOT_OPTION werden die aktuellen Einstellungen angegeben. BOOT_ALWAYS gibt an, dass der Server beim Starten immer auf das virtuelle Mediengerät zurückgreift. BOOT_ONCE gibt an, dass der Server einmal über das virtuelle Gerät startet und die Verbindung der virtuellen Medien beim darauf folgenden Serverstart trennt. NO_BOOT bedeutet, dass die virtuellen Medien während eines Serverneustarts nicht verbunden werden. Der Parameter WRITE_PROTECT_FLAG zeigt an, ob das Image für virtuelle Medien geschrieben werden kann. Der Parameter IMAGE_INSERTED gibt an, ob das virtuelle Mediengerät über ein Skript für virtuelle Medien oder den XML-Befehl für virtuelle Medien verbunden ist.

Eine mögliche GET_VM_STATUS-Rückmeldung lautet:

```
VM_APPLET = CONNECTED | DISCONNECTED
DEVICE = FLOPPY | CDROM
BOOT_OPTION = BOOT_ALWAYS | BOOT_ONCE | NO_BOOT
WRITE_PROTECT_FLAG = YES | NO
IMAGE_INSERTED = YES | NO
```

HINWEIS: Wenn als Startoption BOOT_ONCE ausgewählt ist, werden nach dem Starten des Servers alle Parameter für Skripts für virtuelle Medien auf die Standardeinstellungen zurückgesetzt. Dies gilt insbesondere für die Parameter BOOT_OPTION = NO_BOOT, WRITE_PROTECT = NO und IMAGE_INSERTED = NO.

SET_VM_STATUS

Der Befehl SET_VM_STATUS setzt den Status des virtuellen Medienlaufwerks. Dieser Befehl muss innerhalb eines RIB_INFO-Elements ausgegeben werden, und RIB_INFO muss sich im Schreibmodus befinden. Alle Parameter in diesem Befehl sind optional.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN = "adminname" PASSWORD = "password">
<RIB_INFO MODE = "write">
<SET_VM_STATUS DEVICE = "CDROM">
<VM_BOOT_OPTION value = "BOOT_ONCE"/>
<VM_WRITE_PROTECT value = "Y"/>
</SET_VM_STATUS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

SET_VM_STATUS-Parameter

DEVICE gibt das virtuelle Medienziellaufwerk an. Mögliche Werte sind FLOPPY und CDROM. Wird dieser Parameter nicht angegeben, wird FLOPPY übernommen. Bei diesem Wert wird zwischen Groß- und Kleinschreibung unterschieden.

VM_BOOT_OPTION: Bestimmt den Parameter für die Bootoption des virtuellen Mediums. Mögliche Werte sind BOOT_ALWAYS, BOOT_ONCE oder NO_BOOT. Über diese Werte wird gesteuert, wie sich das virtuelle Mediengerät während der Startphase des Servers verhält. Die Einstellung dieser Werte hat keinen Einfluss auf den aktuellen Status des virtuellen Mediengeräts. Diese Einstellungen werden nur dann wirksam, wenn das virtuelle Mediengerät beim Starten des Servers verbunden ist.

- BOOT_ALWAYS: Stellt für VM_BOOT_OPTION die Option BOOT_ALWAYS ein. Das virtuelle Mediengerät wird beim Starten des Servers immer verbunden. Das virtuelle Mediengerät wird nicht sofort verbunden, wenn VM_BOOT_OPTION eingestellt wird. Das virtuelle Mediengerät wird beim nächsten Starten des Servers nach Einstellen von VM_BOOT_OPTION verbunden.
- BOOT_ONCE: Stellt für VM_BOOT_OPTION die Option BOOT_ONCE ein. Das virtuelle Mediengerät wird beim nächsten Starten des Servers verbunden, jedoch bei weiteren Startvorgängen nicht mehr verbunden. Die Option BOOT_ONCE dient dazu, das virtuelle Mediengerät einmal zu starten, das Gerät zu verwenden, während der Server läuft, und bei nachfolgenden Neustarts des Servers das virtuelle Mediengerät nicht mehr zu verbinden. Das virtuelle Mediengerät wird nicht sofort verbunden, wenn VM_BOOT_OPTION eingestellt wird. Das virtuelle Mediengerät wird beim nächsten Starten des Servers nach Einstellen von VM_BOOT_OPTION verbunden. Nachdem der Server einmal mit dem verbundenen virtuellen Mediengerät gestartet wurde, wird das virtuelle Mediengerät bei nachfolgenden Neustarts des Servers nicht mehr verbunden. Die folgenden Einstellungen für das virtuelle Mediengerät werden auf die Standardwerte zurückgesetzt:
  - BOOT_OPTION = NO_BOOT
  - IMAGE_INSERTED = NO
- NO_BOOT: Stellt wird für VM_BOOT_OPTION die Option NO_BOOT ein. Das virtuelle Mediengerät wird beim nächsten Starten des Servers nicht verbunden. Die Verbindung zum virtuellen Mediengerät wird nicht sofort getrennt, wenn VM_BOOT_OPTION eingestellt wird. Die Verbindung zum virtuellen Mediengerät wird beim nächsten Starten des Servers nach Einstellen von VM_BOOT_OPTION getrennt. Nachdem der Server einmal gestartet wurde, wird das virtuelle Mediengerät nicht verbunden und die folgenden Einstellungen für das virtuelle Mediengerät werden auf die Standardwerte zurückgesetzt:
  - BOOT_OPTION = NO_BOOT
  - IMAGE_INSERTED = NO

Neben den VM_BOOT_OPTIONS sind auch connect und disconnect mögliche Werte. Die Einstellungen connect und disconnect können in derselben Weise zur Steuerung des virtuellen Mediengeräts verwendet werden wie im Virtual Media Applet. Wenn die Parameter CONNECT oder DISCONNECT eingestellt werden, wird das virtuelle Mediengerät sofort mit dem Server verbunden bzw. von ihm getrennt.

- CONNECT: Stellt für VM_BOOT_OPTION die Option CONNECT (Verbinden) ein. Das virtuelle Mediengerät wird sofort mit dem Server verbunden. Die Einstellung von VM_BOOT_OPTION auf CONNECT entspricht dem Klicken auf die Geräte-Schaltfläche **Connect** (Verbinden) im Virtual Media Applet. Nachdem für VM_BOOT_OPTION der Wert `CONNECT` eingestellt wurde, zeigt der Befehl VM_GET_STATUS für VM_BOOT_OPTION die Option BOOT_ALWAYS an. Dies ist so konzipiert und zeigt, dass das virtuelle Mediengerät wie das virtuelle Mediengerät im Applet verbunden ist, das bei jedem Starten des Servers verbunden wird.

- DISCONNECT: Stellt für VM_BOOT_OPTION die Option DISCONNECT (Trennen) ein. Das virtuelle Mediengerät wird sofort vom Server getrennt. Die Einstellung von VM_BOOT_OPTION auf DISCONNECT entspricht dem Klicken auf die Geräte-Schaltfläche **Disconnect** (Trennen) im Virtual Media Applet. Außerdem ist das Einstellen der Option DISCONNECT für VM_BOOT_OPTION gleichbedeutend mit der Ausgabe des Befehls EJECT_VIRTUAL_MEDIA. Wenn für VM_BOOT_OPTION die Option DISCONNECT eingestellt wurde, wird das virtuelle Mediengerät nicht verbunden und die folgenden Einstellungen für das virtuelle Mediengerät werden auf die Standardwerte zurückgesetzt:
  - BOOT_OPTION = NO_BOOT
  - IMAGE_INSERTED = NO

VM_WRITE_PROTECT: Setzt das Schreibschutz-Flag für das virtuelle Diskettenlaufwerk. Für das virtuellen CD-ROM-Laufwerk ist dieser Wert nicht weiter von Bedeutung. Die möglichen Werte sind `Y` oder `N`.

SET_VM_STATUS-Laufzeitfehler

Folgende Laufzeitfehler sind möglich:

- `RIB information is open for read-only access. Write access is required for this operation.`
- `User does not have correct privilege for action. VIRTUAL_MEDIA_PRIV required.`
- `An invalid Virtual Media option has been given.`

CERTIFICATE_SIGNING_REQUEST

Dieser Befehl fordert ein Zertifikat von iLO 2 an. Wenn dieser Befehl eingeht, erzeugt iLO 2 eine Anforderung für eine Zertifikatsunterschrift. Die Anforderung wird wieder an den Benutzer übergeben, der im Tag CERTIFICATE_SIGNING_REQUEST angegeben ist. Für diesen Befehl ist die Version 2.26 oder höher von `CPQLOCFG` erforderlich.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN = "adminname" PASSWORD = "password">
<RIB_INFO MODE = "write">
<CERTIFICATE_SIGNING_REQUEST/>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

CERTIFICATE_SIGNING_REQUEST-Parameter

Für diesen Befehl sind keine Parameter vorhanden.

CERTIFICATE_SIGNING_REQUEST-Fehler

- `Certificate request generation will be available after iLO 2 completes generating SSL keys. Close all active Remote Console sessions and try again later (around 2 minutes for 1024 bit keys and 10 minutes for 2048 bit keys).`

CSR_CERT_SETTINGS

Mit diesem Befehl werden die Zertifikateinstellungen festgelegt, mit denen iLO 2 Zertifikatsignierungsanforderungen erstellt werden. Benutzer können einen benutzerdefinierten

Antragstellernamen wählen oder iLO 2 zum Verwenden gespeicherter Standardwerte auffordern. Benutzer können außerdem zwischen 2048-Bit- oder 1024-Bit-Privatschlüssellänge wählen. Bei Eingang dieses Befehls werden die Einstellungen für vom Benutzer ausgegebene Zertifikate im NVRAM-Speicher von iLO 2 gespeichert. Dieser Befehl erfordert CPQLOCFG, Version 2.26 oder höher.

Beispiel 1 (festgelegte Standardeinstellungen für die Zertifikatsignierungsanforderung):

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="write">
<CSR_CERT_SETTINGS>
<CSR_USE_CERT_CUSTOM_SUBJECT VALUE = "No"/>
<CSR_USE_CERT_2048PKEY VALUE = "Yes" />
<CSR_USE_CERT_FQDN VALUE = "Yes" />
</CSR_CERT_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

Beispiel 2 (festgelegte benutzerdefinierte Einstellungen für die Zertifikatsignierungsanforderung):

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="write">
<CSR_CERT_SETTINGS>
<CSR_USE_CERT_CUSTOM_SUBJECT VALUE = "Yes"/>
<CSR_USE_CERT_2048PKEY VALUE = "Yes" />
<CSR_SUBJECT_COUNTRY VALUE ="US"/>
<CSR_SUBJECT_STATE VALUE ="California"/>
<CSR_SUBJECT_LOCATION VALUE ="San Diego"/>
<CSR_SUBJECT_ORG_NAME VALUE ="Hewlett-Packard LLC"/>
<CSR_SUBJECT_ORGUNIT_NAME VALUE ="Server Group"/>
<CSR_SUBJECT_COMMON_NAME VALUE ="hp.ilo.com"/>
</CSR_CERT_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

CSR_CERT_SETTINGS-Parameter

Einige der folgenden Parameter können je nach der Einstellung der anderen Parameter weggelassen werden. Wenn sich der Benutzer für Antragsteller-Standardeinstellungen entscheidet, sind die CSR_SUBJECT_xxxx-Tags irrelevant. Wenn sich der Benutzer für benutzerdefinierte Antragsteller-Einstellungen entscheidet, ist das CSR_USE_CERT_FQDN-Tag irrelevant. Wenn der Benutzer keine Einstellungen für CSR_USE_CERT_FQDN (bei der Standardauswahl für den Antragsteller), CSR_USE_CERT_2048PKEY, anwendet, dann werden die vom System beibehaltenen Werte für diese Einstellungen verwendet. In einigen Feldern sind keine Nullwerte oder leeren Werte erlaubt. Folglich kann eine leere Zeichenfolge in einigen Feldern einen Fehler zurückgeben.

CSR_USE_CERT_CUSTOM_SUBJECT: Diese Einstellung gibt an, ob beim Erstellen einer Zertifikatsignierungsanforderung benutzerdefinierte oder Standarddaten für Antragsteller verwendet werden sollen. Die Werte sind „Yes“ (Ja), „No“ (Nein), „Default“ (Standard). Dabei wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn dieses Feld auf „Yes“ (Ja) eingestellt ist, sollte das Skript alle 6 CSR_SUBJECT_xxxx-Felder mit korrekten Werten enthalten. Wenn dieses Feld auf „Default“ (Standard) oder „No“ (Nein) eingestellt ist, sind die CSR_SUBJECT_xxxx-Felder irrelevant und werden nicht benötigt. Ein Eintrag in diesem Feld ist erforderlich.

CSR_USE_CERT_FQDN: Diese Einstellung gibt an, ob als gemeinsamer Zertifikatname bei der Erstellung einer Zertifikatsignierungsanforderung der vollqualifizierte Domänenname (FQDN) oder der Kurzname verwendet werden soll. Mögliche Werte sind „Yes“ oder „No“. Dabei wird nicht zwischen Groß- und Kleinschreibung unterschieden. Wenn CSR_USE_CERT_CUSTOM_SUBJECT

auf „Yes“ (Ja) eingestellt ist, dient dieses Feld keinem Zweck, da als gemeinsamer Zertifikatname der vom Benutzer in CSR_SUBJECT_COMMON_NAME vorgegebene Wert verwendet wird.

CSR_USE_CERT_2048PKEY: Diese Einstellung gibt an, ob für die Zertifikatsignierungsanforderung der Privatschlüssel mit 2048-Bit-Länge verwendet werden soll oder nicht. Die Zugriffsoptionen sind `Yes` oder `No`. Dabei wird nicht zwischen Groß- und Kleinschreibung unterschieden.

CSR_SUBJECT_COUNTRY: Dieses Feld ist 2 Zeichen lang. Die Zeichen müssen Großbuchstaben sein. Wenn Sie CSR_USE_CERT_CUSTOM_SUBJECT auf `Yes` (Ja) einstellen, ist ein Eintrag in diesem Feld erforderlich.

CSR_SUBJECT_STATE: Dieses Feld ist maximal 30 Zeichen lang. Es darf nur alphanumerische Zeichen und Leerstellen enthalten. Wenn Sie CSR_USE_CERT_CUSTOM_SUBJECT auf `Yes` (Ja) einstellen, ist ein Eintrag in diesem Feld erforderlich.

CSR_SUBJECT_LOCATION: Dieses Feld ist maximal 60 Zeichen lang. Es darf nur alphanumerische Zeichen, Satzzeichen und Leerstellen enthalten. Wenn Sie CSR_USE_CERT_CUSTOM_SUBJECT auf `Yes` (Ja) einstellen, ist ein Eintrag in diesem Feld erforderlich.

CSR_SUBJECT_ORG_NAME: Dieses Feld ist maximal 60 Zeichen lang. Es darf nur alphanumerische Zeichen, Satzzeichen und Leerstellen enthalten. Wenn Sie CSR_USE_CERT_CUSTOM_SUBJECT auf `Yes` (Ja) einstellen, ist ein Eintrag in diesem Feld erforderlich.

CSR_SUBJECT_ORGUNIT_NAME: Dieses Feld ist maximal 60 Zeichen lang. Es darf nur alphanumerische Zeichen, Satzzeichen und Leerstellen enthalten. Wenn Sie CSR_USE_CERT_CUSTOM_SUBJECT auf `Yes` (Ja) einstellen, ist ein Eintrag in diesem Feld erforderlich.

CSR_SUBJECT_COMMON_NAME: Dieses Feld ist maximal 60 Zeichen lang. Es darf nur alphanumerische Zeichen, Punkte und Bindestriche enthalten. Wenn Sie CSR_USE_CERT_CUSTOM_SUBJECT auf `Yes` (Ja) einstellen, ist ein Eintrag in diesem Feld erforderlich.

CSR_CERT_SETTINGS-Fehler

Folgende CSR_CERT_SETTINGS-Fehlermeldungen können angezeigt werden:

- `RIB information is open for read-only access. Write access is required for this operation.`
- `User does not have correct privilege for action. CONFIG_ILO_PRIV required.`
- `User supplied invalid fields.`
- `User supplied incomplete fields.`

GET_CERT_SUBJECT_INFO

Dieser Befehl dient zum Lesen der in iLO 2 gespeicherten Einstellungen für die Zertifikatsignierungsanforderung. Wird in iLO 2 bereits eine benutzerdefinierte Einstellung gespeichert, werden mit diesem Befehl die Details abgerufen. Die Anforderung wird wieder an den Benutzer übergeben, der im Tag CERTIFICATE_SUBJECT_INFO angegeben ist. Für diesen Befehl ist die Version 2.26 oder höher von CPQLOCFG erforderlich.

Beispiel:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <RIB_INFO MODE="read">
    <GET_CERT_SUBJECT_INFO/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

GET_CERT_SUBJECT_INFO-Parameter

Für diesen Befehl sind keine Parameter vorhanden.

GET_CERT_SUBJECT_INFO-Fehler

Für diesen Befehl sind keine Fehler vorhanden.

IMPORT_CERTIFICATE

Der Befehl IMPORT_CERTIFICATE importiert ein unterzeichnetes Zertifikat in iLO 2. Dabei muss es sich um eine unterzeichnete Version einer Anforderung für eine Zertifikatsunterschrift handeln. Für diesen Befehl ist die Version 2.26 oder höher von `CPQLOCFG` erforderlich.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN = "adminname" PASSWORD = "password">
<RIB_INFO MODE = "write">
<IMPORT_CERTIFICATE>
-----BEGIN CERTIFICATE-----
….
-----END CERTIFICATE-----
</IMPORT_CERTIFICATE>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

IMPORT_CERTIFICATE-Parameter

Für diesen Befehl sind keine Parameter vorhanden.

IMPORT_CERTIFICATE-Fehler

Zu den möglichen IMPORT_CERTIFICATE-Fehlermeldungen gehören:

- `RIB information is open for read-only access. Write access is required for this operation.`
- `Error reading certificate: The imported certificate is invalid.`
- `Invalid certificate common name: The common name in the certificate does not match iLO 2's hostname.`
- `Certificate signature does not match private key: The certificate does not correspond to the private key stored in iLO 2.`

GET_TWOFACTOR_SETTINGS

Mit dem Befehl GET_TWOFACTOR_SETTINGS werden die 2-Faktor-Authentifizierungseinstellungen des jeweiligen iLO 2 angefordert. Damit dieser Befehl richtig übersetzt wird, muss GET_TWOFACTOR_SETTINGS innerhalb eines RIB_INFO-Befehlsblocks stehen; RIB_INFO MODE kann auf „read“ oder „write“ gesetzt sein.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="read">
<GET_TWOFACTOR_SETTINGS/>
</RIB_INFO>
</LOGIN>
```

```
</RIBCL>
```

GET_TWOFACTOR_SETTINGS-Parameter

Keine

GET_TWOFACTOR_SETTINGS-Laufzeitfehler

Keine

GET_TWO_FACTOR_SETTINGS-Rückmeldungen

Ab iLO 2 Version 1.20 können Benutzer mit einem digitalen Zertifikat authentifiziert werden. Abhängig von den 2-Faktor-Authentifizierungseinstellungen von iLO 2 enthält die Antwort auf GET_TWOFACTOR_SETTINGS jeweils andere Daten.

Beispiele für GET_TWOFACTOR_SETTINGS-Rückmeldungen sind:

Beispiel für eine Rückmeldung der 2-Faktor-Authentifizierungseinstellungen bei Standardeinstellungen:

```
<GET_TWOFACTOR_SETTINGS>
<AUTH_TWOFACTOR_ENABLE VALUE="N"/>
<CERT_REVOCATION_CHECK VALUE="N"/>
<CERT_OWNER_SUBJECT/>
</GET_TWOFACTOR_SETTINGS>
```

Beispiel für eine Rückmeldung der 2-Faktor-Authentifizierungseinstellungen, wobei das SAN-Feld im Zertifikat für die Verzeichnisauthentifizierung aktiviert ist:

