Versionshinweise zu Veritas™ Resiliency Platform 3.0

VERITAS™

Veritas Resiliency Platform: Release Notes

Aktualisiert am: 2017-08-24

Dokumentversion: Document version: 3.0 Rev 0

Rechtlicher Hinweis

Offenlegung der unter Lizenz bereitgestellten Software und Dokumentation durch die Regierung der USA erfolgt nur in Übereinstimmung mit dieser Vereinbarung.

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Technischer Support

Der technische Support unterhält weltweit Supportcenter. Alle Supportleistungen werden in Übereinstimmung mit Ihrem Supportvertrag und der jeweils geltenden Richtlinien für technischen Support für Unternehmen erbracht. Informationen zu unseren Supportangeboten und zum Kontakt mit dem technischen Support finden Sie auf unserer Website:

https://www.veritas.com/support

Sie können Ihre Veritas-Kontoinformationen unter folgender URL verwalten:

https://my.veritas.com

Wenn Sie bezüglich eines vorhandenen Supportvertrags Fragen haben, wenden Sie sich per E-Mail an das Team für Ihre Region:

Weltweit (ausgenommen Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Dokumentation

Stellen Sie sicher, dass Sie über die aktuelle Version der Dokumentation verfügen. Jedes Dokument zeigt das Datum der letzten Aktualisierung auf Seite 2. Die Dokumentversion wird auf Seite 2 des jeweiligen Handbuchs angezeigt. Die neueste Dokumentation ist auf der Veritas-Website verfügbar:

https://sort.veritas.com/documents

Dokumentations-Feedback

Ihr Feedback ist uns wichtig. Schlagen Sie Verbesserungen vor oder melden Sie Fehler oder Auslassungen in der Dokumentation. Geben Sie den Titel des Dokuments, die Version des Dokuments, den Titel der Kapitel und den Titel des Abschnitts des Textes bekannt, für den Sie ein Feedback abgeben. Senden Sie das Feedback an:

doc.feedback@veritas.com

Sie können auch Informationen zur Dokumentation einsehen oder eine Frage auf der Veritas Community-Website stellen:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

VERITAS Services and Operations Readiness Tools (SORT) ist eine Website, die Informationen und Tools zum Automatisieren und Vereinfachen bestimmter zeitaufwändiger Verwaltungsaufgaben bietet. Abhängig vom Produkt hilft SORT beim Vorbereiten von Installationen und Upgrades, Identifizieren von Risiken in Ihren Rechenzentren und Optimieren der betrieblichen Effizienz. Informationen darüber, welche Dienste und Tools SORT für Ihr Produkt bereithält, finden Sie im Datenblatt:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Inhalt

Kapitel 1

Überblick

In diesem Kapitel werden folgende Themen behandelt:

Informationen zu Veritas Resiliency Platform

Veritas Resiliency Platform bietet eine einheitliche Lösung, mit der Sie proaktiv die durchgängige Verfügbarkeit der Geschäftsprozesse über Private, Public und Hybrid Clouds aufrechterhalten können. Die Resiliency Platform ermöglicht Ihnen die vollständige Automatisierung aller Resiliency-Vorgänge im Zusammenhang mit virtuellen Computern, Anwendungen und mehrschichtigen Business Services in Ihrem Rechenzentrum. Sie sichert die bestehenden Investitionen in Technologie, indem sie sich in Ihre bestehenden Umgebungen und Infrastruktur integriert.

Für die Datenreplikation können Sie die Resiliency Platform oder eine Drittanbieterlösung verwenden, die von der Veritas Resiliency Platform unterstützt wird. Eine Liste der unterstützten Hersteller und Produkte finden Sie im *Veritas Resiliency Platform Hardware und Software Compatibility Guide*.

Das Resiliency Platform-Datentransfergerät ist eine getrennt lizenzierte Funktion der Veritas Resiliency Platform. Es bietet eine Datenreplikation zwischen geografisch getrennten Rechenzentren und stellt damit eine wirksame Lösung für die Notfallwiederherstellung bereit. Das Resiliency Platform-Datentransfergerät kann für die folgenden Zwecke verwendet werden:

- Für die Wiederherstellung von virtuellen VMware-Computern im Rechenzentrum vor Ort
- Für die Wiederherstellung von virtuellen VMware- und Hyper-V-Computern im Cloud-Rechenzentrum

Die Resiliency Platform verfügt über die folgenden Kernfunktionen:

Sicherheit und Compliance	Veritas Resiliency Platform bietet verbesserte Datenverschlüsselung für Daten während der Verarbeitung.
Vorhersagbarkeit	Kunden können garantiert geschäftskritische Recovery Time Objectives (RTO, Ziele für die Wiederherstellungszeit) und Recovery Point Objective (RPO, Ziele für den Wiederherstellungspunkt) erfüllen.
Compliance	Kunden können die Einhaltung von internen und externen Vorgaben für die Gewährleistung der geschäftlichen Verfügbarkeit durch Überprüfungsberichte und Tests der Notfallwiederherstellung in Echtzeit ohne Betriebsunterbrechung nachweisen.
Automatisierung	Kunden können eine vollständige Automatisierung aller Resiliency-Vorgänge, einschließlich Durchführungsregeln für die Wiederherstellung, und eine Orchestrierung des Startens und Beendens der Wiederherstellung für mehrschichtige Anwendungen nutzen. Damit wird das Risiko von Ausfallzeiten durch Benutzerfehler reduziert.
Flexibilität	Kunden können Ihre vorhandenen Infrastrukturen weiter nutzen, Innovationen nach eigenen Anforderungen einführen und dabei die Flexibilität der Resiliency Platform einsetzen, um Workloads zwischen verschiedenen Standorten oder sogar in die Cloud zu migrieren.

Siehe "Informationen zu Resiliency Platform-Funktionen und -Komponenten" auf Seite 11.

Informationen zu Resiliency Platform-Funktionen und -Komponenten

Im Folgenden finden Sie eine kurze Einführung in die wichtigsten Komponenten der Veritas Resiliency Platform und die zugehörigen Beziehungen. Administratoren, die für die Bereitstellung und Konfiguration des Produkts verantwortlich sind, müssen genaue Kenntnisse darüber haben.

