

# Versionshinweise zu Veritas™ Resiliency Platform 3.1

# Versionshinweise

In diesem Dokument werden folgende Themen behandelt:

- [Versionshinweise](#)
- [Neue Funktionen und Änderungen in Veritas Resiliency Platform 3.1](#)
- [Netzwerk- und Firewall-Anforderungen](#)
- [Verwenden der Produktdokumentation](#)
- [Behobene Probleme](#)
- [Bekannte Probleme: Allgemein](#)
- [Bekannte Probleme: Wiederherstellung in Amazon Web Services \(AWS\)](#)
- [Bekannte Probleme: Wiederherstellung in Azure](#)
- [Bekannte Probleme: Wiederherstellung in vCloud](#)
- [Bekannte Probleme: Resiliency Platform Data Mover bei der Wiederherstellung im lokalen Rechenzentrum](#)
- [Bekannte Probleme: Resiliency Platform Data Mover](#)
- [Bekannte Probleme: Wiederherstellung mithilfe von Replikationsanwendungen anderer Hersteller](#)
- [Bekannte Probleme: NetBackup-Integration](#)
- [Bekannte Probleme: Mehrere Resiliency Manager in einem Rechenzentrum](#)
- [Beschränkungen](#)

# Versionshinweise

**Tabelle 1-1** Versionshinweise zu Veritas Resiliency Plattform 3.1

Informationen zu...	finden Sie unter...
Versionsübersicht	Siehe <a href="#">"Verwenden der Produktdokumentation"</a> auf Seite 8.
Systemanforderungen	Siehe <a href="#">"Netzwerk- und Firewall-Anforderungen"</a> auf Seite 7.
Behobene Probleme	Siehe <a href="#">"Behobene Probleme"</a> auf Seite 9.
Bekannte Probleme	<p>Siehe <a href="#">"Bekannte Probleme: Allgemein"</a> auf Seite 10.</p> <p>Siehe <a href="#">"Bekannte Probleme: Wiederherstellung in Amazon Web Services (AWS)"</a> auf Seite 12.</p> <p>Siehe <a href="#">"Bekannte Probleme: Wiederherstellung in Azure"</a> auf Seite 15.</p> <p>Siehe <a href="#">"Bekannte Probleme: Wiederherstellung in vCloud"</a> auf Seite 15.</p> <p>Siehe <a href="#">"Bekannte Probleme: Resiliency Plattform Data Mover bei der Wiederherstellung im lokalen Rechenzentrum"</a> auf Seite 16.</p> <p>Siehe <a href="#">"Bekannte Probleme: Resiliency Plattform Data Mover"</a> auf Seite 18.</p> <p>Siehe <a href="#">"Bekannte Probleme: Wiederherstellung mithilfe von Replikationsanwendungen anderer Hersteller"</a> auf Seite 19.</p> <p>Siehe <a href="#">"Bekannte Probleme: NetBackup-Integration"</a> auf Seite 20.</p> <p>Siehe <a href="#">"Bekannte Probleme: Mehrere Resiliency Manager in einem Rechenzentrum"</a> auf Seite 22.</p>
Beschränkungen	Siehe <a href="#">"Beschränkungen"</a> auf Seite 23.

## Neue Funktionen und Änderungen in Veritas Resiliency Plattform 3.1

Diese Version von Veritas Resiliency Plattform enthält die folgenden neuen Funktionen, Änderungen und Verbesserungen.

Siehe ["Unterstützung der Objektspeichermodusreplikation für einmalige Migration nach AWS"](#) auf Seite 4.

Siehe ["Unterstützung für mehrere Netzwerkkarten für Replication Gateway-Appliance"](#) auf Seite 5.

Siehe ["Unterstützung der FIPS-Aktivierung für Replication Gateway"](#) auf Seite 5.

Siehe ["Unterstützung für die Zuordnung von einer zu mehreren Netzwerkgruppen für AWS"](#) auf Seite 5.

Siehe ["Unterstützung für das Auswählen mehrerer Replication Gateway-Paare"](#) auf Seite 5.

Siehe ["Bearbeiten der Resiliency Group-Vorgangsverbesserungen"](#) auf Seite 5.

Siehe ["Unterstützung für das Ersetzen eines fehlerfreien Replication Gateways in einem Paar"](#) auf Seite 6.

Siehe ["Verbesserungen der Infrastruktur-Resiliency"](#) auf Seite 6.

Siehe ["Unterstützung für Übernahmeprozess aus dem Cloud-Rechenzentrum"](#) auf Seite 6.

Siehe ["Unterstützung für das Online-Schalten des virtuellen Computers aus dem Speicher für AWS und Azure"](#) auf Seite 6.

Siehe ["RDM-Unterstützung für Replikation mit Resiliency Platform Data Mover"](#) auf Seite 6.

Siehe ["Unterstützung des Azure-Speichertyps "Standard" für die Größe virtueller Computer"](#) auf Seite 7.

Siehe ["Änderungen an den erforderlichen Berechtigungen zum Hinzufügen eines Windows-Hosts"](#) auf Seite 7.

Siehe ["Unterstützung von Windows 16 als Host-Betriebssystem"](#) auf Seite 7.

Siehe ["Unterstützung der japanischen Sprache"](#) auf Seite 7.

## Unterstützung der Objektspeichermodusreplikation für einmalige Migration nach AWS

In Veritas Resiliency Platform 3.1 wurde die Objektspeichermodusreplikation eingeführt, um die von AWS bereitgestellten S3-Objektspeicherdienste zu nutzen. Wenn Sie eine einmalige Migration Ihrer Rechenzentrums-Assets in AWS durchführen möchten, können Sie die Objektspeichermodusreplikation auswählen. Um die einmalige Migration Ihrer Assets auf AWS mit der Objektspeichermodusreplikation zu aktivieren, müssen Sie ein Data Gateway in einer AWS-Umgebung bereitstellen.

Sie können bei Verwendung der Objektspeichermodusreplikation keine Rückmigration Ihrer Assets aus dem AWS-Rechenzentrum in das lokale Rechenzentrum durchführen.

## Unterstützung für mehrere Netzwerkkarten für Replication Gateway-Appliance

Veritas Resiliency Platform 3.1 beinhaltet erstmals Unterstützung für das Konfigurieren von Replication Gateways mit mehreren Netzwerkkarten. Die Replication Gateway-Appliance wird mit drei Netzwerkkarten geliefert. Sie können diese drei Netzwerkkarten konfigurieren, die für die Kommunikation mit dem Infrastructure Management Server (IMS), dem Peer-Replication Gateway und den zu schützenden virtuellen Computern verwendet werden. Wenn Sie nicht planen, drei separate Netzwerke zu verwenden, können Sie die Konfigurierung aller drei Netzwerkkarten überspringen und stattdessen nur ein oder zwei konfigurieren.

