HP Insight Control Server Provisioning 7.2 Administratorhandbuch

HP Teilenummer: 5900-2969
Ausgabedatum: Februar 2013
Ausgabe: 1

Marken

Microsoft, Windows, Windows XP und Windows NT sind eingetragene US-Marken der Microsoft Corporation.

Informationen zum Zugriff auf den Quellcode für die Open Source-Software, die durch HP Insight Control server provisioning verwendet wird, finden Sie im Dokument *HP Insight Management 7.2 Installation und Aktualisierung Versionshinweise* unter http://www.hp.com/go/insightmanagement/docs.

Inhalt

1 Einführung/Überblick

Was ist Insight Control server provisioning?

Insight Control Server Provisioning ist ein virtuelles Gerät, das zum Installieren und Konfigurieren von HP ProLiant Servern eingesetzt wird. Insight Control Server Provisioning verwendet Ressourcen wie OS Build Plans und Skripts, um Bereitstellungsaufträge auszuführen.
IC server provisioning bietet folgende Möglichkeiten:

- Installieren von Windows, Linux und ESXi auf ProLiant Servern
- Aktualisieren von Treibern, Dienstprogrammen und Firmware auf ProLiant Servern mit den HP Service Packs for ProLiant (SPPs)
- Konfigurieren von ProLiant Systemhardware, iLOs, BIOS und HP Smart Array
- Bereitstellen auf Zielservern ohne Verwendung von PXE (HP ProLiant Gen8 und höher)
- Gleichzeitige Ausführung von Bereitstellungsjobs auf mehreren Servern
- Anpassen von ProLiant Bereitstellungen über eine einfach zu bedienende Browserschnittstelle
- Migrieren von HP Insight Control Server Deployment (RDP) zu Insight Control Server Provisioning

Tabelle 1 Informationsquellen

Thema	Informationsquellen
Versionshinweise	Siehe Abschnitt zu Insight Control Server Provisioning im Dokument *HP Insight Control Versionshinweise* unter http://www.hp.com/go/insightcontrol/docs.
Support Matrix	Siehe Abschnitt zu Insight Control Server Provisioning im Dokument *HP Insight Management Support Matrix* unter http://www.hp.com/go/insightcontrol/docs.
Erstmaliges Herunterladen und Einrichten der Appliance	Siehe *HP Insight Control Server Provisioning Installationshandbuch* unter http://www.hp.com/go/insightcontrol/docs.
Online-Hilfe im PDF-Format	Der Inhalt der Online-Hilfe ist im PDF-Format unter http://www.hp.com/go/insightcontrol/docs verfügbar.
Detaillierte Informationen	Detaillierte Informationen zu Strategie und Verwendung finden Sie im *HP Insight Control Server Provisioning Administratorhandbuch* unter http://www.hp.com/go/insightcontrol/docs.
Vorbereitung	Der Abschnitt Schnellstart in der Online-Hilfe unterstützt Sie bei der Verwendung von Insight Control server provisioning zur Durchführung realistischer Aufgaben. Im Abschnitt mit den Vorgehensweisen in der Online-Hilfe finden Sie einführende Informationen und Anleitungen zur Durchführung bestimmter Aufgaben.
Begriffe	Siehe Glossar zu Insight Control server provisioning : „Glossar“ (Seite 52).
Fehlerbehebung sowie bekannte Probleme und Einschränkungen	Der Index zur Fehlerbehebung in der Online-Hilfe enthält Informationen zu Problemen/Empfehlungen, die von Entwicklern von IC server provisioning bereitgestellt werden. Siehe Abschnitt zu Insight Control Server Provisioning im Dokument *HP Insight Control Versionshinweise* unter http://www.hp.com/go/insightcontrol/docs. Siehe Abschnitt zu Insight Control Server Provisioning im Dokument *HP Insight Management Support Matrix* unter http://www.hp.com/go/insightcontrol/docs.
Benutzeroberfläche	Siehe folgendes Thema im Abschnitt mit den Vorgehensweisen in der Online-Hilfe: Navigation auf der Benutzeroberfläche

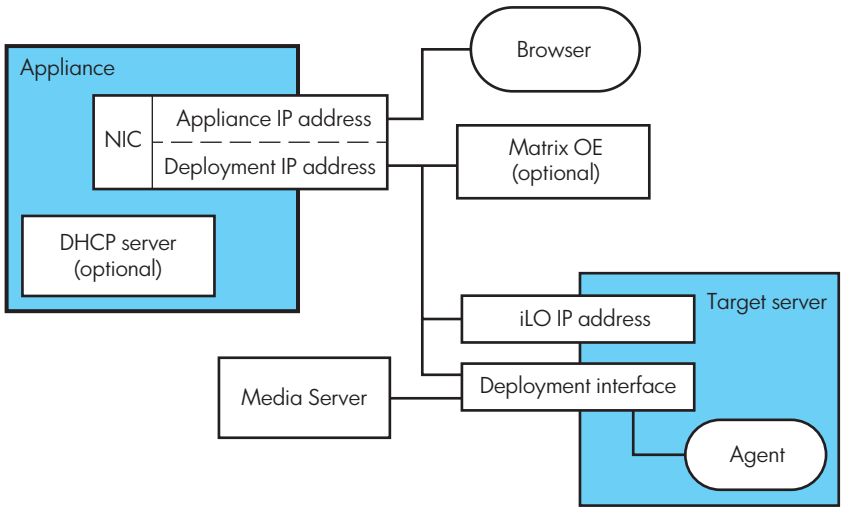
Tabelle 1 Informationsquellen *(Fortsetzung)*

Thema	Informationsquellen
Migration von HP Insight Control Server Deployment	Siehe das White Paper *Data Migration from Insight Control server deployment to Insight Control server provisioning* (Datenmigration von Insight Control Server Deployment zu Insight Control Server Provisioning) unter http://www.hp.com/go/insightcontrol/docs.
White Paper	White Paper zu verschiedenen Themen sind verfügbar unter http://www.hp.com/go/insightcontrol/docs.

1.1 Komponenten von Insight Control server provisioning

Das folgende Diagramm veranschaulicht die Zusammenarbeit von Netzwerken mit virtuellen IC server provisioning-Geräten, Media Server, Zielserver und optional HP Matrix Operating Environment.

Abbildung 1 Komponenten von Insight Control server provisioning



- Das **Gerät** ist das HP Insight Control server provisioning-Produkt, das als virtuelle Maschine zur optimalen Ausführung der Anwendung bereitgestellt wird.
- Im Umfang des Insight Control server provisioning-Geräts ist ein eingebetteter **DHCP server (DHCP-Server)** enthalten. Je nach Umgebung können Sie diesen Server konfigurieren oder über den Bildschirm **Settings (Einstellungen)** des Geräts deaktivieren. Weitere Informationen finden Sie in „Entscheidung für einen geräteinternen oder einen geräteexternen DHCP-Server" (Seite 10).
- Die **Appliance IP address (Geräte-IP-Adresse)** ist die dem Gerät zugewiesene Adresse. Mit dieser IP-Adresse können Sie über einen unterstützten **Browser** zum Gerät navigieren.
- Die **Deployment IP address (Bereitstellungs-IP-Adresse)** ist die vom Bereitstellungsmodul innerhalb des Geräts verwendete IP-Adresse. Sie dient zur Kommunikation mit der IP-Adresse der **Deployment interface (Bereitstellungsschnittstelle)** eines **Target server (Zielserver)** und der entsprechenden **iLO IP address (iLO-IP-Adresse)**. Diese befindet sich in demselben Netzwerk wie die **Appliance IP address (Geräte-IP-Adresse)**. Bei Verwendung von IC server provisioning mit HP Matrix Operating Environment handelt es sich hierbei um die IP-Adresse, die für **Matrix OE** bereitgestellt werden muss.
- Der **Target server (Zielserver)** repräsentiert einen von IC server provisioning verwalteten Server. Auf jedem verwalteten Server wird ein **Agent** ausgeführt. Hierbei handelt es sich um Software, mit der Änderungen auf dem Server vorgenommen werden. Der Agent dient zur Installation und Entfernung von Software, Konfiguration von Hardware und Software und Erstellung von Berichten zum Serverstatus.

- Der **Media Server** enthält die bei der Betriebssystembereitstellung verwendeten vom Anbieter bereitgestellten Betriebssystemmedien. Der Media Server kann auch Medien für andere Zwecke enthalten, zum Beispiel Firmware- und Treiber-Updates, und ist außerdem der Ort, an dem erfasste Images gespeichert werden. Der Media Server ist ein vom Insight Control server provisioning-Gerät getrennter Server und nicht im Umfang der Sicherungs- und Wiederherstellungsfunktionen des Geräts enthalten.

1.2 Hinzufügen von Servern

Bevor Sie einen Job auf einem Zielserver ausführen können, muss dieser Server zunächst Insight Control server provisioning hinzugefügt werden. Dazu stehen verschiedene Möglichkeiten zur Verfügung. Die verschiedenen Methoden und ihre Unterschiede werden in den folgenden Abschnitten beschrieben. Siehe auch „Hinzufügen von Servern, auf denen bereits ein Betriebssystem ausgeführt wird“ (Seite 45).

1.2.1 Hinzufügen eines Servers über iLO

Sie können Insight Control server provisioning einen HP ProLiant Bare-Metal-Server hinzufügen, indem Sie die Zugangsinformationen des im Server eingebetteten iLO-Verwaltungsprozessors angeben. Geben Sie dazu die iLO-IP-Adresse, den Benutzernamen und das Kennwort im Bildschirm **Add server (Server hinzufügen)** des Geräts ein. Das Gerät kontaktiert iLO, verifiziert die Verbindung und fügt den Server der Liste **Servers (Server)** hinzu. Außerdem steht eine REST-API zum Hinzufügen eines Servers über iLO zur Verfügung (siehe „REST-Aufruf zum Hinzufügen eines Servers über iLO“ (Seite 40)).

Beim Hinzufügen eines Servers über iLO verwendet das Gerät standardmäßig iLO zum Starten des Servers in das im Bildschirm **Settings (Einstellungen)** des Geräts angegebene Standardservicebetriebssystem. Durch Starten des Servers im Wartungsmodus kann IC server provisioning eine vollständige Ermittlung durchführen. Es werden alle Serverinformationen, die auf der Eigenschaftenseite **Server** erforderlich sind, erfasst. Dieser Vorgang dauert einige Minuten, da der Server aus- und wieder eingeschaltet und dann gestartet wird.

Wenn der Server nicht im Wartungsmodus gestartet werden soll, wählen Sie die entsprechende Option auf der Seite **Add server (Server hinzufügen)** aus. Mit dieser Option wird der Server der Liste **Servers (Server)** mit dem Anzeigenamen **ILOHOST_<*iLO IP address*>** hinzugefügt und auf der Eigenschaftenseite **Servers (Server)** sind keine Servereigenschaften verfügbar. Dieser Vorgang nimmt weniger Zeit in Anspruch, da der Server nicht gestartet werden muss.

Auf einem Server kann unabhängig vom Wartungsmodus ein Build Plan ausgeführt werden, da die meisten Build Plans den Server im Wartungsmodus starten, sofern er sich nicht bereits in diesem Modus befindet.

1.2.2 PXE-Systemstart eines Servers im Wartungsmodus

Eine andere Möglichkeit, IC server provisioning einen Server hinzuzufügen, besteht in einem PXE-Systemstart dieses Servers in ein Servicebetriebssystem. Wenn der Server den Startvorgang abschließt, kontaktiert der Agent im Servicebetriebssystem das Gerät und registriert es automatisch für das Gerät. Der Server wird dann in der Liste **Servers (Server)** des Geräts angezeigt. Zum Hinzufügen eines Servers mit dieser Methode muss der Server nur eingeschaltet werden.

Wenn auf dem Zielserver kein Betriebssystem installiert ist, erfolgt automatisch ein PXE-Systemstart. Ist ein Betriebssystem auf dem Server installiert, drücken Sie die entsprechende Taste auf der Konsole, um einen PXE-Systemstart auszulösen.

Der Server startet das Standard-Servicebetriebssystem, das auf dem Bildschirm **Settings (Einstellungen)** des Geräts angegeben ist.

HINWEIS: Ein über PXE-Systemstart hinzugefügter Server verfügt automatisch über ein spezielles Zugriffskonto, das auf dem iLO des Servers mit dem Benutzernamen `hp_automatic_integration_user` und einem automatisch generierten Kennwort erstellt wird. Dieses Konto darf nicht gelöscht und das Kennwort auf dem iLO nicht geändert werden.

1.2.3 Auswahl der Methode zum Hinzufügen eines Servers

Die folgenden Punkte unterstützen Sie bei der Entscheidung, welche Methode Sie zum Hinzufügen von Servern verwenden sollten.

Gründe für das Hinzufügen von Servern über iLO

- Sie verfügen über die iLO-Anmeldedaten für Ihre Zielserver.
- Sie verfügen über Gen8 oder neuere Server und möchten HP Intelligent Provisioning verwenden.
- Sie möchten keinen PXE-Systemstart für Gen8 oder die neueren Server ausführen.
- Sie möchten nicht, dass auf Ihren iLOs automatisch ein spezielles Zugriffskonto erstellt wird.

Gründe für das Starten im Wartungsmodus bei Verwendung von iLO

- Es sollen alle Serverinformationen ermittelt werden, sodass sie sichtbar sind und für die Suche in der UI verwendet werden können.
- Vor dem Ausführen eines Build Plan soll die Servernetzwerkverbindung überprüft werden.
- Sie führen einen Build Plan mit Netzwerkpersonalisierung aus, sodass Sie die Bereitstellungs-NIC des Servers einrichten müssen. (Die Netzwerkpersonalisierung kann erst verwendet werden, wenn der Server mindestens einmal im Wartungsmodus gestartet wurde.)
- Der auszuführende Build Plan erfordert das Standard-Servicebetriebssystem, womit Sie später Zeit sparen.
- Der Server soll mit seinem DNS-Standardnamen aufgelistet werden.

Gründe gegen das Starten im Wartungsmodus bei Verwendung von iLO

- Es soll sofort ein Build Plan ausgeführt werden und Sie möchten nicht warten, bis der Server startet.
- Sie möchten den Server ausgeschaltet lassen, bis Sie bereit sind, ihn zu installieren.
- Alle Server sind vom gleichen Typ, sodass Sie nicht die vollständigen Eigenschafteninformationen benötigen.

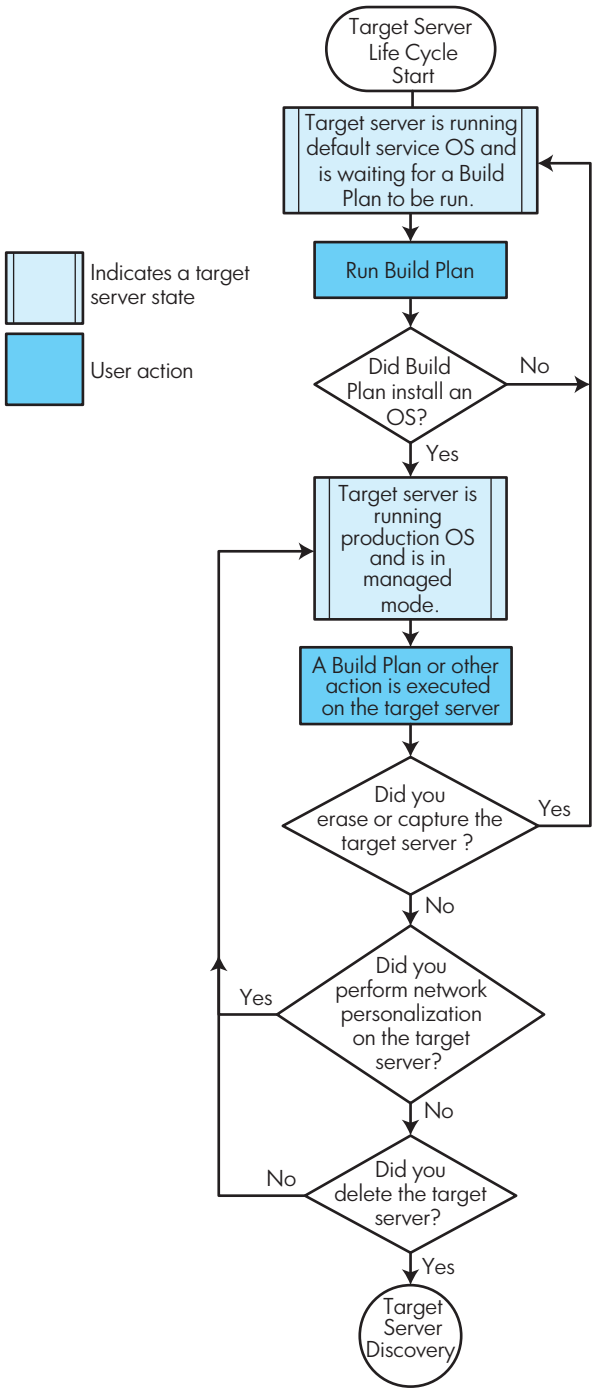
Gründe für den PXE-Start

- Sie verfügen nicht über die iLO-Anmeldedaten für Ihre Zielserver.
- Sie bevorzugen PXE für alle Anforderungen.
- HP Intelligent Provisioning soll nicht auf Gen8 oder neueren Servern verwendet werden.
- Sie bevorzugen eine einfache Ermittlung beim Einschalten, da Ihre Server automatisch einen PXE-Systemstart ausführen.
- Sie verfügen über eine große Anzahl von Servern, wodurch die manuelle Eingabe der iLO-Anmeldedaten undurchführbar wird.

1.3 Serverlebenszyklus

Das folgende Diagramm veranschaulicht den typischen Lebenszyklus eines von Insight Control server provisioning verwalteten Zielservers.

Abbildung 2 Lebenszyklus von Insight Control server provisioning-Zielservern



2 Konfigurieren von Geräteeinstellungen

2.1 Netzwerkkonfiguration

2.1.1 Entscheidung für einen geräteinternen oder einen geräteexternen DHCP-Server

HP Insight Control server provisioning erfordert, dass ein DHCP-Server Zielservern während des Bereitstellungsprozesses IP-Adressen bereitstellt. Insight Control server provisioning verfügt über einen geräteinternen DHCP-Server, den Sie zu diesem Zweck verwenden können. Sie können auch einen eigenen geräteexternen DHCP-Server einrichten. In diesem Abschnitt erhalten Sie Unterstützung bei der Entscheidung, was für Ihren Standort besser ist.

1. Betrachten Sie zunächst Ihre DHCP-Anforderungen bei der Bereitstellung von Servern: Nur IP-Adresse oder erweiterte DHCP-Optionen

   Nur IP-Adresse

   In dieser Konfiguration muss Ihr DHCP-Server den Zielservern nur Standardnetzwerkinformationen (IP-Adresse, Netzmaske usw.) bereitstellen. Diese einfache Konfiguration kann verwendet werden, wenn Ihre Umgebung *alle* der folgenden Bedingungen erfüllt:

   - Sie führen keinen PXE-Systemstart für einen Server aus.
   - Bei Ihren Zielservern handelt es sich ausnahmslos um HP ProLiant Server der Serie Gen8 oder neuer.
   - Sie verwenden die eingebetteten HP Intelligent Provisioning-Funktionen Ihrer ProLiant Server (kein PXE).
   - Zum Hinzufügen von Servern zum Gerät verwenden Sie iLO-IP-Adressen und -Anmeldedaten.

   Erweiterte DHCP-Optionen

   In dieser Konfiguration muss der DHCP-Server Standardnetzwerkinformationen sowie zusätzliche Optionen bereitstellen, sodass die Zielserver einen PXE-Systemstart vom Gerät aus im erforderlichen Servicebetriebssystem ausführen können. Diese erweiterte DHCP-Konfiguration ist erforderlich, wenn Ihre Umgebung *eine* der folgenden Bedingungen erfüllt:

   - Für die Server wird ein PXE-Systemstart ausgeführt (dies umfasst einen PXE-Systemstart zum Hinzufügen von Servern zum Gerät).
   - Ihre Zielserver sind älter als Server der Serie Gen8.
   - Sie verfügen über Zielserver der Serie Gen8, verwenden jedoch kein Intelligent Provisioning.
   - Server sollen nicht über iLO zum Gerät hinzugefügt werden.

2. Überlegen Sie als Nächstes, ob der geräteinterne DHCP-Server verwendet oder ein externer DHCP-Server konfiguriert werden soll.

   Geräteinterner DHCP-Server

   Im Umfang des Insight Control server provisioning-Geräts ist ein integrierter DHCP-Server enthalten, der einfach zu konfigurieren und zu verwenden ist und der alle für den PXE-Systemstart erforderlichen erweiterten Informationen bereitstellt.