Resiliency Manager	Die Komponente, die Resiliency-Fähigkeiten in einer Resiliency Domain bereitstellt. Sie besteht aus lose verknüpften Diensten, einem verteilten Daten-Repository und einer Managementkonsole. Der Resiliency Manager wird als virtuelle Appliance bereitgestellt.
Infrastructure Management Server (IMS)	Die Komponente, die die Asset-Infrastruktur in einem Rechenzentrum erkennt, überwacht und verwaltet. Der IMS überträgt Informationen über die Asset-Infrastruktur an den Resiliency Manager. Der IMS wird als virtuelle Appliance bereitgestellt. Um die Skalierung zu ermöglichen, können mehrere IMS im gleichen Rechenzentrum bereitgestellt werden.
Veritas InfoScale Operations Manager – Managementserver	Dies ist die Komponente, die die Erkennung von InfoScale-Anwendungen ermöglicht, die im Veritas InfoScale Operations Manager, auch als „Veritas InfoScale Operations Manager-Server“ bezeichnet, bereits konfiguriert sind. Sie können die InfoScale-Anwendungen, die in Veritas InfoScale Operations Manager bereits konfiguriert sind, unter Linux, Solaris, AIX und Windows verwalten. Sie müssen diese Komponente nur hinzufügen, wenn Sie die InfoScale-Anwendungen verwalten und wiederherstellen möchten, die bereits in Veritas InfoScale Operations Manager konfiguriert sind.
NetBackup Server	Die Komponente, die eine Wiederherstellung von virtuellen Computern auf einem lokalen oder Remote-Rechenzentrum mit von NetBackup generierten Backup-Images ermöglicht. Sie müssen diese Komponente nur hinzufügen, wenn Sie die virtuellen Computer unter Verwendung von durch NetBackup generierten Backup-Images wiederherstellen möchten.
Replication Gateway	Dies ist die Komponente des Veritas Resiliency Platform-Datentransfergeräts, die als virtuelle Appliance in beiden Rechenzentren bereitgestellt und zur Durchführung einer Replikation zwischen den Rechenzentren verwendet wird. Wenn Sie eine Replikationstechnologie eines Drittanbieters verwenden möchten, ist eine Bereitstellung des Replication Gateways nicht erforderlich.

Resiliency Domain	Der logische Umfang einer Resiliency Platform-Bereitstellung. Eine Erweiterung ist über mehrere Rechenzentren möglich.
Rechenzentrum	Für den Anwendungsfall einer Notfallwiederherstellung muss die Resiliency Domain mindestens zwei Rechenzentren an verschiedenen Standorten, ein Produktionsrechenzentrum und ein Wiederherstellungsrechenzentrum, enthalten. Jedes Rechenzentrum verfügt über einen Resiliency Manager und einen oder mehrere IMS. Wenn Sie das Resiliency Platform-Datentransfergerät für die Replikation verwenden, muss jedes Rechenzentrum auch mindestens ein Replication Gateway haben.
Asset-Infrastruktur	Die Rechenzentrum-Assets, die Sie Resiliency Platform zur Erkennung und Überwachung durch den IMS hinzufügen. Die Asset-Infrastruktur kann Hosts (Windows- oder Linux-Server), Virtualisierungsserver für Hyper-V und VMware sowie Gehäuse (Speichergruppen) umfassen. Sobald die Asset-Infrastruktur vom IMS erkannt wird, werden die erkannten virtuellen Computer oder Anwendungen in der Konsole als Assets aufgeführt, die verwaltet oder geschützt werden sollen.
Resiliency Group	Die Einheit für die Verwaltung und Steuerung in der Resiliency Platform. Sie organisieren Assets, die miteinander in Beziehung stehen, in einer Resiliency Group und verwalten bzw. überwachen sie als einzelne Entität.
Service Objective	Eine Vorlage zur Definition des Typs von Vorgängen und Technologien, die für eine Gruppe von Assets unterstützt werden. Sie können ein Service Objective auf jede Resiliency Group anwenden. Eine Vorlage, die die Merkmale eines Dienstes identifiziert. Dabei kann es sich um Merkmale in Verbindung mit der Verfügbarkeit handeln, beispielsweise lokale Redundanz und eine Anzahl von Knoten in einem Cluster, oder um Merkmale der Notfallwiederherstellung, beispielsweise eine Remote-Wiederherstellung, Recovery Point Objective (RPO), SLA, Unterstützung von Simulationen usw. Das Service Objective wird angewendet, wenn eine Gruppe von Assets einer Resiliency Group hinzugefügt wird. Die Resiliency Platform überwacht die Resiliency Groups basierend auf der Service Objective-Definition und meldet gegebenenfalls die Risiken.

Virtual Business Service (VBS)	Ein mehrschichtiger Business Service, bei dem jede VBS-Ebene eine oder mehrere Resiliency Groups hostet. Mit einem VBS können Sie mehrere Dienste als einzelne Einheit für die Darstellung, die Automatisierung und das gesteuerte Starten und Beenden in der gewünschten Reihenfolge gruppieren. VBS verwendet das Verfahren der vertikalen Gruppierung, um mehrere Dienste zu gruppieren. Sie können Vorgänge zur Notfallwiederherstellung für den gesamten VBS durchführen.

Neue Funktionen und Änderungen in Veritas Resiliency Platform 3.0

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

Automatisierte Unterstützung von Disaster Recovery und Migration für Microsoft Azure

Veritas Resiliency Platform 3.0 enthält erstmalig Unterstützung für die Wiederherstellung der Assets des Rechenzentrums in Microsoft Azure. Sie können Ihre virtuellen VMware- und Hyper-V-Computer für die Wiederherstellung in vCloud mithilfe des Resiliency Platform-Datentransfergeräts konfigurieren und schützen.

Sie können mit Resiliency Platform Workloads auf einer Ebene oder auf mehreren Ebenen zwischen dem lokalen Rechenzentrum und Azure verschieben. Resiliency Platform bietet gesteuerte Optionen für die Wiederherstellung von Workloads im lokalen Rechenzentrum in Azure.

Verbesserte Unterstützung für vCloud Director

Resiliency Platform 3.0 beinhaltet erstmals Unterstützung für die Wiederherstellung von virtuellen VMware- und Hyper-V-Computern in vCloud Director ohne Hinzufügen der vCenter-Server oder Hyper-V-Server. Diese Funktion ermöglicht das Ausführen der Disaster Recovery von virtuellen Computern, ohne dazu auf VMware- oder Hyper-V-Server zuzugreifen.

Unterstützung der deutschen Sprache

Zusätzlich zur in Resiliency Platform 2.2 eingeführten Unterstützung enthält Resiliency Platform 3.0 weitere Komponenten, die auch auf Deutsch verfügbar sind. Ab Version 3.0 wird die lokalisierte Version der Resiliency Platform-Konsole

angezeigt, wenn Sie sich mit einem Browser mit deutschen Standortinformationen einloggen. Das Produkt kann innerhalb einer deutschsprachigen Umgebung verwendet werden.

Weitere Informationen zur in Resiliency Platform 2.2 eingeführten Internationalisierungsunterstützung finden Sie in den *Versionshinweisen zu Veritas Resiliency Platform 2.2*.

Unterstützung für mehrere Resiliency Manager in einem Rechenzentrum

Resiliency Platform 3.0 enthält erstmals Unterstützung für mehrere Resiliency Manager in einem Rechenzentrum. Mehrere Resiliency Manager in einem Rechenzentrum unterstützen die Aufrechterhaltung der Ausfallsicherheit und Fehlertoleranz im Rechenzentrum.

Was wird nicht unterstützt?