## Unterstützung der FIPS-Aktivierung für Replication Gateway

Federal Information Processing Standards (FIPS) ist eine Reihe von Normen der US-Regierung zur Standardisierung kryptografischer Software. Veritas Resiliency Platform 3.1 unterstützt FIPS-Compliance für die Datenverschlüsselung des Resiliency Platform-Replication Gateway. Sie können den FIPS-Modus auf einem Replication Gateway beim Bootstrap oder mit der Option `manage > fips` im klish-Menü aktivieren.

## Unterstützung für die Zuordnung von einer zu mehreren Netzwerkgruppen für AWS

Veritas Resiliency Platform 3.1 unterstützt das Erstellen von Netzwerkgruppen nur mit Subnetzen aus dem Amazon Web Services (AWS)-Cloud-Rechenzentrum. Netzwerkgruppen werden erstellt, wenn Sie möchten, dass Ihre virtuellen Computer in einer Resiliency Group Teil der verschiedenen Verfügbarkeitszonen in AWS-Cloud sind.

## Unterstützung für das Auswählen mehrerer Replication Gateway-Paare

Veritas Resiliency Platform 3.1 beinhaltet erstmals Unterstützung für die Auswahl mehrerer Replication Gateway-Paare beim Konfigurieren der Resiliency Group für die Wiederherstellung.

## Bearbeiten der Resiliency Group-Vorgangverbesserungen

Veritas Resiliency Platform 3.1 ermöglicht das Bearbeiten einer Resiliency Group, die für DR konfiguriert ist, anhand verschiedener Bearbeitungsoptionen, etwa Anpassen der Netzwerke oder Bearbeiten der gesamten Konfiguration.

## Unterstützung für das Ersetzen eines fehlerfreien Replication Gateways in einem Paar

Veritas Resiliency Platform 3.1 beinhaltet erstmals Unterstützung für das Ersetzen eines Replication Gateway in einem Paar, wenn sich beide Gateways in fehlerfreiem Zustand befinden.

## Verbesserungen der Infrastruktur-Resiliency

Veritas Resiliency Platform 3.1 beinhaltet erstmals Unterstützung zum Verschieben von Replication Gateways, Replikations-Server und Hyper-V-Server auf einen neuen Infrastructure Management Server (IMS), wenn der alte IMS nicht mehr verwendet werden kann.

## Unterstützung für Übernahmeprovorgang aus dem Cloud-Rechenzentrum

Veritas Resiliency Platform 3.1 beinhaltet erstmals Unterstützung für die Übernahme einer Resiliency Group aus einem Cloud-Rechenzentrum.

## Unterstützung für das Online-Schalten des virtuellen Computers aus dem Speicher für AWS und Azure

In Veritas Resiliency Platform 3.1 können Sie die Schaltfläche "Speicher, Netzwerk, Computer und Anpassungen aktualisieren" beim Starten einer Resiliency Group verwenden, wenn die Resiliency Group für die Wiederherstellung in AWS oder Azure konfiguriert ist.

Diese Option lädt den Speicher, fügt den virtuellen Computer dem Netzwerk hinzu und schließt die IP-Adressanpassung ab.

## RDM-Unterstützung für Replikation mit Resiliency Platform Data Mover

Veritas Resiliency Platform 3.1 unterstützt Raw Device Mapping (RDM)-Datenträger für die Replikation mit dem Resiliency Platform Data Mover. Die RDM-Datenträger-Unterstützung für den Resiliency Platform Data Mover gilt für die folgenden Anwendungsfälle:

- Wiederherstellung in einem Cloud-Rechenzentrum: Unterstützung für RDM im virtuellen und physischen Kompatibilitätsmodus
- Wiederherstellung in einem lokalen Rechenzentrum: Unterstützung für RDM im virtuellen Kompatibilitätsmodus

## Unterstützung des Azure-Speichertyps "Standard" für die Größe virtueller Computer

Veritas Resiliency Platform 3.1 unterstützt jetzt den Speichertyp "Standard" für die Größe virtueller Computer im Azure-Rechenzentrum.

## Änderungen an den erforderlichen Berechtigungen zum Hinzufügen eines Windows-Host

Veritas Resiliency Platform 3.1 enthält einige Änderungen bei den erforderlichen Berechtigungen zum Hinzufügen eines Windows-Host.

Für das Hinzufügen von einem Windows-Host wird empfohlen, ein Domänenbenutzerkonto mit lokalen Administratorrechten auf dem Windows-Installationshost sowie auf dem hinzuzufügenden Host zu verwenden. Wenn Sie kein Domänenbenutzerkonto mit lokalen Administratorrechten auf beiden Hosts verwenden können, haben Sie die Option, einen Administratorbenutzer oder einen Benutzer in einer lokalen Administratorgruppe mit bestimmten Voraussetzungen zu verwenden.

## Unterstützung von Windows 16 als Host-Betriebssystem

Veritas Resiliency Platform 3.1 unterstützen Windows 16 als Betriebssystem für virtuelle Computer, die mit Resiliency Platform geschützt werden können.

## Unterstützung der japanischen Sprache

Neben Deutsch unterstützt Veritas Resiliency Platform 3.1 auch Japanisch. Ab Version 3.1 wird die lokalisierte Version der Resiliency Platform-Konsole angezeigt, wenn Sie sich mit einem Browser mit japanischen Standortinformationen einloggen. Das Produkt kann innerhalb einer japanischen Umgebung verwendet werden.

# Netzwerk- und Firewall-Anforderungen

Die folgenden Ports werden für Veritas Resiliency Platform verwendet:

- [Wiederherstellen von Assets in AWS](#)
- [Wiederherstellen von Assets in Azure](#)
- [Wiederherstellen von Assets in vCloud Director](#)
- [Wiederherstellen von Assets im lokalen Rechenzentrum mit Resiliency Platform Data Mover](#)

- Wiederherstellen von Assets im lokalen Rechenzentrum mit Replikationsanwendungen anderer Hersteller
- Wiederherstellen von Assets mit NetBackup
- Wiederherstellen von InfoScale-Anwendungen

## Verwenden der Produktdokumentation

Tabelle 1-2 enthält die URLs für die Dokumentation zu Veritas Resiliency Platform und Tabelle 1-3 die Handbücher zu Veritas Resiliency Platform.