```
<GET_TWOFACTOR_SETTINGS>
<AUTH_TWOFACTOR_ENABLE VALUE="Y"/>
<CERT_REVOCATION_CHECK VALUE="N"/>
<CERT_OWNER_SAN/>
</GET_TWOFACTOR_SETTINGS>
```

MOD_TWOFACTOR_SETTINGS

Mit dem Befehl MOD_TWOFACTOR_SETTINGS können die 2-Faktor-Authentifizierungseinstellungen modifiziert werden. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines RIB_INFO-Befehlsblocks stehen; RIB_INFO MODE muss dabei auf „write“ gesetzt sein. Sie müssen über die Berechtigung zum Konfigurieren von RILOE II verfügen, um diesen Befehl ausführen zu können. Wenn Sie den Wert von AUTH_TWOFACTOR_ENABLE ändern, wird iLO 2 zurückgesetzt, damit die neue Änderung wirksam werden kann.

HINWEIS: Die Befehle GET_TWOFACTOR_SETTINGS und MOD_TWOFACTOR_SETTINGS werden mit iLO Firmware Version 1.80 und höher und mit iLO 2 Firmware Version 1.10 und höher unterstützt. iLO 1.80 benötigt `CPQLOCFG` Version 2.24, iLO 1.10 `CPQLOCFG` Version 2.25.

Die 2-Faktor-Authentifizierung kann nur funktionieren, wenn ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle vorhanden ist. Die Einstellung AUTH_TWOFACTOR_ENABLE kann in iLO 2 nur auf `yes` gesetzt werden, wenn zuvor ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle konfiguriert wurde. Wenn lokale Benutzerkonten verwendet werden, muss das Client-Zertifikat außerdem einem lokalen Benutzerkonto zugeordnet sein. Die Zuordnung von Client-Zertifikaten zu lokalen Benutzerkonten ist nicht zwingend erforderlich, wenn iLO 2 die Verzeichnisauthentifizierung verwendet.

Damit die erforderliche Sicherheit gewährleistet ist, werden bei Aktivierung der 2-Faktor-Authentifizierung die folgenden Konfigurationsänderungen vorgenommen:

- „Remote Console Data Encryption“ (Datenverschlüsselung für Remote Console): `Yes` (dadurch wird Telnet-Zugriff deaktiviert)
- „Enable Secure Shell (SSH) Access“ (SSH-Zugriff aktivieren): `No`

- Serial Command Line Interface Status (Status der seriellen Befehlszeilenschnittstelle): `Disabled`

Wenn ein Telnet-, SSH- oder Serial CLI-Zugriff erforderlich ist, aktivieren Sie diese Einstellungen erneut, nachdem Sie die Option der 2-Faktor-Authentifizierung aktiviert haben. Da diese Zugriffsmethoden jedoch keine 2-Faktor-Authentifizierung ermöglichen, ist für den Zugriff auf iLO 2 mit Telnet, SSH oder Serial CLI lediglich eine einfache Authentifizierung erforderlich.

Wenn die 2-Faktor-Authentifizierung aktiviert ist, wird der Zugriff mit dem Dienstprogramm CPQLOCFG deaktiviert, da CPQLOCFG nicht alle Anforderungen für die Authentifizierung erfüllt. Das Utility HPONCFG hingegen ist funktionsbereit, da für die Ausführung dieses Utility Administratorberechtigungen auf dem Hostsystem erforderlich sind.

- Beispiel für das Aktivieren der 2-Faktor-Authentifizierung:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="write">
<MOD_TWOFACTOR_SETTINGS>
<AUTH_TWOFACTOR_ENABLE value="Yes"/>
<CERT_REVOCATION_CHECK value="No"/>
<CERT_OWNER_SAN/>
</MOD_TWOFACTOR_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

- Beispiel für das Importieren einer Zertifizierungsstelle und eines Benutzerzertifikats:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="test" PASSWORD="password">
<RIB_INFO MODE="write">
<MOD_TWOFACTOR_SETTINGS>
<CERT_OWNER_SAN/>
<IMPORT_CA_CERTIFICATE>
-----BEGIN CERTIFICATE-----
MIIEtzCCA5+gAwIBAgIQBGg9C0d7B5pF/l4bVA44hjANBgkqhkiG9w0BAQUFADBM
MRMwEQYKCZImiZPyLGQBGRYDTEFCMRUwEwYKCZImiZPyLGQBGRYFSkpSSUIxHjAc
...
9gVCPSOQUGMMZUeNYOBkTE0e+MrPGL+TqQEyIakF3rjA2PbL1uSY6d4dlCx7izkO
buEpHTPDqs9gZ3U5ht9bjES93UHnDENLopkZ2JgGwH8Y50eBnjq4xml9psbYZn5Y
yWpONE/IjIjJyww=
-----END CERTIFICATE-----
</IMPORT_CA_CERTIFICATE>
<IMPORT_USER_CERTIFICATE USER_LOGIN="apollo">
-----BEGIN CERTIFICATE-----
CZImiZPyLGQBGRYDTEFCMRUwEwYKCZImiZPyLGQBGRYFSkpSSUIxHjAcBgNVBAMT
ODU5NDRaMFYxEzARBgoJkiaJk
...
sjbbpNGpxGsK9GZi5j6UeOYklePyau0TJ3KIm2RPlR2C6XAGz2PTWgsxGlUP9lNH
bfz0+TD0JsschjqK23/vr2GxQ9C/835zRxdu5Dn8JGm3/dFHR2VxgCetIxyR9TQC
ZKTfvIa8N9KvMLZdclSj94jUyMZjYYmCWULW8WySMV70nclvrsI2hi3nwMtt2Zvj
WnbeZujBX9LGz3HdmghgUw4GTwYl3ZG88snuTyXliLPFXVYXvNAhGeWqXtrh7A90
3NprjG7DM1uw
```

```
-----END CERTIFICATE-----
</IMPORT_USER_CERTIFICATE>
</MOD_TWOFACTOR_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

MOD_TWOFACTOR_SETTINGS-Parameter

Alle nachfolgend genannten Parameter sind optional. Wenn ein Parameter nicht angegeben wird, wird der Parameterwert für die angegebene Einstellung beibehalten.

AUTH_TWOFACTOR_ENABLE: Aktiviert oder deaktiviert die 2-Faktor-Authentifizierung. Die möglichen Werte sind `Yes` oder `No`.

CERT_REVOCATION_CHECK> Bewirkt, dass iLO 2 das CRL-Distributionspunktattribut des Client-Zertifikats verwendet, um die Zertifikatsperrliste (CRL) herunterzuladen und sie auf Sperrungen zu überprüfen. Die möglichen Werte sind `Yes` oder `No`. Kann die Zertifikatsperrliste bei der Einstellung „Yes" (Ja) aus irgendeinem Grund nicht heruntergeladen werden, wird die Authentifizierung abgelehnt.

CERT_OWNER_SAN: Bewirkt, dass iLO 2 aus dem alternativen Antragstellernamen den Benutzerhauptnamen extrahiert und diesen für die Authentifizierung beim Laufwerk verwendet, z. B.: `username@domain.extension`.

CERT_OWNER_SUBJECT: Bewirkt, dass iLO 2 den eindeutigen Benutzernamen aus dem Antragstellernamen ableitet. Lautet der Name des Antragstellers `"/DC=com/DC=domain/OU=organization/CN=user"`, leitet iLO 2 Folgendes ab: `"CN=user,OU=organization,DC=domain,DC=com"`.

CERT_OWNER_SAN und CERT_OWNER_SUBJECT: Diese Einstellungen werden nur verwendet, wenn die Verzeichnisauthentifizierung aktiviert ist.

IMPORT_CA_CERTIFICATE: Importiert das Zertifikat als vertrauenswürdige Zertifizierungsstelle (Certificate Authority, CA) in iLO 2. iLO 2 lässt nur Client-Zertifikate zu, die von dieser CA stammen. Die 2-Faktor-Authentifizierung funktioniert nur dann, wenn in iLO 2 ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle konfiguriert wurde.

IMPORT_USER_CERTIFICATE: Importiert das Zertifikat in iLO 2 und ordnet es dem angegebenen lokalen Benutzer zu. Jeder Client, der anhand dieses Zertifikats authentifiziert wird, wird als der lokale Benutzer authentifiziert, dem dieses Zertifikat zugeordnet ist. Der `SHA1`-Hashing-Algorithmus dieses Zertifikats wird auf der Webseite **Modify User** (Benutzer ändern) des Benutzers angezeigt, dem es zugeordnet ist. Die Zuordnung von Client-Zertifikaten zu lokalen Benutzerkonten ist nicht zwingend erforderlich, wenn iLO 2 die Verzeichnisauthentifizierung verwendet. Sie ist nur dann erforderlich, wenn die Authentifizierung anhand lokaler Konten erwünscht ist.

IMPORT_CA_CERTIFICATE und IMPORT_USER_CERTIFICATE: Für diese Einstellungen müssen Base64-codierte Zertifikatdaten in die Tags `BEGIN` und `END` eingeschlossen werden.

MOD_TWOFACTOR_SETTINGS-Laufzeitfehler

Folgende MOD_TWOFACTOR_SETTINGS-Fehlermeldungen können angezeigt werden:

- `RIB information is open for read-only access. Write access is required for this operation.`
- `This setting cannot be changed while Shared Network port is enabled.`

  `iLO 2 has been configured to use shared network port, which will not function if Two-factor authentication is enabled.`

- `This setting cannot be enabled unless a trusted CA certificate has been imported.`

  `A CA certificate must be imported before enabling Two-factor authentication.`

- `User does not have correct privilege for action. CONFIG_ILO_PRIV required.`

DIR_INFO

Der Befehl DIR_INFO darf nur innerhalb eines LOGIN-Befehlsblocks stehen. Beim Übersetzen dieses Befehls wird die lokale Datenbank mit den Verzeichnisinformationen in den Speicher gelesen und deren Bearbeitung vorbereitet. Nur Befehle des Typs DIR_INFO sind innerhalb des DIR_INFO-Befehlsblocks gültig. Der Befehl DIR_INFO erzeugt eine Antwort, die die Host-Anwendung darüber informiert, ob die Datenbank erfolgreich gelesen wurde oder nicht. Wenn die Datenbank von einer anderen Anwendung überschrieben werden kann, schlägt dieser Aufruf fehl.

DIR_INFO erfordert einen MODE-Parameter mit einem Wert „read“ oder „write“. MODE ist ein spezifischer Zeichenfolgeparameter mit einer maximalen Länge von 10 Zeichen, der die beabsichtigte Verarbeitung der Informationen angibt.

Im Schreibmodus können iLO 2 Informationen sowohl gelesen als auch geschrieben werden. Im Lesemodus ist ein Ändern der iLO 2 Informationen nicht möglich.

Beispiel:

```
<DIR_INFO MODE="read">
…… DIR_INFO-Befehle ……
</DIR_INFO>
```

GET_DIR_CONFIG

Mit dem Befehl GET_DIR_CONFIG werden die jeweiligen iLO 2 Verzeichniseinstellungen abgefragt. Damit der Befehl GET_DIR_CONFIG richtig übersetzt wird, muss er innerhalb eines DIR_INFO-Befehlsblocks stehen; DIR_INFO MODE kann auf „read“ oder „write“ gesetzt sein.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<DIR_INFO MODE="read">
<GET_DIR_CONFIG/>
</DIR_INFO>
</LOGIN>
</RIBCL>
```

GET_DIR_CONFIG-Parameter

Keine

GET_DIR_CONFIG-Laufzeitfehler

Keine

GET_DIR_CONFIG-Rückmeldungen

Ab iLO 2 Version 1,80 ist eine Verzeichnisintegration in das HP Lights-Out Schema mit oder ohne Erweiterungen (schemafrei) möglich. Je nach Verzeichniskonfiguration enthält die Antwort auf GET_DIR_CONFIG jeweils andere Daten.

Mögliche GET_DIR_CONFIG-Rückmeldungen sind:

- Beispiel für eine Rückmeldung der Verzeichnisdienste (mit Schemaerweiterung):

```
<GET_DIR_CONFIG>
<DIR_AUTHENTICATION_ENABLED VALUE="Y"/>
<DIR_LOCAL_USER_ACCT VALUE="Y"/>
<DIR_SERVER_ADDRESS VALUE="adserv.demo.com"/>
<DIR_SERVER_PORT VALUE="636"/>
<DIR_OBJECT_DN VALUE="CN=SERVER1_RIB,OU=RIB,DC=HPRIB, DC=LABS"/>
<DIR_USER_CONTEXT1 VALUE="CN=Users0,DC=HPRIB0, DC=LABS"/>
<DIR_USER_CONTEXT2 VALUE="CN=Users1,DC=HPRIB1, DC=LABS"/>
<DIR_USER_CONTEXT3 VALUE=""/>
<DIR_ENABLE_GRP_ACCT VALUE="N"/>
</GET_DIR_CONFIG>
```

- Beispiel für eine Rückmeldung eines schemafreien Verzeichnisses (ohne Schemaerweiterung):

```
<GET_DIR_CONFIG>
<DIR_AUTHENTICATION_ENABLED VALUE="Y"/>
<DIR_LOCAL_USER_ACCT VALUE="Y"/>
<DIR_SERVER_ADDRESS VALUE="adserv.demo.com"/>
<DIR_SERVER_PORT VALUE="636"/>
<DIR_OBJECT_DN VALUE=""/>
<DIR_USER_CONTEXT1 VALUE="CN=Users,DC=demo,DC=com"/>
<DIR_USER_CONTEXT2 VALUE=""/>
<DIR_USER_CONTEXT3 VALUE=""/>
<DIR_ENABLE_GRP_ACCT VALUE="Y"/>
<DIR_GRPACCT1_NAME VALUE="CN=iLOAdmins,CN=Users,DC=demo,DC=com"/>
<DIR_GRPACCT1_PRIV VALUE="1,2,3,4,5"/>
<DIR_GRPACCT2_NAME VALUE="" />
<DIR_GRPACCT2_PRIV VALUE="" />
<DIR_GRPACCT3_NAME VALUE="" />
<DIR_GRPACCT3_PRIV VALUE="" />
<DIR_GRPACCT4_NAME VALUE="" />
<DIR_GRPACCT4_PRIV VALUE="" />
<DIR_GRPACCT5_NAME VALUE="" />
<DIR_GRPACCT5_PRIV VALUE="" />
<DIR_GRPACCT6_NAME VALUE="" />
<DIR_GRPACCT6_PRIV VALUE="" />
</GET_DIR_CONFIG><GET_DIR_CONFIG>
```

IMPORT_SSH_KEY

Der Befehl IMPORT_SSH_KEY importiert einen SSH_KEY und den zugehörigen iLO 2 Benutzernamen in iLO 2. Für diesen Befehl ist CPQLOCFG, Version 2.27 oder höher, erforderlich.

Nachdem Sie mit `ssh-keygen` einen SSH-Schlüssel und die Datei `key.pub` erstellt haben, müssen Sie wie folgt verfahren:

1. Machen Sie die Datei `key.pub` ausfindig, und fügen Sie ihren Inhalt zwischen `"-----BEGIN SSH KEY----"` und `"-----END SSH KEY-----"` ein. Die Datei beginnt mit dem Text `ssh-dss` oder `ssh-rsa`.

2. Hängen Sie am Ende des Schlüssels eine Leerstelle und einen gültigen iLO 2 Benutzernamen an, der auf der Seite **Modify User** (Benutzer ändern) angegeben wird. Beispiel:

   ```
   xxx. . .xxx ASmith.
   ```

   dabei sind *xxx. . .xxx* die Schlüsseldaten

Bei dem Benutzernamen wird zwischen Groß- und Kleinschreibung unterschieden. Er muss daher genauso wie der iLO 2 Benutzername geschrieben werden, damit der SSH-Schlüssel mit dem richtigen Benutzer verknüpft wird.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="write">
<IMPORT_SSH_KEY>
 -----BEGIN SSH KEY-----

ssh-dss ContentOfYourSSHKeyBALftnNE12JR8T8XQqyzqc1tt6FLFRXLRM5PJpOf/
IG4hN45+x+JbaqkhH+aKqFjlfO1NjszHrFN26H1AhWOjY2bEwj2wlJzBMAhXwnPQelQs
CnJDf+zCzbDn+5Va86+qWxm0lsDEChvZPM6wpjkXvHwuInjxTzOGQTq++vmYlo1/AAAA
FQC1MFaZjE995QhX9H1DaDzpsVTXvwAAAIA6ec/hAkas2N762jtlHvSuvZaQRzu49DOt
jXVIpNdJAhTC8O2505PzkGLf5qhrbDnusclCvoH7DuxyHjeOUVxbC5wFQBcGF4VnpYZ8
nGQGt9TQ0iUV+NRwn4CR5ESoi63zTJIvKIYZDT2ISeXhF2iU6txjZzdeEm7vQz3slaY3
dgAAAIAQ46i6FBzJAYXziF/qmWMt4y6SlylOQDAsxPKk7rpxegv8RlTeon/aeL7ojb9G
Q2xnEN5gobaNZxKz2d4/jwg3+qgTDT6V1G+b7+nEI/XHIc717/7oqgiOv4VE3WxN+HE9
JWsv2jwUpAzRGqJOoojRG/CCru0K+jgTOf/di1o0sw== ASmith
 -----END SSH KEY-----
</IMPORT_SSH_KEY>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

IMPORT_SSH_KEY-Parameter

Für diesen Befehl sind keine Parameter vorhanden.

IMPORT_SSH_KEY-Laufzeitfehler

Folgende IMPORT_SSH_KEY-Fehlermeldungen können angezeigt werden:

- `RIB information is open for read-only access. Write access is required for this operation.`
- `Error reading SSH Key: The imported SSH Key is invalid.`
- `Invalid iLO user name: The appended user name is not a valid iLO 2 user.`
- `No slots are available for storing additional SSH Key.`

MOD_DIR_CONFIG

Mit dem Befehl MOD_DIR_CONFIG können die Verzeichniseinstellungen von iLO 2 modifiziert werden. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines DIR_INFO-Befehlsblocks stehen; DIR_INFO MODE muss dabei auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<DIR_INFO MODE="write">
```

```
<MOD_DIR_CONFIG>
<DIR_AUTHENTICATION_ENABLED value="Yes"/>
<DIR_LOCAL_USER_ACCT value="Yes"/>

<!-- For schemaless Directory configuration, ensure that the following
settings are modified as required so that user can logon with Email
format and Netbios formats successfully:-->
<!-- 1. DIR_SERVER_ADDRESS value need to be set to directory server DNS Name or FQDN(Full qualified Domain
Name)-->
<!-- Please check and update the following iLO Network Settings. -->
<!-- 1.The domain name of iLO should match the domain of the directory server. -->

<!--  2.One of the primary, secondary or teritiary DNS server  must
have the same IP address as the Directory server.  -->
<DIR_SERVER_ADDRESS value="dlilo1.mycompu.com"/>
<DIR_SERVER_PORT value="636" />
<DIR_OBJECT_DN value="CN=server1_rib,OU=RIB, DC=mycompu,DC=com"/>
<DIR_OBJECT_PASSWORD value="password"/>
<DIR_USER_CONTEXT_1 value="CN=Users,DC=mycompu, DC=com"/>
<DIR_USER_CONTEXT_2 value="CN=Users2,DC=mycompu, DC=com"/>
<DIR_USER_CONTEXT_3 value="CN=Users3,DC=mycompu, DC=com"/>
<!-- Firmware support information for next 12 tags -->
<!-- iLO2 1.75 and later -->
<!-- iLO - None -->
<!-- Riloe II - None -->
<DIR_USER_CONTEXT_4 value="CN=Users4,DC=mycompu, DC=com"/>
<DIR_USER_CONTEXT_5 value="CN=Users5,DC=mycompu, DC=com"/>
<DIR_USER_CONTEXT_6 value="CN=Users6,DC=mycompu, DC=com"/>
<DIR_USER_CONTEXT_7 value="CN=Users7,DC=mycompu, DC=com"/>
<DIR_USER_CONTEXT_8 value="CN=Users8,DC=mycompu, DC=com"/>
<DIR_USER_CONTEXT_9 value="CN=Users9,DC=mycompu, DC=com"/>
<DIR_USER_CONTEXT_10 value="CN=Users10,DC=mycompu, DC=com"/>
<DIR_USER_CONTEXT_11 value="CN=Users11,DC=mycompu, DC=com"/>
<DIR_USER_CONTEXT_12 value="CN=Users12,DC=mycompu, DC=com"/>
<DIR_USER_CONTEXT_13 value="CN=Users13,DC=mycompu, DC=com"/>
<DIR_USER_CONTEXT_14 value="CN=Users14,DC=mycompu, DC=com"/>
<DIR_USER_CONTEXT_15 value="CN=Users15,DC=mycompu, DC=com"/>
<!-- Set the value to "NO" to enable the HP Extended Schema -->
<!-- and Value "YES" to enable Default Directory Login. -->
<!-- To set Group Accounts and privileges for Default Schema -->
<!-- run Mod_Schemaless_Directory.xml. -->
<DIR_ENABLE_GRP_ACCT value = "yes"/>
</MOD_DIR_CONFIG>
</DIR_INFO>
</LOGIN>
</RIBCL>
```

HINWEIS: Bei Verwendung der Verzeichnisintegration mit Schemaerweiterung sind die folgenden Tags unzulässig:

- `DIR_ENABLE_GRP_ACCT`
- `DIR_GRPACCT1_NAME`
- `DIR_GRPACCT1_PRIV`

Bei Verwendung von schemafreien Verzeichnissen sind die folgenden Tags unzulässig:

- `DIR_OBJECT_DN`
- `DIR_OBJECT_PASSWORD`

MOD_DIR_CONFIG-Parameter

Alle nachfolgend genannten Parameter sind optional. Wenn ein Parameter nicht angegeben wird, wird der Parameterwert für die angegebene Einstellung beibehalten.

DIR_AUTHENTICATION_ENABLED: Aktiviert bzw. deaktiviert die Verzeichnisauthentifizierung. Die möglichen Werte sind `yes` oder `No`.

DIR_ENABLE_GRP_ACCT: Bewirkt, dass iLO 2 die schemafreie Verzeichnisintegration verwendet. Die möglichen Werte sind `yes` oder `No`.

Bei Verwendung der schemafreien Verzeichnisintegration unterstützt iLO 2 variable Berechtigungen, die mit verschiedenen Verzeichnisgruppen verknüpft sind. Diese Gruppen sind im Verzeichnis enthalten, während die zugehörigen iLO 2 Mitgliedsberechtigungen in iLO 2 gespeichert sind.

- DIR_GRPACCT1_NAME: Identifiziert einen Gruppen-Container im Verzeichnis, wie z. B. Administratoren, Benutzer oder Power Users.
- DIR_GRPACCT1_PRIV: Ermöglicht die numerische Identifizierung von iLO 2 Berechtigungen für Gruppenmitglieder. Durch Hinzufügen mehrerer Werte können Sie die verschiedenen Berechtigungen miteinander kombinieren. Diese Berechtigungen werden als Liste kommaseparierter Zahlen (1,2,3,4,5) ausgedrückt, die sich auf Folgendes beziehen:
  - 1: Administer Group Accounts (Gruppenkonten verwalten)
  - 2: Remote Console Access (Remote Console Zugriff)
  - 3: Virtual Power and Reset (Virtueller Netzschalter und virtueller Reset)
  - 4: Virtual Media (Virtuelle Medien)
  - 5: Configure iLO 2 Settings (iLO 2 Einstellungen konfigurieren)

HINWEIS: Verwenden Sie die folgenden Tags **nicht** bei Einsatz der Verzeichnisintegration mit Schemaerweiterung:

- `DIR_ENABLE_GRP_ACCT`
- `DIR_GRPACCT1_NAME`
- `DIR_GRPACCT1_PRIV`

Verwenden Sie die folgenden Tags **nicht** bei Einsatz von schemenfreien Verzeichnissen:

- `DIR_OBJECT_DN`
- `DIR_OBJECT_PASSWORD`

DIR_LOCAL_USER_ACCT: Aktiviert bzw. deaktiviert lokale Benutzerkonten. Die möglichen Werte sind `Yes` oder `No`.

DIR_SERVER_ADDRESS gibt die Adresse des Verzeichnisservers an. Die Verzeichnisserveradresse wird als IP-Adresse oder DNS-Name angegeben.

DIR_SERVER_PORT: Gibt die Portnummer für die Verbindung zum Verzeichnisserver an. Dieser Wert wird vom Verzeichnisadministrator zur Verfügung gestellt. Der sichere LDAP-Port ist 636. Der Verzeichnisserver kann aber auch für eine andere Portnummer konfiguriert werden.

DIR_OBJECT_DN: Gibt den eindeutigen Namen von iLO 2 im Verzeichnisserver an. Dieser Wert wird vom Verzeichnisadministrator zur Verfügung gestellt. DNs (Distinguished Names) sind auf 256 Zeichen begrenzt.

DIR_OBJECT_PASSWORD: Gibt das Kennwort für das iLO 2 Objekt im Verzeichnisserver an. Kennwörter sind auf 39 Zeichen begrenzt.

DIR_USER_CONTEXT_1, DIR_USER_CONTEXT_2 und DIR_USER_CONTEXT_3: Geben durchsuchbare Kontexte für die Benutzersuche an, wenn ein Benutzer anhand von Verzeichnissen authentifiziert werden soll. Wenn der Benutzer nicht anhand des ersten Pfads gefunden werden kann, werden die im zweiten und dritten Pfad angegebenen Parameter verwendet. Die Werte dieser Parameter werden vom Verzeichnisadministrator zur Verfügung gestellt. Verzeichnis-Benutzerkontexte können jeweils eine maximale Länge von 128 Zeichen haben.

MOD_DIR_CONFIG-Laufzeitfehler

Es können folgende MOD_DIR_CONFIG-Fehlermeldungen angezeigt werden:

- Directory information is open for read-only access. (Verzeichnisinformationen sind schreibgeschützt.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) CONFIG_ILO_PRIV required. (CONFIG_ILO_PRIV erforderlich.)

RACK_INFO

Der Befehl RACK_INFO darf nur innerhalb eines LOGIN-Befehlsblocks stehen. Beim Übersetzen dieses Befehls wird die Datenbank mit der Rack-Infrastruktur in den Speicher gelesen und deren Bearbeitung vorbereitet. Nur Befehle des Typs RACK_INFO sind innerhalb des RACK_INFO-Befehlsblocks gültig. Der Befehl RACK_INFO erzeugt eine Antwort, die die Host-Anwendung darüber informiert, ob die Datenbank erfolgreich gelesen wurde oder nicht. Wenn die Datenbank von einer anderen Anwendung überschrieben werden kann, schlägt dieser Aufruf fehl.

Dieser Befehlsblock gilt nur für ProLiant BL Class Server. RACK_INFO erfordert einen MODE-Parameter mit einem Wert „read“ oder „write“. MODE ist ein spezifischer Zeichenfolgeparameter mit einer maximalen Länge von 10 Zeichen, der die beabsichtigte Verarbeitung der Informationen angibt.

Im Schreibmodus können iLO 2 Informationen sowohl gelesen als auch geschrieben werden. Im Lesemodus ist ein Ändern der iLO 2 Informationen nicht möglich.

Folgende RACK_INFO-Fehlermeldungen können angezeigt werden:

- Invalid Mode. (Ungültiger Modus.)
- Server is not a rack server; rack commands do not apply. (Server ist kein Rack-Server; Rack-Befehle sind nicht gültig.)

Beispiel:

```
<RACK_INFO MODE="read">
..... RACK_INFO-Befehle .....
</RACK_INFO>
```

GET_RACK_SETTINGS

Mit dem Befehl GET_RACK_SETTINGS werden die jeweiligen Rack-Einstellungen des jeweiligen iLO 2 abgefragt. Damit der Befehl GET_RACK_SETTINGS richtig übersetzt wird, muss er innerhalb

eines RACK_INFO-Befehlsblocks stehen; RACK_INFO MODE kann auf „read“ oder „write“ gesetzt sein.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RACK_INFO MODE="read">
<GET_RACK_SETTINGS/>
</RACK_INFO>
</LOGIN>
</RIBCL>
```

GET_RACK_SETTINGS-Parameter

Keine

GET_RACK_SETTINGS-Laufzeitfehler

Keine

GET_RACK_SETTINGS-Rückmeldungen

Eine mögliche GET_RACK_SETTINGS-Rückmeldung lautet:

```
<GET_RACK_SETTINGS>
<RACK_NAME VALUE="HPspace"/>
<ENCLOSURE_NAME VALUE="Home"/>
<ENCLOSURE_SN VALUE="44XP0606XP33"/>
<BAY_NAME VALUE="Library"/>
<BAY VALUE="2"/>
<FACILITY_PWR_SOURCE VALUE="N"/>
<RACK_AUTO_PWR VALUE="Y"/>
<SNMP_RACK_ALERTS VALUE="Y"/>
<LOG_RACK_ALERTS VALUE="N"/>
</GET_RACK_SETTINGS >
```

GET_DIAGPORT_SETTINGS

Mit dem GET_DIAGPORT_SETTINGS werden die Diagnoseport-Einstellungen des jeweiligen iLO abgefragt. Damit der Befehl GET_DIAGPORT_SETTINGS richtig übersetzt wird, muss er innerhalb eines RACK_INFO-Befehlsblocks stehen; RACK_INFO MODE kann auf „read“ oder „write“ gesetzt sein.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RACK_INFO MODE="read">
<GET_DIAGPORT_SETTINGS/>
</RACK_INFO>
</LOGIN>
</RIBCL>
```

GET_DIAGPORT_SETTINGS-Parameter

Keine

GET_DIAGPORT_SETTINGS-Laufzeitfehler

Keine

GET_DIAGPORT_SETTINGS-Rückmeldungen

Eine mögliche GET_DIAGPORT_SETTINGS-Rückmeldung lautet:

```
<GET_DIAGPORT_SETTINGS>
<DP_SPEED_AUTOSELECT value="No"/>
<DP_NIC_SPEED value="100"/>
<DP_FULL_DUPLEX value="Yes"/>
<DP_IP_ADDRESS value="192.168.142.56"/>
<DP_SUBNET_MASK value="255.255.0.0"/>
</GET_DIAGPORT_SETTINGS >
```

MOD_DIAGPORT_SETTINGS

Mit dem Befehl MOD_DIAGPORT_SETTINGS können die Einstellungen für das Diagnoseport-Netzwerk von iLO 2 modifiziert werden. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines RACK_INFO-Befehlsblocks stehen; RACK_INFO MODE muss dabei auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="username" PASSWORD="password">
<RACK_INFO MODE="write">
<MOD_DIAGPORT_SETTINGS>
<DP_SPEED_AUTOSELECT value="No"/>
<DP_NIC_SPEED value="100"/>
<DP_FULL_DUPLEX value="Yes"/>
<DP_IP_ADDRESS value="192.168.142.56"/>
<DP_SUBNET_MASK value="255.255.0.0"/>
</MOD_DIAGPORT_SETTINGS>
</RACK_INFO>
</LOGIN>
</RIBCL>
```

MOD_DIAGPORT_SETTINGS-Parameter

Alle nachfolgend genannten Parameter sind optional. Wenn ein Parameter nicht angegeben wird, wird der Parameterwert für die angegebene Einstellung beibehalten.

DP_SPEED_AUTOSELECT wird zum automatischen Auswählen der Transceiver-Geschwindigkeit verwendet. Mögliche Werte sind `Yes` und `No`. Dabei wird nicht zwischen Groß- und Kleinschreibung unterschieden.

DP_NIC_SPEED: Wird zum Einstellen der Transceiver-Geschwindigkeit verwendet, wenn DP_SPEED_AUTOSELECT auf `No` gesetzt wurde. Mögliche Werte sind 10 oder 100. Alle anderen Werte führen zu einem Syntaxfehler.

DP_FULL_DUPLEX legt fest, ob der iLO 2 Diagnoseport den Voll- oder Halbduplexmodus unterstützen soll. Dies trifft nur zu, wenn DP_SPEED_AUTOSELECT auf `No` gesetzt wurde. Mögliche Werte sind `Yes` und `No`. Dabei wird nicht zwischen Groß- und Kleinschreibung unterschieden.

DP_IP_ADDRESS dient zur Auswahl der IP-Adresse für den iLO 2 Diagnoseport. Bei Eingabe einer leeren Zeichenfolge wird die aktuelle Adresse nicht geändert. Das erwartete Format ist *XXX.XXX.XXX.XXX*.

DP_SUBNET_MASK dient zur Auswahl der Subnetzmaske für den iLO 2 Diagnoseport. Bei Eingabe einer leeren Zeichenfolge wird die aktuelle Adresse nicht geändert. Das erwartete Format ist *XXX.XXX.XXX.XXX*.

Nachdem das Skript erfolgreich ausgeführt wurde, wird der iLO 2 Managementprozessor neu gestartet, um die Änderungen anzuwenden.

MOD_DIAGPORT_SETTINGS-Laufzeitfehler

Folgende MOD_DIAGPORT_SETTINGS-Fehlermeldungen können angezeigt werden:

- iLO 2 information is open for read-only access. Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) CONFIG_ILO_PRIV required. (CONFIG_ILO_PRIV erforderlich.)

GET_ENCLOSURE_IP_SETTINGS

GET_ENCLOSURE_IP_SETTINGS fragt die Einstellungen für die statische IP-Schachtkonfiguration von iLO 2 ab. Dieses Attribut muss im RACK_INFO-Befehlsblock enthalten sein. Der RACK_INFO-Befehlsblock kann auf „read“ oder „write“ gesetzt sein.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Admin" PASSWORD="password">
<RACK_INFO MODE="write">
<GET_ENCLOSURE_IP_SETTINGS/>
</RACK_INFO>
</LOGIN>
</RIBCL>
```

GET_ENCLOSURE_IP_SETTINGS-Parameter

Keine

GET_ENCLOSURE_IP_SETTINGS-Rückmeldungen

Eine mögliche GET_ALL_USERS-Rückmeldung lautet:

```
<?xml version="1.0" ?>
<RIBCL VERSION="2.22">
<RESPONSE
STATUS="0x0000"
MESSAGE='No error'
/>
<GET_ENCLOSURE_IP_SETTINGS>
<BAY_ENABLE MASK="0x0002"/>
<IP_ADDRESS VALUE="170.100.12.101"/>
<SUBNET_MASK VALUE="255.255.255.0"/>
<GATEWAY_IP_ADDRESS VALUE="170.100.12.254"/>
<DOMAIN_NAME VALUE=""/>
<PRIM_DNS_SERVER VALUE="0.0.0.0"/>
<SEC_DNS_SERVER VALUE="0.0.0.0"/>
<TER_DNS_SERVER VALUE="0.0.0.0"/>
<PRIM_WINS_SERVER VALUE="0.0.0.0"/>
<SEC_WINS_SERVER VALUE="0.0.0.0"/>
```

```
<STATIC_ROUTE_1 DESTINATION="0.0.0.0"
GATEWAY="0.0.0.0"/>
<STATIC_ROUTE_2 DESTINATION="0.0.0.0"
GATEWAY="0.0.0.0"/>
<STATIC_ROUTE_3 DESTINATION="0.0.0.0"
GATEWAY="0.0.0.0"/>
</GET_ENCLOSURE_IP_SETTINGS>
</RIBCL>
```

MOD_ENCLOSURE_IP_SETTINGS

MOD_ENCLOSURE_IP_SETTINGS ändert die Einstellungen der statischen IP-Schachtkonfiguration. Dieser Befehl ist nur innerhalb eines RACK_INFO-Blocks gültig. Der angemeldete Benutzer muss über die Berechtigung „Configure iLO 2“ (iLO 2 konfigurieren) verfügen. Dieses Attribut muss im RACK_INFO-Befehlsblock enthalten sein. Der RACK_INFO-Befehlsblock kann auf „write“ gesetzt sein.

Beispiel für die Einstellungsänderung:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Admin" PASSWORD="password">
<RACK_INFO MODE="write">
<MOD_ENCLOSURE_IP_SETTINGS>
<BAY_ENABLE MASK="0x3FE"/>
<IP_ADDRESS VALUE="16.100.222.111"/>
<SUBNET_MASK VALUE="255.255.252.0"/>
<GATEWAY_IP_ADDRESS VALUE="16.100.222.1"/>
<DOMAIN_NAME VALUE="sum.one.here.now"/>
<PRIM_DNS_SERVER VALUE="16.11.1.111"/>
<SEC_DNS_SERVER VALUE=""/>
<TER_DNS_SERVER VALUE=""/>
<PRIM_WINS_SERVER VALUE="16.22.2.222"/>
<SEC_WINS_SERVER VALUE=""/>
<STATIC_ROUTE_1 DEST="16.33.3.33"
GATEWAY="16.100.11.11"/>
<STATIC_ROUTE_2 DEST="" GATEWAY=""/>
<STATIC_ROUTE_3 DEST="" GATEWAY=""/>
</MOD_ENCLOSURE_IP_SETTINGS>
</RACK_INFO>
</LOGIN>
</RIBCL>
```

Beispiel für die Änderung von Netzwerkeinstellungen zur Aktivierung der statischen IP-Schachtkonfiguration:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Admin" PASSWORD="password">
<RIB_INFO MODE="write">
<MOD_NETWORK_SETTINGS>
<ENCLOSURE_IP_ENABLE VALUE="Yes"/>
</MOD_NETWORK_SETTINGS>
</RIB_INFO>
</LOGIN>
```

```
</RIBCL>
```

MOD_ENCLOSURE_IP_SETTINGS-Parameter

BAY_ENABLEMASK aktiviert die Verwendung der Adressierung der statischen IP-Schachtkonfiguration. Das Attribut MASK ist eine 16-Bit-Zahl. Jedes Bit stellt einen Steckplatz im Gehäuse dar. Wenn das Bit gesetzt ist, nutzt der entsprechende Steckplatz die Einstellungen der statischen IP-Schachtkonfiguration. LSB repräsentiert Steckplatz 1. `MASK="0x0001"` beispielsweise gestattet nur Steckplatz 1, die statische IP-Schachtkonfiguration zu nutzen. Hier ist eine Hexadezimalzahl oder eine Dezimalzahl möglich. Dieser Befehl muss im MOD_ENCLOSURE_IP_SETTINGS-Block enthalten sein.

ENCLOSURE_IP_ENABLE aktiviert oder deaktiviert die Verwendung der statischen IP-Schachtkonfiguration. Dieses Attribut muss im MOD_NETWORK_SETTINGS-Block enthalten sein. Mögliche Werte sind `Y` und `N`. Dabei wird nicht zwischen Groß- und Kleinschreibung unterschieden. Dieses Attribut gilt nur für Blade-Server.

MOD_ENCLOSURE_IP_SETTINGS-Laufzeitfehler

Folgende Fehlermeldungen können angezeigt werden:

- Rack information is open for read-only access. (Rack-Informationen werden nur für Lesezugriff geöffnet.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) CONFIG_ILO_PRIV required. (CONFIG_ILO_PRIV erforderlich.)

GET_TOPOLOGY

Mit dem Befehl GET_TOPOLOGY wird der jeweilige iLO 2 aufgefordert, die aktuelle Topologie der Rack-Infrastruktur zurückzugeben. Damit der Befehl GET_TOPOLOGY richtig übersetzt wird, muss er innerhalb eines RACK_INFO-Befehlsblocks stehen; RACK_INFO MODE kann auf „read“ oder „write“ gesetzt sein.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RACK_INFO MODE="read">
<GET_TOPOLOGY/>
</RACK_INFO>
</LOGIN>
</RIBCL>
```

GET_TOPOLOGY-Parameter

Keine

GET_TOPOLOGY-Rückmeldung

Eine erfolgreiche Anfrage könnte so aussehen:

```
<RK_TPLGY CNT="3">
<RUID>xxxxxx</RUID>
<ICMB ADDR="0xAA55" MFG="232" PROD_ID="NNN" SER="123" NAME="Power_1">
<LEFT/>
<RIGHT ADDR="0xAB66" SER="123" NAME="Server_1"/>
</ICMB>
<ICMB ADDR="0xAB66" MFG="232" PROD_ID="NNN" SER="456" NAME="Server_1">
<LEFT ADDR="0xAA55" SER="123" NAME="Power_1"/>
```

```
<RIGHT ADDR="0xAC77" SER="123" NAME="Power_2"/>
</ICMB>
<ICMB ADDR="0xAC77" MFG="232" PROD_ID="NNN" SER="789" NAME="Power_2">
<RIGHT/>
</ICMB>
</RK_TPLGY>
```

MOD_BLADE_RACK

Mit dem Befehl MOD_BLADE_RACK werden die Einstellungen für die Rack-Infrastruktur geändert. Damit der Befehl MOD_BLADE_RACK richtig übersetzt wird, muss er innerhalb eines RACK_INFO-Befehlsblocks stehen, und RACK_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RACK_INFO MODE="write">
<MOD_BLADE_RACK>
<RACK_NAME value="CPQ_Rack_1"/>
<ENCLOSURE_NAME value="CPQ_Enclosure_1"/>
<BAY_NAME value="CPQ_Bay_5"/>
<FACILITY_PWR_SOURCE value="Yes"/>
<RACK_AUTO_PWR value="Yes"/>
<SNMP_RACK_ALERTS value="Yes"/>
<LOG_RACK_ALERTS value="Yes"/>
</MOD_BLADE_RACK>
</RACK_INFO>
</LOGIN>
</RIBCL>
```

MOD_BLADE_RACK-Parameter

Alle nachfolgend genannten Parameter sind optional. Wenn ein Parameter nicht angegeben wird, wird der Parameterwert für die angegebene Einstellung beibehalten.

RACK_NAME: Gibt den Namen an, unter dem Gehäuse innerhalb einer Rack-Infrastruktur zu einer logischen Gruppe zusammengefasst werden. Dieser Parameter kann eine beliebige Kombination druckbarer Zeichen enthalten und darf maximal 31 Zeichen umfassen.

ENCLOSURE_NAME: Gibt den Namen an, unter dem die ProLiant BL Class Server, die ein einzelnes Gehäuse bilden, zu einer logischen Gruppe zusammengefasst werden. Dieser Parameter kann eine beliebige Kombination druckbarer Zeichen enthalten und darf maximal 31 Zeichen umfassen.

BAY_NAME: Gibt den Namen an, mit dem ein bestimmter ProLiant BL Class Server identifiziert wird. Dieser Parameter kann eine beliebige Kombination druckbarer Zeichen enthalten und darf maximal 31 Zeichen umfassen.

FACILITY_PWR_SOURCE: Bestimmt die Stromquelle für die Blade-Server. Der Wert `Yes` gibt dem Server die Anweisung, Netzstrom aus dem Rack zu verwenden, und der Wert `No` gibt ihm die Anweisung, die Stromversorgungen der Server Blades zu verwenden.

RACK_AUTO_PWR: Legt fest, ob der Blade-Server beim Einsetzen in das Gehäuse automatisch hochgefahren werden soll. Der Wert `Yes` veranlasst den Blade-Server, automatisch hochzufahren und den normalen Startvorgang zu starten, wenn Strom anliegt. Der Wert `No` macht die manuelle Einschaltung des Blade-Servers erforderlich.

SNMP_RACK_ALERTS: Legt fest, ob Alarmmeldungen von der Rack-Infrastruktur an vom Benutzer definierte SNMP-Trap-Ziele weitergeleitet werden sollen. Mit dem Wert `Yes` wird die Weiterleitung von Rack-Alarmmeldungen aktiviert. Mit dem Wert `No` wird die Weiterleitung von Rack-Alarmmeldungen deaktiviert.

LOG_RACK_ALERTS: Legt fest, ob Alarmmeldungen von der Rack-Infrastruktur protokolliert werden sollen. Mit dem Wert `Yes` wird die Protokollierung von Rack-Alarmmeldungen im IML aktiviert. Mit dem Wert `No` wird die Protokollierung von Rack-Alarmmeldungen im IML deaktiviert.

MOD_BLADE_RACK-Laufzeitfehler

Folgende MOD_BLADE_RACK-Fehlermeldungen können angezeigt werden:

- `Rack information is open for read-only access. Write access is required for this operation.`
- `Rack Name too long.`
- `Enclosure Name too long.`
- `Bay Name too long.`
- `User does not have correct privilege for action. CONFIG_ILO_PRIV required.`

SERVER_INFO

Der Befehl SERVER_INFO darf nur innerhalb eines LOGIN-Befehlsblocks stehen. Nur Befehle des Typs SERVER_INFO sind innerhalb des SERVER_INFO-Befehlsblocks gültig.

SERVER_INFO erfordert einen MODE-Parameter mit einem Wert „read“ oder „write“. MODE ist ein spezifischer Zeichenfolgeparameter mit einer maximalen Länge von 10 Zeichen, der die beabsichtigte Verarbeitung der Informationen angibt.

Im Schreibmodus können iLO 2 Informationen sowohl gelesen als auch geschrieben werden. Im Lesemodus ist ein Ändern der iLO 2 Informationen nicht möglich.

Beispiel:

```
<SERVER_INFO MODE="read">
…… SERVER_INFO commands ……
</SERVER_INFO>
```

Beispiel für den Server-Reset:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="write">
<RESET_SERVER/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

Beispiel für die Einstellung der Host-Stromversorgung:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="write">
<!-- Modify the HOST_POWER attribute to toggle power on the host server -->
<!-- HOST_POWER="No" (Turns host server power off)       -->
<!-- A graceful shutdown will be attempted for ACPI-aware    -->
<!-- operating systems configured to support graceful shutdown. -->
<!-- HOST_POWER="Yes" (Turns host server power on) -->
```

```
<SET_HOST_POWER HOST_POWER="No"/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

GET_SERVER_NAME

Mit dem Befehl GET_SERVER_NAME wird der von iLO 2 verwendete Hostservername abgerufen. Sie können diesen Parameter mit verschiedenen Methoden festlegen. Dazu gehören der Befehl SERVER_NAME, das Host RBSU, die iLO 2 Browser-basierte Benutzeroberfläche und das Laden von HP ProLiant Management Agents.

Dieser Befehl wird ab der iLO 2 Firmware-Version 1.30 unterstützt. iLO bzw. RILOE II unterstützen ihn nicht.

Beispiel:

```
<RIBCL version="2.21">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
<SERVER_INFO MODE="READ">
<GET_SERVER_NAME />
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

iLO 2 wahrt an den verschiedenen Stellen, an denen der Servername verwendet wird, die Einheitlichkeit. Beim Host RBSU ist die Textlänge des Servernamens auf zwei Zeilen mit jeweils 14 Zeichen oder auf insgesamt 28 Zeichen beschränkt.

In der Regel leiten die HP ProLiant Management Agents das Servernamensattribut an iLO 2 weiter. Dieser Befehl kann unter Bedingungen verwendet werden, unter denen keine Management Agents verwendet werden. Das Host-Betriebssystem ist hiervon jedoch nicht betroffen.

GET_SERVER_NAME-Rückmeldung

GET_SERVER_NAME gibt ggf. den derzeit gespeicherten Servernamen zurück. Der Servername ist eine in Anführungszeichen stehende ASCII-Zeichenfolge und kann kein Netzwerkname sein. Beispiel:

```
<SERVER_NAME VALUE="Linux Development Host" />
```

GET_EVENT_NAME-Laufzeitfehler

Keine

SERVER_NAME

Mit dem Befehl SERVER_NAME wird das angegebene Servernamensattribut auf der Benutzeroberfläche und im Host RBSU zugewiesen. Die Einstellung wird nicht an das Betriebssystem des Hosts weitergeleitet und wirkt sich nicht auf das Betriebssystem des Hosts aus.