   - Einfache Konfiguration über die Seite **Settings (Einstellungen)** des Geräts
   - Bereitstellung von Adressen ausschließlich für das Subnetz Ihres Geräts
   - Unterstützung optionaler Informationen, wie DNS und Gateway
   - Ausnahmslose Bereitstellung der für den PXE-Systemstart von Zielservern erforderlichen erweiterten Informationen

Externer DHCP-Server

Ein externer DHCP-Server ist in folgenden Fällen sinnvoll:

- In Ihrem Netzwerk ist bereits ein DHCP-Server enthalten.
- Sie benötigen anspruchsvollere Funktionen als mit der Geräte-UI konfigurierbar.

HINWEIS: Der TFTP-Server des Geräts, der Zielservern einen PXE-Systemstart vom Gerät aus ermöglicht, wird immer ausgeführt, unabhängig davon, ob ein geräteinterner oder ein geräteexterner DHCP-Server verwendet wird.

2.1.2 Einrichten eines geräteexternen DHCP-Servers

Das Insight Control server provisioning-Gerät unterstützt sowohl die Verwendung des geräteinternen DHCP-Servers als auch die Verwendung eines an Ihrem Standort konfigurierten externen DHCP-Servers.

Wenn Sie von Ihrem DHCP-Server mehr Kontrolle oder Funktionen benötigen, als über die Geräte-UI verfügbar sind, sollten Sie den DHCP-Server auf dem Gerät deaktivieren und einen eigenen Server konfigurieren. Details finden Sie unter „Entscheidung für einen geräteinternen oder einen geräteexternen DHCP-Server“ (Seite 10).

Nachfolgend finden Sie Anweisungen zum Konfigurieren eines externen Windows-DHCP-Servers bzw. eines externen Linux ISC DHCP-Servers.

HINWEIS: HP empfiehlt, die Leasedauer auf Ihrem DHCP-Server mindestens auf einen Tag einzustellen, um Probleme durch die Zeitsynchronisation zu vermeiden.

HINWEIS: Diese Anweisungen beziehen sich auf das Konfigurieren der erweiterten DHCP-Optionen, die für den PXE-Systemstart von Zielservern vom Gerät aus erforderlich sind. Wenn Sie keine erweiterten Optionen benötigen, ist abgesehen von der Fähigkeit, Zielservern eine IP-Adresse bereitzustellen, und einer möglichen Verlängerung der Leasedauer, keine spezielle Konfiguration erforderlich.

HINWEIS: Wenn Sie einen externen DHCP-Server verwenden möchten, muss die Option **Service provided by appliance (Von Gerät bereitgestellter Dienst)** auf der Seite **Settings (Einstellungen) DHCP** auf `None` festgelegt sein.

HINWEIS: Die Bereitstellungs-IP-Adresse finden Sie auf der Seite **Settings (Einstellungen) Appliance (Gerät)** unter **Deployment IP (Bereitstellungs-IP)**.

Prozedur 1 So richten Sie einen externen Windows-DHCP-Server ein

1. Fügen Sie Ihrem Windows-System eine DHCP-Serverrolle hinzu.
2. Legen Sie den Bereich fest und starten Sie den Server. Die Leasedauer muss auf einen Tag oder mehr festgelegt werden.
3. Fügen Sie den globalen IPv4-Einstellungen des DHCP-Servers folgende Optionen hinzu:

   Tabelle 2 Globale Windows-DHCP-IPv4-Einstellungen

Code	Optionsname	Datentyp
186	`buildmgr_ip`	IP-Address (IP-Adresse)
187	`buildmgr_port`	Wort

4. Weisen Sie den DHCP-Optionen in Ihrem DHCP-Bereich folgende Werte zu:

Tabelle 3 Windows-DHCP-Optionen

Optionsnummer	Optionsname	Optionswert
66	Boot server (Bootserver)	*<Deployment IP address of appliance>*
67	Boot filename (Startdateiname)	pxelinux.0
186	buildmgr_ip	*<Deployment IP address of appliance>*
187	buildmgr_port	0x1F51

Prozedur 2 So richten Sie einen externen Linux-DHCP-Server ein

Wenn Sie einen ISC-Linux-DHCP-Standardserver verwenden, legen Sie die folgenden Optionen fest, um für Server einen Systemstart vom Gerät aus durchzuführen.

1. Die Leasedauer muss auf mindestens einen Tag festgelegt werden. Beispiel:

   ```
   default-lease-time 86400;
   max-lease-time 129600;
   ```

2. Die folgenden Zeilen müssen in globalen Optionsdeklarationen enthalten sein:

   ```
   option buildmgr_ip code   186 = ip-address;
   option buildmgr_port code 187 = unsigned integer 16;
   ```

3. Die folgenden Optionen und Werte müssen je nach Anforderungen entweder im globalen oder im Umfangsbereich festgelegt werden:

   ```
   next-server <Deployment-IP-Address-of-appliance>;
   filename "pxelinux.0";
   option buildmgr_ip <Deployment-IP-Address-of-appliance>;
   option buildmgr_port 8017;
   option dhcp-parameter-request-list = concat(dhcp-parameter-request-list,ba,bb,fc);
   ```

   Beispiel:

   ```
   next-server 172.1.3.10;
   filename "pxelinux.0";
   option buildmgr_ip 172.1.3.10;
   option buildmgr_port 8017;
   option dhcp-parameter-request-list = concat(dhcp-parameter-request-list,ba,bb,fc);
   ```

Sobald diese Optionen ordnungsgemäß eingerichtet sind, können Sie Ihr Gerät für den PXE-Systemstart von Servern verwenden.

3 Sichern und Wiederherstellen Ihres Geräts

3.1 Übersicht

Insight Control server provisioning stellt Dienste zum Sichern und Wiederherstellen eines Geräts bereit. Sollte ein Gerät verloren gehen oder beschädigt werden, muss es möglicherweise über eine Sicherung wiederhergestellt werden.

Eine Sicherung enthält Konfigurationseinstellungen und Verwaltungsdaten und wird in einer proprietär formatierten Datei gespeichert.

Für Sicherungs- und Wiederherstellungsvorgänge stehen REST-APIs und Beispielskripts zur Verfügung. Beispielskripts sind auf Insight Control Server Provisioning-Medien und in der Zip-Datei des Produktdownloads verfügbar.

Eine Sicherung kann auf demselben Gerät oder auf einem anderen Gerät wiederhergestellt werden. Wenn ein Gerät fehlerhaft ist und nicht repariert werden kann, kann die Sicherung auf einem Ersatzgerät wiederhergestellt werden.

Damit die Sicherung erfolgreich wiederhergestellt wird, muss auf dem Gerät eine Version der Firmware ausgeführt werden, die mit der Sicherung kompatibel ist. Versionen sind kompatibel, wenn die ersten beiden Komponenten der Versionsnummer identisch sind.

Während einer Wiederherstellung gleicht die Gerätefirmware die Daten in der Sicherung mit dem aktuellen Status der verwalteten Umgebung ab. Einige Abweichungen können bei der Wiederherstellung nicht automatisch behoben werden. Nach Abschluss einer Wiederherstellung müssen noch bestehende Inkonsistenzen, auf die in Warnmeldungen hingewiesen wird, manuell vom Geräteadministrator behoben werden.

△ **ACHTUNG:** Durch Wiederherstellen einer Sicherung werden sämtliche Verwaltungsdaten und die meisten Konfigurationseinstellungen auf dem Gerät ersetzt. Das Gerät ist während einer Wiederherstellung nicht betriebsbereit. Eine Wiederherstellung kann mehrere Stunden dauern. Sie kann nach dem Start weder abgebrochen noch rückgängig gemacht werden. Wenn bei der Wiederherstellung ein nicht behebbarer Fehler auftritt, müssen Sie eine neue Gerätevorlage herunterladen. Dieser Vorgang wird im *HP Insight Control Server Provisioning Installation Guide* (HP Insight Control Server Provisioning Installationshandbuch) beschrieben, das unter http://www.hp.com/go/insightcontrol/docs verfügbar ist. Eine Wiederherstellung sollte nur im Falle einer schwerwiegenden Störung verwendet werden. Sie sollte nicht bei kleineren Problemen Anwendung finden, die auf andere Weise gelöst werden können.

3.2 Erstellen und Herunterladen einer Gerätesicherung

3.2.1 Empfohlene Sicherungsverfahren

HP empfiehlt regelmäßige Sicherungen, vorzugsweise einmal täglich. Sicherungen werden während des normalen Betriebs des Geräts vorgenommen. Vor dem Erstellen einer Sicherung müssen Sie nicht darauf warten, dass die Aufgaben abgeschlossen werden. Zum Wiederherstellen einer Sicherung laden Sie sie auf das Gerät hoch und fordern Sie die Gerätewiederherstellung von der Sicherung an.

Eine Sicherung sollte vor und nach dem Aktualisieren der Gerätefirmware ausgeführt werden.

HP empfiehlt die Verwendung eines Unternehmenssicherungs-/-wiederherstellungsprodukts wie HP Data Protector zur Archivierung von Sicherungsdateien. REST-APIs werden zur Integration mit Unternehmenssicherungs-/-wiederherstellungsprodukten bereitgestellt.

Nach einer Sicherung muss die Sicherungsdatei vom Gerät heruntergeladen und an einem sicheren Ort gespeichert werden. Die Sicherungsdatei muss heruntergeladen werden, bevor die nächste Sicherung durchgeführt wird, damit sie nicht überschrieben wird.

Es kann jeweils nur eine Sicherung ausgeführt werden.

Der Name der Sicherungsdatei hat folgendes Format:

`<appliance host name>_backup_<yyyy-mm-dd_hhmmss>.bkp`

Beispiel: `myhost_backup_2012-10-01_092700.bkp`. In diesem Beispiel wurde die Sicherung am 1. Oktober 2012 um 9:27 Uhr für den Gerätehostnamen `myhost` erstellt.

Es sind nur Benutzer mit der Rolle eines Infrastruktur- oder Sicherungsadministrators zum Erstellen einer Sicherung berechtigt. Die Wiederherstellung einer Sicherung kann nur von einem Infrastrukturadministrator vorgenommen werden.

3.2.2 Übersicht über die Sicherungs-REST-API

Die Sicherungs-REST-API stellt REST-Aufrufe für Folgendes bereit:

- Sicherung anfordern
- Sicherungsstatus überprüfen
- Abgeschlossene Sicherung herunterladen
- Sicherung abbrechen

Diese Aufrufe sind in der Tabelle unten zusammengefasst. Für die REST-API-Sicherungsaufrufe ist eine Sitzungs-ID zur Autorisierung erforderlich. Diese erhalten Sie, indem Sie als Benutzer mit der Rolle eines Sicherungs- oder Infrastrukturadministrators die REST-Anforderung zur Anmeldung am Gerät ausgeben.

REST-Aufruf	Anforderungsheader	Anforderungstext	Antwortheader	Antworttext	Beschreibung
POST https://{appl}/rest/backups/	auth: session ID, accept-language: locale, accept-content: application/json, X-API-Version: 1	N/A	N/A	Eine Aufgabenressource, die eine URI zur Prüfung des Sicherungsstatus und eine associatedResourceUri zum Abrufen detaillierter Informationen über die Sicherung enthält	Erstellung einer Sicherung vom Gerät anfordern
GET https://{appl}/{uri}	auth: session ID, accept-language: locale, accept-content: application/json, X-API-Version: 1	N/A	N/A	Eine Aufgabenressource, die den aktuellen Sicherungsstatus enthält	Sicherungsstatus abrufen
GET https://{appl}/{associatedResourceUri}	auth: session ID, accept-language: locale, accept-content: application/json, X-API-Version: 1	N/A	N/A	Eine Sicherungsressource, die detaillierte Informationen über eine Sicherung, einschließlich downloadUri zum Herunterladen der Sicherung, enthält	Detaillierte Informationen über die angeforderte Sicherung, einschließlich Download-URI, abrufen
GET https://{appl}/{downloadUri}	auth: session ID, accept-language: locale, accept-content: application/octet-stream; q=0.8, application/json, X-API-Version: 1	N/A	Anordnung des Inhalts: Sicherungsdateiname	Inhalt der Sicherungsdatei	Sicherung herunterladen

REST-Aufruf	Anforderungsheader	Anforderungstext	Antwortheader	Antworttext	Beschreibung
GET https://{appl}/rest/backups	auth: session ID, accept-language: locale, accept-content: application/json, X-API-Version: 1	N/A	N/A	Eine SimplePaginatedCollection, die die letzte Sicherungsressource enthält	Detaillierte Informationen zur letzten Sicherung abrufen
DELETE https://{appl}/{associatedResourceUri}	auth: session ID, accept-language: locale, accept-content: application/json, X-API-Version: 1	N/A	N/A	Eine Aufgabenressource, die eine URI zur Prüfung des Sicherungsstatus enthält	Sicherung abbrechen

3.2.3 Beispiel für ein Sicherungsskript

Bei dem Beispiel handelt es sich um ein PowerShell-Skript zum Erstellen und Herunterladen einer Sicherung. Das Beispielskript ist auf den Insight Control Server Provisioning-Medien und auf der Zip-Datei des Produktdownloads verfügbar. Dieses Skript verwendet PowerShell Version 3.0. Es führt REST-Aufrufe zum Erstellen und Herunterladen einer Sicherung aus. Das Beispielskript kann zur automatischen regelmäßigen Ausführung geplant werden.

3.2.3.1 So verwenden Sie das Beispielsicherungsskript

Sie können das Beispielskript kopieren und in eine Datei auf einem Windows-System einfügen, auf dem PowerShell Version 3.0 ausgeführt wird.

HP empfiehlt dringend die Installation von `cURL`, um die Leistung zu steigern. Das Beispielskript funktioniert ohne `cURL`, das Herunterladen einer umfassenden Sicherung kann jedoch mehrere Stunden dauern. Sie können `cURL` unter http://curl.haxx.se/download.html herunterladen. Außerdem muss gegebenenfalls die Software Microsoft Visual C++ Redistributable, `MSVCR100.dll`, installiert werden, die unter http://www.microsoft.com/download/en/details.aspx?id=14632 (64 bit) oder unter http://www.microsoft.com/download/en/details.aspx?id=5555 (32 bit) heruntergeladen werden kann. Stellen Sie sicher, dass die Pfadumgebungsvariable den Pfad für `cURL` enthält.

Sie können das Skript interaktiv oder im Stapelmodus ausführen. Zur interaktiven Ausführung verwenden Sie das Skript ohne Parameter. Das Skript fordert Sie zur Eingabe des Gerätehostnamens, des Gerätebenutzernamens und des Kennworts sowie des Namens einer Datei zum Speichern dieser Parameter für Ausführungen im Stapelmodus auf. Geben Sie den Namen und das Kennwort eines Benutzers mit der Rolle eines Sicherungs- oder Infrastrukturadministrators ein. Der Benutzername und das Kennwort werden verschlüsselt gespeichert. Zum Ausführen des Skripts im Stapelmodus geben Sie in der Befehlszeile den Namen der Datei an, die die Parameter enthält.

HP empfiehlt, das Skript beim ersten Mal interaktiv auszuführen. Anschließend können Sie das Skript zur automatischen Ausführung im Hintergrund planen, wobei die beim ersten Lauf erstellte Parameterdatei verwendet wird.

Sie können das Beispielskript bearbeiten und es an Ihre Umgebung anpassen.

3.2.3.2 Ausgabebeispiel

```
Enter Appliance name (https://ipaddress)
https://10.10.10.10
Enter Username
*************
Enter password
********
Would you like to save these credentials to a file? (username and password encrypted)
y
Enter file path and file name to save credentials  (example: C:\users\bob\machine1.txt)
C:\users\jerry\jerry-vm.txt
The file 'C:\users\jerry\jerry-vm.txt' already exists.
```

```
Overwrite existing credentials for this machine?
y
run backup?
y
Login completed successfully.
Backup initiated.
Checking for backup completion, this may take a while.
 Backup progress: [====================]  100 %

Obtained backup file URI, now downloading
Backup download complete!
Backup can be found at C:\Users\jerry\Documents
If you wish to automate this script in the future and re-use login settings currently entered,
then provide the file path to the saved credentials file when running the script.
ie:  C:\Users\jerry\backup.ps1  filepath
```

3.2.3.3 Hauptprozesse und -funktionen des Beispielsicherungsskripts

Das Beispielskript führt folgende Funktionen zum Erstellen und Herunterladen einer Sicherung aus:

1. Es ruft `queryfor-credentials()` auf, um den Gerätehostnamen, den Benutzernamen und das Kennwort abzurufen, indem entweder der Benutzer zur Eingabe aufgefordert wird oder die Daten aus einer Datei gelesen werden.
2. Es ruft `login-appliance()` zur Ausgabe einer REST-Anforderung auf, um eine Sitzungs-ID zur Autorisierung von Sicherungs-REST-Aufrufen zu erhalten.
3. Es ruft `backup-appliance()` auf, um eine REST-Anforderung zum Starten einer Sicherung auszugeben.
4. Es ruft `waitFor-completion()` auf, um REST-Anforderungen auszugeben, mit denen der Sicherungsstatus bis zum Abschluss der Sicherung abgerufen wird.
5. Es ruft `get-backupResource()` auf, um eine REST-Anforderung zur Abfrage der Download-URI auszugeben.
6. Es ruft `download-backup()` auf, um eine REST-Anforderung zur Abfrage der Sicherung auszugeben.

Die folgende Tabelle enthält eine Übersicht der Funktionen im Beispielskript.

Funktion	Beschreibung	Parameter	Ausgabe
`queryfor-credentials`	Sammelt im manuellen Eingabemodus Informationen über den Benutzer (das Skript wurde mit null Argumenten ausgeführt) oder wird im Hintergrund ausgeführt und sammelt Informationen aus dem angegebenen Pfad (das Skript wurde mit Argument ausgeführt)	N/A	Ein Json-formatiertes Objekt, das die für die Anmeldung erforderlichen Werte enthält
`login-appliance`	Sendet eine Webanforderung an das Gerät, um eine autorisierte sessionID zu erhalten	'username': Der Benutzername für die Anmeldung beim Remote-Gerät 'password': Das mit dem Benutzernamen verknüpfte Kennwort 'hostname': Das Gerät, an dem die Anmeldung erfolgen soll	Eine Hashtabelle mit der sessionID
`backup-appliance`	Sendet eine Anforderung zum Starten einer Sicherung	'authValue': Die vom Anmeldungsgerät zur Verfügung gestellte autorisierte sessionID	Gibt eine Hashtabelle mit dem Antworttext aus der Sicherungsanforderung aus

Funktion	Beschreibung	Parameter	Ausgabe
		'hostname': Die Geräteadresse, mit der eine Verbindung hergestellt werden soll	
`waitFor-completion`	Prüft den Status der Sicherung alle fünf Sekunden und stoppt, wenn der Status sich von „Running“ (Läuft) in einen anderen Status ändert	'taskManager': Der Antworttext der Sicherungsgerätefunktion 'authValue': Die vom Anmeldungsgerät autorisierte sessionID 'hostname': Das Gerät, an das die Anforderung gesendet werden soll	Gibt eine Hashtabelle mit der Aufgabenressource aus, die den Sicherungsstatus und eine URI zum Abrufen detaillierter Informationen über die Sicherung enthält
`get-backupResource`	Ruft die Sicherungsressource ab, die detaillierte Informationen über die Sicherung, einschließlich der URI zum Herunterladen der Sicherung, enthält	'taskResource': Die Aufgabenressource, die die Sicherungsressourcen-URI enthält 'authValue': Die autorisierte Sitzungs-ID 'hostname': Das Gerät, an das die Anforderung gesendet werden soll	Gibt eine Hashtabelle mit der Sicherungsressource aus, die die URI zum Herunterladen der Sicherungsdatei enthält
`download-backup`	Lädt die Sicherungsdatei vom Gerät auf das lokale System herunter	'backupResource': Die Sicherungsressource, die die URI zum Herunterladen der Sicherung enthält 'authValue': Die autorisierte Sitzungs-ID 'hostname': Das Gerät, an das die Anforderung gesendet werden soll	Gibt eine Zeichenfolge mit dem absoluten Pfad der Sicherungsdatei im lokalen System aus

3.2.3.4 Tipps zur Fehlerbehebung

Die folgende Tabelle enthält REST-API-Fehlercodes und Lösungen.

HTTP-Fehler	Antworttextfehlercode	Beschreibung	Behebung
401 Unauthorized	AUTHORIZATION	Es wurde ein falscher Benutzername oder ein falsches Kennwort angegeben.	Geben Sie den richtigen Benutzernamen bzw. das richtige Kennwort ein.
404 Not Found	RESOURCE_NOT_FOUND	Es wurde die falsche URI angegeben.	Geben Sie die richtige URI ein. Möglicherweise müssen Sie warten, bis die Gerätesoftware startet. Es kann hilfreich sein, die REST-Anforderung auszugeben, um die letzte Sicherungsressource abzurufen, oder eine andere Sicherung zur Ermittlung der richtigen URI heranzuziehen.