Veritas Resiliency Platform unterstützt folgende Funktionen nicht:

- Für EFI ("Extensible Firmware Interface") aktivierte virtuelle Hyper-V-Computer der 2. Generation werden nicht unterstützt, wenn das Replikationsverfahren das Resiliency Platform-Datentransfergerät ist.
- Fehlertolerante virtuelle VMware-Computer.
- Das Ausführen eines benutzerdefinierten Skripts auf einem Host, der nicht aktiv an die Resiliency Platform-Umgebung über den Infrastructure Management Server (IMS) oder den InfoScale Operations Manager-Verwaltungsserver berichtet.
- Datenbank-Benutzerauthentifizierung für Oracle-Anwendungen.
- Simulations- und Simulationsbereinigungsvorgänge für Anwendungen auf dem Microsoft-Failover-Cluster.
- Simulations- und Simulationsbereinigungsvorgänge für Anwendungen in virtuellen Computern, die Daten auf RAW-Disks haben, die virtuellen Computern zugeordnet sind, und Daten, die über 3PAR RemoteCopy oder NetApp SnapMirror über Fibre Channel repliziert werden.
- Simulations- und Simulationsbereinigungsvorgänge, wenn sich das Wiederherstellungsrechenzentrum in vCloud befindet.
- Übernahmevorgang aus dem AWS-Cloud-Rechenzentrum in ein lokales Rechenzentrum.

- RAW Device Mapping (RDM) wird nicht für die Disaster Recovery für virtuelle Computer mithilfe des Resiliency Platform-Datentransfergeräts unterstützt.
- Das Ersetzen des Replication Gateway im Rechenzentrum vor Ort wird für den Anwendungsfall "Wiederherstellen von virtuellen Computern in vCloud Director ohne Hinzufügen der vCenter-Server oder Hyper-V-Server" nicht unterstützt.
- Das Starten und Beenden von Resiliency Groups wird für den Anwendungsfall "Wiederherstellen von virtuellen Computern in vCloud Director ohne Hinzufügen der vCenter-Server oder Hyper-V-Server" nicht unterstützt.

Die auf Speichergruppen basierte Replikation unterstützt Folgendes nicht:

- Die Kombination von repliziertem und nicht repliziertem Speicher für virtuelle Computer wird nicht unterstützt.
- Kombination von Speicher aus mehreren Speichergruppentypen wird nicht unterstützt.

Verwenden der Produktdokumentation

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

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

URL	Beschreibung
https://sort.veritas.com/documents	Die neueste Version der Produktdokumentation: Produkthandbücher im PDF-Format. Online-Hilfe-Portal. Der Inhalt der Hilfe ist auch in der Produktkonsole verfügbar.
https://www.veritas.com/community/business-continuity/videos	Die Liste der Videos zu Resiliency Platform.
https://www.veritas.com/support/en_US/article.000127401	Die aktuellen Neuerungen in dieser Version.

Tabelle 1-2 Namen der Veritas Resiliency Platform-Handbücher

Titel	Beschreibung
Liste der mit Veritas Resiliency Platform kompatiblen Hardware und Software (HSCL)	Liste der kompatiblen Hardware und Software
Versionshinweise zu Veritas Resiliency Platform	Informationen zur Version wie Hauptfunktionen, bekannte Probleme und Einschränkungen.

Titel	Beschreibung
Überblick und Planungshandbuch zu Veritas Resiliency Platform 3.0	Informationen zum Produkt sowie dessen Funktionen und Einsatzmöglichkeiten.
Benutzerhandbuch zu Veritas Resiliency Platform 3.0	Informationen zum Bereitstellen von Resiliency Platform und Nutzen der Einsatzmöglichkeiten des Produkts.
Veritas Resiliency Platform Drittanbieter-Software-Lizenzvereinbarungen	Informationen zur Software von Drittherstellern, die in Resiliency Platform verwendet wird.

Kapitel 2

Systemanforderungen

In diesem Kapitel werden folgende Themen behandelt:

Unterstützte Hypervisoren für die Bereitstellung der virtuellen Resiliency Platform-Appliance

In diesem Abschnitt werden die Hypervisorversionen aufgeführt, die für die virtuelle Resiliency Platform-Appliance unterstützt werden.

Microsoft Hyper-V:

- Windows Server 2012 mit Hyper-V
- Windows Server 2012 R2 mit Hyper-V

VMware:

- ESXi 5.1, 5.5, 6.0, 6.0U1, 6.0U2, 6.5
- vCenter Server 5.1, 5.5, 6.0, 6.0U1, 6.0U2, 6.5

Hinweis: Die Listen der unterstützten Plattformen für die Bereitstellung der virtuellen Appliance und für die Notfallwiederherstellung virtueller Computer sind unterschiedlich. Informationen zur Plattformunterstützung für die Notfallwiederherstellung virtueller Computer finden Sie in der *Kompatibilitätsliste für Hardware und Software (HSCL) für die Veritas Resiliency Platform*.

Anforderungen an Systemressourcen für die Resiliency Platform

Die Menge an virtuellen CPUs, Arbeitsspeicher und Speicherplatz, die Veritas Resiliency Platform benötigt, wird in diesem Abschnitt aufgeführt.

Die Mindestkonfiguration, die für eine virtuelle Appliance für Resiliency Manager, Infrastructure Management Server (IMS), Replication Gateway und YUM-Repository-Server empfohlen wird:

Tabelle 2-1 Mindestkonfiguration

Komponente	Mindestkonfiguration
Resiliency Manager	60 GB Speicherplatz auf dem Datenträger 32 GB RAM Virtuelle CPU 8
Infrastructure Management Server (IMS)	60 GB Speicherplatz auf dem Datenträger 16 GB RAM Virtuelle CPU 8
Replication Gateway	40 GB Speicherplatz auf dem Datenträger 16 GB RAM Virtuelle CPU 8 Zusätzlicher externer Datenträger von 50 GB
YUM-Repository-Server	60 GB Speicherplatz auf dem Datenträger 4 GB RAM Virtuelle CPU 2

Komponente	Mindestkonfiguration
Zu Veritas Resiliency Platform hinzuzufügende Hosts: ■ Host mit Windows-Installation ■ Anwendungshost ■ Host des Resiliency Platform-Datentransfergeräts ■ Speichererkennungshost ■ Hyper-V-Host	15 GB Speicherplatz auf dem Datenträger 4 GB RAM Dual-Prozessor-CPU Wenn Sie einen einzelnen Host für mehrere Zwecke verwenden, fügen Sie den erforderlichen Speicherplatz und RAM für jeden Zweck hinzu. Beispiel: Wenn Sie einen einzelnen Host als Host mit Windows-Installation und als Anwendungshost verwenden, dann benötigen Sie mindestens 30 GB Speicherplatz und 8 GB RAM. Beachten Sie, dass Sie keinen einzelnen Host gleichzeitig als Host mit Windows-Installation und als Host des Resiliency Platform-Datentransfergeräts verwenden können.

Hinweis: Sie müssen die Ressourcen für den Resiliency Manager und den IMS reservieren, um sicherzustellen, dass diese Ressourcen nicht ausgelagert werden, wenn Hypervisoren überlastet werden.

Wenn die virtuelle Appliance die Mindestkonfiguration nicht einhält, erhalten Sie eine Warnung während des Bootstraps der virtuellen Appliance und Sie müssen bestätigen, dass Sie mit der aktuellen Konfiguration fortfahren möchten.