Um dieses Attribut über die Skript-Oberfläche ändern zu können, müssen Sie über die Berechtigung „Configure iLO Settings“ (iLO Einstellungen konfigurieren) verfügen. Für den Abschnitt SERVER_INFO muss der Modus WRITE festgelegt werden. Andernfalls wird ein Fehler zurückgegeben.

Beispiel:

```
<RIBCL version="2.21">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
<SERVER_INFO MODE="write">
<SERVER_NAME VALUE = "Exchange05" />
</SERVER_INFO>
```

```
</LOGIN
```

SERVER_NAME-Parameter

VALUE ist eine in Anführungszeichen stehende ASCII-Zeichenfolge, die insgesamt weniger als 50 Zeichen lang ist.

SERVER_NAME-Rückmeldung

Wenn dieses Attribut erfolgreich eingestellt wurde, wird keine spezifische Rückmeldung ausgegeben.

SERVER_NAME-Laufzeitfehler

- Wenn die Berechtigung „Configure iLO Settings“ (iLO Einstellungen konfigurieren) nicht vorhanden ist, wird ein Laufzeitfehler zurückgegeben.
- Wird SERVER_INFO nicht zum Schreiben geöffnet, wird ein Laufzeitfehler zurückgegeben.

GET_EMBEDDED_HEALTH

Mit dem Befehl GET_EMBEDDED_HEALTH werden Health-Informationen zum Server abgerufen. Damit der Befehl GET_EMBEDDED_HEALTH richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen. Sie können für SERVER_INFO MODE Lese- oder Schreibzugriff festlegen.

Beispiel:

```
<RIBCL VERSION="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="read">
<GET_EMBEDDED_HEALTH />
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

GET_EMBEDDED_HEALTH-Parameter

Keine

GET_EMBEDDED_HEALTH-Rückmeldungen

Eine mögliche GET_EMBEDDED_HEALTH_DATA-Rückmeldung lautet:

```
IP Address is: 16.100.000.192
cpqlocfg.exe: Receiving (116):
<?xml version="1.0" ?>
<RIBCL VERSION="2.22">
<RESPONSE
STATUS="0x0000"
MESSAGE='No error'
/>
</RIBCL>
cpqlocfg.exe: Receiving (116):
<?xml version="1.0" ?>
<RIBCL VERSION="2.22">
<RESPONSE
STATUS="0x0000"
MESSAGE='No error'
/>
```

```
<GET_EMBEDDED_HEALTH_DATA>
<FANS>
<FAN>
<LABEL VALUE = "Fan Block 1"/>
<ZONE VALUE = "Power Supply"/>
<STATUS VALUE = "Ok"/>
<SPEED VALUE = "25" UNIT="Percentage"/>
</FAN>
<FAN>
<LABEL VALUE = "Fan Block 2"/>
<ZONE VALUE = "CPU 2"/>
<STATUS VALUE = "Ok"/>
<SPEED VALUE = "37" UNIT="Percentage"/>
</FAN>
</FANS>
<TEMPERATURE>
<TEMP>
<LABEL VALUE = "Temp 1"/>
<LOCATION VALUE = "I/O Board"/>
<STATUS VALUE = "Ok"/>
<CURRENTREADING VALUE = "29" UNIT="Celsius"/>
<CAUTION VALUE = "65" UNIT="Celsius"/>
<CRITICAL VALUE = "70" UNIT="Celsius"/>
</TEMP>
<TEMP>
<LABEL VALUE = "Temp 2"/>
<LOCATION VALUE = "Ambient"/>
<STATUS VALUE = "Failed"/>
<CURRENTREADING VALUE = "66" UNIT="Celsius"/>
<CAUTION VALUE = "40" UNIT="Celsius"/>
<CRITICAL VALUE = "45" UNIT="Celsius"/>
</TEMP>
<TEMP>
<LABEL VALUE = "Temp 3"/>
<LOCATION VALUE = "CPU 1"/>
<STATUS VALUE = "Ok"/>
<CURRENTREADING VALUE = "36" UNIT="Celsius"/>
<CAUTION VALUE = "90" UNIT="Celsius"/>
<CRITICAL VALUE = "95" UNIT="Celsius"/>
</TEMP>
<TEMP>
<LABEL VALUE = "Temp 4"/>
<LOCATION VALUE = "CPU 1"/>
<STATUS VALUE = "Ok"/>
<CURRENTREADING VALUE = "32" UNIT="Celsius"/>
<CAUTION VALUE = "90" UNIT="Celsius"/>
<CRITICAL VALUE = "95" UNIT="Celsius"/>
</TEMP>
```

```
<TEMP>
<LABEL VALUE = "Temp 5"/>
<LOCATION VALUE = "Power Supply"/>
<STATUS VALUE = "Ok"/>
<CURRENTREADING VALUE = "32" UNIT="Celsius"/>
<CAUTION VALUE = "51" UNIT="Celsius"/>
<CRITICAL VALUE = "56" UNIT="Celsius"/>
</TEMP>
</TEMPERATURE>
<VRM>
</VRM>
<POWER_SUPPLIES>
</POWER_SUPPLIES>
<HEALTH_AT_A_GLANCE>
<FANS STATUS= "Ok"/>
<FANS REDUNDANCY= "Fully Redundant"/>
<TEMPERATURE STATUS= "FAILED"/>
<VRM STATUS= "Ok"/>
<POWER_SUPPLIES STATUS= "Ok"/>
<POWER_SUPPLIES REDUNDANCY= "unknown"/>
</HEALTH_AT_A_GLANCE>
</GET_EMBEDDED_HEALTH_DATA>
</RIBCL>
cpqlocfg.exe: Script succeeded on "16.100.000.192:000"
```

GET_POWER_READINGS

Mit dem Befehl GET_POWER_READINGS werden die aktuellen Werte der Server-Stromversorgung abgefragt.

GET_POWER_READINGS-Parameter

Keine

GET_POWER_READINGS-Rückmeldungen

Grundsätzlich verfügt der Befehl GET_POWER_READINGS über zwei Rückmeldungen, die davon abhängig sind, ob eine Lizenz für die erweiterte iLO 2 Funktionalität vorhanden ist.

Falls keine derartige Lizenz gegeben ist, lautet eine typische Rückmeldung folgendermaßen:

```
<?xml version="1.0" ?>
<RIBCL VERSION="2.22">
<RESPONSE
STATUS="0x0000"
MESSAGE='No error'
/>
<GET_POWER_READINGS>
<PRESENT_POWER_READING VALUE="275" UNIT="Watts"/>
<!--
Additional information is available with iLO 2 Advanced and iLO 2 Select licenses.
-->
</GET_POWER_READINGS>
```

```
</RIBCL>
cpqlocfg.exe: Script succeeded on "16.100.100.100:100"
```

Falls eine Lizenz für die erweiterte iLO 2 Funktionalität vorhanden ist, sieht eine typische Rückmeldung folgendermaßen aus:

```
<?xml version="1.0" ?>
<RIBCL VERSION="2.22">
<RESPONSE
STATUS="0x0000"
MESSAGE='No error'
/>
<GET_POWER_READINGS>
<PRESENT_POWER_READING VALUE="275" UNIT="Watts"/>
<AVERAGE_POWER_READING VALUE="278" UNIT="Watts"/>
<MAXIMUM_POWER_READING VALUE="283" UNIT="Watts"/>
<MINIMUM_POWER_READING VALUE="270" UNIT="Watts"/>
</GET_POWER_READINGS>
</RIBCL>
```

GET_POWER_CAP

Mit dem Befehl GET_POWER_CAP wird die Stromobergrenze des Servers angefordert. Damit der Befehl GET_POWER_CAP richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen; SERVER_INFO MODE kann auf „read“ oder „write“ gesetzt sein.

Beispiel:

```
<RIBCL VERSION="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="read">
<GET_POWER_CAP/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

GET_POWER_CAP-Parameter

Keine

GET_POWER_CAP-Rückmeldungen

Eine Obergrenze von Null bedeutet, dass auf dem Server derzeit keine Stromobergrenze festgelegt ist. Eine typische Antwort lautet:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="read">
<GET_POWER_CAP/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

SET_POWER_CAP

Mit dem Befehl SET_POWER_CAP wird die Stromobergrenze des Servers festgelegt. Damit der Befehl SET_POWER_CAP richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks

stehen, und SERVER_INFO MODE muss auf „write“ gesetzt sein. Sie müssen über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Diese Eigenschaft kann nicht eingestellt werden, wenn für den Server eine dynamische Obergrenze festgelegt ist. Die dynamische Stromobergrenze wird mit dem Onboard Administrator oder Insight Power Manager festgelegt und geändert.

Beispiel für das Deaktivieren der Stromobergrenze:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="write">
<SET_POWER_CAP POWER_CAP="300"/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

SET_POWER_CAP-Parameter

SET_POWER_CAP POWER_CAP ist die Stromobergrenze auf dem Server. Gültige Werte für die Stromobergrenze werden mithilfe eines auf dem Server durchgeführten Einschaltstromtests bestimmt. Mögliche Werte sind 0 zum Deaktivieren der Stromobergrenze oder ein numerischer Wert in Watt (der im Stromtest bestimmt wurde).

SET_POWER_CAP-Laufzeitfehler

Folgende SET_POWER_CAP-Fehlermeldungen können angezeigt werden:

- Server information is open for read-only access. (Server-Informationen werden für Lesezugriff geöffnet.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- Power Regulator feature is not supported on this server. (Die Power Regulator-Funktion wird auf diesem Server nicht unterstützt.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.)
- The power cap value is invalid. (Der Wert für die Stromobergrenze ist ungültig.)

GET_HOST_POWER_SAVER_STATUS

Mit dem Befehl GET_HOST_POWER_SAVER_STATUS wird der Status der Energieregelungsfunktion für den Prozessor des Servers abgefragt. Damit der Befehl GET_HOST_POWER_SAVER_STATUS richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen. Sie können für SERVER_INFO MODE Lese- oder Schreibzugriff festlegen.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="write">
<GET_HOST_POWER_SAVER_STATUS/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

GET_HOST_POWER_SAVER_STATUS-Parameter

Keine

GET_HOST_POWER_SAVER_STATUS-Laufzeitfehler

Folgende GET_HOST_POWER_SAVER_STATUS-Fehlermeldungen können angezeigt werden:

- Feature not supported (Funktion nicht unterstützt)

GET_HOST_POWER_SAVER_STATUS-Rückmeldungen

In den Antworten werden die folgenden Informationen zurückgegeben:

- ```
  <GET_HOST_POWER_SAVER
  HOST POWER_SAVER=
  "OFF"
  /
  >
  ```
- ```
  <GET_HOST_POWER_SAVER
  HOST POWER_SAVER=
  "MIN"
  /
  >
  ```
- ```
  <GET_HOST_POWER_SAVER
  HOST POWER_SAVER=
  "AUTO"
  /
  >
  ```

SET_HOST_POWER_SAVER

Der Befehl SET_HOST_POWER_SAVER wird verwendet, um die Power Regulator-Einstellung (Energieregelung) für den Serverprozessor zu aktivieren. Damit der Befehl SET_HOST_POWER_SAVER richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen, und SERVER_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum virtuellen Ein-/Ausschalten und Zurücksetzen verfügen, um diesen Befehl ausführen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="write">
<SET_HOST_POWER_SAVER HOST_POWER_SAVER="1"/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

SET_HOST_POWER_SAVER-Parameter

Der Befehl HOST_POWER_SAVER steuert die Dynamic Power Saver-Funktion (dynamischer Energiesparmodus) des Serverprozessors, wenn die Funktion unterstützt wird. Die folgenden Werte sind möglich:

- 1: Betriebssystemsteuermodus
- 2: Statischer HP Niedrigenergiemodus
- 3: Dynamischer HP Energiesparmodus
- 4: Statischer HP Hochenergiemodus
```

SET_HOST_POWER_SAVER-Laufzeitfehler

Folgende SET_HOST_POWER-Fehlermeldungen können angezeigt werden:

- Server information is open for read-only access. (Server-Informationen werden für Lesezugriff geöffnet.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- Power Regulator feature is not supported on this server. (Die Power Regulator-Funktion wird auf diesem Server nicht unterstützt.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) RESET_SERVER_PRIV required. (RESET_SERVER_PRIV erforderlich.)

GET_HOST_POWER_REG_INFO

Mit dem Befehl GET_HOST_POWER_REG_INFO werden Informationen zur Energieregelungsfunktion von iLO 2 abgefragt. Damit der Befehl GET_HOST_POWER_REG_INFO richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen, und SERVER_INFO MODE muss auf „write“ gesetzt sein.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="read">
<GET_HOST_POWER_REG_INFO/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

GET_HOST_POWER_REG_INFO-Parameter

Keine

SET_HOST_POWER_REG_INFO-Laufzeitfehler

GET_HOST_POWER_REG_INFO gibt einen Laufzeitfehler zurück, wenn keine Lizenz für die erweiterte iLO 2 Funktionalität gefunden wird. Beispiel:

```
<RIBCL VERSION="2.22">
<RESPONSE
STATUS="0x0043"
MESSAGE='This feature requires an advanced license'
/>
</RIBCL>
```

GET_HOST_POWER_REG_INFO-Rückmeldungen

Der Befehl GET_HOST_POWER_REG_INFO gibt alle zum Zeitpunkt der Anforderung verfügbaren Daten zurück. Wenn die Anforderung innerhalb der ersten fünf Minuten nach dem Zurücksetzen oder Aus-/Einschalten des Systems oder des iLO 2 Managementprozessors ausgegeben wird, ist nur eine begrenzte Datenmenge verfügbar.

Eine mögliche GET_HOST_POWER_REG_INFO-Rückmeldung innerhalb von fünf Minuten nach dem Zurücksetzen oder Aus-/Einschalten des Systems oder des iLO 2 lautet:

```
<GET_HOST_POWER_REG_INFO>
<NumberProcessors>0</NumberProcessors>
<NumberPstates>0</NumberPstates>
</GET_HOST_POWER_REG_INFO>
```

Eine mögliche GET_HOST_POWER_REG_INFO-Rückmeldung, wenn alle Daten verfügbar sind, ist:

```
<GET_HOST_POWER_REG_INFO>
<NumberProcessors>2</NumberProcessors>
<NumberPstates>3</NumberPstates>
<Processor0>
<CurrentPstate>2</CurrentPstate>
<Pstate0>
<TotalAverage>34.3</TotalAverage>
</Pstate0>
<Pstate1>
<TotalAverage>0</TotalAverage>
</Pstate1>
<Pstate2>
<TotalAverage>65.7</TotalAverage>
</Pstate2>
<Pstate3>
<TotalAverage>0</TotalAverage>
</Pstate3>
......
<Pstate7>
<TotalAverage>0</TotalAverage>
</Pstate7>
</Processor0>
<Processor1>
<CurrentPstate>2</CurrentPstate>
<Pstate0>
<TotalAverage>34.3</TotalAverage>
</Pstate0>
<Pstate1>
<TotalAverage>0</TotalAverage>
</Pstate1>
<Pstate2>
<TotalAverage>65.7</TotalAverage>
</Pstate2>
<Pstate3>
.....
<Pstate7>
<TotalAverage>0</TotalAverage>
</Pstate7>
</Processor1>
</GET_HOST_POWER_REG_INFO>
```

GET_HOST_POWER_STATUS

Mit dem Befehl GET_HOST_POWER_STATUS wird der Betriebsstatus des Servers abgefragt. Damit der Befehl GET_HOST_POWER_STATUS richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen. Sie können für SERVER_INFO MODE Lese- oder Schreibzugriff festlegen.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="write">
<GET_HOST_POWER_STATUS/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

GET_HOST_POWER_STATUS-Parameter

Keine

GET_HOST_POWER_STATUS-Laufzeitfehler

Folgende GET_HOST_POWER_STATUS-Fehlermeldungen können angezeigt werden:

- Host power is OFF. (Stromversorgung des Host ist ausgeschaltet.)
- Host power is ON. (Stromversorgung des Host ist eingeschaltet.)

GET_HOST_POWER_STATUS-Rückmeldungen

In der Antwort werden die folgenden Informationen zurückgegeben:

```
<GET_HOST_POWER
HOST_POWER="OFF"
/>
```

SET_HOST_POWER

Mit dem Befehl SET_HOST_POWER wird die Stellung des Netzschalters des Servers geändert. Damit der Befehl SET_HOST_POWER richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen, und SERVER_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum virtuellen Ein-/Ausschalten und Zurücksetzen verfügen, um diesen Befehl ausführen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="write">
<SET_HOST_POWER HOST_POWER="Yes"/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

SET_HOST_POWER-Parameter

HOST_POWER aktiviert bzw. deaktiviert den virtuellen Netzschalter. Die möglichen Werte sind `Yes` oder `No`.

SET_HOST_POWER-Laufzeitfehler

Folgende SET_HOST_POWER-Fehlermeldungen können angezeigt werden:

- Server information is open for read-only access. (Server-Informationen werden für Lesezugriff geöffnet.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- Virtual Power Button feature is not supported on this server. (Die Funktion des virtuellen Netzschalters wird auf diesem Server nicht unterstützt)

- Host power is already ON. (Der Host ist bereits eingeschaltet.)
- Host power is already OFF. (Der Host ist bereits ausgeschaltet.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) RESET_SERVER_PRIV required. (RESET_SERVER_PRIV erforderlich.)

GET_HOST_PWR_MICRO_VER

Der Befehl GET_HOST_PWR_MICRO_VER schaltet den Netzschalter des Servers ein bzw. aus. Damit der Befehl GET_HOST_PWR_MICRO_VER richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen, und SERVER_INFO MODE muss auf „read“ gesetzt sein.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="admin" PASSWORD="admin123">
<SERVER_INFO MODE="read">
<GET_HOST_PWR_MICRO_VER/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

GET_HOST_PWR_MICRO_VER-Parameter

Keine

GET_HOST_PWR_MICRO_VER-Laufzeitfehler

Folgende _HOST_PWR_MICRO_VER -Fehlermeldungen können angezeigt werden:

- `Error`
  (Fehler), wenn der Strom-Mikroprozessor nicht gelesen werden kann (Hardwareproblem).
- `Power Off`
  (Ausgeschaltet), wenn der Server ausgeschaltet ist.
- `N/A`
  (-), wenn der Server keinen Strom-Mikroprozessor unterstützt.

GET_HOST_PWR_MICRO_VER-Rückmeldungen

- Keine Fehler und zeigt Versionsinformationen an:

  ```
  <GET_HOST_PWR_MICRO_VER>
  <PWR_MICRO VERSION="2.3"/>
  </GET_HOST_PWR_MICRO_VER>
  ```

- Server ist ausgeschaltet:

  ```
  <GET_HOST_PWR_MICRO_VER>
  <PWR_MICRO VERSION="OFF"/>
  </GET_HOST_PWR_MICRO_VER>
  ```

- Strom-Mikroprozessor wird auf dem Server nicht unterstützt:

  ```
  <GET_HOST_PWR_MICRO_VER>
  <PWR_MICRO VERSION="N/A"/>
  </GET_HOST_PWR_MICRO_VER>
  ```

- Version des Strom-Mikroprozessors konnte nicht gelesen werden:

  ```
  <GET_HOST_PWR_MICRO_VER>
  ```

```
<PWR_MICRO VERSION="Error"/>
</GET_HOST_PWR_MICRO_VER>
```

GET_ONE_TIME_BOOT

Der Befehl GET_ONE_TIME_BOOT gibt den Status eine einmaligen Systemstarts zurück. Dieser Befehl muss innerhalb eines SERVER_INFO-Elements ausgegeben werden, und SERVER_INFO muss sich im Lesemodus befinden.

Beispiel:

```
<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN=" adminname" PASSWORD=" password">
  <SERVER_INFO MODE="read">
    <GET_ONE_TIME_BOOT/>
  </SERVER_INFO>
 </LOGIN>
</RIBCL>
```

GET_ONE_TIME_BOOT-Parameter

Für diesen Befehl sind keine Parameter vorhanden.

GET_ONE_TIME_BOOT-Laufzeitfehler

Keine

GET_ONE_TIME_BOOT-Rückmeldungen

Die Rückmeldung zeigt den Status des einmaligen Systemstarts des Hosts an.

Eine mögliche GET_ONE_TIME_BOOT-Rückmeldung ist:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.22">
<RESPONSE
    STATUS="0x0000"
    MESSAGE='No error'
     />
<GET_ONE_TIME_BOOT>
<BOOT_TYPE DEVICE="FLOPPY"/>
</GET_ONE_TIME_BOOT>
</RIBCL>
```

SET_ONE_TIME_BOOT

Der Befehl SET_ONE_TIME_BOOT passt den Startvorgang vorübergehend für einen Zyklus an. Nachdem das Skript erfolgreich ausgeführt wurde, führt der Host einmal den Start des angegebenen Geräts aus. Dieser Befehl muss innerhalb eines SERVER_INFO-Elements ausgegeben werden, und SERVER_INFO muss sich im Schreibmodus befinden. Der Parameter im Befehl ist erforderlich.

Beispiel:

```
<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN=" adminname" PASSWORD=" password">
   <SERVER_INFO MODE="write">
    <SET_ONE_TIME_BOOT value = "FLOPPY"  />
   </SERVER_INFO>
 </LOGIN>
</RIBCL>
```

SET_ONE_TIME_BOOT-Parameter

Dieser Wert gibt den Startoptions-Parameter an. Mögliche Werte sind CDROM, FLOPPY, HDD oder NETWORK.

SET_ONE_TIME_BOOT-Laufzeitfehler

Folgende Laufzeitfehler sind möglich:

- `Server information is open for read-only access. Write access is required for this operation.`
- `User does not have correct privilege for action. RESET_SERVER_PRIV required.`
- `An invalid device option has been given.`

SET_ONE_TIME_BOOT-Rückmeldungen

Die Rückmeldung zeigt den Status des einmaligen Systemstarts des Hosts an.