HTTP-Fehler	Antworttextfehlercode	Beschreibung	Behebung
409 Conflict	BACKUP_IN_PROGRESS	Der angeforderte Vorgang kann nicht ausgeführt werden, da eine Sicherung läuft. Es kann jeweils nur eine Sicherung ausgeführt werden.	Warten Sie, bis die Sicherung abgeschlossen ist, oder brechen Sie die Sicherung ab und wiederholen Sie den Vorgang.
409 Conflict	BACKUP_DOWNLOAD_IN_PROGRESS	Der angeforderte Vorgang kann nicht ausgeführt werden, da eine Sicherung heruntergeladen wird. Eine Sicherung kann nicht ausgeführt werden, während ein Download erfolgt.	Warten Sie, bis der Download beendet ist, und wiederholen Sie den Vorgang.
409 Conflict	BACKUP_UPLOAD_IN_PROGRESS	Der angeforderte Vorgang kann nicht ausgeführt werden, da eine Sicherung zum Zwecke der Wiederherstellung hochgeladen wird.	Warten Sie, bis der Upload und die Wiederherstellung beendet sind, und wiederholen Sie den Vorgang.
409 Conflict	BACKUP_RESTORE_IN_PROGRESS	Der angeforderte Vorgang kann nicht ausgeführt werden, da eine Wiederherstellung ausgeführt wird.	Warten Sie, bis die Wiederherstellung beendet ist, und wiederholen Sie den Vorgang.
500 Internal Server Error	Verschiedene	Es ist ein interner Fehler aufgetreten.	Erstellen Sie einen Support-Dump. Starten Sie das Gerät neu und wiederholen Sie den Vorgang.

3.3 Hochladen und Wiederherstellen einer Sicherung

3.3.1 Empfohlene Wiederherstellungsverfahren

Eine Sicherung kann auf demselben Gerät oder auf einem anderen Gerät wiederhergestellt werden. Wenn ein Gerät fehlerhaft ist und nicht repariert werden kann, kann die Sicherung auf einem Ersatzgerät wiederhergestellt werden.

△ **ACHTUNG:** Die Wiederherstellung muss auf einem Gerät mit denselben Netzwerkeinstellungen wie auf dem Originalgerät erfolgen.

Während einer Wiederherstellung gleicht die Gerätefirmware die Daten in der Sicherung mit dem aktuellen Status der verwalteten Umgebung ab. Einige Abweichungen können bei der Wiederherstellung nicht automatisch behoben werden. Nach Abschluss einer Wiederherstellung

müssen noch bestehende Inkonsistenzen, auf die in Warnmeldungen hingewiesen wird, manuell vom Geräteadministrator behoben werden.

△ **ACHTUNG:** Durch Wiederherstellen einer Sicherung werden sämtliche Verwaltungsdaten und die meisten Konfigurationseinstellungen auf dem Gerät ersetzt. Das Gerät ist während einer Wiederherstellung nicht betriebsbereit. Eine Wiederherstellung kann mehrere Stunden dauern. Sie kann nach dem Start weder abgebrochen noch rückgängig gemacht werden. Wenn bei der Wiederherstellung ein nicht behebbarer Fehler auftritt, müssen Sie eine neue Gerätevorlage herunterladen. Dieser Vorgang wird im *HP Insight Control Server Provisioning Installation Guide* (HP Insight Control Server Provisioning Installationshandbuch) beschrieben, das unter http://www.hp.com/go/insightcontrol/docs verfügbar ist. Eine Wiederherstellung sollte nur im Falle einer schwerwiegenden Störung verwendet werden. Sie sollte nicht bei kleineren Problemen Anwendung finden, die auf andere Weise gelöst werden können.

3.3.2 Vorbereiten einer Wiederherstellung

Führen Sie die folgenden Schritte aus, um eine Wiederherstellung vorzubereiten:

1. Wenn Sie eine Wiederherstellung auf einem neuen Gerät vornehmen, installieren Sie das neue Gerät wie im *HP Insight Control Server Provisioning Installation Guide* (HP Insight Control Server Provisioning Installationshandbuch) beschrieben, das unter https://www.hp.com/go/insightcontrol/docs verfügbar ist.
2. Stellen Sie bei einem neuen Gerät sicher, dass die Netzwerkeinstellungen mit denen des Originalgeräts übereinstimmen.
3. Halten Sie vor dem Starten einer Wiederherstellung alle automatisch geplanten Sicherungen an. Nachdem die Wiederherstellung abgeschlossen ist, starten Sie die automatisch geplanten Sicherungen neu.
4. Vor dem Starten einer Wiederherstellung empfiehlt es sich, einen Support-Dump zu erstellen. Mithilfe des Support-Dumps können Fehler diagnostiziert werden, die vor der Wiederherstellung aufgetreten sind.
5. Vor dem Starten der Wiederherstellung empfiehlt es sich, die vorhandenen Prüfprotokolle herunterzuladen. Bei der Wiederherstellung werden die Prüfprotokolle durch die in der Sicherung enthaltenen Protokolle ersetzt.
6. Stellen Sie vor dem Starten einer Wiederherstellung sicher, dass Sie die Gerätebenutzernamen und Kennwörter vorliegen haben, die zum Zeitpunkt der Sicherung gültig waren. Bei der Wiederherstellung werden die Benutzernamen und Kennwörter auf die Werte zurückgesetzt, die zum Zeitpunkt der Sicherung konfiguriert waren.
7. Wenn Sie die Wiederherstellung auf einem anderen als dem Gerät ausführen, von dem die Sicherung stammt, müssen Sie vor dem Starten der Wiederherstellung zusätzliche Vorsichtsmaßnahmen ergreifen. Nehmen Sie das Originalgerät außer Betrieb oder konfigurieren Sie es neu, sodass es die Geräte, die es zum Zeitpunkt der Sicherung verwaltet hat, nicht mehr verwaltet. Wenn mehrere Geräte versuchen, dieselben Geräte zu verwalten, können schwerwiegende Fehler auftreten.
8. Vor dem Starten einer Wiederherstellung müssen sich alle am Gerät angemeldeten Benutzer abmelden. Andernfalls geht die Arbeit der Benutzer verloren. Die Benutzer werden automatisch abgemeldet, sobald eine Wiederherstellung gestartet wird. Sie können sich während einer Wiederherstellung nicht anmelden.
9. Wenn auf dem wiederherzustellenden Gerät eine Firmwareversion ausgeführt wird, die nicht mit der Sicherung kompatibel ist, installieren Sie vor dem Hochladen der Sicherung eine kompatible Version der Firmware auf dem Gerät. Zur Wiederherstellung einer Sicherung müssen Plattformtyp, Hardwaremodell, Major-Nummer und Minor-Nummer übereinstimmen. Versions- und Build-Nummer müssen nicht übereinstimmen. Das Format der Gerätefirmwareversion lautet:

   `<major number>.<minor number>.<revision number>-<build number>`

Wenn die Sicherung nicht mit der Firmware auf dem Gerät kompatibel ist, wird beim Hochladen ein Fehler zurückgegeben. Aktualisieren Sie in diesem Fall die Firmware oder wählen Sie eine andere Sicherung aus.

10. Machen Sie die Sicherung dem System zugänglich, auf dem die Hochladeanforderung ausgegeben werden soll. Wenn Sie Sicherungsdateien mit einem Unternehmenssicherungs-/-wiederherstellungsprodukt archivieren, führen Sie die für dieses Produkt erforderlichen Schritte zur Vorbereitung der Wiederherstellung aus.

3.3.3 Durchführen einer Wiederherstellung

Führen Sie die folgenden Schritte aus, um eine Wiederherstellung durchzuführen:

HINWEIS: Wenn Sie versuchen, während einer Wiederherstellung eine Verbindung mit dem Gerät herzustellen, können Sie sich nicht anmelden. Die Seite für die Gerätewartung wird eingeblendet und eine Meldung mit dem Hinweis, dass eine Wiederherstellung läuft, wird angezeigt.

1. Führen Sie die Schritte im Abschnitt „Vorbereiten einer Wiederherstellung“ (Seite 19) aus, bevor Sie beginnen.
2. Geben Sie die REST-Anforderung aus, um sich als Benutzer mit der Rolle eines Infrastrukturadministrators beim Gerät anzumelden.
3. Geben Sie die REST-Anforderung aus, um die Sicherungsdatei auf das Gerät hochzuladen. Geben Sie die Sitzungs-ID an, die von der Anmeldeanforderung im Header `auth` zurückgegeben wurde.
4. Prüfen Sie die Antwort auf die Hochladeanforderung, um sicherzustellen, dass das Hochladen erfolgreich war. Beim Hochladen tritt ein Fehler auf, wenn die Sicherungsversion mit der Firmware auf dem Gerät nicht kompatibel ist oder wenn die Sicherung beschädigt ist. Wenn die Sicherung mit der Firmware auf dem Gerät nicht kompatibel ist, aktualisieren Sie die Firmware und wiederholen Sie das Hochladen oder laden Sie eine andere Sicherung hoch. Wenn die Sicherung beschädigt ist, laden Sie eine andere Sicherung hoch.
5. Geben Sie die REST-Anforderung aus, um die Wiederherstellung zu starten.
6. Prüfen Sie die Antwort auf die Wiederherstellungsanforderung, um sicherzustellen, dass die Wiederherstellung erfolgreich gestartet wurde. Beim Wiederherstellen tritt ein Fehler auf, wenn die Sicherungsversion mit der Firmware auf dem Gerät nicht kompatibel ist oder wenn die Sicherung beschädigt ist. Wenn die Sicherung mit der Firmware auf dem Gerät nicht kompatibel ist, aktualisieren Sie die Firmware und wiederholen Sie die Wiederherstellung oder laden Sie eine andere Sicherung hoch. Wenn die Sicherung beschädigt ist, laden Sie eine andere Sicherung hoch.
7. Geben Sie die REST-Anforderungen in periodischen Zeitabständen aus, um Informationen über den Wiederherstellungsverlauf zu erhalten. Eine Wiederherstellung kann mehrere Stunden dauern. Die erforderliche Dauer hängt von der Größe der verwalteten Umgebung ab. Die REST-API gibt den Vollendungsgrad der Wiederherstellung in Prozent sowie eine Beschreibung des laufenden Wiederherstellungsschritts zurück.
8. Nach Abschluss der Wiederherstellung gibt die REST-API eine Meldung mit dem Hinweis zurück, dass die Wiederherstellung erfolgreich abgeschlossen wurde.
9. Die Benutzer können sich nach Abschluss der Wiederherstellung beim Gerät anmelden. Bei einer Wiederherstellung werden die Benutzernamen und Kennwörter auf die Werte zurückgesetzt, die zum Zeitpunkt der Sicherung gültig waren.
10. Es wird eine Meldung mit dem Hinweis auf den erfolgreichen Abschluss der Wiederherstellung eingeblendet.
11. Während der Wiederherstellung gleicht die Gerätefirmware die Daten in der Sicherung automatisch mit dem aktuellen Status der verwalteten Umgebung ab. Beheben Sie Abweichungen, die nicht automatisch behoben werden können, nach der Wiederherstellung manuell. Melden Sie sich nach Abschluss der Wiederherstellung beim Gerät an, um es auf

Warnmeldungen in Verbindung mit Inkonsistenzen zu überprüfen. Führen Sie zum Beheben der Diskrepanzen die in der Warnmeldung angegebenen Anweisungen aus.

12. Führen Sie nach dem Beheben von bei der Wiederherstellung ermittelten Diskrepanzen eine neue Sicherung aus. Starten Sie die regelmäßig geplanten Sicherungen neu.
13. Tritt bei einer Wiederherstellung ein nicht behebbarer Fehler auf, schlagen die REST-API-Wiederherstellungsaufrufe fehl. Eine Fehlermeldung gibt an, dass ein Fehler bei der Wiederherstellung aufgetreten ist und ein neues Gerät über die von HP zur Verfügung gestellte Vorlage bereitgestellt werden muss. Dieser Vorgang ist im *HP Insight Control Server Provisioning Installation Guide* (HP Insight Control Server Provisioning Installationshandbuch) beschreiben, das unter http://www.hp.com/go/insightcontrol/docs verfügbar ist.

3.3.4 Übersicht über die Wiederherstellungs-REST-API

Die Wiederherstellungs-REST-API stellt REST-Aufrufe für Folgendes bereit:

- Sicherung auf das Gerät hochladen
- Wiederherstellung starten
- Wiederherstellungsstatus überprüfen

Diese Aufrufe sind in der Tabelle unten zusammengefasst. Für die REST-API-Aufrufe zum Starten einer Wiederherstellung ist eine Sitzungs-ID zur Autorisierung erforderlich. Die Sitzungs-ID erhalten Sie, wenn Sie die REST-Anforderung zur Anmeldung beim Gerät als Benutzer mit der Rolle eines Infrastrukturadministrators ausgeben. Für die REST-API-Aufrufe zum Abrufen von Informationen über den Wiederherstellungsstatus ist keine Sitzungs-ID erforderlich.

REST-Aufruf	Anforderungsheader	Anforderungstext	Antwort-header	Antworttext	Beschreibung
POST https://{appl}/rest/backups/archive	auth: session ID, content-type: multipart/form-data, accept-language: locale, accept-content: application/json, X-API-Version: 1	Multipart-Formulardaten, die die Sicherungsdatei enthalten	N/A	Eine Sicherungsressource, die den Hochladestatus, eine ID zur Wiederherstellung der Sicherung und andere Informationen über die Sicherung enthält	Sicherung auf das Gerät hochladen
POST https://{appl}/rest/restores	auth: session ID, accept-language: locale, accept-content: application/json, X-API-Version: 1	Ein Json-Objekt mit 2 Elementen. Diese Elemente sind „type“ (Typ) mit den Werten „RESTORE“ (Wiederherstellen) und „backupIdToRestore“ (Sicherungs-ID zur Wiederherstellung), die auf die ID festgelegt wurden, die von der Hochladeanforderung zurückgegeben wurde.	N/A	Eine Wiederherstellungsressource, die den Wiederherstellungsstatus und eine URI zum Abrufen von Informationen zum Wiederherstellungsverlauf enthält	Wiederherstellung einer hochgeladenen Sicherung starten
GET https://{appl}/{uri}	accept-language: locale,	N/A	N/A	Eine Wiederherstellungsressource,	Informationen zum

REST-Aufruf	Anforderungsheader	Anforderungstext	Antwort-header	Antworttext	Beschreibung
	accept-content: application/json, X-API-Version: 1			die den aktuellen Wiederherstellungsstatus und Verlaufsinformationen enthält	Wiederherstellungsverlauf abrufen
GET https://{appl}/rest/restores	accept-language: locale, accept-content: application/json, X-API-Version: 1	N/A	N/A	Eine SimplePaginatedCollection, die die letzte Wiederherstellungsressource enthält	Informationen über die letzte Wiederherstellung oder eine laufende Wiederherstellung abrufen

3.3.5 Beispiel für ein Wiederherstellungsskript

Bei dem Beispiel handelt es sich um ein PowerShell-Skript zum Hochladen und Wiederherstellen einer Sicherung. Dieses Skript verwendet PowerShell Version 3.0. Es führt REST-Aufrufe zum Hochladen und Wiederherstellen einer Sicherung aus. HP empfiehlt dringend die Installation von `cURL`, um die Leistung zu steigern.

3.3.5.1 So verwenden Sie das Beispielwiederherstellungsskript

Sie können das Beispielskript kopieren und in eine Datei auf einem Windows-System einfügen, auf dem PowerShell Version 3.0 ausgeführt wird.

HP empfiehlt dringend die Installation von `cURL`, um die Leistung zu steigern. Das Beispielskript funktioniert ohne `cURL`, das Herunterladen einer umfassenden Sicherung kann jedoch mehrere Stunden dauern. Sie können `cURL` unter http://curl.haxx.se/download.html herunterladen. Außerdem muss gegebenenfalls die Software Microsoft Visual C++ Redistributable, `MSVCR100.dll`, installiert werden, die unter http://www.microsoft.com/download/en/details.aspx?id=14632 (64 bit) oder unter http://www.microsoft.com/download/en/details.aspx?id=5555 (32 bit) heruntergeladen werden kann. Stellen Sie sicher, dass die Pfadumgebungsvariable den Pfad für `cURL` enthält.

Sie können das Skript interaktiv ausführen, um eine Sicherung hochzuladen und wiederherzustellen oder um Statusinformationen über eine laufende Wiederherstellung abzurufen.

Führen Sie das Skript zum Hochladen und Wiederherstellen einer Sicherung ohne Parameter aus. Das Skript fordert Sie zur Eingabe des Gerätehostnamens, des Gerätebenutzernamens und -kennworts sowie des Sicherungsdateipfads auf. Anschließend lädt das Skript die Sicherung hoch, startet die Wiederherstellung und ruft Informationen über den Wiederherstellungsverlauf ab, bis die Wiederherstellung abgeschlossen ist.

Führen Sie das Skript zum Abrufen von Statusinformationen über eine laufende Wiederherstellung mit dem Parameter `-status` und dem Gerätehostnamen im Format `https://{hostname}` aus.

3.3.5.2 Ausgabebeispiel

Beispiel für eine Ausgabe durch Ausführen des Skripts zum Hochladen und Wiederherstellen einer Sicherung:

```
PS C:\Users\Joe> C:\Users\Joe\Documents\restore.ps1
Restoring from backup is a destructive process, continue anyway?
y
Enter directory backup is located in (ie: C:\users\joe\)
C:\users\Joe\Documents
Enter name of backup (ie: appliance_vm1_backup_2012-07-07_555555.bkp
joe_vm_backup_2012-07-07_777777.bkp
Enter appliance IP address (ie: https://10.10.10.10)
```

```
https://10.10.10.1
Enter username
*************
Enter password
********
Login completed successfully
Uploading backup file to appliance, this may take a few minutes...
Upload complete.


Restore progress: [====================]  100 %
Restore complete!
```

Beispiel für eine Ausgabe durch Ausführen des Skripts zum Abrufen von Informationen über den Wiederherstellungsverlauf:

```
C:\users\Joe\Documents\restore.ps1 -status https://10.10.10.1
Restore progress: [====================]  100 %
Restore complete!
```

3.3.5.3 Hauptprozesse und -funktionen des Beispielskripts zur Wiederherstellung einer Sicherung

Das Beispielskript kann entweder zum Starten einer Wiederherstellung oder zum Abrufen von Verlaufsinformationen über eine laufende Wiederherstellung verwendet werden.

Wenn keine Parameter an das Skript übergeben werden, lädt es eine Sicherung hoch und stellt sie wieder her. Das Skript führt Folgendes aus:

1. Es ruft `query-user()` auf, um den Gerätehostnamen, den Benutzernamen und das Kennwort sowie den Sicherungsdateipfad abzurufen.
2. Es ruft `login-appliance` zur Ausgabe einer REST-Anforderung auf, um eine Sitzungs-ID zur Autorisierung von Sicherungs-REST-Aufrufen zu erhalten.
3. Es ruft `uploadTo-appliance()` auf, um die Sicherung auf das Gerät hochzuladen.
4. Es ruft `start-restore()` auf, um die Wiederherstellung zu starten.
5. Es ruft `restore-status()` auf, um den Wiederherstellungsstatus regelmäßig zu überprüfen, bis die Wiederherstellung abgeschlossen ist.

Wenn die Option `-status` an das Skript übergeben wird, überprüft und meldet das Skript den Status der letzten oder einer laufenden Wiederherstellung, bis die Wiederherstellung abgeschlossen ist. Das Skript führt Folgendes aus:

1. Es ruft `recover-restoreID()` auf, um die URI zum Überprüfen des Status der letzten oder einer laufenden Wiederherstellung abzurufen.
2. Es ruft `restore-status()` auf, um den Wiederherstellungsstatus regelmäßig zu überprüfen, bis die Wiederherstellung abgeschlossen ist.

Die folgende Tabelle enthält eine Übersicht der Funktionen im Beispielskript.