Wenn Sie planen, die virtuelle YUM-Appliance nicht zu verwenden, benötigen Sie einen Linux-Server mit mindestens 50 GB Speicherplatz, der als Repository-Server konfiguriert wird. Die Bereitstellung für den Repository-Server ist optional. In Zukunft müssen die Veritas Resiliency Platform-Patches oder -Updates installiert werden.

Wenn Sie einen dynamischen Arbeitsspeicher auf Hyper-V aktivieren möchten, müssen die folgenden Voraussetzungen erfüllt sein:

- Der Arbeitsspeicher für den Start und die Mindestkonfiguration muss mindestens so groß sein wie der Arbeitsspeicher, der vom Hersteller empfohlen wird.
- Wenn Sie dynamischen Speicher auf einem Windows Server 2012-Betriebssystem verwenden, geben Sie die Parameter für den Start-Arbeitsspeicher, den Mindest- und Maximalarbeitsspeicher in Vielfachen von 128 Megabyte (MB) ein. Wenn dies nicht erfolgt, führt dies möglicherweise zu Fehlern des dynamischen Arbeitsspeichers und es erfolgt keine Zunahme des Arbeitsspeichers in einem Gastbetriebssystem.
  Auch wenn Sie einen dynamischen Arbeitsspeicher verwenden, muss die oben genannte Mindestkonfiguration eingehalten werden.

Netzwerk- und Firewall-Anforderungen

Im Folgenden finden Sie die Netzwerkanforderungen für die Veritas Resiliency Platform:

- Bevor Sie den Hostnamen und die IP-Adresse in den "Netzwerkeinstellungen" verwenden, müssen Sie diese beim DNS-Server registrieren.
- Der Hostname oder die IP-Adresse, die für die Produktkonfiguration verwendet werden, dürfen nicht mehrere Einträge im DNS-Server haben. Die IP-Adresse darf beispielsweise nicht mehreren Hostnamen zugeordnet sein oder der Hostname darauf nicht mehreren IP-Adressen zugeordnet sein.
- Stellen Sie sicher, dass Ports 88 und 750 auf dem DNS-Server für die Kommunikation mit IMS geöffnet sind.
- Bei der Wiederherstellung in der Cloud muss Port 53 auf dem DNS-Server für bidirektionale Kommunikation mit dem Cloud-Rechenzentrum geöffnet sein.
- Der Hostname, den Sie für eine virtuelle Appliance verwenden, darf nicht mit einer Ziffer beginnen und darf keinen Unterstrich (_) enthalten.
- Veritas Resiliency Platform unterstützt nur die Internetprotokollversion 4 (IPV4).
- Wenn Sie beabsichtigen, den DHCP-Server zu verwenden, muss sich dieser im selben Subnetz befinden, in dem Sie das Produkt bereitstellen möchten.

Die folgenden Ports werden für die Veritas Resiliency Platform verwendet:

Tabelle 2-2 Für Resiliency Manager verwendete Ports

Verwendete Ports	Zweck	Für die Kommunikation zwischen	Richtung	Protokoll
443	Für die SSL-Kommunikation	Resiliency Manager und Webbrowser	Browser für Resiliency Manager	HTTPS, TLS v1.1+
14176	Für die Kommunikation zwischen dem Resiliency Manager und dem Infrastructure Management Server (IMS)	Resiliency Manager und IMS	Bidirektional	HTTPS, TLS v1.1+

Verwendete Ports	Zweck	Für die Kommunikation zwischen	Richtung	Protokoll
7001	Für die Datenbankreplikation	Resiliency Manager und IMS Bei mehreren Resiliency Managers zwischen diesen	Bidirektional	TCP mit SSL/TLS1.1+
389	Für die Kommunikation mit LDAP/AD-Server	Resiliency Manager und LDAP/AD-Server	Bidirektional	TCP, vom Benutzer bereitgestellt
636	Für die Kommunikation mit LDAP/AD-Server	Resiliency Manager und LDAP/AD-Server	Bidirektional	TCP mit SSL/TLS, vom Benutzer bereitgestellt
22	Für die Kommunikation zwischen Remote-Host und Appliance-klish-Zugriff	Appliance und Hosts	Bidirektional	TCP
123	Für die NTP-Synchronisierung	Appliance und NTP-Server	Bidirektional	TCP
14180	Für den Zugriff auf API-Dienst	Resiliency Manager und API-Dienst	Bidirektional	HTTPS, TLSv1.1+

Tabelle 2-3 Ports für lokalen IMS und Cloud-IMS

Verwendete Ports	Beschreibung	Für die Kommunikation zwischen	Richtung	Protokoll
14176	Für die Kommunikation zwischen dem Resiliency Manager und dem Infrastructure Management Server (IMS)	Resiliency Manager und IMS	Bidirektional	HTTPS, TLSv1.1+
5634	Für IMS-Konfiguration	IMS und Hosts	Bidirektional	HTTPS, TLSv1.1+

Verwendete Ports	Beschreibung	Für die Kommunikation zwischen	Richtung	Protokoll
14161	Für das Ausführen der IMS-Konsole	Resiliency Manager und IMS	Resiliency Manager zu IMS	HTTPS, TLSv1.1+
22	Für die Kommunikation zwischen Remote-Host und Appliance-klish-Zugriff Für die Remote-Bereitstellung der Pakete auf Remote-UNIX-Host von IMS	IMS und Hosts	Bidirektional	TCP
135	Für die Remote-Bereitstellung auf Clientcomputer (eingehender Datenverkehr)	Host und Remote-Windows-Hosts	Bidirektional	TCP
123	Für die NTP-Synchronisierung	Appliance und NTP-Server	Bidirektional	TCP

Tabelle 2-4 Ports für lokales Replication Gateway und Cloud-Replication Gateway

Verwendete Ports	Beschreibung	Für die Kommunikation zwischen	Richtung	Protokoll
33056	Für die Replikation	Lokaler virtueller Computer und Replication Gateway/Speicher-Proxy		TCP
5634	Für die Kommunikation mit IMS	IMS und Replication Gateway/Speicher-Proxy	Bidirektional	HTTPS, TLSv1.1+
8089	Für die Replikation	Komponente in der Cloud und lokale Komponente	Bidirektional	TCP

Tabelle 2-5 Ports für das Ziel-Gateway beim erneuten Synchronisieren

Verwendete Ports	Beschreibung	Für die Kommunikation zwischen	Richtung	Protokoll
67	BOOTP-Server	Ziel-Gateway mit DHCP-Rolle und physischem Host aktiviert	Unidirektional	UDP
68	BOOTP-Client	Ziel-Gateway mit DHCP-Rolle und physischem Host aktiviert	Unidirektional	UDP
69	TFTP-Protokoll	Ziel-Gateway mit PXE-Rolle und physischer Host	Unidirektional	TCP/UDP

Tabelle 2-6 Für virtuelle Computer verwendete Ports

Verwendete Ports	Beschreibung	Für die Kommunikation zwischen	Richtung	Protokoll
22	Für die Kommunikation zwischen Remote-Host und Appliance-klish-Zugriff Für die Remote-Bereitstellung der Pakete auf Remote-UNIX-Host von IMS	IMS und Hosts	Bidirektional	TCP
5634	Für die Kommunikation mit IMS	IMS und Hosts	Bidirektional	HTTPS, TLSv1.1+
33056	Für die Replikation	Virtueller Computer und Replication Gateway		TCP

Kapitel 3

Behobene Probleme

In diesem Kapitel werden folgende Themen behandelt:

Behobene Probleme

Dieses Kapitel enthält die Probleme, die in Veritas Resiliency Platform 3.0 behoben wurden.