Eine mögliche SET_ONE_TIME_BOOT-Rückmeldung ist:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.22">
<RESPONSE
    STATUS="0x0000"
    MESSAGE='No error'
     />
</RIBCL>
```

GET_PERSISTENT_BOOT

Der Befehl GET_PERSISTENT_BOOT gibt die aktuellen Startreihenfolgen-Einstellungen zurück. Dieser Befehl muss innerhalb eines SERVER_INFO-Elements ausgegeben werden, und SERVER_INFO muss sich im Lesemodus befinden.

Beispiel:

```
<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN=" adminname" PASSWORD=" password">
  <SERVER_INFO MODE="read">
   <GET_PERSISTENT_BOOT/>
  </SERVER_INFO>
 </LOGIN>
</RIBCL>
```

GET_PERSISTENT_BOOT-Parameter

Für diesen Befehl sind keine Parameter vorhanden.

GET_PERSISTENT_BOOT-Laufzeitfehler

Keine

GET_PERSISTENT_BOOT-Rückmeldungen

Der Rückmeldung zeigt die aktuellen Startreihenfolgen-Einstellungen an.

Eine mögliche GET_PERSISTENT_BOOT-Rückmeldung ist:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.22">
<RESPONSE
    STATUS="0x0000"
    MESSAGE='No error'
```

```
     />
<GET_PERSISTENT_BOOT
CDROM = "1" FLOPPY = "2" HDD = "3" USB = "4" NETWORK = "5"
    />
</RIBCL>
```

SET_PERSISTENT_BOOT

Der Befehl SET_PERSISTENT_BOOT konfiguriert die Startreihenfolge so neu, dass sie der in der xml-Datei angegebenen Reihenfolge entspricht. Dieser Befehl muss innerhalb eines SERVER_INFO-Elements ausgegeben werden, und SERVER_INFO muss sich im Schreibmodus befinden. Mindestens ein Parameter im Befehl ist erforderlich.

Beispiel:

```
<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
     <SET_PERSISTENT_BOOT>
      <DEVICE value = "CDROM" />
      <DEVICE value = "FLOPPY" />
      <DEVICE value = "HDD" />
      <DEVICE value = "USB" />
      <DEVICE value = "NETWORK" />
     </SET_PERSISTENT_BOOT>
   </SERVER_INFO>
 </LOGIN>
</RIBCL>
```

SET_PERSISTENT_BOOT-Parameter

Der Befehl akzeptiert als Parameter DEVICE ein oder mehrere Startgeräte. Mögliche Werte sind CDROM, FLOPPY, HDD, USB oder NETWORK. Wird kein Gerät angegeben, schlägt das Skript fehl Die Geräte müssen in der Reihenfolge angegeben werden, die als Startreihenfolge festgelegt werden soll. Wenn Sie nicht jede Option auflisten, werden die übrigen Optionen ans Ende der Liste verschoben.

SET_PERSISTENT_BOOT-Laufzeitfehler

Folgende Laufzeitfehler sind möglich:

- `Server info is open for read-only access. Write access is required for this operation.`
- `User does not have correct privilege for action. RESET_SERVER_PRIV required.`
- `An invalid device option has been given.`
- `Too many boot devices has been provided.`
- `Device has been repeated.`
- `Boot device not supported.`

SET_PERSISTENT_BOOT-Rückmeldungen

Eine mögliche SET_PERSISTENT_BOOT-Rückmeldung ist:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.22">
<RESPONSE
    STATUS="0x0000"
    MESSAGE='No error'
```

```
     />
</RIBCL>
```

GET_PWREG_CAPABILITIES

Der Befehl GET_PWREG_CAPABILITIES fordert iLO 2 Leistungsregler-Informationen zu den minimalen und maximalen Systemstromwerten, zu Typ und Kapazität des Netzteils und zur Firmwareversion des Strom-Mikroprozessors an. Damit der Befehl GET_PWREG_CAPABILITIES richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen, und SERVER_INFO MODE muss auf „read“ gesetzt sein.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="read">
<GET_PWREG_CAPABILITIES/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

GET_PWREG_CAPABILITIES-Parameter

Keine

GET_PWREG_CAPABILITIES-Laufzeitfehler

Die möglichen GET_PWREG_CAPABILITIES-Fehlermeldungen lauten u. a.:

- `Error` (Fehler), wenn der Strom-Mikroprozessor nicht gelesen werden kann (Hardwareproblem).
- `Power Off` (Ausgeschaltet), wenn der Server ausgeschaltet ist.
- `N/A` (-), wenn der Server keinen Strom-Mikroprozessor unterstützt.

GET_PWREG_CAPABILITIES-Rückmeldungen

```
<GET_PWREG_CAPABILITIES>
<FWVERSION>"1.77"</FWVERSION>
<THRD ID="0" SOCKET="1" CORE="0" THREAD="0"/>
<QS Q="0" P="0" L="100"/>
<QS Q="1" P="1" L="75"/>
<QS Q="2" P="1" L="75"/>
<QS Q="3" P="1" L="75"/>
<QS Q="4" P="1" L="75"/>
<QS Q="5" P="1" L="75"/>
<QS Q="6" P="1" L="75"/>
<QS Q="7" P="1" L="75"/>
<QS Q="8" P="1" L="75"/>
<THRD ID="1" SOCKET="1" CORE="1" THREAD="0"/>
<QS Q="0" P="0" L="100"/>
<QS Q="1" P="1" L="75"/>
<QS Q="2" P="1" L="75"/>
<QS Q="3" P="1" L="75"/>
<QS Q="4" P="1" L="75"/>
<QS Q="5" P="1" L="75"/>
<QS Q="6" P="1" L="75"/>
```

```
<QS Q="7" P="1" L="75"/>
<QS Q="8" P="1" L="75"/>
<THRD ID="2" SOCKET="1" CORE="2" THREAD="0"/>
<QS Q="0" P="0" L="100"/>
<QS Q="1" P="1" L="75"/>
<QS Q="2" P="1" L="75"/>
<QS Q="3" P="1" L="75"/>
<QS Q="4" P="1" L="75"/>
<QS Q="5" P="1" L="75"/>
<QS Q="6" P="1" L="75"/>
<QS Q="7" P="1" L="75"/>
<QS Q="8" P="1" L="75"/>
<THRD ID="3" SOCKET="1" CORE="3" THREAD="0"/>
<QS Q="0" P="0" L="100"/>
<QS Q="1" P="1" L="75"/>
<QS Q="2" P="1" L="75"/>
<QS Q="3" P="1" L="75"/>
<QS Q="4" P="1" L="75"/>
<QS Q="5" P="1" L="75"/>
<QS Q="6" P="1" L="75"/>
<QS Q="7" P="1" L="75"/>
<QS Q="8" P="1" L="75"/>
<EFFICIENCY_MODE INDEX="0" NAME="OSC">"OS_Control"</EFFICIENCY_MODE>
<EFFICIENCY_MODE INDEX="1" NAME="MIN">"Low_Power"</EFFICIENCY_MODE>
<EFFICIENCY_MODE INDEX="2" NAME="DYN">"Dynamic"</EFFICIENCY_MODE>
<EFFICIENCY_MODE INDEX="3" NAME="MAX">"Max_Power"</EFFICIENCY_MODE>
<HISTORY SIZE="288" INTERVAL="300" TRACE="10"/>
<BUSYMAXPWR>203</BUSYMAXPWR>
<IDLEMAXPWR>168</IDLEMAXPWR>
<ECAP/>
<TEMP/>
<CPU/>
<PWRSPLY TYPE="AC" CAPACITY="800"/>
<PWRALERT VERSION="0"/>
<PWR MICRO VERSION="3.3"/>
</GET_PWREG_CAPABILITIES>
```

RESET_SERVER

Der Befehl RESET_SERVER erzwingt einen Warmstart des Servers, wenn der Server gerade angeschaltet ist. Damit der Befehl RESET_SERVER richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen, und SERVER_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum virtuellen Ein-/Ausschalten und Zurücksetzen verfügen, um diesen Befehl ausführen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="write">
<RESET_SERVER/>
```

```
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

RESET_SERVER-Fehler

Folgende RESET_SERVER-Fehlermeldungen können angezeigt werden:

- Server information is open for read-only access. (Server-Informationen werden für Lesezugriff geöffnet.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- Server is currently powered off. (Der Server ist derzeit ausgeschaltet.)
- User does **not** have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) RESET_SERVER_PRIV required. (RESET_SERVER_PRIV erforderlich.)

RESET_SERVER-Parameter

Keine

PRESS_PWR_BTN

Der Befehl PRESS_PWR_BTN wird verwendet, um ein physisches Drücken des Ein-/Aus-Schalters des Servers zu simulieren. Damit der Befehl PRESS_PWR_BTN richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen, und SERVER_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum virtuellen Ein-/Ausschalten und Zurücksetzen verfügen, um diesen Befehl ausführen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="write">
<PRESS_PWR_BTN/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

PRESS_PWR_BTN-Parameter

Für diesen Befehl sind keine Parameter vorhanden.

PRESS_PWR_BTN-Laufzeitfehler

Folgende Fehlermeldungen können angezeigt werden:

- Server information is open for read-only access. (Server-Informationen werden für Lesezugriff geöffnet.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) RESET_SERVER_PRIV required. (RESET_SERVER_PRIV erforderlich.)

HOLD_PWR_BTN

Der Befehl HOLD_PWR_BTN wird verwendet, um ein physisches Drücken und Halten des Ein-/Aus-Schalters des Servers zu simulieren. Damit der Befehl HOLD_PWR_BTN richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen, und SERVER_INFO MODE muss

auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum virtuellen Ein-/Ausschalten und Zurücksetzen verfügen, um diesen Befehl ausführen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="write">
<HOLD_PWR_BTN/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

HOLD_PWR_BTN-Parameter

Für diesen Befehl sind keine Parameter vorhanden.

HOLD_PWR_BTN-Laufzeitfehler

Folgende Fehlermeldungen können angezeigt werden:

- Server information is open for read-only access. (Server-Informationen werden für Lesezugriff geöffnet.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) RESET_SERVER_PRIV required. (RESET_SERVER_PRIV erforderlich.)

COLD_BOOT_SERVER

Der Befehl COLD_BOOT_SERVER erzwingt einen Kaltstart des Servers, wenn der Server gerade angeschaltet ist. Damit der Befehl COLD_BOOT_SERVER richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen, und SERVER_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum virtuellen Ein-/Ausschalten und Zurücksetzen verfügen, um diesen Befehl ausführen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="write">
<COLD_BOOT_SERVER/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

COLD_BOOT_SERVER-Parameter

Für diesen Befehl sind keine Parameter vorhanden.

COLD_BOOT_SERVER-Laufzeitfehler

Folgende Fehlermeldungen können angezeigt werden:

- Server information is open for read-only access. (Server-Informationen werden für Lesezugriff geöffnet.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- Host power is already OFF. (Der Host ist bereits ausgeschaltet.)

- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) RESET_SERVER_PRIV required. (RESET_SERVER_PRIV erforderlich.)

WARM_BOOT_SERVER

Der Befehl WARM_BOOT_SERVER erzwingt einen Warmstart des Servers, wenn der Server gerade angeschaltet ist. Damit der Befehl WARM_BOOT_SERVER richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen, und SERVER_INFO MODE muss auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum virtuellen Ein-/Ausschalten und Zurücksetzen verfügen, um diesen Befehl ausführen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="write">
<WARM_BOOT_SERVER/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

WARM_BOOT_SERVER-Parameter

Für diesen Befehl sind keine Parameter vorhanden.

WARM_BOOT_SERVER-Laufzeitfehler

Folgende Fehlermeldungen können angezeigt werden:

- Server information is open for read-only access. (Server-Informationen werden für Lesezugriff geöffnet.) Write access is required for this operation. (Für diesen Vorgang sind Schreibzugriffsrechte erforderlich.)
- Host power is already OFF. (Der Host ist bereits ausgeschaltet.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) RESET_SERVER_PRIV required. (RESET_SERVER_PRIV erforderlich.)

SERVER_AUTO_PWR

Mit dem Befehl SERVER_AUTO_PWR werden die Einstellungen für das automatische Einschalten und das verzögerte automatische Einschalten des Servers festgelegt.

Dieser Befehl wird ab der iLO 2 Firmware-Version 1.20 unterstützt. Die iLO Firmware bzw. RILOE II unterstützen ihn nicht.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
<SERVER_INFO MODE="write">
<!-- Enable automatic power on with 30 seconds delay -->
<SERVER_AUTO_PWR VALUE="30" />
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

SERVER_AUTO_PWR-Parameter

Die folgenden Werte sind möglich:

- `Yes`: Aktiviert das automatische Einschalten mit einer Mindestverzögerung.
- `No`: Deaktiviert das automatische Einschalten.
- `15`: Aktiviert das automatische Einschalten mit einer Verzögerung von 15 Sekunden.
- `30`: Aktiviert das automatische Einschalten mit einer Verzögerung von 30 Sekunden.
- `45`: Aktiviert das automatische Einschalten mit einer Verzögerung von 45 Sekunden.
- `60`: Aktiviert das automatische Einschalten mit einer Verzögerung von 60 Sekunden.
- `Random` (Beliebig): Aktiviert das automatische Einschalten mit einer beliebigen Verzögerung von bis zu 60 Sekunden.

SERVER_AUTO_PWR-Laufzeitfehler

Folgende Fehlermeldungen können angezeigt werden:

- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) RESET_SERVER_PRIV required. (RESET_SERVER_PRIV erforderlich.)
- The value specified for SERVER_AUTO_PWR is invalid. (Der für SERVER_AUTO_PWR angegebene Wert ist ungültig.)

GET_SERVER_AUTO_PWR

Mit dem Befehl GET_SERVER_AUTO_PWR werden die Einstellungen für das automatische Einschalten und das verzögerte automatische Einschalten des Servers abgerufen.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
<SERVER_INFO MODE="read">
<GET_SERVER_AUTO_PWR />
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

GET_SERVER_AUTO_PWR-Parameter

Keine

GET_SERVER_AUTO_PWR-Rückmeldung

Eine mögliche GET_SERVER_AUTO_PWR-Rückmeldung lautet:

```
<?xml version="1.0" ?>
<RIBCL VERSION="2.22">
<RESPONSE
STATUS="0x0000"
MESSAGE='No error'
/>
<GET_SERVER_AUTO_PWR>
<!--
Automatically Power On Server is enabled
with 30 seconds power on delay.
```

```
-->
<SERVER_AUTO_PWR VALUE="30" />
</GET_SERVER_AUTO_PWR>
</RIBCL>
```

GET_UID_STATUS

Mit dem Befehl GET_UID_STATUS wird der Status der Server-UID abgefragt. Damit der Befehl GET_UID_STATUS richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen. Sie können für SERVER_INFO MODE Lese- oder Schreibzugriff festlegen.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="write">
<GET UID_STATUS />
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

GET_UID_STATUS-Parameter

Keine

GET_UID_STATUS-Antwort

In der Antwort werden die folgenden Informationen zurückgegeben:

```
<GET_UID_STATUS
UID="OFF"
/>
```

UID_CONTROL

Mit dem Befehl UID_CONTROL wird die UID umgeschaltet. Damit der Befehl UID_CONTROL richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen, und SERVER_INFO MODE muss auf „write“ gesetzt sein.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="write">
<UID_CONTROL UID="Yes"/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

UID_CONTROL-Parameter

Mit UID wird der UID-Status bestimmt. Der Wert `yes` schaltet die UID-LED ein, der Wert `No` schaltet die UID-LED aus.

UID_CONTROL-Fehler

Folgende UID_CONTROL-Fehlermeldungen können angezeigt werden:

- UID is already ON. (UID-LED ist bereits eingeschaltet.)
- UID is already OFF (UID-LED ist bereits ausgeschaltet.)

GET_VPB_CABLE_STATUS (nur RILOE II)

Der Befehl GET_VPB_CABLE_STATUS fragt den Status des Kabels für den virtuellen Netzschalter ab, das möglicherweise an ein RILOE II Board angeschlossen ist. Damit der Befehl GET_VPB_CABLE_STATUS richtig übersetzt wird, muss er innerhalb eines SERVER_INFO-Befehlsblocks stehen. Sie können für SERVER_INFO MODE Lese- oder Schreibzugriff festlegen.

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="read">
<GET_VPB_CABLE_STATUS/>
</SERVER_INFO>
 </LOGIN>
</RIBCL>
```

GET_VPB_CABLE_STATUS-Parameter

Keine

GET_VPB_CABLE_STATUS-Laufzeitfehler

Die möglichen GET_VPB_CABLE_STATUS-Fehlermeldungen lauten u. a.:

- Virtual Power Button cable is attached. (Kabel für virtuellen Netzschalter ist angeschlossen.)
- Virtual Power Button cable is not attached. (Kabel für virtuellen Netzschalter ist nicht angeschlossen.)

GET_VPB_CABLE_STATUS-Rückmeldungen

Eine mögliche GET_VPB_CABLE_STATUS-Rückmeldung lautet:

```
<RIBCL VERSION="2.22">
<RESPONSE
STATUS="0x0000"
MESSAGE='No error'
/>
<GET_VPB_CABLE>
<VIRTUAL POWER BUTTON CABLE="ATTACHED"/>
</GET_VPB_CABLE>
</RIBCL>
```

SSO_INFO

Der Befehl SSO_INFO MODE darf nur innerhalb eines LOGIN-Befehlsblocks stehen. Nur Befehle des Typs SSO_INFO MODE sind innerhalb des SSO_INFO MODE-Befehlsblocks gültig.

SSO_INFO MODE erfordert einen MODE-Parameter mit einem Wert „read“ oder „write“. MODE ist ein spezifischer Zeichenfolgeparameter mit einer maximalen Länge von 10 Zeichen, der die beabsichtigte Verarbeitung der Informationen angibt.

Im Schreibmodus können iLO 2 Informationen sowohl gelesen als auch geschrieben werden. Im Lesemodus ist ein Ändern der iLO 2 Informationen nicht möglich. Sie müssen über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Beispiel:

```
<SSO_INFO MODE="write">
…… SSO_INFO-Befehle ……
</SSO_INFO>
```

Beispiel für das Löschen eines SSO HP SIM Server-Datensatzes nach Indexnummer:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
<SSO_INFO MODE="write">
<DELETE_SERVER INDEX="6" />
</SSO_INFO>
</LOGIN>
</RIBCL>
```

SSO_INFO wird nur auf lizenzierter iLO 2 v1.30 Firmware unterstützt. Ist iLO 2 nicht lizenziert, können diese Einstellungen noch geändert werden. iLO 2 gibt keine Fehlermeldung zurück. Ist keine Lizenz vorhanden, werden jedoch alle SSO-Versuche zurückgewiesen. Weitere Informationen sind im *HP Integrated Lights-Out 2 Benutzerhandbuch* zu finden.

GET_SSO_SETTINGS

Der Befehl GET_SSO_SETTINGS dient zum Abrufen von SSO-Einstellungen für iLO 2. Damit der Befehl GET_SSO_SETTINGS richtig übersetzt wird, muss er innerhalb eines SSO_INFO-Befehlsblocks stehen; SSO_INFO MODE kann dabei auf „read“ oder „write“ gesetzt sein.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
<SSO_INFO MODE="read">
<GET_SSO_SETTINGS/>
</SSO_INFO>
</LOGIN>
</RIBCL>
```

GET_SSO_SETTINGS-Parameter

Keine

GET_SSO_SETTINGS-Rückmeldungen

Es folgt ein Beispiel für eine Rückmeldung auf die SSO-Einstellungen von einem konfigurierten iLO 2. Es sind 0 oder mehr SSO_SERVER-Aufzeichnungen vorhanden, die die Anzahl der auf jedem Server gespeicherten Datensätze widerspiegeln.

```
<GET_SSO_SETTINGS>
<TRUST_MODE VALUE="CERTIFICATE" />
<USER_ROLE LOGIN_PRIV="Y" />
<USER_ROLE REMOTE_CONS_PRIV="N" />
<USER_ROLE RESET_SERVER_PRIV="N" />
<USER_ROLE VIRTUAL_MEDIA_PRIV="N" />
<USER_ROLE CONFIG_ILO_PRIV="N" />
<USER_ROLE ADMIN_PRIV="N" />
<OPERATOR_ROLE LOGIN_PRIV="Y" />
<OPERATOR_ROLE REMOTE_CONS_PRIV="Y" />
<OPERATOR_ROLE RESET_SERVER_PRIV="Y" />
<OPERATOR_ROLE VIRTUAL_MEDIA_PRIV="Y" />
<OPERATOR_ROLE CONFIG_ILO_PRIV="N" />
<OPERATOR_ROLE ADMIN_PRIV="N" />
<ADMINISTRATOR_ROLE LOGIN_PRIV="Y" />
<ADMINISTRATOR_ROLE REMOTE_CONS_PRIV="Y" />
```

```
<ADMINISTRATOR_ROLE RESET_SERVER_PRIV="Y" />
<ADMINISTRATOR_ROLE VIRTUAL_MEDIA_PRIV="Y" />
<ADMINISTRATOR_ROLE CONFIG_ILO_PRIV="Y" />
<ADMINISTRATOR_ROLE ADMIN_PRIV="Y" />
<SSO_SERVER INDEX="0"
 ISSUED_TO="viv.hp.com"
 ISSUED_BY="viv.hp.com"
 VALID_FROM="061108192059Z"
 VALID_UNTIL="161108192059Z">
-----BEGIN CERTIFICATE-----
.
.
.
-----END CERTIFICATE-----
</SSO_SERVER>
<SSO_SERVER INDEX="1">
ant.hp.com
</SSO_SERVER>
</GET_SSO_SETTINGS>
```

MOD_SSO_SETTINGS

Mit dem Befehl MOD_SSO_SETTINGS können die HP SSO-Einstellungen für iLO 2 modifiziert werden. Damit der Befehl MOD_SSO_SETTINGS richtig übersetzt wird, muss er innerhalb eines SSO_INFO-Befehlsblocks stehen; SSO_INFO MODE muss dabei auf „write“ gesetzt sein. Der Benutzer muss über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
 <SSO_INFO MODE="write">
<MOD_SSO_SETTINGS>
<!-- Specify the desired trust mode Options: DISABLED(default),
CERTIFICATE (recommended), NAME, or ALL
-->
<TRUST_MODE="CERTIFICATE" />
<!-- Specify the privileges assigned to the user role -->
<USER_ROLE LOGIN_PRIV="Y" />
<USER_ROLE REMOTE_CONS_PRIV="N" />
<USER_ROLE RESET_SERVER_PRIV="N" />
<USER_ROLE VIRTUAL_MEDIA_PRIV="N" />
<USER_ROLE CONFIG_ILO_PRIV="N" />
<USER_ROLE ADMIN_PRIV="N" />
<!-- Specify the privileges assigned to the operator role -->
<OPERATOR_ROLE LOGIN_PRIV="Y" />
<OPERATOR_ROLE REMOTE_CONS_PRIV="Y" />
<OPERATOR_ROLE RESET_SERVER_PRIV="Y" />
<OPERATOR_ROLE VIRTUAL_MEDIA_PRIV="Y" />
<OPERATOR_ROLE CONFIG_ILO_PRIV="N" />
```