Funktion	Beschreibung	Parameter	Ausgabe
`query-user`	Bezieht Informationen vom Benutzer, die zur Interaktion mit dem Gerät erforderlich sind	N/A	`loginVals`: Eine Hashtabelle mit Informationen, die vom Benutzer bezogen wurden
`login-appliance`	Sendet den Benutzernamen und das Kennwort an das Gerät und ruft eine autorisierte Sitzungs-ID ab	`username`: Der Benutzername, der von der Funktion `query-user` abgerufen wurde `password`: Das Kennwort, das von der Funktion `query-user` abgerufen wurde	`authInfo`: Der Antworttext, der vom Remote-Gerät zurückgegeben wurde, einschließlich `sessionID`

Funktion	Beschreibung	Parameter	Ausgabe
		`hostname`: Die Adresse des Geräts, an die die Anmeldeanforderung gesendet werden soll	
`uploadTo-appliance`	Lädt die vorgesehene Sicherungsdatei auf das Remote-Gerät hoch	`filePath`: Der absolute Dateipfad zur Sicherungsdatei `authInfo`: Die Sitzungs-ID aus der Anmeldeantwort `hostname`: Die Adresse des Geräts, auf das die Datei hochgeladen werden soll `backupFile`: Der Name der hochzuladenden Datei	`uploadResponse`: Der Antworttext für die Hochladeanforderung, die die wiederherzustellende Sicherungs-ID enthält
`start-restore`	Sendet die Anforderung zum Wiederherstellen des Geräts von der Sicherung	`authInfo`: Die Sitzungs-ID aus der Anmeldeantwort `hostname`: Die Adresse des Remote-Geräts, an die die Anforderung gesendet werden soll `uploadResponse`: Der Antworttext der Hochladeanforderung	`restoreResponse`: Der Antworttext von der Wiederherstellungsanforderung, die die ID der laufenden Wiederherstellung enthält
`restore-status`	Prüft das Gerät im Hinblick auf den Status der laufenden Wiederherstellung. Zeigt eine Statusleiste an.	`authInfo`: Die Sitzungs-ID, die von der Anmeldeanforderung bezogen wurde `hostname`: Die Adresse des Remote-Geräts, an die die Anforderung gesendet werden soll `restoreResponse`: Der Antworttext aus der Wiederherstellungsanforderung `recoveredUri`: Die vollständige URI, die zum Abrufen des Wiederherstellungsstatus erforderlich ist (diese wird nur verwendet, wenn das Skript mit dem Status-Flag geöffnet wird)	N/A
`recover-restoreID`	Wird verwendet, wenn die Verbindung unterbrochen oder das Skript geschlossen wird. Sendet eine Anforderung an den Server, um die URI der laufenden Wiederherstellungsaufgabe abzurufen, und gibt die Informationen dann an `restore-status` weiter.	`hostname`: Das Remote-Gerät, an das die Anforderung gesendet werden soll	Gibt die URI der letzten oder laufenden Wiederherstellung zurück

3.3.5.4 Tipps zur Fehlerbehebung

Die folgende Tabelle enthält REST-API-Fehlercodes und Lösungen.

HTTP-Fehler	Antworttextfehlercode	Beschreibung	Behebung
400 Bad Request	INVALID_PARAMETER	Es wurde eine ungültige Sicherungs-ID angegeben.	Geben Sie eine gültige Sicherungs-ID an. Diese muss das Format <*hostname*>_backup_*YYYY-MM-dd_HHmmss* haben.
401 Unauthorized	AUTHORIZATION	Es wurde ein falscher Benutzername oder ein falsches Kennwort angegeben.	Geben Sie den richtigen Benutzernamen bzw. das richtige Kennwort ein.
404 Not Found	RESOURCE_NOT_FOUND	Es wurde die falsche URI angegeben.	Geben Sie die richtige URI ein. Möglicherweise müssen Sie warten, bis die Gerätesoftware startet. Die richtige URI können Sie mithilfe dieses Handbuchs ermitteln. Es kann hilfreich sein, die REST-Anforderung auszugeben, um die letzte Sicherungsressource abzurufen.
409 Conflict	BACKUP_IN_PROGRESS	Der angeforderte Vorgang kann nicht ausgeführt werden, da eine Sicherung läuft. Eine Sicherung kann nicht hochgeladen oder wiederhergestellt werden, während das Gerät eine Sicherung ausführt.	Warten Sie, bis die Sicherung abgeschlossen ist, oder brechen Sie die Sicherung ab und wiederholen Sie den Vorgang.
409 Conflict	BACKUP_DOWNLOAD_IN_PROGRESS	Der angeforderte Vorgang kann nicht ausgeführt werden, da eine Sicherung heruntergeladen wird. Eine Sicherung kann nicht hochgeladen oder wiederhergestellt werden, während ein Download erfolgt.	Warten Sie, bis der Download beendet ist, und wiederholen Sie den Vorgang.
409 Conflict	BACKUP_UPLOAD_IN_PROGRESS	Der angeforderte Vorgang kann nicht ausgeführt werden, da eine Sicherung hochgeladen wird.	Warten Sie, bis der Upload beendet ist, und wiederholen Sie den Vorgang.
409 Conflict	BACKUP_RESTORE_IN_PROGRESS	Der angeforderte Vorgang kann nicht ausgeführt werden, da eine Wiederherstellung ausgeführt wird.	Warten Sie, bis die Wiederherstellung beendet ist, und wiederholen Sie den Vorgang.
500 Internal Server Error	Verschiedene	Es ist ein interner Fehler aufgetreten.	Erstellen Sie einen Support-Dump. Versuchen Sie, eine andere Sicherung wiederherzustellen.

4 Sicherheitshinweise

Insight Control Server Provisioning wird als sicherheitsoptimiertes virtuelles Gerät geliefert. Die Anzahl der offenen Ports und die entsprechend unterstützten Protokolle wurden auf das für den Betrieb von Insight Control Server Provisioning erforderliche Minimum reduziert.

4.1 Voraussetzungen

Das Gerät sollte sich in einem Bereitstellungsnetzwerk, das vom Produktionsnetzwerk getrennt ist, befinden (weitere Informationen finden Sie unter „Optimale Vorgehensweisen bezüglich Sicherheit“ (Seite 35)). Darüber hinaus sollte der Zugriff auf die virtuelle Gerätekonsole auf autorisierte Benutzer beschränkt sein (weitere Informationen finden Sie unter „Einschränken des Konsolenzugriffs“ (Seite 33)).

Das Gerät muss Zugriff auf die iLOs auf Zielservern sowie auf deren Bereitstellungs-NICs haben. Eine Netzwerkkonfiguration umfasst ein separates Verwaltungsnetzwerk, das mit Ziel-iLOs verbunden ist, und ein Bereitstellungsnetzwerk mit DHCP und PXE, das mit Zielbereitstellungs-NICs verbunden ist. Für diesen Konfigurationstyp ist ein Router zwischen dem Verwaltungs- und dem Bereitstellungsnetzwerk erforderlich, der über das Bereitstellungsnetzwerk Zugriff auf die Ziel-iLOs bietet.

Insight Control Server Provisioning legt einen Agenten im Produktionsbetriebssystem an. Dieser Agent muss in umgekehrter Richtung mit dem Gerät kommunizieren können. Voraussetzung ist, dass die Bereitstellungs-NIC im Produktionsbetriebssystem aktiv ist oder dass für diese Kommunikation eine Route zurück zum Bereitstellungsnetzwerk besteht.

4.2 Sicherheitshinweise zu Hypervisor und virtueller Maschine

Als virtuelles Gerät hängt die Sicherheit des Geräts von der Sicherheit des Host-Hypervisors ab, ähnlich wie ein physisches Gerät von der physischen Sicherheit des Rechenzentrums abhängt. Der administrative Zugriff auf den Host-Hypervisor muss kontrolliert werden, um die Sicherheit des Geräts zu gewährleisten. Das Gerätesoftwareabbild auf der virtuellen Maschine wurde sicherheitsoptimiert, doch der Hypervisor muss konfiguriert werden, um den Zugriff zur Sicherheit des Geräts auf die virtuelle Gerätekonsole und die virtuelle Festplatte zu beschränken (VMware-Datei `vmxd`).

4.3 Authentifizierung

Für den Zugriff auf das Gerät ist eine Authentifizierung mit einem Benutzernamen und einem Kennwort erforderlich. Diese Benutzerkonten werden auf dem Gerät konfiguriert. Alle Zugriffe über die Browserschnittstellen erfolgen über SSL, einschließlich Authentifizierung, wodurch die Anmeldedaten während der Übertragung über das Netzwerk geschützt sind.

4.4 Sitzung

Eine Sitzung wird erstellt, wenn ein Benutzer sich über den Browser oder einen anderen Client (z. B. mit der REST-API) beim Gerät anmeldet. Anschließend wird eine Sitzungs-ID für weitere Anforderungen an das Gerät verwendet. Diese muss geschützt sein, da sie den authentifizierten Benutzer repräsentiert.

Eine Sitzung bleibt gültig, bis sich der Benutzer abmeldet oder die Sitzung abläuft. Bei Verwendung der REST-API sollten Sie die inaktive Sitzungsdauer auf einen kürzeren Zeitraum festlegen oder die Standarddauer von 24 Stunden verwenden. Stellen Sie außerdem sicher, dass Sie sich abmelden und die Sitzung beenden, wenn Sie fertig sind. Der Bildschirmschoner bzw. Systemsperrmechanismus des Betriebssystems bietet einen gewissen Schutz, doch die UI sollte nicht offen und ungeschützt verbleiben. Wenn die Browser-UI geschlossen wird, ohne dass eine Abmeldung erfolgt, läuft der Sitzungstoken ab und ist nach 20 Minuten ungültig. Die Browsersitzung wird in einem Sitzungscookie

im Speicher abgelegt und nach dem Schließen des Browsers nicht beibehalten. Als Best Practice empfiehlt es sich, sich vor dem Schließen des Browsers abzumelden.

4.5 Autorisierung

Der Zugriff auf das Gerät wird durch Rollen beschränkt, die beschreiben, welche Aufgaben ein authentifizierter Benutzer auf dem Gerät ausführen darf. Jedem Benutzer muss mindestens eine Rolle zugewiesen werden.

4.5.1 Benutzerkonten und Rollen

Benutzerkonten auf dem Insight Control server provisioning-Gerät muss eine Rolle zugewiesen werden. Die Rolle bestimmt, welche Lese- und Schreibberechtigungen das Benutzerkonto hat. Ein Serveradministrator kann beispielsweise keinen OS Build Plan bearbeiten.

Folgende Rollen sind im Umfang von IC server provisioning enthalten:

Infrastrukturadministrator

- Alle Berechtigungen, sodass ein Benutzer mit dieser Rolle jede Aktion auf dem Gerät ausführen kann, einschließlich Verwaltung von Bereitstellungsinhalten (OS Build Plans, Skripts usw.)

Serveradministrator

- Ausführung von OS Build Plans
- Verwaltung von Servern, einschließlich Hinzufügen, Löschen und Ändern von Servern
- keine Berechtigung zum Ändern von Bereitstellungsinhalten (OS Build Plans, Skripts, Konfigurationsdateien oder Pakete)
- keine Berechtigung zum Verwalten von Benutzern
- keine Berechtigung zum Ändern von Geräteeinstellungen

Sicherungsadministrator

- nur Ausführung von Sicherungs- und Wiederherstellungsvorgängen
- zur Verwendung mit Sicherungsskripts, sodass Anmeldedaten für Infrastrukturadministratoren nicht in einem Skript gespeichert werden müssen
- keine Anmeldung beim Gerät mit diesen Konten zulässig

Nur Lesen

- nur Anzeigen von Geräteinformationen

Informationen zum Hinzufügen, Löschen und Bearbeiten von Benutzerkonten finden Sie in der Insight Control server provisioning-Online-Hilfe.

4.6 Überprüfung

Das Überprüfungsprotokoll enthält einen Datensatz mit wichtigen Aktionen, die auf dem Gerät ausgeführt wurden. Das Protokoll kann von Benutzern entweder mit der Rolle eines Infrastrukturadministrators oder eines Serveradministrators heruntergeladen werden. Wählen Sie dazu unter **Settings (Einstellungen)** die Option **Actions (Aktionen)→Download audit log (Überprüfungsprotokoll herunterladen)**. Benutzeraktionen ist eine Protokoll-ID zugewiesen, sodass Sie den Pfad des Benutzers im Überprüfungsprotokoll verfolgen können. Einige Aktionen werden vom Gerät ausgeführt und haben daher keine zugewiesene Protokoll-ID.

Die Struktur eines Eintrags im Überprüfungsprotokoll sieht wie folgt aus:

- Datum, Uhrzeit,
- Interne Komponenten-ID,
- <reserved>

- Benutzerdomäne,
- Benutzername/ID,
- Protokoll-ID,
- Aufgaben-ID,
- Quellhost/IP,
- Ergebnis,
- Aktion,
- Schweregrad,
- Objekttyp,
- Objektkennzeichnung,
- Meldung

Beispiel für Protokolleinträge mit einer Benutzeran- und -abmeldung:

```
2012-11-16 14:55:20.706 CST,Authentication,,,administrator,jrWI9ych,,,
SUCCESS,LOGIN,INFO,CREDENTIAL,,Authentication SUCCESS

2012-11-16 14:58:15.201 CST,Authentication,,,MISSING_UID,jrWI9ych,,,
SUCCESS,LOGOUT,INFO,CREDENTIAL,,TERMINATING SESSION
```

Die Überprüfungsprotokolle werden regelmäßig überschrieben, damit sie nicht zu groß werden. Es empfiehlt sich, sie zu überwachen und in regelmäßigen Abständen herunterzuladen, um einen langfristigen Überprüfungsverlauf beizubehalten.

Zusätzliche detaillierte Überprüfungsinformationen für Bereitstellungsziele sind in der Überprüfungsprotokoll-Zip-Datei enthalten. Alle Vorgänge, die über die Geräte-UI oder die REST-Schnittstellen ausgeführt wurden, sind im Überprüfungsprotokoll enthalten. Vorgänge, die im Rahmen von Matrix Operating Environment ausgeführt wurden, laufen über eine andere Schnittstelle. Diese Vorgänge werden sowohl in den Überprüfungsprotokollen von Matrix Operating Environment als auch auf dem Insight Control server provisioning-Gerät erfasst. So können die über diese Schnittstelle ausgeführten Vorgänge mit den in Matrix Operating Environment und den über die Geräte-UI ausgeführten Vorgängen abgeglichen werden.

Der Name der Datei mit den zusätzlichen Überprüfungsinformationen innerhalb der `audit-logs-<date>.zip`-Datei lautet `deployment-audit-logs.zip`. Diese Zip-Datei enthält eine Reihe von Systemprotokollen im Pfad `var/opt/opsware/ogfs/mnt/audit/event/<system name>/audit.log.0`. In diesen Überprüfungsprotokollen werden Aktionen, die über die Geräte-UI ausgeführt wurden, so erfasst, als wären sie vom Benutzer `applianceserviceaccount` ausgeführt worden. Im Gegensatz dazu werden die Aktionen, die über Matrix Operating Environment ausgeführt wurden, als vom Benutzer `matrixuser` ausgeführt erfasst. Es können weitere Aktionen für interne Benutzer, einschließlich `detuser`, `integration` und `buildmgr`, erfasst werden.

4.7 Kommunikationsprotokolle

4.7.1 SSL

Für den Zugriff auf das Gerät über die Browserschnittstelle wird grundsätzlich HTTPS (HTTP über SSL) verwendet. Dadurch werden die Daten verschlüsselt über das Netzwerk übertragen und die Datenintegrität wird gewährleistet. Unter „Algorithmen“ (Seite 33) finden Sie eine Liste der unterstützten Cipher Suites.

4.8 Zertifikatverwaltung

Ein Zertifikat dient zur Authentifizierung des Geräts über SSL. Das Zertifikat enthält einen öffentlichen Schlüssel und das Gerät speichert den entsprechenden privaten Schlüssel, der eindeutig an den öffentlichen Schlüssel gebunden ist. Im Zertifikat ist außerdem der Name des Geräts enthalten, mit dem der Browser das Gerät identifiziert.

Es finden sich zwei Namensfelder im Zertifikat.

- „Common Name (CN)" (Allgemeiner Name) ist ein obligatorisches Feld. Standardmäßig wird der vollqualifizierte Name verwendet.
- Das Feld „Alternative Name" (Alternativer Name) ist optional, wird jedoch empfohlen, da es mehrere Namen (einschließlich IP-Adressen) zulässt, um Warnmeldungen vom Browser zu Namensabweichungen zu minimieren. Standardmäßig wird in diesem Feld der vollqualifizierte Name, eine Kurzbezeichnung und die IP-Adresse des Systems eingetragen.

Diese Felder können geändert werden, wenn Sie ein selbstsigniertes Zertifikat oder eine Zertifikatsignierungsanforderung manuell erstellen.

HINWEIS: Wenn Sie einen Eintrag im Feld „Alternative Name" (Alternativer Name) vornehmen, muss der Name aus dem Feld „Common Name" (Allgemeiner Name) enthalten sein.

Das vom Gerät generierte Standardzertifikat ist selbstsigniert, d. h., es wird vollständig automatisch erstellt. Standardmäßig vertrauen Browser selbstsignierten Zertifikaten nicht, da sie keine Daten über sie vorliegen haben. Der Browser zeigt eine Warnmeldung an, damit der Benutzer den Inhalt des selbstsignierten Zertifikats überprüfen kann, bevor er es akzeptiert.

Zur Vereinfachung der Zertifikatverwaltung kann eine Zertifizierungsstelle (CA) verwendet werden. In diesem Fall werden Zertifikate von der vertrauenswürdigen Zertifizierungsstelle ausgegeben. Wenn der Browser bereits für die Zertifizierungsstelle konfiguriert ist, werden die von der Zertifizierungsstelle signierten Zertifikate ebenfalls als vertrauenswürdig eingestuft. Eine Zertifizierungsstelle kann intern von Ihrem Unternehmen betrieben und verwaltet werden oder es kann sich um einen Fremdanbieter handeln. Das Gerät unterstützt den Import eines von einer Zertifizierungsstelle signierten Zertifikats und die Verwendung dieses Zertifikats statt des selbstsignierten Zertifikats.

Um ein von der Zertifizierungsstelle signiertes Zertifikat zu erhalten, müssen Sie zunächst eine Zertifikatsignierungsanforderung (Certificate Signing Request, CSR) generieren. Wählen Sie unter **Settings (Einstellungen)** die Optionen **Actions (Aktionen)→Create certificate signing request (Zertifikatsignierungsanforderung erstellen)**. Übermitteln Sie die entsprechende Antwort dann an Ihre Zertifizierungsstelle, wie angewiesen. Nachdem die Zertifizierungsstelle das Zertifikat signiert und ausgegeben hat, importieren Sie die Antwort wieder in Ihr Gerät. Wählen Sie unter **Settings (Einstellungen)** die Optionen **Actions (Aktionen)→Import certificate (Zertifikat importieren)**. Schneiden Sie den Inhalt des ausgegebenen Zertifikats aus und fügen Sie ihn in das Textfeld ein. Drücken Sie dann die Taste **OK**.

4.8.1 Herunterladen

Zum Herunterladen des Gerätezertifikats für den manuellen Import in einen Browser verwenden Sie den Browser wie nachfolgend beschrieben:

- Firefox: Während des Prozesses **Add Exception (Ausnahme hinzufügen)** können Sie das Zertifikat mit der Schaltfläche **View (Ansicht)** anzeigen und überprüfen. Anschließend können Sie das Zertifikat über die Registerkarte **Details** als X.509-Zertifikat (PEM) exportieren.
- Internet Explorer: Klicken Sie im Bereich **Certificate error (Zertifikatfehler)** auf **View certificate (Zertifikat anzeigen)** und dann auf die Registerkarte **Details**. Hier können Sie das Zertifikat überprüfen und anschließend die Option **Copy to File (In Datei kopieren)** auswählen. Speichern Sie das Zertifikat im base-64-codierten X.509-Format.

4.9 Browser

4.9.1 Allgemein

- SSL/TLS: SSL v3 und TLS sollten aktiviert sein. SSL v2 gilt als unsicher und sollte nicht im Browser aktiviert sein, sofern keine besondere Notwendigkeit besteht.
- Die Cookies müssen aktiviert sein. Ein Cookie dient zum Speichern der authentifizierten Sitzungs-ID des Benutzers.
- Zertifikate in Firefox oder Internet Explorer werden weiter unten näher beschrieben. Da das Standardgerätezertifikat selbstsigniert ist, erhalten Sie zunächst eine Warnmeldung vom Browser.

4.9.2 Firefox

Wenn die Zertifikatwarnmeldung `This Connection is Untrusted` angezeigt wird und Sie unter **I Understand the Risks (Ich verstehe die Risiken)** die Option **Add Exception (Ausnahme hinzufügen)** auswählen, wird eine Ausnahme hinzugefügt, allerdings nur für den bestimmten Namen, zu dem navigiert wird. Wenn Sie mit einem anderen Namen zum gleichen System navigieren, erhalten Sie erneut die Warnmeldung von Firefox. Sie können entweder für diesen Namen eine weitere Ausnahme hinzufügen oder zum ursprünglichen Namen navigieren.

Sie können das Zertifikat außerhalb dieser Warnung manuell in Firefox importieren. In diesem Fall wird der Name durch Platzhalterzeichen ersetzt. Sie müssen jedoch die Vertrauenswürdigkeit für dieses Zertifikat aktivieren. Wählen Sie im Bereich **Advanced (Erweitert)** unter **Options (Optionen)** die Registerkarte **Encryption (Verschlüsselung)** und dann die Schaltfläche **View Certificates (Zertifikate anzeigen)**. Über die Schaltfläche **Import (Importieren)** können Sie ein Zertifikat importieren. Wählen Sie anschließend das Zertifikat und die Schaltfläche **Edit Trust (Vertrauensstatus bearbeiten)** aus und aktivieren Sie die Option **Trust the authenticity of this certificate (Echtheit dieses Zertifikats vertrauen)**.

