

Rapid Recovery 6.1.2 Versionshinweisen

Juni 2017

Diese Versionshinweise enthalten Informationen über die Rapid Recovery Version, Build 6.1.2.115.

Folgende Themen werden behandelt:

- [Über diese Version](#)
- [Bezeichnungen für Rapid Recovery Versionen](#)
- [Verbesserungen](#)
- [Veraltet mit dieser Version](#)
- [Behobene Probleme](#)
- [Bekannte Probleme](#)
- [Rapid Recovery Systemanforderungen](#)
- [Produktlizenzierung](#)
- [Erste Schritte mit Rapid Recovery](#)
- [Weitere Ressourcen](#)
- [Globalisierung](#)
- [Über uns](#)

Über diese Version

Rapid Recovery Software ermöglicht schnelle Sicherungen mit geprüfter Wiederherstellung für VMs und physische Server, die sich vor Ort oder an einem Remote-Standort befinden können. Rapid Recovery ist eine Software für IT-Mitarbeiter, die eine leistungsstarke, preisgünstige und benutzerfreundliche [Sicherungs-, Replikations- und Wiederherstellungslösung](#) benötigen, die Schutz für Server und geschäftskritische Anwendungen wie Microsoft SQL Server, Microsoft Exchange und Microsoft SharePoint bietet. Wenn Sie Rapid Recovery nutzen, können Sie kontinuierlich allen wichtigen Daten und Anwendungen von einer einzigen webbasierte Managementkonsole aus sichern und schützen.

Da es sich bei Rapid Recovery 6.1.2 um ein Wartungsupdate handelt, gelten die [Verbesserungen](#) und [Fehlerkorrekturen](#) speziell für diese Version. Nur die [bekanntesten Probleme](#) sind kumulativ. Informationen zu neuen Funktionen, verbesserten Funktionen, gelösten Problemen, bekannten Problemen oder Komponentenänderungen für andere Versionen finden Sie in den jeweiligen Versionshinweisen für die entsprechende Version von Rapid Recovery auf unserer [Webseite](#) für technische Dokumentation. Beispiel:

- Spezifische Informationen für die aktuellste Hauptversion Rapid Recovery 6.0 finden Sie in den [Rapid Recovery 6.0.1 Versionshinweisen](#).
- Spezifische Informationen zur aktuellsten Wartungsversion Rapid Recovery 6.1 finden Sie in den [Rapid Recovery 6.1 Versionshinweisen](#).
- Spezifischen Informationen zur aktuellsten bisherigen Wartungsversion Rapid Recovery 6.1.1 finden Sie in den [Rapid Recovery 6.1.1 Versionshinweisen](#).



NOTE: Die Standardansicht der [Webseite](#) für technische Dokumentation zeigt Dokumentationen für die aktuellste allgemein verfügbare Version der Rapid Recovery Software an. Mithilfe der Filter am oberen Rand der Seite können Sie Dokumentationen für eine andere Softwareversion oder für eine Sicherungs- und Wiederherstellungs-Appliance der Quest DL Serie anzeigen. Sie können die Ansicht auch nach Handbuchkategorie filtern.

Markenänderung

Version 6.1.2 beinhaltet die vollständige Markenänderung des Rapid Recovery Produkts und der Dokumentation, um die Marke Quest Software widerzuspiegeln. Weitere Informationen zu Quest finden Sie unter [Über uns](#).

Vor Version 6.0x hieß Rapid Recovery noch AppAssure. Alle Komponenten des Produkts wurden an die neue Marke angepasst, um den nächsten Schritt in ihrer Weiterentwicklung widerzuspiegeln. Details sind im Abschnitt über die [umbenannten Komponenten](#) der *Rapid Recovery 6.0.1 Versionshinweise* beschrieben.

Repository-Upgrade-Beratung

Die Aktualisierung der Core-Software auf Version 6.1 von einer früheren Version (zum Beispiel Rapid Recovery 6.0x oder AppAssure 5.x) ändert das Schema in Ihrem Repository. Dank der Aktualisierungen können Sie neue Funktionen mit der aktuellen Version nutzen, einschließlich der Möglichkeit zum Schutz von Gästen auf dem Microsoft Hyper-V-Host, ohne dass dazu eine Installation des Rapid Recovery-Agents auf jedem einzelnen Gast notwendig ist.