Tabelle 3-1 In Veritas Resiliency Platform 3.0 behobene Probleme

Vorfallnummer	Zusammenfassung
5170	Informationsfehler zu Replikation
8465	Resiliency Group- und VBS-Namen in Diagrammen werden in Japanisch und Chinesisch falsch angezeigt
8433	Häufigkeit der Anwendungserkennung kann für die hochgeladenen Anwendungs-Bundles nicht von der Konsole bearbeitet werden
8617	Der Metering-Bericht funktioniert nicht für Replikationsverfahren von Drittanbietern
5167	VMDK- und VMX-Dateien müssen sich im selben Ordner befinden
5092	Der Vorgang zum Bearbeiten einer Resiliency Group kann nach der Simulation oder nach der Simulationsbereinigung fehlschlagen
8654	Eine zuvor konfigurierte Netzwerkzuordnung funktioniert möglicherweise nicht nach dem erneuten Hinzufügen eines VMware vCenter-Servers
8697	Replikationsinformationen werden für virtuelle Hyper-V-Computer in der Microsoft-Failover-Clustering-Umgebung, die nicht englische Schriftzeichen im CSV-Pfad enthalten, nicht erkannt

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

Kapitel 4

Bekannte Probleme

In diesem Kapitel werden folgende Themen behandelt:

- Die DR-Konfiguration (Disaster Recovery) für die Resiliency Group schlägt fehl, wenn das Microsoft Hyper-V-Replikat konfiguriert wurde, nachdem Sie Resiliency Platform einen virtuellen Computer hinzugefügt haben.
- Im Bestandsbericht der virtuellen Computer wird von der Resiliency Platform nicht der zugewiesene Arbeitsspeicher, sondern der gesamte Arbeitsspeicher der virtuellen Computer ausgewiesen.
- Bestimmte Validierungen funktionieren nicht beim Erstellen einer Resiliency Group mit Anwendungen (3721289)
- Die Simulation funktioniert nach dem Abbruch nicht
- Die DR-Konfiguration schlägt fehl, wenn virtuelle Computer in der Resiliency Group zu verschiedenen Servern gehören
- 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.
- Der Lizenzablaufstatus ist bei Resiliency Managern in verschiedenen Zeitzonen inkonsistent.
- In der Hyper-V-Gastumgebung wird angezeigt, dass der beschreibbare Datenträger schreibgeschützt ist. (3785911)
- Lange SRDF-Gerätegruppennamen werden nicht erkannt (3786826)
- Mehrere Repository-Pfade sind auf demselben Host für den Repository-Server nicht zulässig (3734149)
- Der Status "Unbekannt" wird für die Resiliency Groups für heruntergefahrene Rechenzentren angezeigt, die Teil eines VBS sind (3794650)

- Eine benutzerdefinierte Oracle-Anwendung wird nicht erkannt, wenn die Instanznamen nicht übereinstimmen (3796579)
- DR-Vorgänge für VBS schlagen fehl, wenn die Resiliency Group für Anwendungen mit nicht konfigurierter DR im VBS hinzugefügt wird (3794105)
- Der abgelaufene Resiliency Plan kann nicht ausgeführt werden, auch nachdem der Zeitplan bearbeitet wurde (3861955)
- Resiliency Groups für Hitachi-Gehäuse werden auf dem Dashboard unter Top RG im Diagramm der Zeitverzögerung der Replikation nicht angezeigt (3861173)
- Die Snapshot-Festplatte ist nach dem Simulationsvorgang in Hyper-V mit SRDF-Replikation schreibgeschützt (3862088)
- Die statische IP-Anpassung funktioniert unter bestimmten Umständen möglicherweise nicht (3862916, 3862237)
- Nach einer Standortwiederherstellung müssen alle Assets manuell aktualisiert werden (3861929)
- Datenträgerauslastungsrisiko nach DR-Vorgängen nicht behoben
- Die Migration reagiert nicht mehr, wenn der Vorgang von einem nicht verfügbaren Standort aus eingeleitet wird (3862253)
- Remote-Clustergruppen-Abhängigkeiten werden vor der Migration nicht validiert (3863082)
- Das Migrieren eines VBS kann nach einem Ausfall nicht durchgeführt werden (3862124)
- Der Resiliency Group-Zustand wird nicht aktualisiert, wenn der Produktionsstandort heruntergefahren ist (3863081)
- Die DNS-Anpassung funktioniert nicht, wenn der vollständig qualifizierte Domänenname (FQDN) nicht definiert ist (5037)
- Einige Versionen von VMware Tools werden nicht unterstützt (4969)
- Einloggen bei der Resiliency Manager-Konsole schlägt manchmal fehl
- Warnmeldung wird für die Netzwerkzuordnung angezeigt (8644)
- Neu hinzugefügte NIC-Informationen werden nicht angezeigt (10856)
- Validierungen, die beim Konfigurieren von Resiliency Groups für die Remote-Wiederherstellung angezeigt werden (10961)

Die DR-Konfiguration (Disaster Recovery) für die Resiliency Group schlägt fehl, wenn das Microsoft Hyper-V-Replikat konfiguriert wurde, nachdem Sie Resiliency Platform einen virtuellen Computer hinzugefügt haben.

Dieses Problem gilt für die Konfiguration der Disaster Recovery für eine Resiliency Group. Die DR-Konfiguration schlägt fehl, wenn ein Hyper-V-Replikat auf dem virtuellen Hyper-V-Computer konfiguriert wurde, nachdem Sie den virtuellen Computer dem Infrastructure Management Server (IMS) hinzugefügt haben.

Problemumgehung:

Verwenden Sie die Resiliency Platform-Konsole, um den Hyper-V-Host manuell zu aktualisieren. Sie erkennt die Hyper-V-Replikat-Informationen und die DR-Konfiguration funktioniert wie erwartet.

Im Bestandsbericht der virtuellen Computer wird von der Resiliency Platform nicht der zugewiesene Arbeitsspeicher, sondern der gesamte Arbeitsspeicher der virtuellen Computer ausgewiesen.

Im Bestandsbericht der virtuellen Computer wird von der Resiliency Platform-Konsole für die virtuellen Computer auf dem Hyper-V-Server der gesamte Arbeitsspeicher und nicht der zugewiesene Arbeitsspeicher ausgewiesen.