**Tabelle 1-2** URLs für die Dokumentation zu Veritas Resiliency Platform

URL	Beschreibung
<a href="https://sort.veritas.com/documents">https://sort.veritas.com/documents</a>	Die neueste Version der Produktdokumentation: Produkt Handbücher im PDF-Format. Online-Hilfe-Portal. Der Inhalt der Hilfe ist auch in der Produktkonsole verfügbar.
<a href="https://www.veritas.com/community/business-continuity/videos">https://www.veritas.com/community/business-continuity/videos</a>	Die Liste der Videos zu Resiliency Platform.
<a href="https://www.veritas.com/support/en_US/article.100040713">https://www.veritas.com/support/en_US/article.100040713</a>	Die aktuellen Neuerungen in dieser Version.

**Tabelle 1-3** Namen der Veritas Resiliency Platform-Handbücher

Titel	Beschreibung
<i>Liste der mit Veritas Resiliency Platform kompatiblen Hardware und Software (HSCL)</i>	Liste der kompatiblen Hardware und Software
<i>Versionshinweise zu Veritas Resiliency Platform</i>	Informationen zur Version wie Hauptfunktionen, bekannte bzw. behobene Probleme und Einschränkungen.
<i>Überblick und Planungshandbuch zu Veritas Resiliency Platform 3.1</i>	Informationen zum Produkt sowie dessen Funktionen und Einsatzmöglichkeiten.
<i>Benutzerhandbuch zu Veritas Resiliency Platform 3.1</i>	Informationen zum Bereitstellen von Resiliency Platform und Nutzen der Einsatzmöglichkeiten des Produkts.
<i>Veritas Resiliency Platform Drittanbieter-Software-Lizenzvereinbarungen</i>	Informationen zur Software von Drittherstellern, die in Resiliency Platform verwendet wird.

# Behobene Probleme

Dieses Kapitel enthält die Probleme, die in Veritas Resiliency Platform 3.1 behoben wurden.

**Tabelle 1-4** In Veritas Resiliency Platform 3.1 behobene Probleme

Vorfallnummer	Zusammenfassung
–	Datenträgerauslastungsrisiko nach DR-Vorgängen nicht behoben
–	Die Konfiguration der Notfallwiederherstellung für die Resiliency Group schlägt fehl, wenn das Microsoft Hyper-V Replica konfiguriert wurde, nachdem Sie Resiliency Platform einen virtuellen Computer hinzugefügt haben
–	Die DR-Konfiguration schlägt fehl, wenn virtuelle Computer in der Resiliency Group zu verschiedenen Servern gehören
–	Einloggen bei der Resiliency Manager-Konsole schlägt manchmal fehl
–	Eine zuvor konfigurierte Netzwerkzuordnung funktioniert möglicherweise nicht nach dem erneuten Hinzufügen eines VMware vCenter-Servers
–	Im Bericht "Inventar der virtuellen Computer" wird von der Resiliency Platform nicht der zugewiesene Arbeitsspeicher, sondern der gesamte Arbeitsspeicher der virtuellen Computer ausgewiesen
3721289	Bestimmte Validierungen funktionieren nicht beim Erstellen einer Resiliency Group mit Anwendungen
3794650	Der Status "Unbekannt" wird für die Resiliency Groups für heruntergefahrte Rechenzentren angezeigt, die Teil eines VBS sind
3794105	DR-Vorgänge für VBS schlagen fehl, wenn die Resiliency Group für Anwendungen mit nicht konfigurierter DR im VBS hinzugefügt wird
3861929	Nach einer Standortwiederherstellung müssen alle Assets manuell aktualisiert werden
3862253	Die Migration reagiert nicht mehr, wenn der Vorgang von einem nicht verfügbaren Standort aus eingeleitet wird
8697	Replikationsinformationen werden für virtuelle Hyper-V-Computer in der Microsoft-Failover-Clustering-Umgebung, die nicht englische Schriftzeichen im CSV-Pfad enthalten, nicht erkannt

## Bekannte Probleme: Allgemein

Im Folgenden werden die bekanntesten allgemeinen Probleme mit Veritas Resiliency Platform aufgeführt:

Siehe ["Der Lizenzablaufstatus ist bei Resiliency Managern in verschiedenen Zeitzonen inkonsistent."](#) auf Seite 10.

Siehe ["Die statische IP-Anpassung funktioniert unter bestimmten Umständen möglicherweise nicht \(3862916, 3862237\)"](#) auf Seite 10.

Siehe ["Remote-Clustergruppen-Abhängigkeiten werden vor der Migration nicht validiert \(3863082\)"](#) auf Seite 11.

Siehe ["Der Resiliency Group-Zustand wird nicht aktualisiert, wenn der Produktionsstandort heruntergefahren ist \(3863081\)"](#) auf Seite 11.

Siehe ["Die DNS-Anpassung funktioniert nicht, wenn der vollständig qualifizierte Domänenname \(FQDN\) nicht definiert ist \(5037\)"](#) auf Seite 11.

Siehe ["Einige Versionen von VMware Tools werden nicht unterstützt \(4969\)"](#) auf Seite 11.

Siehe ["Warnmeldung wird für die Netzwerkzuordnung angezeigt \(8644\) "](#) auf Seite 12.

Siehe ["Das Ersetzen eines Live-Replication Gateway kann nicht erneut ausgeführt werden, wenn der Vorgang bei einer bestimmten Unteraufgabe fehlschlägt \(13063\)"](#) auf Seite 12.

### Der Lizenzablaufstatus ist bei Resiliency Managern in verschiedenen Zeitzonen inkonsistent.

Wenn Resiliency Manager in verschiedenen Zeitzonen konfiguriert sind, kann die Lizenz auf einem Resiliency Manager ablaufen, bevor die Lizenz auf einem anderen Resiliency Manager abläuft. Dieses Verhalten tritt auf dem zweiten Resiliency Manager fast 12 Stunden lang auf.

### Die statische IP-Anpassung funktioniert unter bestimmten Umständen möglicherweise nicht (3862916, 3862237)

Hyper-V bietet Linux Integration Services (LIS), die die statische IP-Anpassung für einen Linux-Gast ermöglichen. Der Vorgang funktioniert jedoch manchmal nicht wie erwartet aufgrund von Kompatibilitätsproblemen. In solchen Fällen wird die IP-Adresse für den Linux-Gast nicht zugewiesen.

Probleumgehung:

Melden Sie sich bei der virtuellen Computerkonsole an und weisen Sie manuell die IP-Adresse zu.