4.9.3 Internet Explorer

Die Zertifikatwarnmeldung bietet keine Möglichkeit, das Zertifikat anzuzeigen oder zu importieren. Sie können sie nur umgehen und fortfahren. Ein Zertifikat können Sie manuell über die Option **Internet Options (Internetoptionen)** importieren. Wählen Sie auf der Registerkarte **Content (Inhalt)** die Option **Certificates (Zertifikate)** und dann **Import (Importieren)**. Wenn Sie zur Eingabe des Zertifikatspeichers aufgefordert werden, wählen Sie die Option **Place… (Ort...)** und dann den Speicher **Trusted Root Certification Authorities (Vertrauenswürdige Root-Zertifizierungsstellen)**.

4.9.4 Best Practices für Browser

- Melden Sie sich ab, bevor Sie den Browser schließen. Ein Cookie dient im Browser zum Speichern der authentifizierten Sitzungs-ID des Benutzers. Da das Cookie arbeitsspeicherbasiert ist, wird es beim Schließen des Browsers gelöscht. Dies wirkt sich jedoch nicht auf die Sitzung auf dem Gerät aus. Durch das Abmelden wird sichergestellt, dass die Sitzung auf dem Gerät annulliert wird.
- Vermeiden Sie Links von außerhalb der Geräte-GUI. Klicken Sie möglichst nicht auf Links z. B. in E-Mails oder IM, während Sie beim Gerät angemeldet sind. Es könnte sich um böswillige Links handeln, die Ihre angemeldete Sitzung ausnutzen. Aus dem gleichen Grund sollten Sie es vermeiden, mit demselben Browser-Fenster, z. B. mit anderen Registerkarten desselben Browsers, auf andere Websites zu navigieren. Verwenden Sie einen anderen Browser, um einen separaten Navigationsprozess sicherzustellen. Nutzen Sie z. B. Firefox für das Gerät und Internet Explorer für andere Navigationsprozesse.

4.10 Anmeldedaten

Kennwörter für lokale Benutzerkonten werden in einem Salted Hash gespeichert. Kennwortfelder im Browser sind maskiert, sodass die Kennwörter nicht angezeigt werden. Kennwörter werden bei der Übertragung über das Netzwerk mit SSL zwischen dem Gerät und dem Browser geschützt. Kennwörter für lokale Benutzerkonten müssen mindestens acht Zeichen lang sein. Es werden keine zusätzlichen Regeln für die Komplexität von Kennwörtern vom System erzwungen. Kennwortsicherheit und -ablauf müssen über die Sicherheitsrichtlinie der Website kontrolliert werden (siehe „Optimale Vorgehensweisen bezüglich Sicherheit“ (Seite 35)).

Das Konto `matrixuser` ist kein lokales Benutzerkonto, das auf die UI zugreifen kann. Es wird über einen anderen Kanal verwendet, um die zugrunde liegende SA Foundation aus Matrix Operating Environment zu betreiben. Das Kennwort kann über die UI festgelegt werden und wird nicht angezeigt. Es kann bei Bedarf erneut eingegeben werden, falls der Wert verloren geht. Dieses Kennwort wird nicht im Klartext gespeichert und ist nicht abrufbar.

In die UI eingegebene iLO-Anmeldedaten werden in einem wiederherstellbaren Format gespeichert, da sie an iLO übergeben werden müssen.

Anmeldedaten für Media Server werden in einem wiederherstellbaren Format gespeichert, da sie zur Herstellung der Verbindung mit der Media Server-Freigabe verwendet werden müssen.

Die Standardkennwörter für Betriebssysteminstallationen können in verschlüsselter Form gespeichert werden. Weitere Informationen zu den Standardkennwörtern für OSBPs finden Sie in der Insight Control server provisioning-Online-Hilfe.

4.11 Browserunabhängige Clients

Das Gerät unterstützt eine begrenzte Zahl von REST-APIs. Anforderungen für diese APIs können nicht nur von einem Browser, sondern von jedem beliebigen Client ausgegeben werden. In diesem Fall obliegt es dem Aufrufer, sicherzustellen, dass die entsprechenden Sicherheitsmaßnahmen in Bezug auf die Vertraulichkeit der Anmeldedaten, einschließlich Sitzungs-Token, die für Datenanforderungen und Antworten über die Verschlüsselung der Anmeldedaten mit HTTPS hinaus verwendet werden, eingehalten werden.

4.11.1 Kennwörter

Kennwörter werden zumeist von einem Client wie cURL im Klartext angezeigt und gespeichert. Angezeigte Kennwörter und gespeicherte Daten dürfen für nicht autorisierte Benutzer nicht zugänglich sein. Gleiches gilt für Sitzungs-IDs, auch wenn diese mitunter nur vorübergehend gültig sind.

Primär dient eine REST-Verbindung zur skriptgestützten automatischen Sicherung. Zu diesem Zweck wird die Rolle des Sicherungsadministrators mit beschränkten Berechtigungen zur Verfügung gestellt. So verfügen die mit einem automatischen Sicherungsskript gespeicherten Anmeldedaten nur über die für die Ausführung einer Sicherung erforderlichen Berechtigungen.

4.11.2 SSL/Zertifikat

Der Client sollte HTTPS als Protokoll festlegen, um sicherzustellen, dass SSL zum Schutz sensibler Daten im Netzwerk verwendet wird. Das Gerätezertifikat ist möglicherweise für den Client erforderlich, damit die SSL-Verbindung erfolgen kann. Das Zertifikat kann von einem Browser, der auf das Gerät verweist, abgerufen werden. Weitere Informationen zum Herunterladen des Zertifikats finden Sie unter „Herunterladen“ (Seite 29).

4.12 Geräteoptimierung

4.12.1 Portliste

In der folgenden Tabelle sind die Ports aufgeführt, die für Insight Control server provisioning geöffnet sein müssen.

Port	Beschreibung
22 (tcp)	SSH
80 (tcp)	HTTP
443 (tcp)	HTTPS
3001 (tcp)	SA Agent-Kommunikation
67 (udp)	DHCP
69 (udp)	TFTP
8017 (tcp, udp)	Agent-Gateway
8081 (tcp)	Agent-Cache
111 (tcp, udp)	RPC – für die NFS-Startdatei
2049 (tcp, udp)	NFS – nur für Startdateien
892 (tcp, udp)	mountd
123 (udp)	NTP

4.12.2 Konsolenzugriff

Der Konsolenzugriff wird zu drei Zwecken bereitgestellt: UI-Kiosk, Zurücksetzen des Administratorkennworts für das Gerät und Zugriff durch einen HP Services-Techniker vor Ort. Der Zugriff auf die lokale Konsole selbst, z. B. mit dem vSphere-Client, sollte eingeschränkt sein, um nicht autorisierte Benutzer daran zu hindern, sich über die Konsole anzumelden. Siehe „Einschränken des Konsolenzugriffs“ (Seite 33). Der UI-Kiosk wird in einer grafischen Konsole angezeigt, während die Kennwortrücksetzung und der HP Services-Zugriff über eine nicht grafische Konsole verfügbar sind.

Führen Sie die folgenden Schritte aus, um von einer Konsole auf die andere zu wechseln:

Öffnen Sie das Gerät in vSphere.

1. Drücken und halten Sie die Tasten **Strg+Alt**.
2. Drücken Sie die Leertaste und lassen Sie sie los.
3. Drücken Sie **F1**, um die nicht grafische Konsole auszuwählen, oder **F2** für die grafische Konsole.
4. Lassen Sie die Tasten **Strg+Alt** los.

4.12.3 Konsolen-UI-Kiosk

Der Browser ist im Kioskmodus gesperrt und eingeschränkt, um potenziellen Missbrauch oder Sicherheitslücken zu vermeiden. Er ist nicht als vollwertiger Ersatz Ihres eigenen Browsers gedacht, sondern als Mittel, um für die Erstkonfiguration auf das Gerät zuzugreifen und das Gerätenetzwerk so zu konfigurieren, dass ein Remote-Zugriff erfolgen kann.

4.12.4 Zurücksetzen des Administratorkennworts für das Gerät

Wenn das Kennwort des Benutzers `Administrator` verloren geht, kann es über die Gerätekonsole zurückgesetzt werden. Folgende Schritte sind zum Zurücksetzen des Kennworts erforderlich:

1. Öffnen Sie die Gerätekonsole in vSphere und zeigen Sie die nicht grafische Konsole an.

2. Geben Sie den Benutzernamen **`pwreset`** ein.
3. Das Gerät zeigt einen Challenge-Schlüssel an. Beispiel:

```
<hostname> login: pwreset
     Challenge = xyaay42a3a
     Password:
```

4. Wenden Sie sich an den HP Support, um ein Einmalkennwort zu erhalten, mit dem Sie das `administrator`-Kennwort für das Insight Control server provisioning-Gerät zurücksetzen können. Der Challenge-Schlüssel muss dem Supportmitarbeiter mitgeteilt werden.
5. Anhand des Challenge-Codes generiert der HP Support-Mitarbeiter ein Einmalkennwort. Dabei handelt es sich um eine einfach einzugebende, durch Leerzeichen getrennte Zeichenfolge. Beispiel:

```
VET ROME DUE HESS FAR GAS
```

6. Wenn dieses Kennwort eingegeben wird, zeigt das Gerät ein neues, automatisch generiertes Kennwort an. Merken Sie sich das Kennwort und drücken Sie die **Eingabetaste**.
7. Das neu generierte Kennwort läuft vorzeitig ab. Wenn Sie sich mit diesem Kennwort als `Administrator` beim Gerät anmelden, werden Sie aufgefordert, es zu ändern. Dies entspricht der Vorgehensweise beim Standardkennwort, das unmittelbar bei der Erstkonfiguration geändert werden muss.

Die Funktion zum Zurücksetzen des `Administrator`-Kennworts kann nicht deaktiviert werden.

4.12.5 Aktivieren oder Deaktivieren des Zugriffs durch HP Support-Services

Beim erstmaligen Starten des Geräts haben Sie die Möglichkeit, den Zugriff von HP Support-Services zu aktivieren oder zu deaktivieren. Standardmäßig ist der Zugriff aktiviert, damit HP Support über die Systemkonsole auf Ihr System zugreifen und für schwerwiegende Probleme, die Sie gemeldet haben, eine Diagnose durchführen kann.

Beim Zugriff durch HP Support-Services handelt es sich um eine Shell auf Stammverzeichnisebene, sodass der HP Support-Techniker vor Ort jedes Problem auf dem Gerät vollständig beheben kann. Der HP Support-Mitarbeiter vor Ort kann ein Einmalkennwort für den Shell-Zugriff anfordern. Dazu wird ein Challenge-/Antwortmechanismus ähnlich wie dem Mechanismus zum Zurücksetzen des Kennworts verwendet.

Nach der Erstkonfiguration können Sie den Zugriff durch den HP Support über die UI auf der Seite **Settings (Einstellungen)** aktivieren oder deaktivieren, indem Sie **Actions (Aktionen)→Edit HP support access (Zugriff durch den HP Support bearbeiten)** auswählen. Außerdem ist eine REST-API verfügbar, mit der der Zugriff durch HP Support-Services aktiviert oder deaktiviert werden kann (siehe „REST-Anruf zum Aktivieren bzw. Deaktivieren des Support-Zugriffs“ (Seite 39)).

HP empfiehlt, den Zugriff durch Support-Services aktiviert zu lassen. Sollte ein Problem auftreten, das den Zugriff durch Support-Services erfordert, kann nicht garantiert werden, dass der Zugriff gegebenenfalls erneut aktiviert werden kann.

4.12.6 Einschränken des Konsolenzugriffs

Um den Zugriff auf die Konsole einzuschränken, müssen Sie auch den Zugriff auf die virtuelle Festplatte einschränken. Weitere Informationen finden Sie im *VMware vSphere Security Hardening Guide* (VMware vSphere Sicherheitsoptimierung Handbuch) in den Abschnitten „Host Communications between vSphere Client and ESX Server uses SSL with default certificates — these can be updated“ (Host-Kommunikation zwischen vSphere Client und ESX Server verwendet SSL mit Standardzertifikaten – diese können aktualisiert werden) und „Describe VM protection“ (VM-Schutz beschreiben).

4.12.7 Algorithmen

Die folgenden Algorithmen werden verwendet:

- SSL (siehe nachstehende Tabelle „Unterstützte Cipher Suites“)

- Kennwörter für lokales Benutzerkonto: Hash-Wert mit SHA-256
- Sonstige Kennwörter: mit 128-Bit-Blowfish verschlüsselt
- Sicherungen/Support-Dumps
  - Verschlüsselung: AES 128-Bit
  - Hash: SHA-256
- Support-Dump: AES-Schlüssel wird separat mit 2048-Bit-RSA verschlüsselt
- Aktualisierungen: nicht verschlüsselt, digital signiert mit SHA-256 und 2048–Bit-RSA

Die folgenden SSL Cipher Suites werden auf dem Webserver des Insight Control server provisioning-Geräts aktiviert. Diese Cipher Suites werden für die Verbindung zwischen dem Browser und dem IC server provisioning-Gerät verwendet.

Tabelle 4 Unterstützte Cipher Suites

		Kx	Au	Enc	Mac
DHE-RSA-AES256-SHA	SSLv3	DH	RSA	AES (256)	SHA1
AES256-SHA	SSLv3	RSA	RSA	AES (256)	SHA1
EDH-RSA-DES-CBC3-SHA	SSLv3	DH	RSA	3DES (168)	SHA1
DES-CBC3-SHA	SSLv3	RSA	RSA	3DES (168)	SHA1
DHE-RSA-AES128-SHA	SSLv3	DH	RSA	AES (128)	SHA1
AES128-SHA	SSLv3	RSA	RSA	AES (128)	SHA1

4.13 Downloads vom Gerät

Die folgenden Daten können vom Gerät heruntergeladen werden:

- Support-Dump – Alle Daten im Support-Dump werden verschlüsselt und können nur vom HP Support aufgerufen werden.
- Sicherung – Alle Daten in der Sicherung sind proprietär formatiert; HP empfiehlt Kunden, diese Daten gemäß den jeweiligen Unternehmensanforderungen zu verschlüsseln.
- Prüfprotokolle – Sitzungs-IDs werden nicht protokolliert, nur entsprechende Protokoll-IDs. Kennwörter und andere sensible Daten werden nicht protokolliert.
- SSL-Zertifikat – Zertifikate enthalten öffentliche Daten.
- Media Server-Einrichtungstool – keine Daten enthalten.
- WinPE-Generierungstool – keine Daten enthalten.

4.14 Media Server-Sicherheit

Insight Control Server Provisioning erfordert einen Media Server zum geräteexternen Hosten von Betriebssystemverteilungen, erfassten Betriebssystem-Images und HP SPPs. Dies ist entweder ein Windows- oder ein Linux-Server, und der Zugriff darauf sollte mithilfe von standardmäßigen Betriebssystemmechanismen gesteuert werden.

Die Setup Utility „Windows Media Server“ aktiviert NTLMv2 für mehr Sicherheit. Dieses Utility erstellt eine CIFS-Freigabe auf dem angegebenen Verzeichnis sowie Unterverzeichnisse für Medien und Images. Das Utility benötigt einen Benutzernamen, um diesem Lese-/Schreibzugriff auf die Freigabe zu erteilen. Das Utility erstellt auch ein virtuelles IIS-Verzeichnis mit Lesezugriff im Medienunterverzeichnis. Die CIFS-Freigabe wird zur Windows-Bereitstellung und Imageerfassung verwendet. Das virtuelle HTTP-Verzeichnis wird für Linux- und ESX-Bereitstellungen verwendet.

Die Anmeldedaten für den Freigabebenutzer werden in einem wiederherstellbaren Format auf dem Gerät gespeichert und in OS Build Plans auf dem Media Server verwendet. Der für die Freigabe vorgesehene Benutzer sollte eingeschränkte Rechte haben. Der Benutzer muss über Lese- und Schreibzugriff auf die Freigabe verfügen, darf sich aber nicht beim Media Server anmelden können. Für die Verwaltung des Media Server-Betriebssystems und der Betriebssystemverteilung sollte ein anderer Server verwendet werden.

Wenn die Windows-Imageerfassung nicht verwendet wird, kann die Freigabe mit Lesezugriff erstellt werden. Wenn die Windows-Imageerfassung verwendet wird, kann dem Freigabebenutzer über das Media Server-Betriebssystem Lesezugriff auf das Medienunterverzeichnis erteilt werden.

In einem White Paper werden die Schritte beschrieben, die für die manuelle Einrichtung eines Linux-Media Servers erforderlich sind – es wird kein Utility bereitgestellt. Für das Freigabebenutzerkonto und den webbasierten Zugriff gelten die gleichen Einschränkungen.

4.15 Optimale Vorgehensweisen bezüglich Sicherheit

Die meisten Richtlinien und Vorgehensweisen zur Sicherheit in einer herkömmlichen Umgebung treffen auch in einer virtualisierten Umgebung zu. In einer virtualisierten Umgebung müssen diese Richtlinien jedoch möglicherweise abgewandelt und ergänzt werden. Die folgenden Vorgehensweisen zur Sicherheit werden von HP in einer virtualisierten Umgebung empfohlen. Diese Liste ist nicht vollständig, da es aufgrund unterschiedlicher Sicherheitsrichtlinien und Implementierungspraktiken schwierig ist, eine umfassende und endgültige Liste zu erstellen. Sie stellt jedoch eine gute Ausgangsbasis dar.

- Verwenden Sie ein separates Bereitstellungsnetzwerk. Zur Förderung der Sicherheit und Leistung rät HP zu Folgendem:
  - Einrichten eines privaten Bereitstellungsnetzwerks getrennt vom Produktionsnetzwerk
  - Gewähren von reinem Administratorzugriff auf das Bereitstellungsnetzwerk
  - Verwenden einer Firewall zum Einschränken des Datenverkehrs im Bereitstellungsnetzwerk
- Schränken Sie den Zugriff auf die Gerätekonsole durch autorisierte Benutzer ein. Weitere Informationen finden Sie unter „Einschränken des Konsolenzugriffs“ (Seite 33).
- Eliminieren oder deaktivieren Sie nicht benötigte Services in der Verwaltungsumgebung. Konfigurieren Sie alle Hostsysteme, Verwaltungssysteme und Netzwerkgeräte so, dass nicht benötigte Dienste entweder eliminiert oder deaktiviert werden. Dazu gehören auch nicht benutzte Netzwerk-Ports. Dadurch wird die Anzahl von Angriffsvektoren in Ihrer Umgebung beachtlich reduziert. Das Gerät ist bereits entsprechend konfiguriert.
- Vergewissern Sie sich, dass ein Prozess vorhanden ist, der regelmäßig nach Patches für alle Komponenten in Ihrer Umgebung sucht und sie installiert.
- Sicherheitsrichtlinien und -prozesse müssen auf die Verwendung von Virtualisierungstechnologien in der Umgebung ausgerichtet sein:
  - Unterrichten Sie Administratoren über ihre sich ändernden Rollen und Aufgabenbereiche in einer virtuellen Umgebung.
  - Wenn in Ihrer Umgebung ein Angriffserkennungssystem verwendet wird, stellen Sie sicher, dass dieses System den Netzwerkdatenverkehr im virtuellen Switch (innerhalb eines Hypervisors) einsehen kann.
  - Mindern Sie das potenzielle Ausschnüffeln von VLAN-Datenverkehr, indem Sie den promisken Modus im Hypervisor ausschalten und den über das VLAN fließenden Datenverkehr verschlüsseln.

    HINWEIS: In den meisten Fällen kann der promiske Modus nicht bei einem VM-Guest verwendet werden (der Guest kann ihn aktivieren, aber er funktioniert nicht), wenn er im Hypervisor deaktiviert ist.

- Halten Sie Vertrauenszonen (DMZ getrennt von Produktionsmaschinen) aufrecht.
- Vergewissern Sie sich, dass FC-Geräte über geeignete Zugriffssteuerungen verfügen.
- Verwenden Sie LUN-Maskierung auf Speicher- und Rechenhosts.
- Vergewissern Sie sich, dass LUNs in der Hostkonfiguration definiert statt ermittelt werden.
- Verwenden Sie hardwarebasiertes Zoning auf Port-WWN, falls möglich.
- Vergewissern Sie sich, dass die Kommunikation mit den WWNs auf Switch-Port-Ebene erzwungen wird.