Bestimmte Validierungen funktionieren nicht beim Erstellen einer Resiliency Group mit Anwendungen (3721289)

Wenn Sie eine Resiliency Group für Anwendungen erstellen, funktionieren die folgenden Validierungen nicht:

- Prüfen Sie, ob das Resiliency Platform Applications Enablement Add-On auf dem Host bereitgestellt ist. Wenn die Aktivierung des Veritas Resiliency Platform Applications Enablement Add-Ons auf dem verwalteten Host nicht ordnungsgemäß installiert ist, schlägt das Erstellen der Resiliency Group für Anwendungen fehl. In diesem Fall müssen Sie das Add-On auf dem Host installieren, bevor die Resiliency Group für Anwendungen erstellt wird.
- Wenn der Workflow fehlschlägt, sollte die Resiliency Group nicht erstellt werden.

Die Simulation funktioniert nach dem Abbruch nicht

Wenn Sie eine Simulation abbrechen, funktioniert diese später nicht mehr.

Problemumgehung:

Führen Sie die Simulationsbereinigung durch, bevor Sie die Simulation erneut vornehmen.

Die DR-Konfiguration schlägt fehl, wenn virtuelle Computer in der Resiliency Group zu verschiedenen Servern gehören

Wenn Sie versuchen, Disaster Recovery für eine Resiliency Group durch mehrere virtuelle Computer zu konfigurieren, die zu verschiedenen Servern gehören, schlägt der Vorgang fehl.

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.

Problemumgehung:

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

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.

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.

Mehrere Repository-Pfade sind auf demselben Host für den Repository-Server nicht zulässig (3734149)

Während Sie einen Repository-Server hinzufügen, können Sie nicht mehrere Repository-Pfade auf demselben Host als mehrere Einträge für Repository-Server hinzufügen.

Der Status "Unbekannt" wird für die Resiliency Groups für heruntergefahrene Rechenzentren angezeigt, die Teil eines VBS sind (3794650)

Wenn ein Virtual Business Service (VBS) eine Resiliency Group enthält, die zu heruntergefahren Rechenzentren gehört, wird der Status der einzelnen Resiliency Group als "Unbekannt" angezeigt.

Eine benutzerdefinierte Oracle-Anwendung wird nicht erkannt, wenn die Instanznamen nicht übereinstimmen (3796579)

Wenn Sie eine benutzerdefinierte Oracle-Anwendung hinzufügen, die von Resiliency Platform erkannt werden soll, enthält die Anzeige "Anwendungseingaben" zwei Felder für "Instanzname ". Sie müssen den gleichen Namen in jedem Feld angeben. Andernfalls wird die Anwendung nicht erkannt.

DR-Vorgänge für VBS schlagen fehl, wenn die Resiliency Group für Anwendungen mit nicht konfigurierter DR im VBS hinzugefügt wird (3794105)

Der Benutzer kann Disaster Recovery-Vorgänge nicht ausführen, wenn der VBS aus einer Resiliency Group für Anwendungen besteht, die nicht für die Notfallwiederherstellung konfiguriert ist.

Der abgelaufene Resiliency Plan kann nicht ausgeführt werden, auch nachdem der Zeitplan bearbeitet wurde (3861955)

Sobald ein Resiliency Plan-Zeitplan abgelaufen ist, kann er auch nach dem Bearbeiten des Zeitplans nicht ausgeführt werden. Wenn Sie versuchen, den Zeitplan zu bearbeiten, wird kein Fehler festgestellt, aber der Plan wird zum bearbeiteten Zeitplan nicht ausgeführt.

Problemumgehung:

Löschen Sie den vorherigen Resiliency Plan-Zeitplan und erstellen Sie einen neuen.

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

Bei Hitachi-Gehäusen werden die Resiliency Groups auf dem Dashboard unter Top RG für die Zeitverzögerung der Replikation nicht angezeigt, da die Zeitverzögerung der Replikation für Hitachi-Gehäuse 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)

Wir verwenden den Befehl `Diskpart` zum Löschen des Schreibschutz-Flags. Der Befehl funktioniert jedoch nicht periodisch. Daher wird die Snapshot-Festplatte während des Simulationsvorgangs in der Hyper-V-SRDF-Replikationsumgebung manchmal nur im schreibgeschützten Modus bereitgestellt.

Problemumgehung:

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

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 ist jedoch manchmal nicht erfolgreich, obwohl er Erfolg meldet. In solchen Fällen wird die IP-Adresse für den Linux-Gast nicht zugewiesen.

Problemumgehung:

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

Nach einer Standortwiederherstellung müssen alle Assets manuell aktualisiert werden (3861929)

Nachdem ein primärer Standort wiederhergestellt wurde, müssen Sie alle Asset-Konfigurationen wie zum Beispiel Konfigurationen von Gehäusen, virtueller Computer und von Erkennungshosts manuell aktualisieren.

Im Folgenden sehen Sie die Reihenfolge, in der die Asset-Konfiguration aktualisiert werden muss:

- Aktualisieren Sie für EMC VNX, EMC RecoverPoint und Hitachi den Erkennungshost zuerst und dann die Gehäuse. Schließlich aktualisieren Sie die VMware-vCenter-Server.
- Für NetApp aktualisieren Sie zuerst den VMware vCenter-Server und aktualisieren Sie dann die Gehäuse.

Datenträgerauslastungsrisiko nach DR-Vorgängen nicht behoben

Das Datenträgerauslastungsrisiko wird nicht aufgelöst, wenn der Datenträger verfügbar gemacht wird, nachdem die Resiliency Group, die mit dem Risiko verbunden ist, zum Wiederherstellungsstandort migriert wurde.

Die Migration reagiert nicht mehr, wenn der Vorgang von einem nicht verfügbaren Standort aus eingeleitet wird (3862253)

Wenn Sie versuchen, die Migration anstelle der Übernahme von einem Standort auszuführen, der derzeit nicht verfügbar ist, reagiert der Vorgang zeitlich unbeschränkt nicht mehr.

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

Veritas Resiliency Platform ermöglicht es Ihnen, eine globale Dienstgruppe zu 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.

Das Migrieren eines VBS kann nach einem Ausfall nicht durchgeführt werden (3862124)

Wenn der Arbeitsablauf fehlschlägt, während ein VBS migriert wird, kann die Migration nicht wiederholt werden.

Problemumgehung:

Beheben Sie das Problem, das den Fehlschlag verursacht hat, und stellen Sie den VBS im Produktionsrechenzentrum online. Führen Sie dann die Migration erneut durch. Sie können auch versuchen, die Migration für eine einzelne Resiliency Group durchzuführen, nachdem Sie das Problem behoben haben, das den Fehlschlag verursacht hat.

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.

Einloggen bei der Resiliency Manager-Konsole schlägt manchmal fehl

In manchen Fällen schlägt das Einloggen bei der Resiliency Manager-Konsole fehl.

Problemumgehung:

Beenden Sie die Resiliency Manager-Instanz und starten Sie diese dann neu.

Warnmeldung wird für die Netzwerkzuordnung angezeigt (8644)

Manchmal erhalten Sie eine Fehlermeldung in der nachstehenden Form, wenn Sie einen Disaster Recovery-Vorgang 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.

Neu hinzugefügte NIC-Informationen werden nicht angezeigt (10856)

Wenn eine Netzwerkkarte (NIC) an einen virtuellen Computer angeschlossen wird und die nachfolgend beschriebenen Bedingungen erfüllt sind, wird die neue Netzwerkkarte nicht im Teilfenster "Netzwerkkonfiguration" aufgelistet, wenn Sie die Resiliency Group für die Remote-Wiederherstellung konfigurieren.