## Remote-Clustergruppen-Abhängigkeiten werden vor der Migration nicht validiert (3863082)

Mit Veritas Resiliency Platform können Sie eine globale Dienstgruppe migrieren, die als Resiliency Group zugeordnet ist und abhängige Dienstgruppen auf dem DR-Cluster hat, die nicht online sind. Als Folge davon kann der Vorgang zum Start der Resiliency Group am Wiederherstellungsstandort fehlschlagen.

## Der Resiliency Group-Zustand wird nicht aktualisiert, wenn der Produktionsstandort heruntergefahren ist (3863081)

Wenn der Produktionsstandort ausfällt, auf dem eine Resiliency Group online ist, wird der Resiliency Group-Zustand nicht geändert. Jedoch ist der Zustand der Anwendung "Online (veraltet)". Damit wird darauf hingewiesen, dass der Online-Zustand der Resiliency Group veraltet und möglicherweise nicht aktuell ist.

## Die DNS-Anpassung funktioniert nicht, wenn der vollständig qualifizierte Domänenname (FQDN) nicht definiert ist (5037)

Dieses Problem tritt auf, wenn der FQDN nicht für virtuelle Computer definiert ist, die auf der Hyper-V-Plattform (Linux und Windows) ausgeführt werden.

## Einige Versionen von VMware Tools werden nicht unterstützt (4969)

Resiliency Platform verwendet die vSphere Webdienst-API "ValidateCredentialsInGuest()", die mit einigen Versionen von VMware Tools nicht funktioniert, die in virtuellen Gastcomputern installiert sind. Dieses Problem kann zu einem Fehler bei der IP-Anpassung von virtuellen Computern unter Windows in einer vSphere-Umgebung führen.

Problemumgehung:

Installieren Sie die neueste Version von VMware Tools.

Die vSphere-Webdienst-API "ValidateCredentialsInGuest()" funktioniert mit VMware Tools Version 9.4.10.2092844.

## Warnmeldung wird für die Netzwerkzuordnung angezeigt (8644)

Manchmal erhalten Sie eine Fehlermeldung in der nachstehenden Form, wenn Sie eine Notfallwiederherstellung durchführen, auch wenn die Netzwerkzuordnung in der Umgebung durchgeführt wurde:

Einige virtuelle Computer können sich nach der Migration möglicherweise nicht mit dem Netzwerk verbinden, da die erforderliche Netzwerkzuordnung nicht definiert wurde.

Problemumgehung:

Sie müssen auf "Weiter" klicken und der Vorgang wird wie erwartet fortgeführt.

## Das Ersetzen eines Live-Replication Gateway kann nicht erneut ausgeführt werden, wenn der Vorgang bei einer bestimmten Unteraufgabe fehlschlägt (13063)

Wenn beim Ersetzen eines Live-Replication Gateway der Vorgang bei der Unteraufgabe "Konfiguration des Veritas-Replikationssatzes auf Veritas Replication Gateway aufheben" fehlschlägt, wird auch bei erneuter Ausführung der Vorgang nicht verarbeitet. Der Arbeitsablauf könnte auf der Seite "Zuletzt durchgeführte Aktivitäten" als abgeschlossen angezeigt werden, obwohl der Vorgang nicht ausgeführt wurde.

Problemumgehung:

Wenden Sie sich an den Veritas-Support.

# Bekannte Probleme: Wiederherstellung in Amazon Web Services (AWS)

Im Folgenden finden Sie die bekannten Probleme für die Wiederherstellung in AWS:

Siehe ["Einige für DHCP aktivierte Netzwerkkarten sind in der Cloud nach der Migration nicht vorhanden \(7407\)"](#) auf Seite 13.

Siehe ["Mindestens eine Netzwerkkarte eines migrierten virtuellen Computers unter Windows ist nicht sichtbar \(7718\)"](#) auf Seite 13.

Siehe ["Cloud-IP-Adressen werden den lokalen Netzwerkadaptern hinzugefügt, nachdem sie in das lokale Rechenzentrum zurück migriert wurden und ein Neustart durchgeführt wurde \(7713\)"](#) auf Seite 14.

Siehe ["Vorgänge zum Migrieren oder Übernehmen schlagen bei der Unteraufgabe "Netzwerk für AWS hinzufügen" und "Netzwerkschnittstelle erstellen" fehl \(7719\)"](#) auf Seite 14.

Siehe "[Manchmal fährt das Netzwerk mit nur einem Netzwerkkarten hoch, obwohl mehrere Netzwerkkarten vorhanden sind \(8232\)](#)" auf Seite 14.

Zusätzlich zu den oben aufgeführten bekannten Problemen treten auch die für Resiliency Platform Data Mover aufgeführten Probleme auf:

Siehe "[Bekannte Probleme: Resiliency Platform Data Mover](#)" auf Seite 18.

## Einige für DHCP aktivierte Netzwerkkarten sind in der Cloud nach der Migration nicht vorhanden (7407)

Wenn DHCP für Netzwerkkarten aktiviert ist, aber das Erstellen von Netzwerkpaaren nicht abgeschlossen ist, werden diese Netzwerkkarten während der Migration ignoriert.

Probleumgehung:

Erstellen Sie ein Netzwerkpaar mit für DHCP aktivierte Netzwerkkarten, damit die IP-Adressen in der AWS Cloud angezeigt werden. Oder Sie müssen die Netzwerkschnittstelle nach Abschluss der Migration manuell erstellen.

## Mindestens eine Netzwerkkarte eines migrierten virtuellen Computers unter Windows ist nicht sichtbar (7718)

Nach der Migration ist mindestens eine Netzwerkkarte (NIC), die mit einem virtuellen Computer unter Windows verbunden ist, im Betriebssystem nicht sichtbar. Sie sind möglicherweise nicht in der Lage, die Verbindung mit dem migrierten virtuellen Computer unter Verwendung der IP-Adresse herzustellen, die dieser unsichtbaren NIC zugewiesen ist.

Probleumgehung:

Im Gerätemanager werden alle Netzwerkkarten unter den Netzwerkanschlüssen aufgeführt. Die Netzwerkkarten, die unter den Netzwerkverbindungen nicht sichtbar sind, sind auch hier aufgeführt, aber sie zeigen eine Fehlermeldung der folgenden Art:

`Windows konnte keine Treiber für diese Schnittstelle laden.`

Klicken Sie mit der rechten Maustaste auf die Netzwerkschnittstelle, die die Fehlermeldung anzeigt, und klicken Sie auf "Gerät deinstallieren".

Suchen Sie nach der Deinstallation nach Änderungen an der Hardware im Gerätemanager. Die Netzwerkkarte wird richtig installiert und ist sichtbar.