- Grenzen Sie administrative Rollen und Aufgabenbereiche (Host-Administrator, Netzwerkadministrator und Virtualisierungsadministrator) klar voneinander ab.
- Viele Komponenten, die Zertifikate verwenden, werden mit vom Anbieter signierten Zertifikaten bereitgestellt. Um ein höheres Maß an Sicherheit für diese Komponenten zu erzielen, füllen Sie sie zum Zeitpunkt der Bereitstellung mit vertrauenswürdigen Zertifikaten.
- Ändern Sie für lokale Konten auf dem Gerät regelmäßig die Kennwörter in Übereinstimmung mit Ihren Kennwortrichtlinien, und berücksichtigen Sie außerdem die folgenden Richtlinien:
  - Standardkennwörter sollten unverzüglich in ein relevanteres und sicheres Kennwort geändert werden.
  - Administratoren sollten die Kennwörter von Verwaltungsgeräten genauso oft und entsprechend den gleichen Richtlinien wie Server-Administratorkennwörter ändern.
  - Kennwörter sollten mindestens drei der folgenden vier Elemente enthalten: numerische Zeichen, Sonderzeichen, Kleinbuchstaben und Großbuchstaben.
- Verwenden Sie (zum Validieren von Endpunkten) die gegenseitige Geräteauthentifizierung, sofern verfügbar, sowie Benutzerauthentifizierungsmechanismen.
- Schränken Sie den Zugriff auf den iLO Remote Console-Port ein.
  - Für iLO 2: Deaktivieren Sie den `telnet`-Zugriff auf iLO 2.
  - Für iLO der ersten Generation: Erfordern Sie Remote Console-Datenverschlüsselung, und setzen Sie „Remote Console Port Configuration“ (Konfiguration des Remote Console-Ports) auf „Automatic“ (Automatisch).
  - Diese Änderungen erzwingen die Verschlüsselung von Remote Console-Sitzungen und lassen den Port geschlossen, es sei denn, die Remote Console wird angehängt.
- Verbinden Sie keine Verwaltungssysteme (z. B. das Gerät, iLO und OA) direkt mit dem Internet. Falls Sie Zugriff auf das Internet benötigen, verwenden Sie ein Unternehmens-VPN, das Firewall-Schutz bietet.
- Für Servicearbeiten berücksichtigen Sie entsprechende Vorgehensweisen und Prozeduren, beispielsweise aus der ITIL. Besuchen Sie _http://www.itil-officialsite.com/home/home.aspx.
- Berücksichtigen Sie die Benchmarks des Center for Internet Security (CIS), verfügbar unter http://benchmarks.cisecurity.org/. Es werden Benchmarks für HP-UX, Windows, Linux, Citrix Xen Server und VMware Server aufgeführt.

5 Weiterführende Themen

5.1 REST-APIs zum Aktivieren des Zugriffs durch den HP Support oder zum Hinzufügen eines Servers über iLO

REST (Representational State Transfer)-Aufrufe zum Aktivieren/Deaktivieren des Zugriffs durch HP Support-Services oder zum Hinzufügen eines Servers über iLO erfordern drei REST-Aufrufe. Mit dem ersten Aufruf werden eine Benutzersitzung eingerichtet und ein Authentifizierungs-Token generiert; mit dem zweiten REST-Aufruf wird der Zugriff über Services aktiviert/deaktiviert oder ein Server über iLO hinzugefügt. Schließlich muss die Benutzersitzung mit einem REST-Aufruf zum Abmelden beendet werden.

In dieser Diskussion verwenden wir die Open Source-cURL-Utility zum Tätigen von REST-Aufrufen. Das cURL-Open Source-Projekt befindet sich unter: http://curl.haxx.se/. Sie können cURL über eine Befehlszeile unter Linux oder Windows auslösen.

Jeder REST-Aufruf ist eine HTTP-Anforderung und zugehörige Antwort. Die Anforderung umfasst die URL, den Nachrichtentyp, HTTP-Kopfzeilen, Anforderungstext und Antworttext.

5.1.1 REST-Anruf zum Erstellen der Benutzersitzung und Abrufen des Authentifizierungs-Token

Für den REST-Aufruf zum Erstellen der Benutzersitzung müssen Sie die Anmeldedaten des Administratorbenutzers eines Geräts (*<administrator-user>*/*<administrator-password>*, wie unten angegeben) weitergeben, damit der REST-Aufruf mit einem Benutzerautorisierungs-Token (*<user-authorization-token>*, wie unten angegeben) antwortet.

Eine Liste der Komponenten des REST-Aufrufs wird im Folgenden gezeigt:

REST-Komponente	Beschreibung
URL:	https://<appliance-hostname-or-address>/rest/login-sessions?action=login Ort für die Bereitstellung von <appliance-hostname-or-address>
Nachrichtentyp:	POST
HTTP-Kopfzeilen:	accept: application/json content-type: application/json accept-language: en-us (optional)
Anforderungstext:	{"userName":"<administrator-user>","password":"<administrator-password>"} Ort für die Bereitstellung des Benutzernamens und des Kennworts des Geräteadministrators
Antworttext:	{"sessionID":"<user-authorization-token>"} Ort für die Bereitstellung des Benutzerautorisierungs-Token zur Verwendung im zweiten REST-Anruf

Sie lösen cURL auf folgende Weise aus und erhalten die zugehörige Antwort (siehe unten):

cURL-Befehl unter Linux:

```
curl -i -k -H "accept: application/json" -H "content-type: application/json"
-H "accept-language: en-us" -X POST
https://<appliance-hostname-or-address>/rest/login-sessions?action=login
-d '{"userName":"<administrator-user>","password":"<administrator-password>"}'
```

cURL-Befehl unter Windows:

```
curl -i -k -H "accept: application/json" -H "content-type: application/json"
-H "accept-language: en-us" -X POST
https://<appliance-hostname-or-address>/rest/login-sessions?action=login
```

```
-d {\"userName\":\"<administrator-user>\",\"password\":\"<administrator-password>\"}
```

Antwort bei Erfolg:

```
HTTP/1.1 200 OK
Date: Fri, 08 Feb 2013 20:44:01 GMT
Content-Type: application/json
Via: 1.1 cic.dns.hp
cache-control: no-cache
Transfer-Encoding: chunked

{"sessionID":"<user-authorization-token>"}
```

Wenn die Anfrage fehlschlägt, wird eine Fehlerdiagnose angezeigt. Häufige Fehler sind „HTTP error 404 not found“ (HTTP-Fehler 404 nicht gefunden), falls die URL nicht korrekt ist, oder eine Ausnahme, falls der Benutzer oder das Kennwort nicht korrekt ist.

5.1.2 REST-Anruf zum Abmelden bei der Benutzersitzung

Für den REST-Anruf zum Abmelden bei der Benutzersitzung müssen Sie den Benutzerautorisierungs-Token weitergeben.

REST-Komponente	Beschreibung
URL:	https://<appliance-hostname-or-address>/rest/login-sessions?action=logout Ort für die Bereitstellung von <appliance-hostname-or-address>
Nachrichtentyp:	DELETE (LÖSCHEN)
HTTP-Kopfzeilen:	accept: application/json content-type: application/json accept-language: en-us (optional) auth: <user-authorization-token> Ort für die Bereitstellung von <user-authorization-token>
Anforderungstext:	Keine
Antworttext:	Keine Bei erfolgreicher Abmeldung

Sie lösen cURL auf folgende Weise aus und erhalten die zugehörige Antwort (siehe unten):

cURL-Befehl unter Linux:

```
curl -i -k -H "accept: application/json" -H "content-type: application/json"
-H "accept-language: en-us" -H "auth: <user-authorization-token>" -X DELETE
https://<appliance-hostname-or-address>/rest/login-sessions?action=logout
```

cURL-Befehl unter Windows:

```
curl -i -k -H "accept: application/json" -H "content-type: application/json"
-H "accept-language: en-us" -H "auth: <user-authorization-token>" -X DELETE
https://<appliance-hostname-or-address>/rest/login-sessions?action=logout
```

Antwort bei Erfolg:

```
HTTP/1.1 204 No Content
Date: Wed, 20 Feb 2013 15:36:40 GMT
Via: 1.1 cic.dns.hp
cache-control: no-cache
Content-Length: 0
Content-Type: text/plain; charset=UTF-8

Response Body: None
```

Wenn die Anforderung fehlschlägt, werden Sie zur Fehlerdiagnose zurückgeleitet. Häufige Fehler sind „HTTP error 404 not found“ (HTTP-Fehler 404 nicht gefunden), falls die URL nicht korrekt ist.

5.1.3 REST-Anruf zum Aktivieren bzw. Deaktivieren des Support-Zugriffs

Sie können nicht nur den Zugriff auf Ihr Insight Control Server Provisioning-Gerät durch den HP Support über die UI aktivieren oder deaktivieren (wählen Sie auf der Seite **Settings** (Einstellungen) die Optionen **Actions (Aktionen)→Edit HP support access (Zugriff auf HP-Support bearbeiten)**), sondern haben auch die Möglichkeit, diese Aufgabe programmatisch durchzuführen. Dieser alternative Ansatz ist hilfreich, wenn die Benutzeroberfläche des Geräts nicht antwortet und Sie den Zugriff durch HP Support zum Diagnostizieren eines Problems aktivieren müssen.

Für die Programmierung müssen drei REST-Aufrufe des Insight Control server provisioning-Geräts durchgeführt werden. Beim ersten Aufruf wird eine Benutzersitzung eingerichtet. Beim zweiten Aufruf wird der Support-Zugriff auf das Gerät aktiviert bzw. deaktiviert. Beim dritten Aufruf wird die Abmeldung bei der Sitzung durchgeführt.

Weitere Informationen zum Durchführen des ersten REST-Aufrufs finden Sie unter „REST-Anruf zum Erstellen der Benutzersitzung und Abrufen des Authentifizierungs-Token“ (Seite 37).

Der zweite REST-Aufruf dient zum Aktivieren bzw. Deaktivieren des Support-Zugriffs auf das Gerät. In diesem REST-Aufruf müssen Sie den `<user-authentication-token>` bereitstellen, den Sie vom ersten Anmelde-REST-Aufruf erhalten haben, und Sie müssen entweder `true` oder `false` weitergeben, um anzugeben, ob der Zugriff durch Services aktiviert werden soll.

Weitere Informationen zum Durchführen des dritten REST-Aufrufs für die Abmeldung bei der Benutzersitzung finden Sie unter „REST-Anruf zum Abmelden bei der Benutzersitzung“ (Seite 38).

Eine Liste der Komponenten des REST-Aufrufs wird im Folgenden gezeigt:

REST-Komponente	Beschreibung
URL:	https://`<appliance-hostname-or-address>`/rest/appliance/settings/enableServiceAccess Ort für die Bereitstellung von `<appliance-hostname-or-address>`
Nachrichtentyp:	PUT
HTTP-Kopfzeilen:	accept: application/json content-type: application/json accept-language: en-us (optional) auth: `<user-authorization-token>` Ort für die Bereitstellung von `<user-authorization-token>`
Anforderungstext:	“`<true/false>`” Angeben, ob der Support-Zugriff aktiviert werden soll
Antworttext:	„true“ falls der Zugriff durch Services erfolgreich aktiviert oder deaktiviert wurde

Sie lösen cURL auf folgende Weise aus und erhalten die zugehörige Antwort (siehe unten):

cURL-Befehl unter Linux:

```
curl -i -k -H "accept: application/json" -H "content-type: application/json"
-H "accept-language:en-us"
-H "auth: <user-authorization-token>" -X PUT
https://<appliance-hostname-or-address>/rest/appliance/settings/enableServiceAccess
-d "true/false"
```

cURL-Befehl unter Windows:

```
curl -i -k -H "accept: application/json" -H "content-type: application/json"
-H "accept-language:en-us"
```

```
-H "auth: <user-authorization-token>" -X PUT
https://<appliance-hostname-or-address>/rest/appliance/settings/enableServiceAccess
-d \"<true/false>\"
```

Antwort bei Erfolg:

```
HTTP/1.1 200 OK
Date: Fri, 08 Feb 2013 20:46:13 GMT
Content-Type: application/json
Via: 1.1 cic.dns.hp
cache-control: no-cache
Transfer-Encoding: chunked

True
```

Wenn die Anforderung fehlschlägt, werden Sie zur Fehlerdiagnose zurückgeleitet. Häufige Fehler sind „HTTP error 404 not found" (HTTP-Fehler 404 nicht gefunden), falls die URL nicht korrekt ist, oder eine Ausnahme, falls der zugehörige Benutzer zum Aktivieren/Deaktivieren des Zugriffs durch Services nicht berechtigt ist.

Nachfolgend finden Sie ein Beispiel für ein Linux-Shell-Skript mit cURL, das sich beim Gerät anmeldet, den Support-Zugriff aktiviert/deaktiviert und sich wieder abmeldet.

```
#!/bin/sh
# login
AUTH=`curl -k -X POST -H "accept:application/json" -H "content-type: application/json"
https://<appliance-hostname-or-address>/rest/login-sessions?action=logout
-d '{"userName":"<administrator-name>","password":"<administrator-password>"}' | perl -e 'while (<>)
{/{"sessionID":"(.*)"}/ && print $1;}'`
# This REST call either enables or disables support access to the appliance.
curl -i -k -H "accept:application/json" -H "content-type:application/json"
-H "accept-language:en-us"
-H "auth: ${AUTH}" -X PUT
https://<appliance-hostname-or-address>/rest/appliance/settings/enableServiceAccess
-d "<true/false>"
# logout
curl -k -i -X DELETE -H "auth:${AUTH}"
https://<appliance-hostname-or-address>/rest/login-sessions?action=logout
```

5.1.4 REST-Aufruf zum Hinzufügen eines Servers über iLO

Sie können REST-Aufrufe zum Hinzufügen eines Servers über iLO verwenden.

Für die Programmierung müssen drei REST-Aufrufe des Insight Control Server Provisioning-Geräts durchgeführt werden. Der erste Aufruf wird zum Abrufen eines Authentifizierungs-Tokens oder einer Sitzungs-ID verwendet. Daraufhin tätigen Sie unter Verwendung dieser Sitzungs-ID den REST-Aufruf, um die eigentliche Registrierung durchzuführen. Mit dem dritten Aufruf melden Sie sich bei der Sitzung ab.

Weitere Informationen zum Durchführen des ersten REST-Aufrufs zum Erstellen der Benutzersitzung finden Sie unter „REST-Anruf zum Erstellen der Benutzersitzung und Abrufen des Authentifizierungs-Token" (Seite 37).

Mit dem zweiten REST-Aufruf wird ein Server über iLO hinzugefügt. In diesem REST-Aufruf müssen Sie den *<user-authentication-token>* bereitstellen, den Sie beim ersten Anmelde-REST-Aufruf erhalten haben. Darüber hinaus müssen Sie die IP-Adresse des iLO sowie den Benutzernamen und das Kennwort des iLO-Administrators bereitstellen.

Weitere Informationen zum Durchführen des dritten REST-Aufrufs für die Abmeldung bei der Benutzersitzung finden Sie unter „REST-Anruf zum Abmelden bei der Benutzersitzung" (Seite 38).

Es gibt zwei REST-Aufrufe, die zum Hinzufügen eines Servers über den zugehörigen iLO verwendet werden können. Mit einem dieser Aufrufe wird der Server hinzugefügt und im Wartungsmodus gestartet. Mit dem anderen Aufruf wird der Server zwar hinzugefügt, jedoch nicht im Wartungsmodus gestartet. Bei Angabe des optionalen Anforderungsparameters „addstyle" wird der Server hinzugefügt, ohne den Server in den Wartungsmodus zu versetzen. Wenn dieser Parameter nicht vorhanden ist, wird der Server im Wartungsmodus gestartet.

REST-Anruf zum Hinzufügen eines Servers über iLO, wobei der Server im Wartungsmodus gestartet wird

Eine Liste der Komponenten des REST-Aufrufs wird im Folgenden gezeigt.

REST-Komponente	Beschreibung
URL:	https://<appliance-hostname-or-address>/rest/os-deployment-ilos Ort für die Bereitstellung von <appliance-hostname-or-address>
Nachrichtentyp:	POST
HTTP-Kopfzeilen:	accept: application/json content-type: application/json accept-language: en-us (optional) auth: <user-authorization-token> Ort für die Bereitstellung von <user-authorization-token>
Anforderungstext:	{"type":"OSDIlo","username":"<iLO-administrator-user>","password":"<iLO-administrator-password>","port":<port>,"ipAddress":"<iLO-IP-address>"} „Type“ ist der Ressourcenname. Sie stellen Folgendes bereit: <iLO-administrator-user>, <iLO-administrator-password>, den für die Verbindung mit iLO zu verwendenden Port und die <iLO-IP-address> von IPv4
Antworttext:	{"uri":"/rest/os-deployment-jobs/JobID"} gibt URI mit Job-ID aus

Sie lösen cURL auf folgende Weise aus und erhalten die zugehörige Antwort (siehe unten):

cURL-Befehl unter Linux:

```
curl -i -k -X POST -H "auth: <user-authorization-token>" -H "content-type:application/json"
-H "accept:application/json" -H "accept-language:en-us"
https://<appliance-hostname-or-address>/rest/os-deployment-ilos
-d '{"type":"OSDIlo","username":"<iLO-administrator-user>",
"password":"<iLO-administrator-password>",
"port":443,"ipAddress":"<iLO-IP-address>"}'
```

cURL-Befehl unter Windows:

```
curl -i -k -X POST -H "auth: <user-authorization-token>" -H "content-type:application/json"
-H "accept:application/json" -H "accept-language:en-us"
https://<appliance-hostname-or-address>/rest/os-deployment-ilos
-d {\"type\":\"OSDIlo\",\"username\":\"<iLO-administrator-use>r\",
\"password\":\"<iLO-administrator-password>\",
\"port\":443,\"ipAddress\":\"<iLO-IP-address>\"}
```

Antwort bei Erfolg:

```
HTTP/1.1 202 Accepted
Date: Wed, 20 Feb 2013 17:33:30 GMT
Content-Type: application/json
Via: 1.1 cic.dns.hp
cache-control: no-cache
Transfer-Encoding: chunked

This response is accompanied by returned job URI.
```

Nachfolgend sehen Sie ein Beispielskript, das sich auf dem Gerät anmeldet, den Server über iLO hinzufügt und sich wieder abmeldet. Dieses Skript verwendet cURL.

```
#!/bin/sh
# login
AUTH=`curl -k -X POST -H "accept:application/json" -H "content-type: application/json"
https://<appliance-hostname-or-address>/rest/login-sessions?action=login
-d '{"userName":"<administrator-name>","password":"<administrator-password>"}' | perl -e 'while (<>)
```

```
{/{"sessionID":"(.*)"}/ && print $1;}'`
# This script invokes a job to add iLO-managed server.
curl -i -k -X POST -H "auth:${AUTH}" -H "content-type:application/json" -H "accept:application/json"
-H "accept-language:en-us"  https://<appliance-hostname-or-address>/rest/os-deployment-ilos
-d '{"type":"OSDIlo","username":"<administrator-name>","password":"<administrator-password>",
"port":443,"ipAddress":"<iLO-IP-address>"}'
# logout
curl -k -i -X DELETE -H "auth:${AUTH}"
https://<appliance-hostname-or-address>/rest/login-sessions?action=logout
```

REST-Anruf zum Hinzufügen eines Servers über iLO, wobei der Server nicht im Wartungsmodus gestartet wird

Eine Liste der Komponenten des REST-Aufrufs wird im Folgenden gezeigt.