- Der virtuelle Computer gehört zu einer Resiliency Group.
- "IP-Adressanpassung anwenden" ist aktiviert.
- IP-Adressen werden bearbeitet.

Problemumgehung:

Bearbeiten Sie die Resiliency Group, um das Kontrollkästchen "IP-Adressanpassung anwenden" zu deaktivieren, und schließen Sie den Assistenten ab.

Bearbeiten Sie die Resiliency Group erneut, und aktivieren Sie das Kontrollkästchen "IP-Adressanpassung anwenden". Die Daten zur neuen Netzwerkkarte werden nun unter "IP-Adressanpassung" angezeigt.

Dieses Problem tritt nicht auf, wenn IP-Adressen nicht bearbeitet werden.

Validierungen, die beim Konfigurieren von Resiliency Groups für die Remote-Wiederherstellung angezeigt werden (10961)

Die Meldung "Datenträger stimmt nicht überein" bzw. "Fehlende Validierungen für Datenträger-Korrelationen" wird beim Konfigurieren einer Resiliency Group für die Remote-Wiederherstellung in den folgenden Situationen angezeigt:

- Sie entfernen einen virtuellen Computer aus einer Resiliency Group, die mehr als einen virtuellen Computer enthält, und versuchen dann, diesen wieder hinzuzufügen.
- Wenn eine Resiliency Group nur einen einzigen virtuellen Computer enthält, und Sie löschen diese Resiliency Group und erstellen diese dann erneut und verwenden dabei denselben virtuellen Computer.

Problemumgehung:

Warten Sie mindestens 40 Minuten, bis die Erkennung des virtuellen Computers abgeschlossen ist. Sie können den virtuellen Computer auch manuell aktualisieren.

Ein Vorgang schlägt möglicherweise fehl, wenn er zur gleichen Zeit ausgeführt wird wie die Migration eines virtuellen Computers mithilfe von vMotion (6476)

Wenn ein virtueller Computer mithilfe von vMotion oder über DRS migriert und zur gleichen Zeit ein VRP-Vorgang auf diesem virtuellen Computer ausgeführt wird, schlägt der Vorgang möglicherweise fehl, da die Ressourcen sich in einem vorübergehenden Zustand befinden.

Problemumgehung:

Sie müssen den Vorgang nach Abschluss der Migration des virtuellen Computers erneut starten.

Die VLAN-Zuordnung ist unbedingt erforderlich für DRS-fähige virtuelle VMware-Computer (10322)

Wenn vSphere DRS für einen HA-Cluster unter VMware aktiviert ist und eine Port-Gruppe über einen Distributed Switch mit dem virtuellen Computer verbunden ist, dann müssen Sie eine VLAN-Zuordnung ausführen, damit der Migrationsvorgang ausgeführt werden kann.

Dies gilt nur für vCenter-Server und ESXi-Versionen, die älter sind als Version 6.5.

Beim Vorgang "Resiliency Group erstellen" wird ein Fehler für virtuelle Computer mit RHEL 7.0 und RHEL 7.1 mit der Open-VM-Tools-Version 9.4.X angezeigt (8479)

Wenn Sie versuchen, eine Resiliency Group mit virtuellen Computern mit RHEL 7.0 und 7.1 mit der Open-VM-Tools-Version 9.4.X zu konfigurieren, dann wird für den Vorgang der folgende Fehler angezeigt:

```
Erkennung der vom Dateisystem verwendeten Größe für den virtuellen
Computer für die Lizenzierung nicht möglich
```

Problemumgehung:

Installieren Sie Open VM Tools 9.10.X oder höher auf den virtuellen Computern mit RHEL 7.0 und RHEL 7.1 und konfigurieren Sie dann die Resiliency Group.

DR-Vorgänge schlagen fehl, wenn die Anzahl der Datenträger der virtuellen Computer im Cloud-Rechenzentrum mit der Anzahl der virtuellen Computer im lokalen Rechenzentrum identisch ist (10982)

Wenn die Größe der ausgewählten virtuellen Computer in der Cloud über die exakt gleiche Anzahl an Datenträgern verfügt wie die lokalen virtuellen Computer, schlagen die DR-Vorgänge mit der folgenden Fehlermeldung fehl:

```
Die maximal zulässige Anzahl an Datenträgern, die mit einem virtuellen Computer dieser Größe verknüpft werden können, ist 'x'.", "Code": 409, "message_id": "OperationNotAllowed"
```

Problemumgehung:

Fügen Sie bei der Konfiguration für DR einen zusätzlichen Datenträger zur Anzahl der Datenträger der lokalen virtuellen Computer hinzu und wählen Sie dann die Größe der virtuellen Computer in der Cloud entsprechend aus.

Der Simulationsvorgang wird für das Cloud-Rechenzentrum nach dem Bearbeiten der Resiliency Group, um einen virtuellen Computer zu entfernen, nicht sofort gestartet (10992)

Wenn das Zielrechenzentrum ein Cloud-Rechenzentrum ist und Sie einen virtuellen Computer durch Bearbeiten der Resiliency Group entfernt haben, können Sie den Simulationsvorgang möglicherweise nicht mehr starten.

Problemumgehung:

Aktualisieren Sie die Cloud-Erkennung und bearbeiten Sie die Resiliency Group dann erneut.

Durch das Entfernen eines virtuellen Computers mit Windows-Datentransfergerät wird das Replikations-Add-On nicht deinstalliert (11024)

Wenn Sie einen virtuellen Windows-Computer, der in der Ansicht "Host auf Replikation vorbereiten" aufgelistet ist, entfernen, wird dadurch das Resiliency Platform Replikations-Add-on auf diesem Host nicht deinstalliert.

Problemumgehung:

Sie müssen das Paket "`Veritas Resiliency Platform SR IO Tap Driver`" manuell aus der Systemsteuerung des virtuellen Computers entfernen.

Bekannte Probleme: Resiliency Platform-Datentransfergerät

Die folgenden bekannten Probleme gelten für das Resiliency Platform-Datentransfergerät:

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.

Problemumgehung:

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

Iofilter-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 Iofilter-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.

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

Wenn Sie eine Festplatte dem geschützten virtuellen Computer hinzufügen, 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.

Nach dem Löschen eines Datenträgers von einem virtuellen Computer kann ein Vorgang nicht durchgeführt werden (5182)

Wenn Sie einen Datenträger aus einem virtuellen Computer löschen, können Sie keinen Vorgang für die zugehörige Resiliency Group durchführen.

Problemumgehung:

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

Das Risiko "Datentransfergerät – virtueller Computer im No-Op-Modus" kann nicht aufgelöst werden (5183)

Das Risiko "Datentransfergerät – virtueller Computer im No-Op-Modus" kann nicht aufgelöst werden, sobald es erzeugt wurde.

Risiken wurden nach dem Snapshot des virtuellen Computers, der mit dem Datentransfergerät repliziert wurde, nicht generiert (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.