## Cloud-IP-Adressen werden den lokalen Netzwerkadaptern hinzugefügt, nachdem sie in das lokale Rechenzentrum zurück migriert wurden und ein Neustart durchgeführt wurde (7713)

Nach der erfolgreichen Migration in das Produktionsrechenzentrum (lokal) und dem Neustart der virtuellen Windows-Computer werden die Cloud-IP-Adressen den lokalen Netzwerkkarten zugeordnet.

Dies ist auf bestimmte Probleme im Netzwerkskript zurückzuführen, wodurch Cloud-IP-Adressen den lokalen Netzwerkkarten hinzugefügt werden, nachdem ein Neustart nach einer Migration erfolgt ist.

Problemumgehung:

Sie müssen die zusätzlichen IP-Adressen manuell aus den lokalen Netzwerkkarten entfernen.

## Vorgänge zum Migrieren oder Übernehmen schlagen bei der Unteraufgabe "Netzwerk für AWS hinzufügen" und "Netzwerkschnittstelle erstellen" fehl (7719)

Aufgrund bestimmter Fehler werden die Cloud-IP-Adressen den lokalen Netzwerkadaptern hinzugefügt, nachdem Sie in das lokale Rechenzentrum migriert wurden. Wenn Sie danach den Vorgang zum Bearbeiten der Resiliency Group durchführen oder die Resiliency Group löschen und danach erneut erstellen, schlägt das Migrieren und Übernehmen mit der folgenden Fehlermeldung fehl:

```
Fehler (InvalidParameterValue) beim Aufrufen des Vorgangs  
"CreateNetworkInterface": Ungültiger Wert der Parameteradresse: []
```

Problemumgehung:

Starten Sie den virtuellen Computer und entfernen Sie die Cloud-IP-Adresse manuell.

Aktualisieren Sie den Host und vCenter Server oder Hyper-V.

Bearbeiten Sie die Resiliency Group und führen Sie das Migrieren bzw. Übernehmen danach erneut durch.

## Manchmal fährt das Netzwerk mit nur einem Netzwerkadapter hoch, obwohl mehrere Netzwerkadapter vorhanden sind (8232)

Manchmal sind die virtuellen RHEL-Computer, die mehrere Netzwerkadapter haben, nur über eine NIC-IP zugänglich, nachdem DR-Vorgänge wie Migration, Übernahme und Simulation durchgeführt wurden. Dies liegt daran, dass der DHCP-Client nicht in der Lage ist, das DHCP-Angebot vom Server zu erhalten, sodass die

Routingtabelle die Last nicht erhält. Daher sind die virtuellen Computer über andere NIC-IPs nicht zugänglich.

Probleumgehung:

Greifen Sie mithilfe der verfügbaren IP-Adresse auf den virtuellen Computer zu und starten Sie die Netzwerkdienste erneut.

## **Bekannte Probleme: Wiederherstellung in Azure**

Dieses bekannte Problem gilt für die Wiederherstellung in Azure:

Siehe ["Es werden falsche Optionen zum Auswählen der Größe des virtuellen Computers während der Bearbeitung angezeigt \(13068\)"](#) auf Seite 15.

Zusätzlich zum oben aufgeführten bekannten Problem treten auch die für Resiliency Platform Data Mover aufgeführten Probleme auf:

Siehe ["Bekannte Probleme: Resiliency Platform Data Mover"](#) auf Seite 18.

### **Es werden falsche Optionen zum Auswählen der Größe des virtuellen Computers während der Bearbeitung angezeigt (13068)**

Beim Konfigurieren einer Resiliency Group für die Wiederherstellung auf Azure wird als Größe des virtuellen Computers der unterstützte Premium-Speichertyp ausgewählt. Während der Bearbeitung der Resiliency Group werden in der Dropdown-Liste für die Auswahl der Größe des virtuellen Computers auch die Optionen für die vom Standardspeichertyp unterstützten Größen virtueller Computer angezeigt.

Wenn Sie die Größe für den unterstützten Standardspeichertyp für unterstützte virtuelle Computer auswählen, wird der Vorgang für die Resiliency Group erfolgreich ausgeführt, ohne dass Fehler auftreten, die Migration oder Übernahme schlägt jedoch fehl.

Probleumgehung:

Stellen Sie sicher, dass die vom Premium-Speichertyp unterstützte Größe des virtuellen Computers ausgewählt ist.

## **Bekannte Probleme: Wiederherstellung in vCloud**

Dieses bekannte Problem gilt für die Wiederherstellung in vCloud Director:

Siehe ["Details der Resiliency Group in der Konsole zeigen veraltete Einträge des virtuellen vCloud-Computers nach der Migration einer Resiliency Group zurück zum lokalen Standort \(8326\)"](#) auf Seite 16.

**Bekannte Probleme: Resiliency Platform Data Mover bei der Wiederherstellung im lokalen Rechenzentrum**

Zusätzlich zu den oben aufgeführten bekannten Problemen treten auch die für Resiliency Platform Data Mover aufgeführten Probleme auf:

Siehe ["Bekannte Probleme: Resiliency Platform Data Mover"](#) auf Seite 18.

## Details der Resiliency Group in der Konsole zeigen veraltete Einträge des virtuellen vCloud-Computers nach der Migration einer Resiliency Group zurück zum lokalen Standort (8326)

Nachdem eine Resiliency Group zurück zum lokalen Standort migriert wurde, kann die Detailseite der Resiliency Group in manchen Fällen in der Konsole veraltete Einträge des virtuellen vCloud-Computers enthalten. Der Vorgang ist erfolgreich und es treten sonst keine schädlichen Nebeneffekte auf.

## Bekannte Probleme: Resiliency Platform Data Mover bei der Wiederherstellung im lokalen Rechenzentrum

Im Folgenden finden Sie die bekannten Probleme bei Resiliency Platform Data Mover bei der Wiederherstellung im lokalen Rechenzentrum:

Siehe ["Der Schutz des virtuellen Computers mithilfe des Datentransfergeräts ist aufgrund einer Richtlinie eingeschränkt \(5181\)"](#) auf Seite 17.

Siehe ["Iofilter-Bundle aus ESX-Hosts wurde nicht entfernt, auch nachdem die Konfiguration der virtuellen Computer aufgehoben wurde \(5178\)"](#) auf Seite 17.

Siehe ["Die Speicherrichtlinie muss manuell entfernt werden, nachdem die Konfiguration aller virtuellen Computer aufgehoben wurde \(5180\)"](#) auf Seite 17.

Siehe ["Das Risiko "Data Mover – virtueller Computer im No-Op-Modus" kann nicht behoben werden \(5183\)"](#) auf Seite 17.