```
<OPERATOR_ROLE ADMIN_PRIV="N" />
<!-- Specify the privileges assigned to the administrator role -->
<ADMINISTRATOR_ROLE LOGIN_PRIV="Y" />
<ADMINISTRATOR_ROLE REMOTE_CONS_PRIV="Y" />
<ADMINISTRATOR_ROLE RESET_SERVER_PRIV="Y" />
<ADMINISTRATOR_ROLE VIRTUAL_MEDIA_PRIV="Y" />
<ADMINISTRATOR_ROLE CONFIG_ILO_PRIV="Y" />
<ADMINISTRATOR_ROLE ADMIN_PRIV="Y" />
</MOD_SSO_SETTINGS>
 </SSO_INFO>
 </LOGIN>
</RIBCL>
```

MOD_SSO_SETTINGS-Parameter

TRUST_MODE legt die Single Sign-On-Vertrauensstufe fest. Die aktuelle Einstellung wird unverändert übernommen, wenn diese Einstellung im Skript ausgelassen wird. Akzeptierte Werte sind:

- Deaktiviert HP SIM SSO auf diesem Prozessor.
- Certificate (Zertifikat): Akzeptiert nur SSO-Anforderungen, die anhand eines Zertifikats authentifiziert wurden.
- Name: Vertraut SSO-Anforderungen von dem genannten HP SIM Server.
- All (Alle): Akzeptiert alle SSO-Anforderungen vom Netzwerk.

iLO Berechtigungen werden mit Rollennamen verknüpft. Die angegebenen Berechtigungen werden entsprechend für die betreffende Rolle festgelegt, und eine weggelassene Berechtigung wird unverändert übernommen. Sie können eine Berechtigung für die Rolle mit dem Argument „Y“ aktivieren und die Berechtigung für die Rolle mit dem Argument „N“ deaktivieren.

Es gibt drei Rollen zur Zuweisung von Berechtigungen. Durch Weglassen einer Rolle wird die aktuelle Zuweisung unverändert übernommen:

- USER_ROLE: Mit dem Benutzer verknüpfte Berechtigungen
- OPERATOR_ROLE: Mit dem Bediener verknüpfte Berechtigungen
- ADMINISTRATOR_ROLE: Mit dem Administrator verknüpfte Berechtigungen

Für jede Rolle gibt es mehrere Berechtigungen, die abgeändert werden können. Die Berechtigung wird im Rollen-Tag angegeben. Wird eine Berechtigung weggelassen, wird der aktuelle Wert unverändert übernommen. Jede Berechtigungszuweisung ist ein boolescher Wert und kann auf „Y“ (Berechtigung erteilt) oder auf „N“ (Berechtigung verweigert) gesetzt werden. Weitere Einzelheiten über Kontoberechtigungen sind im Abschnitt „User Administration (Benutzeradministration)“ im Benutzerhandbuch zu finden.

- LOGIN_PRIV: Gestattet die Anmeldung für diese Rolle.
- REMOTE_CONS_PRIV: Gewährt Zugriff auf die Ressourcen der Remote Console.
- RESET_SERVER_PRIV: Gewährt Zugriff auf die Steuerung des Netzschalters und des Resets.
- VIRTUAL_MEDIA_PRIV: Gewährt Zugriff auf virtuelle Medien- Ressourcen.
- CONFIG_ILO_PRIV: Gestattet die Änderung von Einstellungen.
- ADMIN_PRIV: Gestattet die Änderung lokaler Benutzerkonten.

MOD_SSO_SETTINGS-Laufzeitfehler

- Incorrect firmware version. (Inkorrekte Firmwareversion.) SSO is only support on iLO 2 v1.30 firmware or later. (Inkorrekte Firmwareversion. SSO wird nur auf auf der iLO 2 Firmware ab Version 1.30 unterstützt.)
- User does not have correct privilege for action. (Benutzer verfügt nicht über die erforderliche Berechtigung für diese Aktion.) CONFIG_ILO_PRIV required. (CONFIG_ILO_PRIV erforderlich.)
- SSO_INFO must be in write mode. (SSO_INFO muss sich im Schreibmodus befinden.)

SSO_SERVER

Mit dem Befehl SSO_SERVER werden HP SIM Trusted SSO Server-Datensätze erstellt. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines SSO_INFO-Befehlsblocks stehen, und SSO_INFO MODE muss auf „write“ gesetzt sein. Sie müssen über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können. Dieser Befehl kann mit MOD_SSO_SETTINGS kombiniert werden.

Mit mehreren Instanzen dieses Befehls können Sie mehrere SSO-Server-Datensätze angeben. Die Server werden in der Reihenfolge hinzugefügt, in der die Datensätze angegeben werden. Doppelte Datensätze werden möglicherweise verworfen und lösen eine Fehlermeldung aus. Die Anzahl der vom Lights-Out Prozessor gespeicherten Datensätze ist von der Größe der Einträge abhängig, da Zertifikate keine feste Größe aufweisen. Normalerweise können mehrere Zertifikate gespeichert werden.

Ein HP SIM Trusted Server-Datensatz kann auf drei Arten mit diesem Befehl hinzugefügt werden:

- Der Server kann unter dem Netzwerknamen angegeben werden (als SSO-Vertrauensstufe ist NAME oder ALL erforderlich; CERTIFICATE für Vertrauen nach Zertifikat wird nicht unterstützt). Verwenden Sie einen vollständig qualifizierten Netzwerknamen.
- Das Serverzertifikat kann vom iLO 2 importiert werden (der LOM-Prozessor fordert das Zertifikat über eine anonyme HTTP-Anforderung von dem angegebenen HIP SIM Server an). Diese Methode funktioniert nur, wenn der iLO 2 Prozessor den HP SIM Server während der Verarbeitung dieses Befehls auf dem Netzwerk erreichen kann.
- Das Server-Zertifikat kann direkt auf iLO 2 installiert werden. Das x.509-Zertifikat muss jedoch im Voraus eingeholt werden. Mit dieser Methode können Sie den iLO 2 zuerst konfigurieren, bevor sie ihn in einem Netzwerk mit dem HP SIM Server platzieren. Auch ermöglicht sie Ihnen, den Inhalt des HP SIM Server-Zertifikats zu überprüfen. Weitere Methoden zum Anfordern des Zertifikats vom HP SIM Server finden Sie im *HP Integrated Lights-Out 2 Benutzerhandbuch* oder im *HP SIM Benutzerhandbuch*.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
<SSO_INFO MODE="write">
<!-- Add an SSO server record using the network name
(works for TRUST_MODE NAME or ALL) -->
<SSO_SERVER NAME="hpsim1.hp.net" />
<!-- Add an SSO server record using indirect iLO import
from the network name -->
<SSO_SERVER IMPORT_FROM="hpsim2.hp.net" />
<!-- Add an SSO server certificate record using direct
import of certificate data -->
<IMPORT_CERTIFICATE>
-----BEGIN CERTIFICATE-----
.
```

```
.
.
-----END CERTIFICATE-----
</IMPORT_CERTIFICATE>
</SSO_INFO>
</LOGIN>
</RIBCL>
```

SSO_SERVER-Parameter

NAME gibt an, dass der Server unter dem Netzwerknamen angegeben wird. Dieser Parameter erhält eine in Anführungszeichen stehende Zeichenfolge mit dem vollständig qualifizierten Netzwerknamen des HP SIM Trusted Servers. Der Name wird erst bei einem SSO-Anmeldeversuch von iLO 2 überprüft. Beispielsweise lautet die Syntax zum Hinzufügen eines HP SIM Trusted Servernamens `<SSO_SERVER NAME="hpsim1.hp.net" />`.

- IMPORT_FROM: Gibt an, dass iLO 2 das HP SIM Trusted Server-Zertifikat von HP SIM anfordern sollte. Diese Anforderung wird mithilfe einer anonymen HTTP-Anforderung ähnlich der folgenden Anforderung implementiert:

  ```
  http://<SIM-Netzwerkadresse>:280/GetCertificate
  ```

  iLO 2 fordert das Zertifikat an, wenn dieser Befehl verarbeitet wird. Wenn der HP SIM Server nicht erreichbar ist, tritt ein Fehler auf. iLO 2 wird mit der dem folgenden Beispiel ähnelnden Syntax zum Importieren eines Server-Zertifikats aufgefordert:

  ```
  <SSO_SERVER IMPORT_FROM="hpsim2.hp.net" />
  ```

- IMPORT_CERTIFICATE: Gibt an, dass iLO 2 die nachfolgenden literalen .PEM-codierten x.509-Zertifikatdaten importieren sollte. Die Daten werden in einem Textblock codiert, der den Text `-----BEGIN CERTIFICATE-----` und `-----END CERTIFICATE-----` enthält. Die Syntax zum Importieren eines HP SIM Trusted Server-Zertifikats ähnelt dem folgenden Beispiel:

  ```
  <SSO_SERVER>
  -----BEGIN CERTIFICATE-----
  MIIC3TCCAkYCBESzwFUwDQYJKoZIhvcNAQEFBQAwgbUxCzAJBgNVBAYTAlVTMRMwE.............
  kXzhuVzPfWzQ+a2E9tGAE/YgNGTfS9vKkVLUf6QoP/RQpYpkl5BxrsN3gM/PeT3zrxyTleE=
  -----END CERTIFICATE-----
  </SSO_SERVER>
  ```

  Das Zertifikat wird vor dem Speichern von iLO 2 überprüft, um sicherzustellen, dass es decodiert werden kann. Ist das Zertifikat bereits vorhanden oder beschädigt, tritt ein Fehler auf.

  iLO 2 unterstützt nicht die Sperrung von Zertifikaten und erkennt keine Zertifikate an, die anscheinend abgelaufen sind. Sie müssen alle gesperrten oder abgelaufenen Zertifikate entfernen.

SSO_SERVER-Laufzeitfehler

Ein Laufzeitfehler wird erzeugt:

- Wenn ein Zertifkat ein Duplikat ist.
- Wenn ein Zertifikat beschädigt ist.
- Wenn der HP SIM Server nicht mit IMPORT_FROM erreicht werden kann.
- Wenn die HP SIM Trusted Server Datenbank voll ist. Sie müssen andere Datensätze löschen, um genügend Platz zum Hinzufügen eines neuen Eintrags zu schaffen.
- Wenn der Vertrauensmodus falsch eingestellt ist.

DELETE_SERVER

Mit dem Befehl DELETE_SERVER wird ein HP SIM Trusted SSO Server-Datensatz entfernt. Damit dieser Befehl richtig übersetzt wird, muss er innerhalb eines SSO_INFO-Befehlsblocks stehen, und SSO_INFO MODE muss auf „write“ gesetzt sein. Sie müssen über die Berechtigung zum Konfigurieren von iLO 2 verfügen, um diesen Befehl ausführen zu können.

Mit mehreren Instanzen dieses Befehls können Sie mehrere SSO-Server-Datensätze angeben. Die Server werden in der Reihenfolge gelöscht, in der die Datensätze angegeben werden, und die Datensätze werden nach jedem Löschvorgang neu durchnummeriert. Sie können die Datensätze von den höchsten zu den niedrigsten löschen, wenn Sie mehrere Datensätze auf einmal löschen möchten.

Beispiel:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
<SSO_INFO MODE="write">
<DELETE_SERVER INDEX="6" />
</SSO_INFO>
</LOGIN>
</RIBCL>
```

DELETE_SERVER-Parameter

INDEX gibt die zu löschende Datensatznummer an. Diese Nummer entspricht dem mit dem Befehl GET_SSO_SETTINGS zurückgegebenen Index. Der Index ist 0-basiert; der erste Datensatz ist Index 0, der zweite Datensatz ist Index 1 usw.

DELETE_SERVER-Laufzeitfehler

Bei einem ungültigen Index wird ein Laufzeitfehler ausgegeben.

10 HPQLOMGC-Befehlssprache

Verwenden von HPQLOMGC

HPQLOMGC liest Verzeichniseinstellungen für den Managementprozessor aus einer XML-Datei. Als Skript wird eine Untermenge der RIBCL verwendet. Es wurde erweitert und unterstützt nun Firmware-Images von mehreren Managementprozessoren. Auf iLO 2 Geräten steht HPQLOMGC nicht zur Verfügung.

Folgendes Beispiel zeigt eine XML-Datei:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="user" PASSWORD="password">
<DIR_INFO MODE="write">
<ILO_CONFIG>
<UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\fw\ilo140.brk" />
</ILO_CONFIG>
<RILOE_CONFIG>
<UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\fw\riloe.brk" />
</RILOE_CONFIG>
<RILOE2_CONFIG>
<UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\fw\riloeii.brk" />
</RILOE2_CONFIG>
<MOD_DIR_CONFIG>
<DIR_AUTHENTICATION_ENABLED value="YES" />
<DIR_LOCAL_USER_ACCT value="YES" />
<DIR_SERVER_ADDRESS value="administration.wins.hp.com" />
<DIR_SERVER_PORT value="636" />
<DIR_OBJECT_DN value="CN=RILOP5,CN=Users,DC=RILOEGRP2,DC=HP" />
<DIR_OBJECT_PASSWORD value="aurora" />
<DIR_USER_CONTEXT_1 value="CN=Users,DC=RILOEGRP2,DC=HP" />
<DIR_USER_CONTEXT_2 value="" />
<DIR_USER_CONTEXT_3 value="" />
<DIR_ROLE value="CN=RILOEROLE,CN=Users,DC=RILOEGRP2,DC=HP" />
<DIR_LOGIN_NAME value="RILOEGRP2\Adminl" />
<DIR_LOGIN_PASSWORD value="aurora" />
</MOD_DIR_CONFIG>
</DIR_INFO>
</LOGIN>
</RIBCL>
```

ILO_CONFIG

RIBCL unterstützt nur ein Firmware-Image pro XML-Datei. Die Befehlssprache für HPQLOMGC wurde so geändert, dass nun jeder Managementprozessor über ein eigenes Firmware-Image in einer einzigen XML-Datei verfügen kann. Diese Befehle müssen innerhalb eines DIR_INFO-Blocks ausgegeben werden, und DIR_INFO muss sich im Schreibmodus befinden. Der Managementprozessor wird nach Abschluss des Firmware-Upgrades zurückgesetzt. Zum Aktualisieren der Firmware muss der Benutzer mit der entsprechenden Berechtigung angemeldet sein.

Diese Befehlszeile verwendet die folgenden Parameter:

- UPDATE_RIB_FIRMWARE IMAGE_LOCATION
  Weitere Informationen finden Sie unter „UPDATE_RIB_FIRMWARE-Parameter“.
- MOD_DIR_CONFIG

11 iLO 2 Ports

Aktivieren der Funktion Shared Network Port von iLO 2 über XML-Skripts

Informationen darüber, wie Sie mit dem Befehl SHARED_NETWORK_PORT den gemeinsam genutzten Netzwerkport von iLO 2 über XML-Skripts aktivieren, finden Sie unter Kapitel 9, „Verwenden von RIBCL“.

Das folgende Beispielskript konfiguriert iLO 2 für die Auswahl des gemeinsam genutzten Netzwerkports. Sie können das Skript an Ihre Anforderungen anpassen. Wenn Sie das Skript auf Plattformen verwenden, die den gemeinsam genutzten Netzwerkport nicht unterstützen, wird ein Fehler angezeigt.

```
<RIBCL version="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="WRITE">
<MOD_NETWORK_SETTINGS>
<SHARED_NETWORK_PORT VALUE="Y" />
</MOD_NETWORK_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

Reaktivieren des dedizierten NIC Management-Ports

Sie können den dedizierten NIC-Management-Port von iLO 2 über die Benutzeroberfläche, das RBSU, CLP oder XML reaktivieren. Sie können den dedizierten NIC-Management-Port von iLO über das ILO 2 RBSU oder XLM-Skripts reaktivieren. Weitere Informationen zur Verwendung des Befehls SHARED_NETWORK_PORT finden Sie unter Kapitel 9, „Verwenden von RIBCL“.

So reaktivieren Sie den dedizierten Management-Port über das RBSU:

1. Schließen Sie den dedizierten NIC-Management-Port an das LAN an, in dem der Server verwaltet wird.
2. Starten Sie den Server neu.
3. Wenn Sie während des POST entsprechend aufgefordert werden, drücken Sie die Taste **F8**, um das iLO RBSU aufzurufen.
4. Wählen Sie **Network > NIC > TCP/IP** (Netzwerk > NIC > TCP/IP), und drücken Sie die **Eingabetaste**.
5. Drücken Sie im Menü „Network Configuration“ (Netzwerkkonfiguration) die **Leertaste**, um den Eintrag im Feld „Network Interface Adapter Field“ (Netzwerkschnittstellenadapter-Feld) auf `ON` zu setzen.
6. Drücken Sie die Taste **F10**, um die Konfiguration zu speichern.
7. Wählen Sie **File > Exit** (Datei > Beenden), und drücken Sie die **Eingabetaste**.

Nachdem der iLO zurückgesetzt wurde, wird der dedizierte iLO Management-NIC-Port aktiviert.

Um den dedizierten iLO Port über XML-Skripts zu reaktivieren, verwenden Sie das folgende RIBCL-Beispielskript. Das Beispielskript konfiguriert iLO für die Auswahl des gemeinsam genutzten iLO Netzwerkports. Sie können das Skript an Ihre Anforderungen anpassen. Wenn Sie das Skript auf Plattformen verwenden, die den gemeinsam genutzten Netzwerkport nicht unterstützen, wird ein Fehler angezeigt.

```
<RIBCL version="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="WRITE">
<MOD_NETWORK_SETTINGS>
```

```
<SHARED_NETWORK_PORT VALUE="N" />
</MOD_NETWORK_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

12 iLO 2 Parameter

Statusübersichtsparameter

Parameter	Definition
Server name (Servername)	Zeigt den Systemnamen an. Wenn die Insight Management Agents mit dem Betriebssystem des Hostservers verwendet werden, übermitteln sie den Servernamen an iLO 2.
UUID	Identifiziert den Host. Obwohl die UUID bei der Herstellung des Systems zugewiesen wird, können Sie diese Einstellung mit dem System-RBSU während des POST ändern.
Server Serial Number / Product ID (Server-Seriennummer/Produkt-ID)	Identifiziert die Seriennummer des Servers. Obwohl die Seriennummer bei der Herstellung des Systems zugewiesen wird, können Sie diese Einstellungen mit dem System-RBSU während des POST ändern. Die Produkt-ID dient zur Unterscheidung zwischen verschiedenen Systemen mit ähnlichen Seriennummern. Obwohl die Produkt-ID bei der Herstellung des Systems zugewiesen wird, können Sie diese Einstellung mit dem System-RBSU während des POST ändern.
Virtual UUID (Virtuelle UUID)	Erscheint, wenn sie von anderer HP Software zugewiesen wurde. Dieser Wert wird nur angezeigt, wenn er festgelegt wurde.
Virtual Serial Number (Virtuelle Seriennummer)	Die virtuelle Seriennummer wird angezeigt, wenn sie von anderer HP Software zugewiesen wurde. Dieser Wert wird nur angezeigt, wenn er festgelegt wurde.
System Health (Systemzustand)	Repräsentiert die interne Zustandsanzeige des Servers, sofern unterstützt. Sie gibt einen Überblick über Probleme mit Lüftern, Temperaturfühlern, VRMs und anderen überwachten Subsystemen im Server. Weitere Einzelheiten finden Sie auf der Seite „System Health“ (Systemstatus).
System-ROM	Modell und Version der aktiven System-ROM. Wenn das System einen Backup-System-ROM unterstützt, wird außerdem das Sicherungsdatum angezeigt.
Internal Health LED (LED für den internen Zustand)	Repräsentiert den Status der LED für den internen Zustand des Servers zu dem Zeitpunkt, als diese Seite geladen wurde.
TPM Status	Repräsentiert den Konfigurationsstatus des Trusted Platform Module im System.
Server Power (Server-Stromversorgung)	Gibt an, ob der Host eingeschaltet (ON) oder im Standbymodus (OFF) ist.
UID Light (UID-LED)	Repräsentiert den Status der Geräteidentifizierungs-LED zu dem Zeitpunkt, als die Seite geladen wurde. Der UID-Status kann neben den physischen UID-Tasten am Servergehäuse auch über die Schaltfläche neben dem UID-Symbol gesteuert werden. Die UID hilft bei der Identifizierung und Lokalisierung eines Systems und gibt zu erkennen, dass auf dem Host gerade ein kritischer Vorgang abläuft, wie z. B. der Remote Console Zugriff oder eine Firmwareaktualisierung. Der aktuelle Zustand der UID-LED (ON oder OFF) ist der letzte mit einer dieser Methoden gewählte Zustand. Wird ein neuer Zustand gewählt, während die UID-LED blinkt, wird dieser neue Zustand zum aktuellen Zustand und wirksam, sobald die UID-LED nicht mehr blinkt. Während die UID-LED blinkt, wird der aktuelle Zustand der UID zusammen mit dem Tag (FLASHING) angezeigt. Wenn die UID-LED aufhört zu blinken, wird dieser Tag entfernt.
Last Used Remote Console (Zuletzt verwendete Remote Console)	Zeigt die zuletzt gestartete Remote Console und deren Verfügbarkeit an. Auf diese Weise können Sie Ihre bevorzugte Remote Console schnell starten. Sie können die Remote Console verwenden, sofern sie verfügbar ist und Sie über die entsprechenden Benutzerberechtigungen verfügen. Wenn die Konsole bereits verwendet wird, wird durch Starten der Remote Console auf die Aneignungsschaltfläche zugegriffen. Sie können eine andere Konsole wählen,

Parameter	Definition
	indem Sie dem Link „Last Used Remote Console“ (Zuletzt verwendete Remote Console) folgen.
Latest IML Entry (Letzter IML-Eintrag)	Der aktuellste Eintrag im Integrated Management Log.
iLO 2 Name	Zeigt den Namen an, der dem Integrated Lights-Out 2 Subsystem zugewiesen wurde. Standardmäßig wird der Seriennummer des Systems „iLO“ vorangestellt. Dieser Wert wird als Netzwerkname verwendet und sollte eindeutig sein.
License Type (Lizenztyp)	Zeigt an, ob im System eine Funktionslizenz installiert ist. Auf einige Funktionen des iLO 2 kann nur nach Erwerb einer optionalen Lizenz zugegriffen werden.
iLO 2 Firmware version (iLO 2 Firmware-Version)	Zeigt Informationen über die Version der derzeit installierten iLO 2 Firmware an.
Active Sessions (Aktive Sitzungen)	Zeigt die derzeit bei iLO 2 angemeldeten Benutzer an.
Latest iLO 2 Event Log Entry (Letzter iLO 2 Ereignisprotokoll-Eintrag)	Zeigt den aktuellsten Eintrag im iLO 2 Ereignisprotokoll an.
iLO 2 Date/Time (iLO 2 Date/Time)	Zeigt das Datum (*MM/TT/JJJJ*) an, das durch die interne Uhr des Integrated Lights-Out 2 Subsystems angegeben wird. Die interne Uhr von iLO 2 wird bei POST und bei Ausführen der Insight Agents mit dem Hostsystem synchronisiert.