REST-Komponente	Beschreibung
URL:	https://<appliance-hostname-or-address>/rest/os-deployment-ilos/?addstyle=old Ort für die Bereitstellung von <appliance-hostname-or-address>
Nachrichtentyp:	POST
HTTP-Kopfzeilen:	accept: application/json content-type: application/json accept-language: en-us (optional) auth: <user-authorization-token> Ort für die Bereitstellung von <user-authorization-token>
Anforderungstext:	{"type":"OSDIlo","username":"<iLO-administrator-user>","password": "<iLO-administrator-password>","port":<port>,"ipAddress":"<iLO-IP-address>"} „Type“ ist der Ressourcenname. Sie stellen Folgendes bereit: <iLO-administrator-user>, <iLO-administrator-password>, den für die Verbindung mit iLO zu verwendenden Port und die <iLO-IP-address> von IPv4
Antworttext:	{"uri":"/rest/os-deployment-jobs/JobID"} gibt URI mit Job-ID aus

Sie lösen cURL auf folgende Weise aus und erhalten die zugehörige Antwort (siehe unten):

cURL-Befehl unter Linux:

```
curl -i -k -X POST -H "auth:${AUTH}" -H "content-type:application/json"
-H "accept:application/json" -H "accept-language:en-us"
https://<appliance-hostname-or-address>/rest/os-deployment-ilos?addstyle=old
-d '{"type":"OSDIlo","username":"<iLO-administrator-user>",
"password":"<iLO-administrator-password>",
"port":443,"ipAddress":"<iLO-IP-address>"}'
```

cURL-Befehl unter Windows:

```
curl -i -k -X POST -H "auth: <user-authorization-toke>n" -H "content-type:application/json"
-H "accept:application/json" -H "accept-language:en-us"
https://<appliance-hostname-or-address>/rest/os-deployment-ilos?addstyle=old
-d {\"type\":\"OSDIlo\",\"username\":\"<iLO-administrator-user>\",
\"password\":\"<iLO-administrator-password>\",
\"port\":443,\"ipAddress\":\"<iLO-IP-address>\"}
```

Antwort bei Erfolg:

```
HTTP/1.1 202 Accepted
Date: Wed, 20 Feb 2013 17:33:30 GMT
Content-Type: application/json
Via: 1.1 cic.dns.hp
cache-control: no-cache
Transfer-Encoding: chunked
```

```
This response is accompanied by returned job URI.
```

Nachfolgend sehen Sie ein Beispielskript, das sich auf dem Gerät anmeldet, den Server über iLO hinzufügt und sich wieder abmeldet. Dieses Skript verwendet cURL.

```
#!/bin/sh
# login
AUTH=`curl -k -X POST -H "accept:application/json" -H "content-type: application/json"
https://<appliance-hostname-or-address>/rest/login-sessions?action=login
-d '{"userName":"<administrator-name>","password":<administrator-password>"}' ' | perl -e 'while (<>)
{/{"sessionID":"(.*)"}/ && print $1;}'`
# This script invokes a  job to add iLO-managed server.
curl -i -k -X POST -H "auth:${AUTH}" -H "content-type:application/json"
-H "accept:application/json" -H "accept-language:en-us"
https://<appliance-hostname-or-address>/rest/os-deployment-ilos/?addstyle=old
-d '{"type":"OSDIlo","username":"<iLO-administrator-user>","password":"<iLOadministrator-password>",
"port":443,"ipaddress":"<iLO-IP-address>"}'
# logout
curl -k -i -X DELETE -H "auth:${AUTH}"
https://<appliance-hostname-or-address>/rest/login-sessions?action=logout
```

Nachdem das Registrierungsverfahren eingeleitet wurde, werden in der linken Spalte der Seite **Jobs** (Aufträge) zwei iLO-bezogene Aufträge angezeigt. Erster Auftrag – „Registers IloManagerService“ (IloManagerService registrieren) enthält die Jobdetails zum Hinzufügen eines Servers über iLO. Zweiter Auftrag – „Add iLO-managed Server“ (iLO-verwalteten Server hinzufügen) enthält Jobdetails zum Starten eines Servers unter dem Standard-Servicebetriebssystem, in der Regel Linux PE.

Häufige Fehler beim Registrieren eines Servers über iLO:

500 – Internal Server Error (Interner Serverfehler)

Behebung: Erstellen Sie einen Support-Dump.

403 – Request Forbidden (Anforderung unzulässig)

Ursache: Der Benutzer kann mit den bereitgestellten Anmeldedaten nicht angemeldet werden

Behebung: Melden Sie sich unter Verwendung gültiger Anmeldedaten erneut an.

409 – Conflict (Konflikt)

Ursache: Die vom Benutzer bereitgestellte iLO-IP-Adresse wurde bereits für die Registrierung und iLO verwendet.

Behebung: Löschen Sie den Server mit der doppelten iLO, und versuchen Sie es erneut oder verwenden Sie eine andere iLO-Adresse.

404 – Not Found (Nicht gefunden)

Ursache: Der Server kann nicht gefunden werden.

Behebung: Stellen Sie sicher, dass der Server vorhanden ist bzw. nicht gelöscht wurde.

400 – Bad Request (Ungültige Anforderung)

Ursache: Beim Tätigen eines REST-Aufrufs ist einer der bereitgestellten Parameter möglicherweise nicht vorhanden, fehlerhaft oder ungültig.

Behebung: Stellen Sie sicher, dass die Parameter das richtige Format haben.

5.2 REST-API zum Herstellen und Herunterladen eines Support-Dumps

Sie können nicht nur einen Support-Dump von Ihrem Insight Control Server Provisioning-Gerät über die UI herunterladen, sondern diese Aufgabe auch programmatisch durchführen. Dieser alternative Ansatz ist hilfreich, wenn die Benutzeroberfläche des Geräts nicht antwortet und Sie einen Support-Dump zum Diagnostizieren eines Problems abrufen müssen.

Für die Programmierung müssen zwei REST-Aufrufe des Insight Control-Serverbereitstellungsgeräts durchgeführt werden. Mit dem ersten Anruf wird der Support-Dump auf dem Gerät erstellt. Mit dem zweiten Aufruf wird der Support-Dump heruntergeladen.

In dieser Diskussion verwenden wir die Open Source-cURL-Utility zum Tätigen von REST-Aufrufen. Das cURL-Open Source-Projekt befindet sich unter: http://curl.haxx.se/. Sie können cURL über eine Befehlszeile unter Linux oder Windows auslösen.

Eine Liste der Komponenten des REST-Aufrufs zum Erstellen des Support-Dumps wird im Folgenden gezeigt:

REST-Komponente	Beschreibung
URL:	https://<appliance-hostname-or-address>/rest/appliance/support-dumps Ort für die Bereitstellung von <appliance-hostname-or-address>
Nachrichtentyp:	POST
HTTP-Kopfzeilen:	accept: application/json content-type: application/json
Anforderungstext:	{"errorCode": "<support-dump-error>"} wo <support-dump-error> zum Generieren des Support-Dump-Dateinamens verwendet wird
Antworttext:	{"type":"DumpDataInfoDto", "dumpFileSize":8087, "uri": "<support-dump-filename>", "category":null, "eTag":null, "created":"Tue Jun 19 03:11:25 MDT 2012", "modified":null } Verwenden Sie <support-dump-filename> im nachfolgenden REST-Aufruf, um den Support-Dump herunterzuladen.

Sie lösen cURL auf folgende Weise aus und erhalten die zugehörige Antwort (siehe unten):

cURL-Befehl unter Linux:

```
curl -i -k -H "accept: application/json" -H "content-type: application/json" -H "accept-language:en-us"
-X POST https://<appliance-hostname-or-address>/rest/appliance/support-dumps
-d `{"errorCode": "<support-dump-error>"}'
```

cURL-Befehl unter Windows:

```
curl -i -k -H "accept: application/json" -H "content-type: application/json" -H "accept-language:en-us"
-X POST https://<appliance-hostname-or-address>/rest/appliance/support-dumps
-d "{\"errorCode\": \"<support-dump-error>\"}"
```

Antwort bei Erfolg:

```
HTTP/1.1 200 OK
Date: Fri, 08 Feb 2013 20:46:13 GMT
Content-Type: application/json
Via: 1.1 cic.dns.hp
cache-control: no-cache
Transfer-Encoding: chunked
```

Wenn die Anforderung fehlschlägt, wird eine Fehlerdiagnose angezeigt. Häufige Fehler sind „HTTP error 404 not found“ (HTTP-Fehler 404 nicht gefunden), falls die URL nicht korrekt ist.

Eine Liste der Komponenten des REST-Aufrufs zum Herunterladen des Support-Dumps wird im Folgenden gezeigt:

REST-Komponente	Beschreibung
URL:	https://<appliance-hostname-or-address>/rest/appliance/support-dumps/<support-dump-filename> unter der Sie <appliance-hostname-or-address> bereitstellen und

REST-Komponente	Beschreibung
	<support-dump-filename> vom vorherigen Aufruf abgerufen wird, um den Support-Dump zu erstellen
Nachrichtentyp:	GET
HTTP-Kopfzeilen:	accept: application/json content-type: application/json

Sie können den von der GET-Nachricht abgerufenen verschlüsselten Support-Dump mithilfe der „-o“-Option an eine <output-support-dump-file> weiterleiten.

Häufiger cURL-Fehler unter Linux und Windows:

```
curl -i -k -X GET https://<appliance-hostname-or-address>/rest/appliance/support-dumps/
<support-dump-filename> -o <output-support-dump-file>
```

Wenn die Anforderung fehlschlägt, wird eine Fehlerdiagnose angezeigt. Häufige Fehler sind „HTTP error 404 not found“ (HTTP-Fehler 404 nicht gefunden), falls die URL nicht korrekt ist.

5.3 Hinzufügen von Servern, auf denen bereits ein Betriebssystem ausgeführt wird

Server, auf denen bereits ein Betriebssystem ausgeführt wird, können zu IC server provisioning ohne Neustart hinzugefügt werden, indem der HP Server Automation (SA)-Agent dem Zielserver hinzugefügt und dann der iLO des Servers registriert wird.

So fügen Sie den HP Server Automation-Agent zu einem verwalteten Server hinzu:

1. Bestimmen Sie den Dateinamen des SA-Agent über http://*xxx.xxx.xxx.xxx*:8081, wobei *xxx.xxx.xxx.xxx* die IP-Adresse der Bereitstellung oder der DNS-Name des virtuellen IC server provisioning-Geräts ist. Suchen Sie nach den Dateien mit der Endung .current. Abhängig von der Version des Betriebssystems und dem Architekturtyp sind unterschiedliche Agent-Dateien verfügbar.

   Nachfolgend finden Sie eine Liste der SA-Agent-Dateien:

Betriebssystem	SA-Agent zum Herunterladen
Windows 2008 x64	opsware-agent-NT-6.0-X64.current
Windows 2008 R2 x64	opsware-agent-NT-6.1-X64.current
Windows 2012 x64	opsware-agent-NT-6.2-X64.current
Red Hat EL 5.x	opsware-agent-LINUX-5SERVER-X86_64.current
Red Hat EL 6.x	opsware-agent-LINUX-5SERVER-X86_64.current
SLES 11	opsware-agent-LINUX-SLES-11-X86_64.current

HINWEIS: Es gibt keinen SA-Agent, der unter VMware ESXi ausgeführt wird.

2. Laden Sie den SA-Agent anhand des genauen Dateinamens in der URL ohne die Dateierweiterung .current herunter, http://*xxx.xxx.xxx.xxx*:8081/<*filename*>, wobei <*filename*> der Name der SA-Agent-Datei ist.

WICHTIG: Laden Sie die Datei nicht herunter, indem Sie die Agent-Dateien auflisten und dann mit der rechten Maustaste auf **Save** (Speichern) klicken, um sie zu speichern. Die Datei enthält nur HTML-Inhalte und funktioniert nicht in Verbindung mit IC server provisioning.

3. Sobald eine Windows-Agent-Datei heruntergeladen wurde, benennen Sie die Datei mit einer `.exe`-Dateierweiterung um. Für Linux wird der Dateiname ohne Erweiterung verwendet.
4. Installieren Sie den SA-Agent auf dem Zielserver mit den Parametern `–s --opsw_gw_list coreip:3001`, wobei `coreip` die IP-Adresse des virtuellen IC server provisioning-Geräts ist. Vergewissern Sie sich, dass Sie die IP-Adresse der Bereitstellung, nicht die IP-Adresse des Geräts verwenden.
5. Vergewissern Sie sich, dass der Zielserver in IC server provisioning angezeigt wird.
6. Damit auf diesem Zielserver ein OSBP ausgeführt werden kann, muss der iLO ebenfalls bei IC server provisioning registriert werden. Hierfür stehen Ihnen folgende Möglichkeiten zur Verfügung:
   a. Sie können die iLO-Informationen eines jeden Zielservers manuell hinzufügen. Wählen Sie auf der Seite IC server provisioning **Servers** (Server) den Pfad **Actions (Aktionen)→Add Servers (Server hinzufügen)**, geben Sie die iLO-IP-Adresse und die Anmeldedaten des Zielservers ein, und aktivieren Sie das Kontrollkästchen **Do not boot to maintenance** (Nicht im Wartungsmodus starten). Wählen Sie **Add** (Hinzufügen), um die iLO-Registrierung zu starten, oder **Add+** (Hinzufügen+), um weitere IP-Adressen einzugeben.
   b. Sie können die iLO-Informationen eines jeden Servers mit dem programmatischen REST-Aufruf (siehe „REST-Aufruf zum Hinzufügen eines Servers über iLO“ (Seite 40)) hinzufügen. Verwenden Sie diejenige Option, die den Server nicht im Wartungsmodus startet.
7. Vergewissern Sie sich, dass der iLO ordnungsgemäß auf dem Server registriert wurde, indem Sie zur Seite **Servers** (Server) wechseln und überprüfen, ob die IP-Adresse des iLO dort aufgelistet wird.

6 Support und andere Ressourcen

6.1 Kontaktaufnahme mit HP

6.1.1 Vor der Kontaktaufnahme mit HP

Stellen Sie sicher, dass Ihnen die folgenden Informationen vorliegen, bevor Sie sich an HP wenden:

- Registrierungsnummer beim Technischen Support (sofern zutreffend)
- Insight Control server provisioning-Version
- Eventuell vorliegende Fehlermeldungen
- Software und Hardware von Fremdherstellern
- Betriebssystem und Revisionsstufe
- Support-Dump (optional): „Erstellen eines Support-Dumps“ (Seite 47)

6.1.2 Erstellen eines Support-Dumps

6.1.2.1 In folgenden Fällen muss möglicherweise ein Support-Dump erstellt werden

- Bestimmte von Insight Control server provisioning angezeigte Fehlermeldungen empfehlen das Erstellen eines Support-Dumps des Geräts, der zur Auswertung an den HP Support gesendet wird.
- Im Fall eines Problems, das Ihrer Meinung die Auswertung von internen Gerätedaten erfordert, empfiehlt HP das sofortige Erstellen eines Support-Dumps, um wichtige Daten besser erfassen zu können.
- In einigen Fällen werden Sie vom HP Support möglicherweise dazu aufgefordert, im Rahmen eines Serviceauftrags einen Support-Dump zu erstellen.

6.1.2.2 So erstellen Sie einen Support-Dump

Diese Support-Dump-Funktion erfasst Protokolle, Informationen zur Systemkonfiguration und zum Status, und erstellt dann eine verschlüsselte, komprimierte Datei, die zur Fehlerbehebung an den HP-Support gesendet werden kann. Das nachfolgende Verfahren verwendet die UI. Sie können auch eine REST-API verwenden, falls die UI nicht verfügbar ist (siehe „REST-API zum Herstellen und Herunterladen eines Support-Dumps“ (Seite 43)

1. Melden Sie sich auf dem Gerät mit Administratorberechtigungen an.
2. Navigieren Sie über das Hauptmenü zur Seite **Settings** (Einstellungen).
3. Wählen Sie **Actions (Aktionen)→Create support dump (Support-Dump erstellen)**.

   Während der Support-Dump erstellt wird, können Sie mit der Durchführung anderer Aufgaben fortfahren.
4. Nachdem der Support-Dump erstellt wurde, werden Sie zum Speichern der Datei `tar.gz` aufgefordert. Wenn in Ihren Browsereinstellungen ein Standardordner für Downloads angegeben ist, werden Downloads standardmäßig in diesem Ordner gespeichert.
5. Wenden Sie sich an den HP Support, um Anweisungen zur Bereitstellung des Support-Dumps zu erhalten.

6.1.2.3 Inhalte von Support-Dumps

Ein Support-Dump erfasst die folgenden Informationen von Ihrem Gerät.

Alle Informationen zur Gerätekonfiguration:

- Revision der Gerätesoftware

- Netzwerkkonfiguration
- DNS-Server
- NTP-Server

Informationen zum ausgeführten Gerät:

- Alle Prozesse
- Arbeitsspeicher
- Festplattenspeicherkapazität
- Netzwerkstatistiken
- Routing
- Hardwareinformationen

Protokolldaten:

- Alle standardmäßigen Linux-Betriebssystemprotokolle
- Alle Geräteprotokolle
- Protokolle aller Aufträge, die in den letzten drei Tagen ausgeführt wurden
- Installationsprotokolle
- Das Systemüberwachungsprotokoll

Weitere Informationen:

- Ein Statusbericht aller Prozesse
- Datumsangaben zu allen verwendeten Zertifikaten

HINWEIS: Die folgenden Elemente sind möglicherweise als Ergebnis der oben genannten Datenerfassung im Support-Dump enthalten:

- IP-Adressen (des Geräts, von Zielsystemen und verbundenen Browsern)
- Hostnamen
- System-UUIDs
- Benutzernamen (in einem Support-Dump werden niemals Kennwörter erfasst)
- Informationen zur Netzwerkkonfiguration
- WWIDs

6.1.3 HP Kontaktinformationen

HP Partner in Ihrer Nähe:

- Rufen Sie die Webseite „Contact HP worldwide“ (in englischer Sprache) auf: (http://welcome.hp.com/country/us/en/wwcontact.html)

HP Website für technische Unterstützung:

- Kontaktoptionen für die USA finden Sie auf der Webseite „Contact HP United States“: (http://welcome.hp.com/country/us/en/contact_us.html) So erreichen Sie HP telefonisch:
  - Wählen Sie in den USA 1-800-HP-INVENT (1-800-474-6836). Dieser Service ist 24 Stunden täglich verfügbar. Zwecks kontinuierlicher Qualitätsverbesserung können die Aufrufe aufgezeichnet oder überwacht werden.
  - Rufen Sie in anderen Ländern die Webseite „Contact HP worldwide“ (in englischer Sprache) auf: http://welcome.hp.com/country/us/en/wwcontact.html

6.1.4 Abonnementservice

HP empfiehlt, Ihr Produkt auf der Subscriber's Choice for Business Website zu registrieren: http://www.hp.com/country/us/en/contact_us.html. Nach der Registrierung erhalten Sie eine E-Mail-Benachrichtigung über die Verbesserungen des Produkts, neue Treiberversionen, Firmwareaktualisierungen und andere Produkt-Ressourcen.

6.2 Weiterführende Informationen

6.2.1 Dokumente

Die folgenden Dokumente sind verfügbar unter http://www.hp.com/go/insightcontrol/docs.

- *HP Insight Control Server Provisioning Online Help* (HP Insight Control Serverbereitstellung Onlinehilfe) (im PDF-Format)
- *HP Insight Control Server Provisioning Administrator Guide*
- Das White Paper *Data Migration from HP Insight Control server deployment to HP Insight Control server provisioning* (Datenmigration von Insight Control Server Deployment zu HP Insight Control server provisioning)

6.2.2 Websites

- Website für Software-Downloads: http://www.hp.com/go/insightupdates
- Website für HP Insight Control server provisioning-Dokumentation: http://www.hp.com/go/insightcontrol/docs

6.3 Typografische Konventionen

In diesem Dokument kommen die folgenden Schreibweisen zu Anwendung:

`%`, `$` oder `#`	Das Prozentzeichen repräsentiert die Systemeingabeaufforderung der C-Shell. Das Dollarzeichen steht für die Systemeingabeaufforderungen der Bourne-, Korn- und POSIX-Shells. Das Nummernzeichen steht für die Superuser-Eingabeaufforderung.
audit(5)	Eine Hilfeseite. Der Name der Hilfeseite lautet *audit*, und sie befindet sich in Abschnitt 5.
`Command`	Ein Befehlsname oder eine qualifizierte Befehlsphrase.
`Computer output`	Auf dem Computer angezeigter Text.
Strg+x	Eine Tastenkombination. Eine Tastenkombination wie **Strg+A** bedeutet, dass Sie die Taste **Strg** gedrückt halten müssen, während Sie eine zweite Taste auf der Tastatur oder die Maustaste drücken.
`UMGEBUNGSVARIABLE`	Der Name der Umgebungsvariablen, z. B. `PATH`.
ERROR NAME	Der Name eines Fehlers, wie er üblicherweise in der Variablen `errno` zurückgegeben wird.
Taste	Der Name einer Tastaturtaste. **Eingabetaste** und **Eingabe** beziehen sich beide auf die gleiche Taste.
Begriff	Definierter Gebrauch eines wichtigen Worts oder Ausdrucks.
`Benutzereingabe`	Befehle und anderer Text, den Sie eingeben.
`Variable`	Der Name eines Platzhalters in einem Befehl, einer Funktion oder anderen Syntax, der durch einen tatsächlichen Wert zu ersetzen ist.
[]	Inhalte zwischen eckigen Klammern sind in der Syntax optional. Falls mehrere durch | voneinander getrennte Inhalte vorhanden sind, darf nur einer der Inhalte gewählt werden.