Siehe ["Risiken wurden nach dem Snapshot des virtuellen Computers, der mit Data Mover repliziert wurde, nicht erzeugt \(6886\)"](#) auf Seite 17.

Zusätzlich zu den oben aufgeführten bekannten Problemen treten auch die für Resiliency Platform Data Mover aufgeführten Probleme auf:

Siehe ["Bekannte Probleme: Resiliency Platform Data Mover"](#) auf Seite 18.

## Der Schutz des virtuellen Computers mithilfe des Datentransfergeräts ist aufgrund einer Richtlinie eingeschränkt (5181)

Der Schutz des virtuellen Computers mithilfe des Datentransfergeräts ist aufgrund der Richtlinie SPBM (Storage Policy Based Management) von VMware eingeschränkt. Sie sind möglicherweise nicht in der Lage, die virtuellen Computer zu schützen, wenn eine nicht standardmäßige Richtlinie damit verbunden ist, die keinen vtstap-Filter hat.

Probleumlösung:

Sie müssen die Richtlinie mit vtstap-Filter und einer der Regeln erneut anwenden.

## lofilter-Bundle aus ESX-Hosts wurde nicht entfernt, auch nachdem die Konfiguration der virtuellen Computer aufgehoben wurde (5178)

Wenn Sie das Resiliency Platform-Datentransfergerät verwenden, wird das lofilter-Bundle nicht aus dem Cluster entfernt, auch wenn Sie die Konfiguration für die Wiederherstellung der virtuellen Computer in der Clusterkonfiguration aufheben.

## Die Speicherrichtlinie muss manuell entfernt werden, nachdem die Konfiguration aller virtuellen Computer aufgehoben wurde (5180)

Die Speicherrichtlinie für virtuelle Computer wird nicht automatisch entfernt, wenn die Konfiguration aller geschützten virtuellen Computer im VMware vSphere-Server entfernt wurde. Sie müssen aus den Speicherrichtlinien des virtuellen Computers manuell entfernt werden.

## Das Risiko "Data Mover – virtueller Computer im No-Op-Modus" kann nicht behoben werden (5183)

Das Risiko "Data Mover – virtueller Computer im No-Op-Modus" kann nicht behoben werden.

## Risiken wurden nach dem Snapshot des virtuellen Computers, der mit Data Mover repliziert wurde, nicht erzeugt (6886)

Wenn Sie einen Snapshot des virtuellen Computers erstellen, der Teil einer Resiliency Group ist und mit dem Resiliency Platform-Datentransfergerät repliziert wird, werden die Risiken nach der Aufnahme des Snapshots nicht generiert.

Probleumlösung:

Sie müssen einen Resiliency Group-Bearbeitungsvorgang durchführen, nachdem Sie den Snapshot von einem virtuellen Computer ausgeführt haben.

## Bekannte Probleme: Resiliency Platform Data Mover

Im Folgenden finden Sie die bekannten Probleme bei Resiliency Platform Data Mover bei der Wiederherstellung im Cloud-Rechenzentrum oder im lokalen Rechenzentrum:

Siehe ["Die Replikation wird angehalten, wenn Sie den Vorgang zum Hinzufügen oder Löschen einer Festplatte durchführen \(5182\)"](#) auf Seite 18.

Siehe ["Details des Wiederherstellungsrechenzentrums werden nach dem Upgrade nicht angezeigt \(13024\)"](#) auf Seite 18.

### Die Replikation wird angehalten, wenn Sie den Vorgang zum Hinzufügen oder Löschen einer Festplatte durchführen (5182)

Wenn Sie eine Festplatte dem geschützten virtuellen Computer hinzufügen oder darauf löschen, wird die Replikation angehalten und Sie sind nicht in der Lage, einen Vorgang für die zugeordnete Resiliency Group durchzuführen.

Problemumgehung:

Bearbeiten Sie die Resiliency Group, um den betroffenen virtuellen Computer zu entfernen und wieder hinzuzufügen.

### Details des Wiederherstellungsrechenzentrums werden nach dem Upgrade nicht angezeigt (13024)

Nach dem Upgrade auf 3.1 werden beim Bearbeiten einer Resiliency Group, die bereits für die Remote-Wiederherstellung konfiguriert ist, die Details des Wiederherstellungsrechenzentrums nicht im Fenster "Prüfungsumgebung" angezeigt. Dies geschieht, wenn der Name der Festplatte länger als 128 Zeichen ist.

Problemumgehung:

Wenden Sie sich an Veritas-Support, um eine vollständige Erkennung auf beiden Replication Gateways zu starten.

Alternativ dazu können Sie die Resiliency Group löschen und sie für die Wiederherstellung neu konfigurieren. Beachten Sie, dass beim Löschen und erneuten Konfigurieren eine vollständige Synchronisierung der Daten aus dem Produktions- in das Wiederherstellungsrechenzentrum erfolgt.

# Bekannte Probleme: Wiederherstellung mithilfe von Replikationsanwendungen anderer Hersteller

Im Folgenden finden Sie die bekannten Probleme für die Wiederherstellung mit Replikationsanwendungen anderer Hersteller:

Siehe ["Für Resiliency Groups, die virtuelle VMware-Computer enthalten und bei denen der NFS-Datenspeicher auf einem NetApp-Datenträger mit der Subzeichenfolge "vol" geladen ist, dann die Migration oder Übernahme fehlschlagen."](#) auf Seite 19.

Siehe ["In der Hyper-V-Gastumgebung wird angezeigt, dass der beschreibbare Datenträger schreibgeschützt ist. \(3785911\)"](#) auf Seite 19.

Siehe ["Lange SRDF-Gerätegruppennamen werden nicht erkannt \(3786826\)"](#) auf Seite 20.

Siehe ["Resiliency Groups für Hitachi-Enclosures werden auf dem Dashboard unter Top RG im Diagramm der Zeitverzögerung der Replikation nicht angezeigt \(3861173\)"](#) auf Seite 20.

Siehe ["Die Snapshot-Festplatte ist nach dem Simulationsvorgang in Hyper-V mit SRDF-Replikation schreibgeschützt \(3862088\)"](#) auf Seite 20.

**Für Resiliency Groups, die virtuelle VMware-Computer enthalten und bei denen der NFS-Datenspeicher auf einem NetApp-Datenträger mit der Subzeichenfolge "vol" geladen ist, dann die Migration oder Übernahme fehlschlagen.**

Wenn ein VMware-Datenspeicher auf einem mit NetApp replizierten Datenträger geladen ist und der Datenträgername die Subzeichenfolge "vol" enthält, schlägt die Migration der entsprechenden Resiliency Groups über mehrere Rechenzentren möglicherweise fehl.