Parameter für die Benutzeradministration

Parameter	Standardwert	Definition
User name (Benutzername)	Administrator	Dies ist der tatsächliche Name des Benutzers, wie er in der Benutzerliste und im Ereignisprotokoll angezeigt wird. Es handelt sich nicht um den Anmeldenamen. Der Benutzername darf maximal 39 Zeichen lang sein.
Login name (Anmeldename)	Administrator	Hierbei handelt es sich um einen Namen, bei dem zwischen Groß- und Kleinschreibung unterschieden wird und den der Benutzer für die Anmeldung bei iLO 2 verwenden muss.
Password (Kennwort)	Eine zufällige alphanumerische Zeichenfolge aus 8 Zeichen, werkseitig zugewiesen	Hierbei handelt es sich um ein Kennwort, bei dem zwischen Groß- und Kleinschreibung unterschieden wird und das der Benutzer für die Anmeldung bei iLO 2 verwenden muss. Die Mindestlänge des Kennworts kann in „Security Options“ (Sicherheitsoptionen) festgelegt werden. Diese Mindestlänge kann auf einen Wert zwischen 0 und 39 Zeichen eingestellt werden. Die Standard-Mindestlänge beträgt 8 Zeichen. Zur Bestätigung muss das Kennwort zweimal eingegeben werden.
Administer user accounts (Benutzerkonten verwalten)	Ja	Diese Berechtigung gestattet einem Benutzer, Benutzerkonten hinzuzufügen, zu ändern und zu löschen. Außerdem kann ein Benutzer mit dieser Berechtigung die Berechtigungen sämtlicher Benutzer ändern und auch einem anderen Benutzer sämtliche Berechtigungen gewähren.
Remote console access (Fernzugriff auf die Konsole)	Ja	Diese Berechtigung ermöglicht einem Benutzer den Remote-Zugriff auf die Remote Console

Parameter	Standardwert	Definition
		eines verwalteten Systems, einschließlich Kontrolle über Bildschirm, Tastatur und Maus.
Virtual power and reset (Virtueller Netzschalter und Zurücksetzen)	Ja	Diese Berechtigung gestattet einem Benutzer, die Host-Plattform aus- und wieder einzuschalten und zurückzusetzen.
Virtuelle Medien	Ja	Diese Berechtigung gestattet einem Benutzer, ein virtuelles Medium der Host-Plattform zu nutzen.
Configure iLO 2 settings (iLO 2 Einstellungen konfigurieren)	Ja	Mit dieser Berechtigung kann ein Benutzer die meisten iLO 2 Einstellungen (z. B. die Sicherheitseinstellungen) konfigurieren. Die Administration von Benutzerkonten ist in dieser Berechtigung nicht enthalten. Nachdem iLO 2 korrekt konfiguriert wurde, kann durch die Rücknahme der Berechtigung für alle Benutzer verhindert werden, dass die iLO 2 Konfiguration nachträglich geändert wird. Ein Benutzer mit der Berechtigung „Administer Group Accounts“ (Gruppenkonten verwalten) kann diese Berechtigung aktivieren bzw. deaktivieren. iLO 2 kann auch dann neu konfiguriert werden, wenn das iLO 2 RBSU aktiviert ist.

Parameter für allgemeine Einstellungen

Einstellungen (Parameter) auf der Seite „Access Options“ (Zugriffsoptionen) der iLO 2 Benutzeroberfläche.

Parameter	Standardwert	Beschreibung
Idle Connection Timeout [minutes] (Zeitüberschreitung bei inaktiver Verbindung, in Minuten)	30 Minuten	Diese Einstellung legt das Zeitintervall für Benutzerinaktivität in Minuten fest, nach dem der Webserver und die Remote Console-Sitzung automatisch beendet werden. Die folgenden Einstellungen sind gültig: 15, 30, 60, 120 Minuten oder 0 (unbegrenzt). Bei einem unbegrenzten Timeout-Wert werden inaktive Benutzer nicht abgemeldet.
Lights-Out Functionality (Lights-Out-Funktionalität)	Aktiviert	Mit diesem Parameter wird die Verbindung zu iLO 2 aktiviert. Wenn er deaktiviert ist, werden keine Verbindungen zu iLO 2 zugelassen. Das iLO 2 10/100 Netzwerk und die Kommunikation mit den Treibern des Betriebssystems werden abgeschaltet, wenn die Lights-Out Funktionalität deaktiviert wird. Der iLO 2 Diagnoseport für einen HP ProLiant BL p-Class Server wird ebenfalls deaktiviert. Wenn die iLO 2 Funktionalität deaktiviert ist (einschließlich des iLO 2 Diagnoseports), müssen Sie zur Aktivierung von iLO 2 den Security Override-Schalter des Servers verwenden. Der Serverdokumentation können Sie die Position des Security Override-Schalters entnehmen, und wie er zur Übersteuerung der Sicherheit einzustellen ist. Schalten Sie den Server ein, und verwenden Sie das iLO 2 RBSU, um für die Lights-Out Funktionalität „Enabled“ (Aktiviert) einzustellen.
iLO 2 ROM-Based Setup Utility	Aktiviert	Diese Einstellung aktiviert oder deaktiviert das iLO 2 ROM-Based Setup Utility. Normalerweise fordert das iLO 2 Options-ROM zum Drücken von **F8** auf, um RBSU

Parameter	Standardwert	Beschreibung
		aufzurufen, aber wenn iLO 2 oder iLO 2 RBSU deaktiviert ist, wird die RBSU-Eingabeaufforderung umgangen.
Require Login for iLO 2 RBSU (Anmeldung für iLO 2 RBSU erforderlich)	Disabled (Deaktiviert)	Mit diesem Parameter wird RBSU Zugriff mit oder ohne Benutzeranmeldeinformationen gewährt. Lautet die Einstellung dieses Parameters „Enabled" (Aktiviert), wird beim Drücken von **F8** während des POST zum Aufruf des iLO 2 RBSU ein Anmeldedialogfeld angezeigt.
Show iLO 2 during POST (iLO 2 während POST anzeigen)	Disabled (Deaktiviert)	Mit diesem Parameter wird festgelegt, ob während des POST des Hostservers die IP-Adresse für das iLO 2 Netzwerk angezeigt wird.
Serial Command Line Interface Status (Status der seriellen Befehlszeilenschnittstelle)	Enabled-Authentication Required (Aktiviert – Authentifizierung erforderlich)	Mit diesem Parameter können Sie das Anmeldemodell des CLI-Merkmals über den seriellen Port ändern. Die folgenden Einstellungen sind gültig: • Enabled–Authentication Required (Aktiviert – Authentifizierung erforderlich) • Enabled – No Authentication (Aktiviert – Keine Authentifizierung) • Disabled (Deaktiviert)
Serial Command Line Interface Speed (Geschwindigkeit der seriellen Befehlszeilenschnittstelle)	9600	Über diesen Parameter können Sie die Übertragungsgeschwindigkeit des seriellen Ports für das CLI-Merkmal über den seriellen Port ändern. Die folgenden Geschwindigkeiten (in Bit/s) sind gültig: 9600, 19200, 38400, 57600 und 115200. Zur Sicherstellung des ordnungsgemäßen Betriebs muss die Konfiguration des seriellen Ports folgendermaßen lauten: Keine Parität, 8 Datenbits und 1 Stopp-Bit (N/8/1). Die über diesen Parameter eingestellte serielle Portgeschwindigkeit muss der im System-ROM RBSU konfigurierten seriellen Portgeschwindigkeit entsprechen.
Minimum Password Length (Mindestlänge von Kennwörtern)	8	Dieser Parameter gibt die minimale Anzahl Zeichen vor, die beim Ändern oder Festlegen eines Kennworts angegeben werden müssen. Die Anzahl der Zeichen kann auf einen Wert von 0 bis 39 festgelegt werden.
Server Name (Servername)		Mit diesem Parameter können Sie den Namen des Hostservers angeben. Dieser Wert wird bei der Verwendung von HP ProLiant Management Agents zugewiesen. Wenn Sie die Agents nicht verwenden und in einer Meldung auf einen unbenannten Host hingewiesen wird, können Sie die Einstellung hier ändern. Wenn die Agents ausgeführt werden, kann der von Ihnen zugewiesene Wert überschrieben werden. Um eine Aktualisierung des Browsers zu erzwingen, speichern Sie diese Einstellung, und drücken Sie die Taste **F5**.
Authentication Failure Logging (Protokollierung fehlgeschlagener Authentifizierungen)	Enabled-Every 3rd Failure (Aktiviert – jede 3. fehlgeschlagene Anmeldung)	Mit dieser Einstellung können Sie die Protokollierungskriterien für fehlgeschlagene Authentifizierungen konfigurieren. Alle Anmeldetypen werden unterstützt und funktionieren unabhängig voneinander. Die folgenden Einstellungen sind gültig: • Enabled-Every Failure (Aktiviert – jede fehlgeschlagene Anmeldung): Nach jedem fehlgeschlagenen Anmeldeversuch wird ein Eintrag für eine fehlgeschlagene Anmeldung protokolliert. • Enabled-Every 2nd Failure (Aktiviert – jede zweite fehlgeschlagene Anmeldung): Nach jedem zweiten fehlgeschlagenen Anmeldeversuch wird ein Eintrag für eine fehlgeschlagene Anmeldung protokolliert.

Parameter	Standardwert	Beschreibung
		• Enabled-Every 3rd Failure (Aktiviert – jede dritte fehlgeschlagene Anmeldung): Nach jedem dritten fehlgeschlagenen Anmeldeversuch wird ein Eintrag für eine fehlgeschlagene Anmeldung protokolliert. • Enabled-Every 5th Failure (Aktiviert – jede fünfte fehlgeschlagene Anmeldung): Nach jedem fünften fehlgeschlagenen Anmeldeversuch wird ein Eintrag für eine fehlgeschlagene Anmeldung protokolliert. • Disabled (Deaktiviert): Es wird kein fehlgeschlagener Anmeldeversuch protokolliert.

Einstellungen (Parameter) auf der Seite „Services“ (Dienste) der iLO 2 Benutzeroberfläche.

Parameter	Standardwert	Beschreibung
Secure Shell (SSH) Access (SSH-Zugriff)	Aktiviert	Mit diesem Parameter können Sie festlegen, ob das SSH-Merkmal für iLO 2 aktiviert oder deaktiviert werden soll.
Secure Shell (SSH) Port (SSH-Port)	22	Mit diesem Parameter können Sie für SSH-Kommunikationsvorgänge den iLO 2 SSH-Port konfigurieren.
Telnet Access (Telnet-Zugriff)	Disabled (Deaktiviert)	Mit diesem Parameter können Sie einen Telnet-Client mit dem Remote Console/Telnet-Port verbinden und das iLO 2 CLP somit zugänglich machen. Die folgenden Einstellungen sind gültig: • Enabled (Aktiviert): iLO 2 ermöglicht es Telnet-Clients, eine Verbindung zum Remote Console/Telnet-Port herzustellen. Netzwerkport-Scanner können erkennen, dass iLO 2 Daten von diesem Port empfängt. Zwischen dem iLO 2 CLP und Telnet-Clients sind unverschlüsselte Kommunikationsvorgänge möglich. • Disabled (Deaktiviert): iLO 2 ermöglicht es Telnet-Clients nicht, eine Verbindung zum Remote Console/Telnet-Port herzustellen. Netzwerkport-Scanner erkennen normalerweise nicht, ob dieser Port auf iLO 2 offen ist. Wenn Remote Console geöffnet wird, empfängt iLO 2 einige Sekunden lang Daten auf diesem Port, Telnet-Verbindungen werden jedoch nicht akzeptiert. Die Kommunikationsvorgänge zwischen iLO 2 und Remote Console sind immer verschlüsselt.
Remote Console/Telnet Port (Port für Remote Console/Telnet)	23	Mit diesem Parameter können Sie festlegen, welchen Port das iLO 2 für Kommunikationsvorgänge mit der Remote Console verwendet.
Web Server Non-SSL Port (Nicht-SSL-Port für Webserver)	80	Mit diesem Parameter können Sie festlegen, welchen Port der in iLO 2 integrierte Webserver für unverschlüsselte Kommunikationsvorgänge verwendet.
Web Server SSL Port (SSL-Port für Webserver)	443	Mit diesem Parameter können Sie festlegen, welchen Port der in iLO 2 integrierte Webserver für verschlüsselte Kommunikationsvorgänge verwendet.
Terminal Services Passthrough	Disabled (Deaktiviert)	Mit diesem Parameter können Sie steuern, ob über iLO 2 eine Verbindung zwischen einem Microsoft Terminal Services-Client und einem auf dem Host

Parameter	Standardwert	Beschreibung
		ausgeführten Terminal Services-Server unterstützt wird. Die folgenden Einstellungen sind gültig: • Automatic (Automatisch): Der Terminal Services-Client wird beim Start von Remote Console ebenfalls gestartet. • Enabled (Aktiviert): Die Passthrough-Funktion ist aktiviert und kann den Terminal Services-Client direkt mit iLO 2 verbinden, ohne dass eine Anmeldung bei iLO 2 erfolgen muss. • Disabled (Deaktiviert): Die Passthrough-Funktion ist deaktiviert.
Terminal Services Port (Port für Terminal Services)	3389	Mit diesem Parameter können Sie den Terminal Services-Port festlegen, den iLO 2 für verschlüsselte Kommunikationsvorgänge mit der Pass-Through-Software von Terminal Services auf dem Server verwendet. Wenn für den Terminal Services-Port eine andere Einstellung als die Standardeinstellung konfiguriert wird, müssen Sie die Portnummer manuell ändern.
Virtual Media Port (Port für Virtual Media)	17988	Mit diesem Parameter können Sie den Port zur Unterstützung von Virtual Media in iLO 2 Kommunikationsvorgängen festlegen.
Shared Remote Console Port (Port für Shared Remote Console)	9300	Mit diesem Parameter können Sie den Port für die Shared Remote Console angeben. Der Port für die Shared Remote Console wird auf dem Client geöffnet, um zusätzlichen Benutzern Peer-to-Peer den Aufbau einer Verbindung zur Remote Console zu gestatten. Dieser Port ist nur geöffnet, wenn die Shared Remote Console verwendet wird.
Console Replay Port (Port für die Konsolenwiedergabe)	17990	Mit diesem Parameter können Sie den Port für die Konsolenwiedergabe angeben. Der Konsolenwiedergabe-Port wird auf dem Client geöffnet, um die Übertragung interner wiederzugebender Erfassungsbuffer zum Client zu aktivieren. Dieser Port ist nur geöffnet, wenn ein Erfassungspuffer zum Client übertragen wird.
Raw Serial Data Port (Port unverarbeiteter serieller Daten)	3002	Dieser Parameter gibt die Adresse für den „Raw Serial Data Port“ (Port unverarbeiteter serieller Daten) an. Dieser Port ist nur offen, während mit dem Utility `WiLODbg.exe` ein Remote-Debugging des Hostservers durchgeführt wird.

Einstellungen (Parameter) auf der Seite „Encryption“ (Verschlüsselung) der iLO 2 Benutzeroberfläche.

Parameter	Standardwert	Beschreibung
Current cipher (Aktuelle Verschlüsselungsstärke)		Zeigt die aktuelle Verschlüsselungsstärke für diese Webbrowser-Sitzung an. Nach der Anmeldung bei iLO 2 mit dem Webbrowser handeln der Browser und iLO 2 die für die Sitzung zu verwendende Verschlüsselungsstärke aus. Diese Webseite zeigt die ausgehandelte Verschlüsselungsstärke an.
Enforce AES/3DES Encryption (AES/3DES-Verschlüsselung erzwingen)		Mit diesem Parameter können Sie die AES/3DES-Verschlüsselung aktivieren oder deaktivieren. • Disabled (Deaktiviert): Es wird keine AES/3DES-Verschlüsselung verwendet.

Parameter	Standardwert	Beschreibung
		• Enabled (Aktiviert): Für eine Verbindung zu iLO 2 ist als Verschlüsselungsstärke mindestens AES oder 3DES erforderlich.

Netzwerkparameter

Parameter	Standardwert	Definition
NIC	Ja	Mit diesem Parameter können Sie festlegen, dass der NIC den Zustand von iLO 2 angibt. Die Standardeinstellung lautet `yes` (aktiviert). Wenn DHCP deaktiviert ist, müssen Sie dem iLO 2 eine statische IPAdresse zuweisen. Verwenden Sie hierfür den iLO 2 Parameter für die Zuweisung von IP-Adressen.
DHCP	Ja	Ermöglicht die Auswahl statischer IPAdressen (deaktiviert) oder aktiviert die Verwendung eines DHCP-Servers zur Ermittlung einer IP-Adresse für das iLO 2 Subsystem. Wenn DHCP aktiviert ist, kann weder eine IP-Adresse noch eine Subnet-Maske für iLO 2 festgelegt werden. Die Aktivierung von DHCP ermöglicht die Konfiguration folgender DHCPOptionen: • Use DHCP Supplied Gateway (DHCP-Gateway verwenden) • Use DHCP Supplied DNS Servers (DHCP-DNS-Server verwenden) • Use DHCP Supplied WINS Servers (DHCP-WINS-Server verwenden) • Use DHCP Supplied Static Routes (Statische DHCP-Verbindungswege verwenden) • Use DHCP Supplied Domain Name (DHCP-Domänenname verwenden)
IP Address (IP-Adresse)	Nicht zutreffend (DHCP)	Mit diesem Parameter können Sie iLO 2 eine statische IP-Adresse im Netzwerk zuweisen. Standardmäßig wird die IPAdresse durch DHCP zugewiesen.
Subnet mask (Subnetzmaske)	Nicht zutreffend (DHCP)	Mit diesem Parameters weisen Sie die Subnetzmaske des Standard-Gateways zu. Standardmäßig wird die Subnetzmaske durch DHCP zugewiesen.
Gateway IP address (Gateway-IP-Adresse)	Nicht zutreffend (DHCP)	Mit diesem Parameter können Sie die IPAdresse des Netzwerk-Routers zuweisen, der das iLO 2 Subnetz mit einem anderen Subnetz verbindet, in dem sich die Management-Konsole befindet. Das Gateway wird standardmäßig von DHCP zugewiesen.
iLO 2 subsystem name (Name des iLO 2 Subsystems)	iLO 2*XXXXXXXXXXXX*, wobei die 12 *X* für die Seriennummer des Servers stehen (werkseitig zugewiesen)	iLO 2 verfügt ab Werk über einen DNS/WINS-Namen. Dieser DNS/WINS-Name lautet „iLO 2“, ergänzt um die Seriennummer des Servers. Der Name steht auch auf dem Etikett der iLO 2 Klammer.
Domain name (Domänenname)	Nicht zutreffend (DHCP)	Geben Sie den Namen der Domäne ein, zu der iLO 2 gehören wird. Standardmäßig wird der Domänenname durch DHCP zugewiesen.
Link	Automatic (Automatisch)	Konfiguriert den Duplexmodus des Netzwerk-Sendeempfängers.