Nach der Änderung der Struktur auf Ihrem Repository durch ein Upgrade besteht keine Möglichkeit zum Downgrade der Core-Version. Wenn Sie in Zukunft feststellen sollten, dass Sie eine frühere Core-Version verwenden möchten, nachdem Sie ein Upgrade dieser Version durchgeführt haben, müssen Sie die Daten in Ihrem Repository archivieren. Sie können daraufhin die Informationen manuell erneut importieren, was einen erheblichen Aufwand bedeutet.

Hinweise zur Systemanforderungsdokumentation

Bei jeder neuen Softwareversion überprüfen und aktualisieren wir die Systemanforderungen für die Rapid Recovery-Software und -Komponenten. Wenn Sie lokalisierte Versionen der Produktdokumentation verwenden, informieren Sie sich in den Versionshinweisen über die aktuellsten Systemanforderungen. Versionshinweise werden von Zeit zu Zeit aktualisiert und in einem Versionszyklus neu herausgegeben.

Bezeichnungen für Rapid Recovery Versionen

Die Bezeichnungen der Rapid Recovery Versionen lassen sich in bis zu vier Gruppen einteilen. Jede Gruppe besteht aus einer Reihe von Zahlen, die durch Dezimalpunkte getrennt sind.

- Die erste Zahl gibt den **Haupt-Release** an. Diese Versionen beinhaltet wesentliche Änderungen an der Benutzeroberfläche, dem Repository oder dem Verhalten der Anwendung.
- **Neben-Releases** werden durch die zweite Zahl gekennzeichnet, die von der ersten Zahl durch den ersten Dezimalpunkt getrennt ist. Mit Neben-Releases werden neue Funktionen eingeführt, deren Umfang geringer ist als der von in Haupt-Releases implementierten Änderungen.
- **Wartungsversionen** werden durch die dritte Zahl gekennzeichnet, die nach einem zweiten Dezimalpunkt auf die zweite Zahl folgt. Für gegenwärtige und künftige Releasenummern gilt: Wenn die dritte Zahl größer als 0 ist, handelt es sich um eine Wartungsversion. Wartungsversionen dienen der Korrektur von zuvor erkannten Fehlern oder Verhaltensweisen.
- Die **Buildnummern** (normalerweise bestehend aus 3 oder 4 Stellen) bilden die vierte Gruppe von Zahlen. Dieser Teil dient dazu, die Version des beim Entwicklungsprozess generierten Softwareprogramms zu differenzieren.
 - Bei der Rapid Recovery Agenten-Software können die Buildnummern für Windows- und Linux-Versionen unterschiedlich sein. Wenn die ersten drei Zahlen der Versionsnummer übereinstimmen, gibt es keine Probleme bei der Interoperabilität zwischen Core und Agent.
 - Aktualisierte Builds desselben Softwarerelease werden während eines Releasezyklus möglicherweise über das Lizenzportal zur Verfügung gestellt werden. Wenn also Ihre Core-Software so konfiguriert ist, dass die Version der Agenten-Software auf geschützten Maschinen automatisch aktualisiert wird,

sind unter Umständen Abweichungen bei den Buildnummern desselben Release feststellbar. Diese Abweichungen haben keine negativen Auswirkungen auf die Funktionalität.

- Die Buildnummer von rein softwarebasierten Core-Versionen und den auf den Sicherungs- und Wiederherstellungs-Appliances der Quest DL Serie verwendeten Versionen können ebenfalls voneinander abweichen.
- Die Buildnummern von Core und Add-on-Komponente für Kaseya unterscheiden sich.
- Die unterschiedlichen Buildnummern haben keinen Einfluss auf die Replikation.

Bei Version 6.1.2.115 gibt die erste Ziffer (6) den Haupt-Release an. Die zweite Ziffer (1) entspricht dem Neben-Release. Die dritte Ziffer (2) gibt an, dass es sich um eine Wartungsversion zu Version 6.1 handelt, die ausschließlich Fehlerkorrekturen enthält. In diesem Fall umfasst die Wartungsversion ebenfalls die Markenänderung in Quest. Die Buildnummer (115) kommt zuletzt und wird im Allgemeinen nur in den Versionshinweisen aufgeführt. Die Buildnummer dieses Release sind für die Core-Software, die Windows- und Linux-Agenten-Software und Komponenten wie Local Mount Utility identisch.

Verbesserungen

In diesem Abschnitt sind implementierte Verbesserungen in Rapid Recovery Version 6.1.2 oder zuvor nicht in der technischen Produktdokumentation beschriebene Verbesserungen aufgeführt.