Problemumgebung:

Benennen Sie den NetApp-Datenträger um, um die Subzeichenfolge "vol" aus dem Namen zu entfernen.

**In der Hyper-V-Gastumgebung wird angezeigt, dass der beschreibbare Datenträger schreibgeschützt ist. (3785911)**

Wenn in der Hyper-V Gastumgebung ein Datenträger beschreibbar ist, der Festplattenmanager oder ein anderes Windows-Dienstprogramm aber zeigt, dass

die Festplatte sich im Schreibschutzstatus befindet, müssen Sie den Hyper-V-Gastcomputer erneut starten.

Dies kann beim Migrieren und Übernehmen im Wiederherstellungsrechenzentrum vorkommen.

## Lange SRDF-Gerätegruppennamen werden nicht erkannt (3786826)

Symmetrix Remote Data Facility (SRDF)-Gerätegruppen mit Namen, die länger als 18 Zeichen sind, können in der Resilience Manager-Webkonsole nicht erkannt werden.

## Resiliency Groups für Hitachi-Enclosures werden auf dem Dashboard unter Top RG im Diagramm der Zeitverzögerung der Replikation nicht angezeigt (3861173)

Bei Hitachi-Enclosures werden die Resiliency Groups auf dem Dashboard unter Top RG für die Zeitverzögerung der Replikation nicht angezeigt, da die Zeitverzögerung der Replikation für Hitachi-Enclosure in Prozentsätzen ausgewiesen wird und das Diagramm, das auf dem Dashboard angezeigt wird, das Format *HH:MM:SS* hat.

[Die Detailseite der Resiliency Group zeigt hingegen die Zeitverzögerung der Replikation für eine bestimmte Resiliency Group an.]

## Die Snapshot-Festplatte ist nach dem Simulationsvorgang in Hyper-V mit SRDF-Replikation schreibgeschützt (3862088)

Der Befehl `Diskpart` wird verwendet, um das Schreibschutz-Flag in der Hyper-V-SRDF-Replikationsumgebung zu löschen. Der Befehl könnte jedoch zeitweilig fehlschlagen. Daher wird die Snapshot-Festplatte während des Simulationsvorgangs möglicherweise nur im schreibgeschützten Modus bereitgestellt.

Problemumgehung:

- Stellen Sie die Festplatte offline und dann wieder online.
- Schalten Sie den virtuellen Computer ein.

## Bekannte Probleme: NetBackup-Integration

Im Folgenden sind die bekannten Probleme bei der NetBackup-Integration aufgeführt:

Siehe "[MAC Adresse beginnend mit 00: 0c:29 wird nicht für virtuelle VMware-Computer unterstützt \(7103\)](#)" auf Seite 21.

Siehe "[Ein virtueller Computer, der von mehreren NBU-Masterservern gesichert wird, wird nur einem Masterserver in der Konsole zugewiesen \(7608\)](#)" auf Seite 21.

Siehe "[Ein vorübergehender virtueller Computer verbleibt in einem Szenario im ESX-Server \(7413\)](#)" auf Seite 21.

Siehe "[Die Wiederherstellung schlägt manchmal fehl, wenn der Remote-Master-Server entfernt und erneut hinzugefügt wird \(8600\)](#)" auf Seite 22.

Siehe "[Websocket-Verbindung wird nach dem Upgrade getrennt \(12814\)](#)" auf Seite 22.

## MAC Adresse beginnend mit 00: 0c:29 wird nicht für virtuelle VMware-Computer unterstützt (7103)

Wenn Sie ein Image auf einem virtuellen VMware-Computer mit einer MAC-Adresse beginnend mit 00:0c:29 wiederherstellen möchten, wird der Computer nicht hochgefahren.

Probleumgehung:

Sie müssen die Einstellungen des virtuellen Computers bearbeiten und den MAC-Adressentyp des Netzwerkadapters auf "Automatisch" ändern. Diese Option ändert die MAC-Adresse des Computers. Sie können dann den virtuellen Computer erneut einschalten.

## Ein virtueller Computer, der von mehreren NBU-Masterservern gesichert wird, wird nur einem Masterserver in der Konsole zugewiesen (7608)

Wenn ein virtueller Computer von mehreren NBU-Masterservern gesichert wird, wird er nur einem Masterserver in der Resiliency Manager-Konsole zugewiesen. Sie können eine Resiliency Group erstellen oder den virtuellen Computer nur mit dem zugeordneten Masterserver wiederherstellen.

## Ein vorübergehender virtueller Computer verbleibt in einem Szenario im ESX-Server (7413)

Wenn Sie eine Resiliency Group von Standort A nach Standort B wiederherstellen und dann zurück an Standort A wiederherstellen, werden zwei virtuelle Computer auf dem ESX-Server des Standorts A sichtbar.

Probleumgehung:

**Bekannte Probleme: Mehrere Resiliency Manager in einem Rechenzentrum**

Starten Sie die Dienste auf dem vCenter Server erneut.

## Die Wiederherstellung schlägt manchmal fehl, wenn der Remote-Master-Server entfernt und erneut hinzugefügt wird (8600)

Die Wiederherstellung schlägt manchmal fehl, wenn einer der zugeordneten NetBackup-Master-Server aus der Resiliency Platform-Konsole entfernt und erneut hinzugefügt wurde.

Probleumlösung:

Sie müssen beide Masterserver entfernen und danach wieder hinzufügen.

## Websocket-Verbindung wird nach dem Upgrade getrennt (12814)

Nach dem Upgrade auf Version 3.1 wird die Websocket-Verbindung mit dem NetBackup-Master-Server getrennt.

Probleumlösung:

Um die Verbindung wiederherzustellen, müssen Sie die Bearbeitung ausführen oder den Master-Server entfernen und erneut hinzufügen.

# Bekannte Probleme: Mehrere Resiliency Manager in einem Rechenzentrum

Im Folgenden finden Sie die bekannten Probleme, die für mehrere Resiliency Manager in einem Rechenzentrum gelten:

Siehe ["Ein neu hinzugefügter Resiliency Manager kann einen vorhandenen Resiliency Manager, der offline ist, nicht entfernen \(10821\)"](#) auf Seite 22.

Siehe ["In einem Cloud-Rechenzentrum können DR-Vorgänge nur von dem mit dem Cloud-IMS verknüpften Resiliency Manager aus ausgeführt werden \(10895\)"](#) auf Seite 23.