Netzwerk-DHCP/DNS-Parameter

Parameter	Standardwert	Definition
DHCP	Aktiviert	Ermöglicht die Auswahl statischer IPAdressen (deaktiviert) oder aktiviert die Verwendung eines DHCP-Servers zur Ermittlung einer IP-Adresse für das iLO 2 Subsystem. Wenn DHCP aktiviert ist, kann weder eine IP-Adresse noch eine Subnet-Maske für iLO 2 festgelegt werden. Die Aktivierung von DHCP ermöglicht die Konfiguration folgender DHCPOptionen: • Use DHCP Supplied Gateway (DHCP-Gateway verwenden) • Use DHCP Supplied DNS Servers (DHCP-DNS-Server verwenden) • Use DHCP Supplied WINS Servers (DHCP-WINS-Server verwenden) • Use DHCP Supplied Static Routes (Statische DHCP-Verbindungswege verwenden) • Use DHCP Supplied Domain Name (DHCP-Domänenname verwenden)
IP-Address (IP-Adresse)	Nicht zutreffend (DHCP)	Mit diesem Parameter können Sie iLO 2 eine statische IP-Adresse im Netzwerk zuweisen. Standardmäßig wird die IPAdresse durch DHCP zugewiesen.
Domain Name (Domänenname)	Nicht zutreffend (DHCP)	Geben Sie den Namen der Domäne ein, zu der iLO 2 gehören wird. Standardmäßig wird der Domänenname durch DHCP zugewiesen.
Use DHCP Supplied Gateway (DHCP-Gateway verwenden)	Aktiviert	Legt fest, ob iLO 2 das Gateway des DHCP-Servers verwendet. Bei Deaktivierung muss ein Gateway in das Feld „Gateway IP Address“ (Gateway-IP-Adresse) eingegeben werden.
Use DHCP Supplied DNS Servers (DHCP-DNS-Server verwenden)	Aktiviert	Aktiviert bzw. deaktiviert die Verwendung der DNS-Serverliste des DHCP-Servers durch iLO 2. Bei Deaktivierung geben Sie die entsprechenden Werte in die Felder „Primary/Secondary/Tertiary DNS Server“ (Primärer, sekundärer und tertiärer DNS-Server) ein.
Use DHCP Supplied WINS Servers (DHCP-WINS-Server verwenden)	Aktiviert	Aktiviert bzw. deaktiviert die Verwendung der WINS-Serverliste des DHCP-Servers durch iLO 2. Bei Deaktivierung geben Sie die entsprechenden Werte in die Felder „Primary/Secondary WINS Server“ (Primärer und sekundärer WINS-Server) ein.
Use DHCP supplied static routes (Statische DHCP-Verbindungswege verwenden)	Aktiviert	Legt fest, ob iLO 2 den statischen Verbindungsweg des DHCP-Servers verwendet. Bei Deaktivierung geben Sie die entsprechenden Werte in die Felder „Static Route #1, #2, #3“ (Statischer Verbindungsweg 1, 2, 3) ein.
Use DHCP Supplied Domain Name (DHCP-Domänenname verwenden)	Aktiviert	Aktiviert bzw. deaktiviert die Verwendung des Domänennamens des DHCP-Servers durch iLO 2. Bei Deaktivierung geben Sie einen Namen in das Feld „Domain Name“ ein.
WINS Server Registration (WINS-Server-registrierung)	Aktiviert	iLO 2 wird automatisch bei einem WINSServer registriert. Standardmäßig werden die WINS-Serveradressen durch DHCP zugewiesen.
DDNS Server Registration (DDNS-Server-registrierung)	Aktiviert	iLO 2 wird automatisch bei einem DNSServer registriert. Standardmäßig werden die DNS-Serveradressen durch DHCP zugewiesen.
Ping gateway on startup (Ping-Signal	Disabled (Deaktiviert)	Diese Option veranlasst iLO 2, bei der Initialisierung vier ICMP-Echo-Anforderungspakete an das Gateway zu senden. Durch

Parameter	Standardwert	Definition
an Gateway bei Start)		diese Option wird sichergestellt, dass der ARP-Cache-Eintrag für iLO 2 im Router, der für das Routen von Paketen von und zu iLO 2 verantwortlich ist, aktuell ist.
Domain name (Domänenname)	Nicht zutreffend (DHCP)	Geben Sie den Namen der Domäne ein, zu der iLO 2 gehören wird. Standardmäßig wird der Domänenname durch DHCP zugewiesen.
DHCP-Server	Nicht zutreffend (DHCP)	Wenn DHCP auf `yes` eingestellt ist, wird diese Einstellung automatisch erkannt. Sie können diesen Wert nicht ändern.
Primary, Secondary, and Tertiary DNS Server (Primärer, sekundärer und tertiärer DNS-Server)	Nicht zutreffend (DHCP)	Mit diesem Parameter können Sie im Netzwerk eindeutige IP-Adressen für DNS-Server zuweisen. Standardmäßig werden primäre, sekundäre und tertiäre DNS-Server durch DHCP zugewiesen.
Primary and Secondary WINS Server (Primärer und sekundärer WINS-Server)	Nicht zutreffend (DHCP)	Mit diesem Parameter können Sie im Netzwerk eindeutige IP-Adressen für WINS-Server zuweisen. Standardmäßig werden primäre und sekundäre WINS-Server durch DHCP zugewiesen.
Static Route #1, #2, #3 (Statischer Verbindungsweg 1, 2, 3)	Sowohl für Ziel- als auch Gateway-Adresse nicht zutreffend (DHCP)	Mit diesem Parameter können Sie im Netzwerk ein eindeutiges Ziel eines statischen Verbindungswegs und ein Gateway-IP-Adressenpaar festlegen. Es können bis zu drei statische Verbindungsweg-Paare zugewiesen werden. Standardmäßig werden die statischen Verbindungswege durch DHCP zugewiesen.
Parameter für Blade-Server		
Parameter für Diagnoseport-Konfiguration		
Transceiver speed autoselect (Automatische Auswahl der Transceiver-Geschwindigkeit)	Ja	Aktiviert bzw. deaktiviert die Fähigkeit des Transceivers, die Geschwindigkeit und den Duplexmodus des Netzwerks automatisch zu erkennen. „Speed“ (Geschwindigkeit) und „Duplex“ sind deaktiviert, wenn „Autoselect“ (Autom. auswählen) auf `yes` eingestellt ist.
Speed (Geschwindigkeit)	Nicht zutreffend (Autoselect, wird automatisch ausgewählt)	Konfiguriert die Geschwindigkeit des Diagnoseports. Die Geschwindigkeit muss der Geschwindigkeit des Diagnoseport-Netzwerks entsprechen. Wenn die Option „Autoselect“ (Autom. auswählen) auf `yes` gesetzt ist, wird die Geschwindigkeit von iLO 2 automatisch konfiguriert.
Duplex	Nicht zutreffend (Autoselect, wird automatisch ausgewählt)	Konfiguriert den Duplexmodus des Diagnoseports. Der Duplexmodus muss dem Duplexmodus des Diagnoseport-Netzwerks entsprechen. Wenn die Option „Autoselect“ (Autom. auswählen) auf `yes` gesetzt ist, wird die Geschwindigkeit von iLO 2 automatisch konfiguriert.
IP Address (IP-Adresse)	192.168.1.1	Die IP-Adresse des Diagnoseports. Bei Verwendung von DHCP wird die IP-Adresse des Diagnoseports automatisch geliefert. Andernfalls muss hier eine statische IP-Adresse eingegeben werden.
Subnet mask (Subnetzmaske)	255.255.255.0	Die Subnetzmaske für das IP-Netzwerk des Diagnoseports. Bei Verwendung von DHCP wird die Subnetzmaske automatisch geliefert. Andernfalls muss hier die Subnetzmaske für das Netzwerk eingegeben werden.

Parameter für SNMP/Insight Manager Einstellungen

Parameter	Standardwert	Definition
SNMP Alert Destination(s) (Adresse(n) für SNMP-Alarmmeldungen)	Nein	Geben Sie die IP-Adresse des Remote Management PCs ein, der SNMP-Trap-Alarmmeldungen von iLO 2 erhalten soll. Sie können bis zu drei IP-Adresse für den Erhalt von SNMP-Alarmmeldungen vorsehen.
Enable iLO 2 SNMP alerts (iLO 2 SNMP-Alarmmeldungen aktivieren)	Nein	Die iLO 2 Alarmbedingungen werden von iLO 2 erkannt und sind unabhängig von dem jeweiligen Betriebssystems des Hostservers. Bei diesen Alarmmeldungen kann es sich um Insight Manager SNMP-Traps handeln. Diese Alarmmeldungen beziehen sich auf wichtige Ereignisse, wie z. B. einen Stromausfall des Servers oder einen Reset des Servers. Sie umfassen zudem iLO 2 Ereignisse wie z. B. deaktivierte Sicherheit oder fehlgeschlagene Anmeldeversuche. iLO 2 leitet die Alarmmeldungen an eine HP SIMconsole weiter und verwendet dabei die angegebenen Ziele.
Forward Insight Manager Agent SNMP Alerts (Insight Manager Agent SNMP-Alarmmeldungen weiterleiten)	Nein	Wenn die Option auf `yes` gesetzt ist, werden diese Alarmmeldungen von den Insight Management Agents generiert, die für jedes unterstützte Netzwerkbetriebssystem bereitgestellt werden. Diese Agents müssen auf dem Hostserver installiert sein, damit die Alarmmeldungen empfangen werden können. Diese Alarmmeldungen werden an HP SIM-Clients innerhalb des Netzwerks gesendet und asynchron von iLO 2 an die IP-Adressen weitergeleitet, die für ihren Erhalt konfiguriert wurden.
Enable SNMP Pass-Thru (SNMP-Pass-Through aktivieren)	Ja	Die Option „Enable SNMP Pass-Through“ (SNMP-Pass-Through aktivieren) ermöglicht es dem System, SNMP-Pakete vom Insight Management Agent zu übergeben. Wenn die Option auf `No` gesetzt ist, wird der gesamte SNMP-Datenverkehr angehalten und nicht von iLO 2 durchgereicht.
Insight Manager Web Agent URL (URL von Insight Manager Web Agent)		Die Option „Insight Manager Web Agent URL“ (URL von Insight Manager Web Agent) bietet Ihnen die Möglichkeit, die IP-Adresse oder den DNS-Namen des Hostservers einzugeben, auf dem die Insight Manager Web Agents ausgeführt werden. Nach Eingabe der Daten in dieses Feld kann iLO 2 einen Link von den iLO 2 Webseiten zu den Seiten des Web Agent erstellen.
Level of data returned (Umfang der zurückgegebenen Daten)	Medium (Mittel)	Die Option „Level of Data Returned“ legt den Umfang der Daten fest, die auf eine anonyme Abfrage von iLO 2 Informationen von HP SIM zurückgegeben werden. Mit Ausnahme der Option „None Data Level“ (Keine Datenrückgabe) werden grundsätzlich ausreichend Daten zurückgegeben, um eine Integration mit HP SIM zu ermöglichen. Die Einstellungen „Medium“ (Mittel) und „High“ (Hoch) ermöglichen HP SIM und Systems Insight Manager die Zuweisung des Managementprozessors zum Hostserver. „None Data Level“ legt fest, dass iLO 2 nicht auf HP SIM-Abfragen antwortet.

Parameter für Verzeichniseinstellungen

Parameter	Standardwert	Definition
Disable directory authentication (Verzeichnisauthentifizierung deaktivieren)	Nein	Dieser Parameter aktiviert bzw. deaktiviert die Verzeichnisauthentifizierung. Wenn die Verzeichnisunterstützung ordnungsgemäß konfiguriert

Parameter	Standardwert	Definition
		wurde, können sich Benutzer mit den Verzeichnis-Anmeldeinformationen bei iLO 2 anmelden.
Schema-free directory (Schemafreies Verzeichnis)	Ja	Dieser Parameter aktiviert oder deaktiviert die Verwendung schemafreier Verzeichnisse.
Use HP extended schema (HP erweitertes Schema verwenden)	Nein	Dieser Parameter aktiviert oder deaktiviert die Verwendung von Verzeichnissen mit erweitertem Schema.
Enable local user accounts (Lokale Benutzerkonten aktivieren)	Ja	Diese Option ermöglicht es einem Benutzer, sich mit einem lokalen Benutzerkonto anstatt mit einem Verzeichniskonto anzumelden. Standardmäßig ist diese Einstellung „Enabled" (Aktiviert).
Directory server address (Verzeichnisserveradresse)	0.0.0.0	Dieser Parameter gibt den DNS-Namen bzw. die IP-Adresse des Verzeichnisservers an. HP empfiehlt, einen DNS-Namen oder einen Multi-Host-DNS-Namen zu verwenden. Wenn eine IP-Adresse verwendet wird, ist das Verzeichnis nicht verfügbar, wenn dieser Server ausgefallen/ausgeschaltet ist.
Directory server LDAP port (LDAP-Port für Verzeichnisserver)	636	Diese Option legt die Portnummer für die Verbindung zum Verzeichnisserver fest. Die Nummer des SSL-gesicherten LDAP-Ports ist 636.
LOM object distinguished name (Eindeutiger Name für LOM-Objekt)		Diese Option gibt den eindeutigen iLO 2 Namen in dem betreffenden Verzeichnis an. DNs (Distinguished Names, eindeutige Namen) für LOM Objekte sind auf 256 Zeichen begrenzt.
LOM object password (Kennwort für LOM-Objekt)		Dieser Parameter gibt das Kennwort des iLO 2 Objekts für den Zugriff auf das Verzeichnis an. Kennwörter für LOM Objekte sind auf 39 Zeichen begrenzt. **HINWEIS:** Das Feld „LOM Object Password" (Kennwort für LOM-Objekt) wird zurzeit nicht verwendet. Dieses Feld ist aus Gründen der Aufwärtskompatibilität mit zukünftigen Firmware-Versionen vorgesehen.
LOM object password confirm (Bestätigung des Kennworts für LOM-Objekt)		Verhindert Tippfehler bei der Eingabe von Kennwörtern. Wenn Sie das Kennwort für das LOM-Objekt ändern, geben Sie auch in dieses Feld das neue Kennwort ein.
Directory user context 1, directory user context 2, … directory user context 15 (Verzeichnis-benutzerkontext 1, Verzeichnis-benutzerkontext 2, … Verzeichnisbenutzerkontext 15)		Mit diesen Parametern können Sie bis zu 15 durchsuchbare Kontexte für die Benutzersuche angeben, wenn ein Benutzer anhand des Verzeichnisses authentifiziert werden soll. Verzeichnis-Benutzerkontexte können jeweils eine maximale Länge von 128 Zeichen haben. Mithilfe von Verzeichnis-Benutzerkontexten können Sie die Benutzer-Container des Verzeichnisses angeben, die bei einem iLO 2 Anmeldeversuch automatisch durchsucht werden. Dadurch entfällt die Notwendigkeit, einen vollständigen DN für den Benutzer im Anmeldebildschirm einzugeben. Der Suchkontext „ou=lights out devices,o=corp" ermöglicht es dem Benutzer „cn=manager,ou=lights out devices,o=corp", sich bei iLO 2 einfach mit „manager" anzumelden. Active Directory lässt ein weiteres Suchkontextformat zu: „@hostname" (z. B. „@directory.corp").

Parameter für BL p-Class

Parameter	Standardwert	Definition
Rack Name (Rack-Name)	Vom Rack bereitgestellt	Der Rack-Name wird verwendet, um die Komponenten eines einzelnen Racks logisch zusammenzufassen. Geänderte

Parameter	Standardwert	Definition
		Rack-Namen werden an alle anderen im Rack angeschlossenen Komponenten übermittelt. Der Name trägt bei der Protokollierung und bei Alarmmeldungen zur Identifizierung der Komponente bei.
Enclosure Name (Gehäusename)	Vom Rack bereitgestellt	Der Gehäusename wird verwendet, um die Server-Blades in einem einzelnen Gehäuse logisch zusammenzufassen. Geänderte Gehäusenamen werden an alle im selben Gehäuse angeschlossenen Server-Blades übermittelt. Der Name trägt bei der Protokollierung und bei Alarmmeldungen zur Identifizierung der Komponente bei.
Bay name (Einschubsname)		Der Schachtname wird beim Erstellen von Protokolleinträgen und Alarmmeldungen verwendet, um Unterstützung beim Identifizieren einer Komponente oder einer Funktion zu geben.
Bay (Einschub)	Vom Rack bereitgestellt	Das ProLiant BL p-Class Gehäuse kann zwischen einem und acht Server-Blades unterstützen. Die Schächte sind von links nach rechts von 1 bis 8 nummeriert. Die Schachtnummer dient als Hilfe bei der physischen Identifizierung eines fehlerhaften Server-Blade oder anderer Fehlerzustände. Diese Angaben dienen lediglich zur Information.
Serial Number (Rack-Seriennummer)	Vom Rack bereitgestellt	Die Rack-Seriennummer identifiziert die Komponenten im Rack als logische Gruppierung. Die Seriennummer wird beim Hochfahren der verschiedenen Komponenten bestimmt, um eine eindeutige Rack-Seriennummer zu erstellen. Beim Austauschen von Komponenten (Server-Blade-Gehäuse oder Netzteilen) wird die Seriennummer des Racks geändert.
Enclosure Serial Number (Gehäuse-Seriennummer)	Vom Rack bereitgestellt	Die Seriennummer des Gehäuses bezeichnet das jeweilige Server-Blade-Gehäuse, in dem sich der entsprechende Server-Blade befindet.
Blade serial number (Blade-Seriennummer)	Vom Blade-Server bereitgestellt	Die Blade-Seriennummer identifiziert die Seriennummer des Server-Blade-Produkts.
Power source (Energiequelle)	Rack liefert Energie	Das Server-Blade-Gehäuse kann in zwei verschiedenen Konfigurationen in einem Rack installiert sein: • Mit den Server-Blade-Netzteilen kann normaler Netzstrom zur Stromversorgung des Racks in 48 V Gleichstrom umgewandelt werden. Wählen Sie in dieser Konfiguration **Rack Provides Power** (Strom wird vom Rack bereitgestellt) als Stromquelle aus. Bei dieser Einstellung kann jede Server-Blade, jedes Gehäuse und jedes Netzteil Stromversorgungsanforderungen übermitteln, um eine angemessene Stromversorgung zu gewährleisten, ohne Stromausfälle zu riskieren. • Wenn die Einrichtung direkt 48 V Gleichstrom liefern kann und keine Netzteile benötigt werden, wählen Sie **Facility Provides 48V** (48-V-Strom wird von der Einrichtung bereitgestellt) aus. Der jeweilige Server-Blade muss beim Ein- oder Ausschalten nicht mit der Stromversorgungs-Infrastruktur kommunizieren. **HINWEIS:** Damit alle Server-Blades und die anderen Komponenten des Racks ausreichend mit Strom versorgt werden, ist es wichtig, dass die Anforderungen an die Stromversorgung ordnungsgemäß erfüllt werden.
Enable automatic power on (Automatisches Einschalten aktivieren)	Leuchtet	Jeder Server-Blade kann so konfiguriert werden, dass er automatisch eingeschaltet wird, wenn er im Gehäuse eingesetzt ist. Je nach Stromversorgungseinstellungen kommuniziert der Server-Blade mit dem Rack, um zu bestimmen, ob zum Einschalten genug Strom zur Verfügung steht. Wenn der Strom zur Verfügung steht, schaltet sich der Server-Blade automatisch ein und beginnt mit dem normalen Server-Startvorgang.
Enable Rack Alert Logging [IML]	Leuchtet	Wenn der Server-Blade Alarmmeldungen empfängt, können diese Ereignisse im IML protokolliert werden. Diese Ereignisse können

Parameter	Standardwert	Definition
(Protokollierung von Rack-Alarmmeldungen aktivieren, IML)		über die Registerkarte „iLO 2 System **Status – IML** (iLO 2 Systemstatus – IML) angezeigt werden. Es stehen weitere IML-Anzeigetools zur Verfügung, mit denen die Anzeige unter dem auf dem Server-Blade installierten Betriebssystem möglich ist.

iLO Advanced Pack License Key (iLO Advanced Pack Lizenzschlüssel)

Die Option „iLO 2 Advanced Pack License Key“ (iLO 2 Advanced Pack Lizenzschlüssel) wird verwendet, um die erweiterten Funktionen von iLO 2 wie beispielsweise grafische Remote Console, virtuelle Medien (Diskette und CD-ROM) sowie Verzeichnisunterstützung zu aktivieren. Geben Sie den aus 25 Zeichen bestehenden Schlüssel in dieses Feld ein, um die Funktionen zu aktivieren.

13 Technischer Support

HP Kontaktinformationen

Für den Namen eines HP Partners in Ihrer Nähe:

- Rufen Sie die Webseite „Contact HP worldwide“ (in englischer Sprache) unter http://www.hp.com/go/assistance auf.

Für technischen Support von HP:

- HP Kontaktinformationen für andere Länder finden Sie auf der Website „Contact HP worldwide“ unter http://www.hp.com/go/assistance.

  Per Telefon kontaktieren Sie HP wie folgt:

  - Unter der Telefonnummer 1-800-334-5144. Dieser Service ist 24 Stunden täglich verfügbar. Um eine ständige Qualitätsverbesserung zu erreichen, können Anrufe ggf. aufgezeichnet oder überwacht werden.
  - Wenn Sie ein Care Pack (Service-Upgrade) erworben haben, rufen Sie in den USA unter der Telefonnummer 1-800-633-3600 an. Weitere Informationen über Care Packs finden Sie auf der HP Website unter http://h20559.www2.hp.com/portal/site/cpc?ac.admitted=1337622897556.2043657423.175170253.

Vor der Kontaktaufnahme mit HP

Bitte halten Sie die nachfolgend aufgeführten Informationen bereit, wenn Sie bei HP anrufen:

- Registrierungsnummer beim Technischen Support (sofern zutreffend)
- Seriennummer des Produkts
- Modellname und -nummer des Produkts
- Produkt-Identifizierungsnummer
- Eventuell vorliegende Fehlermeldungen
- Zusätzlich installierte Platinen oder Hardware
- Software und Hardware von Fremdherstellern
- Betriebssystem und Revisionsstufe

Akronyme und Abkürzungen

ASCII	American Standard Code for Information Interchange
ASM	Advanced Server Management (Erweiterte Serververwaltung)
ASR	Automatic Server Recovery (Automatische Serverwiederherstellung)
BMC	Baseboard Management Controller
CA	Certificate Authority (Zertifizierungsstelle)
CGI	Common Gateway Interface (Allgemeine Gateway-Schnittstelle)
CLI	Command Line Interface (Befehlszeilenschnittstelle)
CLP	Command Line Protocol (Befehlszeilenprotokoll)
CR	Zertifikatsanforderung
DAV	Distributed Authoring and Versioning
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DLL	Dynamic Link Library
DNS	Domain Name System
DSA	Digital Signature Algorithm
EMS	Emergency Management Services
EULA (Endbenutzer-Lizenzvereinbarung)	Endbenutzer-Lizenzvereinbarung (EULA)
FEH	Fatal Exception Handler
FSMO	Flexible Single-Master Operation
GUI	Graphical User Interface (Grafische Benutzeroberfläche)
HB	Heartbeat
HPONCFG	HP Lights-Out Online Configuration Utility
HPQLOMGC	HP Lights-Out Migration Command Line
ICMP	Internet Control Message Protocol
IIS	Internet Information Services
iLO	Integrated Lights-Out
IML	Integrated Management Log
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
ISIP	Enclosure Bay Static IP (Gehäuseeinschub – Statische IP)
JVM	Java Virtual Machine
KCS	Keyboard Controller Style (Tastatur-Controller-Stil)
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode (Leuchtdiode)
LOM	Lights-Out Management
LSB	Least Significant Bit (Niedrigstwertiges Bit)
MAC	Media Access Control
MLA	Master License Agreement (Master-Lizenzvertrag)
MMC	Microsoft Management Console
MP	Multilink Point-to-Point Protocol

MTU	Maximum Transmission Unit (Max. Übertragungseinheit)
NIC	Network Interface Controller
NMI	Non-Maskable Interrupt
NVRAM	Non-Volatile Memory (Nicht flüchtiger Speicher)
PERL	Practical Extraction and Report Language
PKCS	Public-Key Cryptography Standards
POST	Power-On Self-Test (Selbsttest beim Systemstart)
PSP	ProLiant Support Pack
RAS	Remote Access Service
RBSU	ROM-Based Setup Utility (ROM-basiertes SetupProgramm)
RDP	Remote Desktop Protocol
RIB	Remote Insight Board
RIBCL	Remote Insight Board Command Language (Befehlssprache für das Remote Insight Board)
RILOE	Remote Insight Lights-Out Edition
RILOE II	Remote Insight Lights-Out Edition II
RSA	Verschlüsselungsverfahren nach Rivest, Shamir und Adelman, das auf dem Prinzip des öffentlichen Schlüssels beruht
RSM	Remote Server Management
SLES	SUSE Linux Enterprise Server
SMASH	System Management Architecture for Server Hardware
SMS	System Management Server
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UART	Universal Asynchronous Receiver-Transmitter (Universeller asynchroner Sender/Empfänger)
UID	Unit Identification (Geräteidentifizierung)
USB	Universal Serial Bus
VM	Virtual Machine
VPN	Virtual Private Networking
WINS	Windows Internet Naming Service
WS	Web Services (Webdienste)
XML	Extensible Markup Language

Stichwortverzeichnis

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Z