{}	Inhalte zwischen geschweiften Klammern sind in der Syntax obligatorisch. Falls mehrere durch | voneinander getrennte Inhalte vorhanden sind, darf nur einer der Inhalte gewählt werden.
…	Das vorhergehende Element kann beliebig oft wiederholt werden.
□	Weist auf die Fortsetzung eines Codebeispiels hin.
|	Trennzeichen zwischen mehreren Optionen in einer Liste.
VORSICHT	Mit dem Wort WARNUNG sind wichtige Informationen gekennzeichnet, die bei Nichtbefolgung zu Gesundheitsschäden oder nicht wieder behebbaren Systemproblemen führen können.
ACHTUNG	Mit ACHTUNG sind wichtige Informationen gekennzeichnet, die bei Nichtbefolgung zu Datenverlust, Datenfehlern oder Schäden an Hardware oder Software führen können.
WICHTIG	Dieses Kennzeichen weist auf wichtige Informationen zu Erläuterung eines Begriffs oder zur Ausführung einer Aufgabe hin.
HINWEIS	Ein HINWEIS enthält zusätzliche Informationen zur Betonung oder Ergänzung wichtiger Punkte im Haupttext.

6.4 Customer Self Repair (Reparatur durch den Kunden)

HP Produkte sind mit vielen Customer Self Repair-Teilen konzipiert, um die Reparaturzeit zu minimieren und mehr Flexibilität beim Austauschen von defekten Teilen zu ermöglichen. Wenn HP (bzw. ein HP Serviceanbieter oder Servicepartner) während des Diagnosezeitraums ermittelt, dass die Reparatur mit einem Customer Self Repair-Teil durchgeführt werden kann, liefert HP dieses Ersatzteil direkt an Sie, damit Sie es ersetzen können. Es gibt zwei Kategorien von Customer Self Repair-Teilen:

- Erforderlich – Teile, die im Rahmen des Customer Self Repair-Programms ersetzt werden müssen. Wenn Sie diese Teile von HP ersetzen lassen, werden Ihnen die Versand- und Arbeitskosten für diesen Service berechnet.
- Optional – Teile, für die Customer Self Repair optional ist. Diese Teile sind auch für Customer Self Repair ausgelegt. Wenn Sie jedoch den Austausch dieser Teile von HP vornehmen lassen möchten, können bei diesem Service je nach den für Ihr Produkt vorgesehenen Garantiebedingungen zusätzliche Kosten anfallen.

HINWEIS: Einige Teile sind nicht für Customer Self Repair ausgelegt. Um den Garantieanspruch des Kunden zu erfüllen, muss das Teil von einem HP Servicepartner ersetzt werden. Im illustrierten Teilekatalog sind diese Teile mit *No* bzw. „Nein“ gekennzeichnet.

Basierend auf der Verfügbarkeit und den geografischen Möglichkeiten werden Customer Self Repair-Teile innerhalb von zwei Werktagen ausgeliefert. Lieferungen am selben Tag oder innerhalb von vier Stunden sind unter Entrichtung zusätzlicher Gebühren möglich, sofern es die geografischen Gegebenheiten zulassen. Falls Sie Hilfe benötigen, wenden Sie sich an den Technischen Support von HP. Ein Techniker wird Ihnen über das Telefon Hilfe leisten. Im Begleitmaterial, das im Lieferumfang des Customer Self Repair-Teils enthalten ist, wird angegeben, ob das defekte Teil an HP zurückgesandt werden muss. In Fällen, in denen das defekte Teil an HP zurückgegeben werden muss, müssen Sie es innerhalb eines bestimmten Zeitraums, in der Regel fünf (5) Werktage, an HP zurücksenden. Das defekte Teil muss zusammen mit der zugehörigen Dokumentation im bereitgestellten Verpackungsmaterial zurückgesandt werden. Wenn Sie das defekte Teil nicht an HP zurücksenden, wird Ihnen der Ersatz möglicherweise berechnet. Im Rahmen des Customer Self Repair-Programms übernimmt HP alle Liefer- und Rücksendekosten und bestimmt das zu beauftragende Kurier-/Transportunternehmen.

Weitere Informationen zum HP Customer Self Repair-Programm erhalten Sie von Ihrem Serviceanbieter. Für das Nordamerikaprogramm besuchen Sie die HP Website (http://www.hp.com/go/selfrepair).

7 Feedback zur Dokumentation

HP hat sich zur Bereitstellung von Dokumentation verpflichtet, die Ihre Anforderungen erfüllt. Um uns in unseren Bemühungen zu unterstützen, die Dokumentation ständig zu verbessern, senden Sie bitte Fehler, Vorschläge oder Kommentare an Documentation Feedback (**docsfeedback@hp.com**). Geben Sie dabei den Dokumenttitel, die Teilenummer, die Versionsnummer oder die URL an.

Glossar

Agent Software auf verwalteten Servern, die zur Durchführung von Änderungen an den Servern verwendet wird. Zu den unterstützten Funktionen gehören die Installation und Entfernung von Software, die Konfiguration von Hardware und Software und die Erstellung von Berichten zum Serverstatus.

Aktualisierung Siehe Aktualisierung eines virtuellen Geräts.

Aktualisierung eines virtuellen Geräts Herunterladen und Installieren einer Updateversion der HP Insight Control server provisioning-Appliance, um Software-Updates und neue Inhalte für die Bereitstellung von Betriebssystemen zu integrieren.

Anlage Die Gruppe von Prozessen, die auf einem einzigen HP Insight Control server provisioning-Gerät verwaltet werden. In der Regel befinden sich diese Server in demselben Netzwerk oder in angeschlossenen Netzwerken. Eine Anlage kann ein Rechenzentrum, ein Serverraum oder ein Computerlabor oder ein Teil davon sein.

Antwortdatei Siehe Konfigurationsdatei.

AutoYaST-Datei Der Begriff, der verwendet wird, wenn es um eine SUSE Linux Enterprise Server (SLES)-Konfigurationsdatei geht.

Bare-Metal Beschreibt einen Server, auf dem kein Produktionsbetriebssystem installiert ist. Dies kann ein nagelneuer Server ohne installiertes Betriebssystem sein. Ein Bare-Metal-Server ist in der Regel ein Server, der bei der Managementsoftware noch nicht registriert ist, oder ein neu hinzugefügter Server ohne installiertes Produktionsbetriebssystem.

Bare-Metal-Ermittlung

Der Prozess, bei dem ein Bare-Metal-Server bei der Bereitstellungssoftware registriert wird. Um ein Bare-Metal-System zu ermitteln, wird dieses System in der Regel in einem speziellen Servicebetriebssystem gebootet. Das Servicebetriebssystem enthält genügend Software, um verschiedene Details über den Server zurück an die Managementsoftware zu melden und ein Produktionsbetriebssystem zu implementieren. Die Bare-Metal-Ermittlung kann manchmal mit dem iLO des Servers erfolgen. In diesem Fall ist das Servicebetriebssystem nicht erforderlich.

Benutzerdefiniertes Attribut

Ein einfaches benutzerdefiniertes Name/Wert-Paar, das als variable Substitution in Skripts und anderen Gerätefunktionen verwendet wird. Dabei wird der Name des benutzerdefinierten Attributs durch den Wert dieses benutzerdefinierten Attributs ersetzt. Benutzerdefinierte Attribute stehen niemals allein; sie sind immer mit einem Objekt in der Verwaltungsdatenbank, wie zum Beispiel Servern, Gruppen oder OS Build Plans, verknüpft. Benutzerdefinierte Attribute können durch Vererbung aus einem übergeordneten Objekt übernommen werden. Zum Beispiel übernimmt (erbt) ein Server in einer Gruppe die benutzerdefinierten Attribute aus dieser Gruppe.

bereitgestellt Auf einem Server in diesem Zustand ist ein Betriebssystem installiert.

Bereitstellung Siehe Einrichtung.

Bereitstellung Installieren eines Betriebssystems auf einem Zielserver durch skriptgesteuerte Installation oder Bereitstellung eines erfassten Image.

Bereitstellungs-Image

Siehe Imageinstallation.

Bereitstellungsjob Siehe Job.

Betriebssystem-Verteilungsdateien

Die Dateien, aus denen ein Betriebssystem besteht, bevor dieses Betriebssystem auf einem Server installiert wird. Diese Dateien werden von den Herstellern der Betriebssysteme, wie Microsoft, Red Hat, VMware und Novell, den Verbrauchern als ISO-Images oder auf physischen CDs/DVDs bereitgestellt.

Betriebssystempersonalisierung

Der Prozess, bei dem ein aktiver Server die Merkmale erhält, die ihn einzigartig machen, wie zum Beispiel IP-Konfiguration, Hostname und Domäne. Ein Server kann bei der Erstinstallation oder nach der Installation des Betriebssystems personalisiert werden.

BLOB-Speicher Ein Bereich des Speichers, auf den sowohl der iLO als auch die eingebettete Softwareumgebung zugreifen können. Durch das Lesen und Schreiben von Dateien im BLOB-Speicher kann die Managementsoftware über den iLO mit der eingebetteten Umgebung kommunizieren. Dadurch ist es nicht erforderlich, über die Produktionsnetzwerkschnittstellen des Servers zu kommunizieren.

Dateirepository Siehe Media Server.

erfasstes Image Ein Datenspeicher, der alle Informationen von einem Zielserver enthält, einschließlich der Dateien, Plattenpartitionen und allen anderen Komponenten, die für eine vollständige Neuerstellung des Zielservers auf dem gleichen oder einem anderen Server erforderlich sind. Das erfasste Image enthält keine Partitionen, nur Dateisystemdaten. Siehe auch Imageinstallation.

Gehäuse Ein Chassis, das mehrere Blade Server und Verbindungsmodule enthält.

Gerät Siehe Virtuelles Gerät.

HP Scripting Toolkit (STK) Ein Produkt für die unbeaufsichtigte Serverinstallation.

HPSUM HP Smart Update Manager, ein einheitliches Tool für die Aktualisierung von Firmware und Treibern.

iLO Siehe Integrated Lights-Out (iLO).

iLO Virtual Media Eine Funktion von HP Integrated Lights-Out (iLO), mit der Sie ein Wechselspeichergerät oder eine Imagedatei auf einem Client-Computer so mit dem Server verbinden können, dass das Gerät bzw. diese Datei als lokales Gerät behandelt wird. Der Server kann von diesem virtuellen Gerät booten oder es in einem aktiven Betriebssystem verwenden.

Imageinstallation Der Prozess zum Installieren eines Servers unter Verwendung eines zuvor erfassten Image des Datenträgers, um ein Duplikat des ursprünglichen Servers zu erstellen. Im Gegensatz dazu siehe skriptgesteuerte Installation.

Installation mittels Skripts Die Betriebssystembereitstellungs-Methode, bei der Konfigurationsdateien und Betriebssystem-Verteilungsdateien verwendet werden, um ein Betriebssystem auf einem Zielserver als unbeaufsichtigte Installation zu implementieren. Dies ist die normale Methode zur Installation des Betriebssystems durch den Betriebssystemanbieter, wobei der interaktive Installationsprozess automatisiert ist. Im Gegensatz dazu siehe Imageinstallation.

Integrated Lights-Out (iLO) Ein unabhängiger Mikroprozessor in ProLiant Servern, der mehrere Möglichkeiten bietet, Server über Fernzugriff zu konfigurieren, zu aktualisieren und zu betreiben. iLO kann die meisten Funktionen, die ansonsten direkt an den Servern im Rechenzentrum, im Computerraum oder am externen Standort ausgeführt werden müssen, über Fernzugriff ausführen. Siehe http://www.hp.com/go/ilo.

integrierte Bereitstellung Siehe integrierte Bereitstellungsfunktionen.

integrierte Bereitstellungsfunktionen

Ein Satz Bereitstellungstools und Servicebetriebssysteme, die in HP ProLiant Server ab der Serie Gen8 integriert sind. Mit diesen integrierten Tools ist es möglich, einen ProLiant Server ohne Netzwerkboot (PXE) oder Wechselmedien zu implementieren und zu konfigurieren und aufgetretene Fehler zu beheben.

Intelligent Provisioning Eine Einzelserverbereitstellung mit der HP ProLiant Gen8 iLO Management Engine. Siehe auch integrierte Bereitstellungsfunktionen.

Job Eine Aufgabe, die auf dem Insight Control server provisioning-Gerät ausgeführt wird. Jobs wirken sich in der Regel auf den Status eines Zielservers aus und schließen die Ausführung eines OS Build Plan ein.

Kickstart-Datei Der Begriff, der verwendet wird, wenn es um eine Red Hat Enterprise Linux- oder VMware ESXi-Installationsdatei geht. Generell wird der Begriff Konfigurationsdatei verwendet.

Konfigurationsdatei

Der Oberbegriff für unbeaufsichtigte Windows- und Linux-Installationsdateien. Diese Dateien enthalten alle Informationen, die zum Installieren des Betriebssystems ohne Benutzereingriff erforderlich sind. Bezieht sich auch auf Dienstprogramme zur Hardwarekonfiguration, wie BIOS-Konfiguration und Array Controller-Konfiguration. Kunden können neue Konfigurationen

für ihre eigenen Zwecke erstellen. Weitere Informationen finden Sie unter AutoYaST-Datei und kickstart-Datei.

LinuxPE Das Servicebetriebssystem für das Linux-Betriebssystem.

Media Server Ein Server, der die bei der Betriebssystembereitstellung verwendeten vom Anbieter bereitgestellten Betriebssystemmedien enthält. Der Zugriff auf die Betriebssystemmedien auf dem Media Server erfolgt über das Netzwerk mittels HTTP für Linux und ESXi bzw. mittels SMB für Windows. Der Media Server kann auch Medien für andere Zwecke enthalten, zum Beispiel Firmware- und Treiber-Updates, und ist außerdem der Ort, an dem erfasste Images gespeichert werden. Der Media Server ist ein vom Insight Control server provisioning-Gerät getrennter Server.

Medien Software auf dem Media Server, die vom Anbieter bereitgestellte Betriebssystem-Verteilungsdateien, von HP bereitgestellte Betriebssystem-Verteilungsdateien, erfasste Images und Firmware- und Treiber-Updates, wie zum Beispiel HP Service Packs for Proliant (HP SPP), enthalten können.

Microsoft WAIK Windows Automated Installation Kit. Ein Satz Tools, einschließlich WinPE, von Microsoft für die Bereitstellung des Windows-Betriebssystems. WAIK war erstmalig für Windows Vista verfügbar.

nicht bereitgestellt Ein Server, auf dem ein SA-Agent installiert ist, der von Insight Control server provisioning gesteuert wird und der auf die Installation eines Betriebssystems wartet. Siehe Wartungsmodus.

nicht erreichbar Ein Serverstatus, bei dem der Server durch die Insight Control server provisioning-Appliance nicht kontaktiert werden kann.

Offline-Firmwareaktualisierung

Eine Methode zum Aktualisieren der System-Firmware, bei der der Server als Teil des Prozesses offline geschaltet und neu gestartet werden muss. Bei einer Offline-Aktualisierung wird das System heruntergefahren und in einem Servicebetriebssystem gebootet, in dem dann die Firmwareaktualisierung erfolgt. Nach Abschluss der Aktualisierung kann das System wieder online geschaltet werden.

OGFS-Skript Ein Skript, das im Opsware Global File System ausgeführt wird. OGFS-Skripts werden auf dem Insight Control server provisioning-Gerät ausgeführt und in der Regel in Shell oder Python geschrieben.

Opsware Global File System (OGFS) Das OGFS entspricht dem SA-Datenmodell in Form einer hierarchischen Struktur aus Dateiverzeichnissen und Textdateien. Zum Beispiel enthält im OGFS das Verzeichnis `/opsw/Server` die Informationen über Zielserver. Es sind auch Unterverzeichnisse vorhanden, die den Inhalt der Zielserver (wie zum Beispiel Dateisysteme und Registrierungen) widerspiegeln. Wenn Sie die erforderlichen Berechtigungen besitzen, können Sie die Dateisysteme der Zielserver in der Global Shell anzeigen und sogar ändern.

OS Build Plan Eine Abfolge aus OS Build Plan-Schritten, die in bestimmter Reihenfolge ausgeführt werden, um eine Aufgabe auf einem Zielserver auszuführen. OS Build Plans werden in der Regel für die Einrichtung von Betriebssystemen verwendet, können aber auch für nahezu jede Aufgabe, die automatisiert werden kann, verwendet werden.

OS Build Plan-Schritt Eine autonome Operation, wie zum Beispiel "Skript ausführen" oder "Paket installieren", im Rahmen eines OS Build Plan.

Paket Eine komprimierte (gepackte) Datei, die ausführbare Dateien, Konfigurationsinformationen und Skriptdateien enthält. Ein Beispiel für ein Paket ist eine ZIP-Datei mit der Erweiterung `.zip` mit Windows-Treibern für unbeaufsichtigte Installationen.

Preboot Environment Siehe Servicebetriebssystem.

PXE-frei Siehe integrierte Bereitstellungsfunktionen.

Schritt Siehe OS Build Plan-Schritt.

Server Automation (SA) HP Server Automation-Software. Siehe http://www.hp.com/go/serverautomation.

Serverermittlung Der Prozess, bei dem ein Server auf dem Insight Control server provisioning-Gerät ermittelt wird. Bei Bare-Metal-Systemen wird der Server in einem Servicebetriebssystem mit einem installierten Agenten gebootet, der die Registrierung bei der Appliance durchführt. Bei Servern mit bereits installiertem Betriebssystem wird der Agent auf dem aktiven Betriebssystem installiert und führt

dann die Registrierung bei der Appliance durch. Sobald ein Server bei Insight Control server provisioning registriert ist, kann er für die Bereitstellung ausgewählt werden.

Serverstatus

Tabelle 5 Serverstatus

	Der Server ist bereitgestellt und OK.
	Auf einem bereitgestellten Server wird ein Job ausgeführt.
	Dies ist ein nicht bereitgestellter Server, der bereitgestellt werden kann.
	Auf einem nicht bereitgestellten oder bereitgestellten Server wird gerade die Bereitstellung ausgeführt.
	Neustartphase eines Jobs, der gerade auf einem bereitgestellten Server ausgeführt wird.
	Auf diesem Server ist die Bereitstellung fehlgeschlagen. Er ist für die Bereitstellung verfügbar.
	Der Server ist nicht erreichbar. Das bedeutet, HP Insight Control server provisioning kann nicht mit dem Server kommunizieren.
	Serverstatus ist Insight Control server provisioning nicht bekannt.

Siehe auch Wartungsmodus, bereitgestellt und nicht erreichbar.

Servicebetriebssystem

Ein spezielles Betriebssystem, das vollständig im Arbeitsspeicher des Systems ausgeführt wird und verwendet wird, um verschiedene Wartungsfunktionen auf einem Server, einschließlich der Vorbereitung eines Systems für die Betriebssysteminstallation, auszuführen. Insight Control server provisioning besitzt Servicebetriebssysteme auf der Basis von Linux und Windows. Siehe auch LinuxPE und WinPE.

Skript

Durch Insight Control server provisioning werden Skripts der folgenden Typen unterstützt:

- UNIX – Bourne-Shell (sh), C-Shell (csh) und Korn-Shell (ksh)
- OGFS – Opsware Global File System
- Windows .BAT – Windows-Batchdatei
- Windows VBScript – Erstellen von Visual Basic-Skripts
- Python – Programmiersprache Python

SLES

Steht für SUSE Linux Enterprise Server. Ein Betriebssystem, das von SUSE auf der Basis von Linux entwickelt wurde.

Software-Repository

Siehe Media Server.

Softwarepaket

Siehe Paket.

SPP

HP Service Pack for ProLiant. Siehe http://www.hp.com/go/spp.

Status

Siehe Serverstatus und Jobstatus.

STK

Siehe HP Scripting Toolkit (STK).

unattend-Datei

Der Begriff, der verwendet wird, wenn es um eine Windows-Installationsdatei geht. Generell wird der Begriff Konfigurationsdatei verwendet.

unbeaufsichtigte Installation

Die automatische Installation eines Windows- oder Linux-Betriebssystems, bei der kein Benutzereingriff erforderlich ist.

Verbindungsmodul Ein spezielles Ethernet-, FC- oder FCoE-Verbindungsmodul für die Arbeit in einem Blade-Gehäuse.

Verteilungsdateien Siehe Betriebssystem-Verteilungsdateien.

verwalteter Server Ein bereitgestellter Server, auf dem ein SA-Agent installiert ist und der vom Insight Control server provisioning-Gerät gesteuert wird.

virtuelles Gerät Eine virtuelle Maschine mit einer vorinstallierten Softwareanwendung, die für die Ausführung der Anwendung optimiert wurde.

WAIK Siehe Microsoft WAIK.

Wartungsmodus Ein Serverstatus, bei dem ein Server mit einem Servicebetriebssystem gebootet wird und eine Wartungsversion des SA OGFS-Agenten ausführt. Server im Wartungsmodus warten in der Regel auf ihre Einrichtung.

WIM-Installation Eine Installation mit dem Windows Imaging Format. Siehe Imageinstallation.

WinPE Die Vorinstallationsumgebung Windows Preinstallation Environment ist das Servicebetriebssystem für das Betriebssystem Windows.

Zielserver Der Server, für den ein Insight Control server provisioning-Vorgang bestimmt ist. Auf einem Zielserver wird ein SA-Agent ausgeführt.

Stichwortverzeichnis