## Ein neu hinzugefügter Resiliency Manager kann einen vorhandenen Resiliency Manager, der offline ist, nicht entfernen (10821)

Wenn ein neuer Resiliency Manager einem Rechenzentrum hinzugefügt wird, während ein Resiliency Manager im anderen Rechenzentrum offline ist, dann kann der neu hinzugefügte Resiliency Manager den Resiliency Manager, der offline ist, nicht entfernen.

Probleumlösung:

Loggen Sie sich bei klish ein und geben Sie folgenden Befehl ein, um den Datenbankdienst neu zu starten:

```
services rm restart db
```

Nun können Sie den Resiliency Manager, der offline ist, entfernen.

In einem Cloud-Rechenzentrum können DR-Vorgänge nur von dem mit dem Cloud-IMS verknüpften Resiliency Manager aus ausgeführt werden (10895)

In einer Cloud-Bereitstellung mit mehreren Resiliency Managern können DR-Vorgänge nur von dem mit dem Cloud-IMS verknüpften Resiliency Manager aus ausgeführt werden.

## Beschränkungen

Veritas Resiliency Platform unterstützt folgende Funktionen nicht:

Siehe ["Die Simulation wird nicht unterstützt, wenn der Datenträger unter Verwendung asynchroner Replikation in IBM XIV-Enclosures konfiguriert ist"](#) auf Seite 23.

Siehe ["Einschränkungen für Windows-Hosts vor Ort für die Replikation mit dem Resiliency Platform-Datentransfergerät"](#) auf Seite 24.

Siehe ["Hyper-V-Hosts mit Snapshots werden für die Wiederherstellung in AWS nicht unterstützt"](#) auf Seite 24.

Siehe ["Der Computername virtueller Computer in vCloud ist unterschiedlich, wenn der Name die Anzahl zulässiger Zeichen überschreitet"](#) auf Seite 24.

Siehe ["Die Lokalisierung für das Hinzufügen des Anwendungstyps wird nicht unterstützt"](#) auf Seite 24.

Siehe ["Einschränkungen im Zusammenhang mit lokalisierten Versionen"](#) auf Seite 25.

Siehe ["Der Name des virtuellen Computers darf eine Länge von 35 Zeichen nicht überschreiten"](#) auf Seite 25.

Die Simulation wird nicht unterstützt, wenn der Datenträger unter Verwendung asynchroner Replikation in IBM XIV-Enclosures konfiguriert ist

Wenn die Konsistenzgruppe oder der Datenträger mit einer asynchronen Replikation in einer IBM XIV-Speichergruppe konfiguriert ist, wird der Snapshot-Vorgang durch das XIV-Enclosure nicht unterstützt. Wenn die Resiliency Group mit virtuellen

Computern konfiguriert ist, die für die Replikation mit einer asynchronen Konsistenzgruppe oder auf der Basis eines Datenträgers konfiguriert sind, schlägt die Simulation beim Schritt "Snapshot erstellen" fehl.

## Einschränkungen für Windows-Hosts vor Ort für die Replikation mit dem Resiliency Platform-Datentransfergerät

Folgende Beschränkungen gelten nur für lokale Hosts auf der Windows-Plattform und bei einer Replikation mit dem Resiliency Platform-Datentransfergerät:

- Um den Vorgang zur Initialisierung der Festplatte durchzuführen, muss sich die Konsistenzgruppe im Zustand "Angehalten" oder "Beendet" befinden.
- Wenn die Systemwiederherstellung manuell erfolgt, müssen Sie zuerst die Replikation beenden und dann mithilfe der CLI erneut starten.
  - "C:\Programme\Veritas\VRTS\itrptap\cli\vxtpaction.exe" stop -cg <CGID>
  - "C:\Programme\Veritas\VRTS\itrptap\cli\vxtpaction.exe" start -cg <CGID>
 Dabei gilt: *CGID* ist die Konsistenzgruppen-ID.

## Hyper-V-Hosts mit Snapshots werden für die Wiederherstellung in AWS nicht unterstützt

Ein Hyper-V-Host mit Snapshots wird für die Wiederherstellung in AWS nicht unterstützt.

## Der Computername virtueller Computer in vCloud ist unterschiedlich, wenn der Name die Anzahl zulässiger Zeichen überschreitet

Die maximale Anzahl zulässiger Zeichen für einen Computernamen in vCloud ist 15 für Windows und 63 für Linux. Wenn der Hostname im vollständig qualifizierten Domännennamen (FQDN) eines virtuellen Computers die Beschränkung überschreitet, erhält der Computername des virtuellen Computers in vCloud nach Migration oder Übernahme einen Standardnamen.

Der Name kann gegebenenfalls bearbeitet werden.

## Die Lokalisierung für das Hinzufügen des Anwendungstyps wird nicht unterstützt

Die Lokalisierung für das Hinzufügen eines Anwendungstyps wird aufgrund von Beschränkungen der zugrunde liegenden Systeme nicht unterstützt. Der Assistent "Anwendungstyp hinzufügen" auf der Registerkarte "Einstellungen" >

Anwendungssupport > Hochgeladen" akzeptiert nur Eingaben mit englischen Schriftzeichen.

## Einschränkungen im Zusammenhang mit lokalisierten Versionen

Nachfolgend sind einige Einschränkungen im Zusammenhang mit den lokalisierten Versionen von Veritas Resiliency Platform 3.1 aufgelistet:

- Resiliency Plan-Aufgabennamen werden lokalisiert, aber nach einmaligem Speichern ändert sich das Verhalten nicht im Gebietsschema des Browsers
- Der Textinhalt von Benachrichtigungen ist nicht lokalisiert
- Der Textinhalt von E-Mails ist nicht lokalisiert
- Die Ergebnisse der Aufgabe "Aktivitäten" sind nicht lokalisiert
- Aufgaben der Stufe MH sind nicht lokalisiert
- Für die deutsche Version von Active Directory ist der Gruppenname des Benutzers eine Pflichteingabe
- Wenn die IP-Adressanpassung durchgeführt wurde, wird auf der Seite "Konfiguration der Resiliency Group" die Tabelle "Details der IP-Adressanpassung" angezeigt. Diese Tabelle wird nicht in der japanischen und deutschen Version angezeigt.
- Einige Felder im Bereich "Bericht planen" und "Gespeicherte Pläne" werden in der japanischen Version nicht angezeigt.

## Der Name des virtuellen Computers darf eine Länge von 35 Zeichen nicht überschreiten

Wenn die Wiederherstellung auf Azure ausgeführt wird, darf der Name des virtuellen Computers eine Länge von 35 Zeichen nicht überschreiten.