Problemumgehung:

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

Bekannte Probleme: Wiederherstellung auf Amazon Web Services (AWS)

Die folgenden bekannten Probleme treten bei AWS auf:

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.

Problemumgehung

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.

Problemumgehung:

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.

Problemumgehung

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

Bekannte Probleme: Wiederherstellung in vCloud

Die folgenden bekannten Probleme gelten für die Wiederherstellung in vCloud Director:

Das Zurück-Migrieren des Virtual Business Service (VBS) aus vCloud Director in ein lokales Rechenzentrum schlägt fehl (10975)

Wenn Sie versuchen, einen Virtual Business Service (VBS) von vCloud Director in ein lokales Rechenzentrum zurück zu migrieren, schlägt der Vorgang fehl.

Bekannte Probleme: NetBackup-Integration

Die folgenden bekannten Probleme treten bei der NetBackup-Integration auf:

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.

Problemumgehung:

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.

Problemumgehung:

Starten Sie die Dienste auf dem vCenter Server erneut.

Vorgänge für virtuelle Computer funktionieren nicht, wenn der Remote-Masterserver neu konfiguriert wird (8600)

Wenn der Remote-Masterserver neu konfiguriert wird, wird die Remote-Masterzuordnung für den virtuellen Computer entfernt, sodass kein Vorgang für den virtuellen Computer funktioniert.

Problemumgehung:

Sie müssen beide Masterserver entfernen und danach wieder hinzufügen.

Bekannte Probleme: Mehrere Resiliency Manager in einem Rechenzentrum

Die folgenden bekannten Probleme können auftreten, wenn sich mehrere Resiliency Manager in einem Rechenzentrum befinden:

In einem Cloud-Rechenzentrum kann DR 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.

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.

Problemumgehung:

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.

Kapitel 5

Beschränkungen

In diesem Kapitel werden folgende Themen behandelt:

Die Simulation wird nicht unterstützt, wenn der Datenträger unter Verwendung asynchroner Replikation in IBM XIV-Gehäuse 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-Gehäuse 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" fehlt.

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\VRTSitrptap\cli\vxtapaction.exe" stop –cg <*CGID*>
  - "C:\Programme\Veritas\VRTSitrptap\cli\vxtapaction.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 Domänennamen (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 3.0 aufgelistet:

- Der Aufgabenname eines Resiliency Plans ändert sich beim Ändern der Browser-Standorteinstellungen nicht.
- Der Textinhalt von Benachrichtigungen ist nicht lokalisiert.
- Der Textinhalt von E-Mails ist nicht lokalisiert.
- Das Ergebnis der Aufgabe "Aktivitäten" ist nicht lokalisiert.
- Die Aufgabe "Host-Stufe" ist nicht lokalisiert.
- Für die deutsche Version von Active Directory ist der Gruppenname des Benutzers eine Pflichteingabe.
- Die Hauptaufgabe des Arbeitsablaufs für Resiliency Groups, die vor dem Upgrade erstellt wurden, ist nicht lokalisiert.
- Arbeitsabläufe, die vor dem Upgrade ausgeführt wurden, sind nicht lokalisiert.
- Die in der Resiliency Platform-Konsole angezeigten Statusanzeigen von Resiliency Manager, IMS oder InfoScale Operations Manager-Server sind nicht lokalisiert.

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.

Anhang A

Sicherheitsfunktionen der virtuellen Appliance

Dieser Anhang enthält folgende Themen:

Sicherheit des Betriebssystems

Das Betriebssystem der Veritas Resiliency Platform-Appliance ist vor Ausnutzung potenzieller Sicherheitslücken geschützt, indem von Resiliency Platform nicht genutzten Pakete des Betriebssystems entfernt werden. Alle Standard-Yum-Repository-Dateien, die im Betriebssystem enthalten sind, werden entfernt.

Die Tastenkombination "Strg + Alt + Entf" wurde deaktiviert, damit ein versehentlicher Neustart der virtuellen Appliance vermieden wird. Exec Shield wird aktiviert, um die virtuelle Appliance vor Stack-, Heap- und Integer-Überläufen zu schützen.

Managementsicherheit

Nur zwei Benutzer sind in der Appliance verfügbar: Administratorbenutzer und Supportbenutzer. Diese beiden Benutzerkonten werden verwendet, um basierend auf der Anforderung auf die Appliance zuzugreifen.

Für die Appliance stehen nur die Admin-Anmeldedaten zur Verfügung. Die Kennwortrichtlinie der Admin-Identifikationsdaten wird geändert, damit der Benutzer aufgefordert wird, das Kennwort beim ersten Einloggen zu ändern.

Wenn das Kennwort des Administratorbenutzers verloren gegangen ist, müssen Sie den Veritas-Support bitten, das Kennwort des Administratorbenutzers zurückzusetzen.

Bei erfolgreichem Abschluss des Produkt-Bootstrap kann der Administratorbenutzer nur auf ein begrenztes Menü mit Befehlen über klish zugreifen. Neben dem Administratorbenutzer wird auch der Supportbenutzer in der Appliance unterstützt, aber das Remote-Einloggen des Supportbenutzers ist deaktiviert. Für den Zugriff auf den Supportbenutzer ist ein Einloggen als Administrator und der Einsatz von klish erforderlich. Die Option `support > shell` wird im klish -Menü bereitgestellt, damit der Benutzer zur Supportrolle wechseln und auf die Bash-Shell für den Support zugreifen kann. Nachdem Sie diese Option ausgewählt haben, erhält der Supportbenutzer Superuser-Rechte. Der Einsatz dieser Option wird nicht empfohlen und sollte nur mit Unterstützung durch den technischen Support erfolgen.

Die Zeitüberschreitung der Bash-Shells aller Benutzer wird auf 900 Sekunden festgelegt.

Netzwerksicherheit

Die TCP-Zeitstempel-Antworten sind in der virtuellen Resiliency Platform-Appliance deaktiviert. Eine weitere Funktion der Netzwerksicherheit der Appliance besteht darin, dass während des Bootstrap des Produkts nur die vom Produkt für die Kommunikation und die Datenübertragung verwendeten Ports in der Firewall geöffnet werden, und alle anderen Kommunikationsvorgänge werden blockiert.

Ungewöhnliche Netzwerkprotokolle, wie DCCP, SCTP, RDC und TIPC wurden deaktiviert, damit sie nicht von jedem Vorgang dynamisch geladen werden können.

Siehe "Netzwerk- und Firewall-Anforderungen" auf Seite 21.

Sicherheit der Zugriffssteuerung

Die virtuelle Resiliency Platform-Appliance implementiert bestimmte Maßnahmen zur Zugriffssteuerung. "umask" wird für die gesamte Appliance auf 0700 festgelegt. Die Zugriffsberechtigungen für einige Dateien wie beispielsweise aus Stamm- oder Root-Ordner, Protokollverzeichnis usw. sind eingeschränkt. Alle Sicherheits- und Autorisierungsbenachrichtigungen werden in der Appliance protokolliert.

Physische Sicherheit

In der virtuellen Resiliency Platform-Appliance ist der Zugriff auf den USB-Speicher deaktiviert.