Folgende Themen werden behandelt:

- [Zusätzliche unterstützte Linux-Distributionen](#)
- [Exchange Server 2016 DAG-Unterstützung](#)
- [Eingeschränkte Unterstützung für vSphere/ESXi 6.5](#)

Zusätzliche unterstützte Linux-Distributionen

Rapid Recovery Version 6.1.2 umfasst Aktualisierungen seiner NBD-Implementierung (Network Block Device), die den Support für Rapid Recovery Agent bis Version 7.3 von CentOS, Red Hat Enterprise Linux (RHEL) und Oracle Linux ausweiten.

Diese drei Linux-Betriebssysteme basieren auf einer Drittanbieterkomponente, NBD, um das Auslesen und Schreiben von Daten in Blöcken mit fester Größe über ein TCP/IP-Netzwerk zu unterstützen. Die übrigen von Rapid Recovery Agent unterstützten Linux-Distributionen beinhalten NBD im Kernel.

Exchange Server 2016 DAG-Unterstützung

Rapid Recovery bietet ab sofort Unterstützung für Exchange Server 2016 DAG-Cluster. Die Anwendungs- und Clusterkonfiguration wurde mit Version 6.1.1 und Version 6.1.2 von Rapid Recovery getestet, und ihre Kompatibilität mit beiden Versionen der Software wurde verifiziert.

Eingeschränkte Unterstützung für vSphere/ESXi 6.5

Ab Version 6.1 bietet Rapid Recovery eingeschränkte Unterstützung für vSphere/ESXi 6.5. Sofern nicht anderslautend beschrieben, können für ESXi 6 unterstützte Funktionen nun auch mit ESXi 6.5 verwendet werden. Lesen Sie die folgenden Informationen zum besseren Verständnis sorgfältig durch.

Die folgenden Funktionen werden unterstützt:

- Schutz virtueller Maschinen auf ESXi 6.5
- Replikation von Wiederherstellungspunkten von ESXi 6.5
- Virtueller Export von Wiederherstellungspunkten nach ESXi 6.5

Es gelten die folgenden Einschränkungen:

- Sie können virtuelle Maschinen nur dann nach vCenter/ESXi 6.5 exportieren, wenn auf dem Quellcomputer nicht die Option „Secure Boot“ (Sicherer Start) verwendet wird.
- Verschlüsselte virtuelle Maschinen können auf ESXi 6.5 nur mit VDDK 6.5 agentenlos geschützt werden. Diese Einschränkung gilt nicht, wenn auf der virtuellen Maschine die Agenten-Software installiert ist. Die Unterstützung für diese Funktion wird voraussichtlich mit Rapid Recovery ab Version 7.0.0 bereitgestellt, die ein Upgrade auf VDDK 6.5 beinhaltet.
- Virtuelle Maschinen, die auf ESXi 6.5 agentenlos geschützt werden, können nicht übertragen werden, wenn der Übertragungsmodus auf „SAN“ (Storage Area Network) eingestellt ist. Die Option „SAN“ für den Übertragungsmodus ist nur für agentenlosen Schutz verfügbar.

Im Allgemeinen können mit ESXi 6.5 neu eingeführte Funktionen möglicherweise nicht verwendet werden und werden erst unterstützt, wenn VDDK in einer künftigen Version von Rapid Recovery aktualisiert und getestet wurde.

Veraltet mit dieser Version

In diesem Abschnitt finden Sie eine Liste von Funktionen, Elementen oder zugehörigen Komponenten, die in Rapid Recovery Version 6.1.2 veraltet sind.

Folgende Themen werden behandelt:

- [Microsoft Exchange Server 2007 SP1 Rollup 5 veraltet](#)

Microsoft Exchange Server 2007 SP1 Rollup 5 veraltet

Microsoft beendete den erweiterten Support für Exchange Server 2007 am 11. April 2017, basierend auf deren Richtlinie zum Supportlebenszyklus.

Quest testete Exchange Server 2007 SP1 Rollup 5 mit Rapid Recovery Version 6.1.2 und konnte keine Probleme feststellen. Daher wird Kunden mit einer Supportvereinbarung für Version 6.1.2 eingeschränkter Support für diese Version von Exchange Server bereitgestellt. Tests dieser Version von Exchange mit Rapid Recovery 7.0.0 sind ebenfalls geplant und werden in dieser Version unterstützt.

Diese Version von Exchange Server ist jedoch veraltet, und der Support wird in einer zukünftigen Version von Rapid Recovery eingestellt. Kunden, die Rapid Recovery zur Sicherung von Exchange Server 2007 SP1 nutzen, wird empfohlen, eine Aktualisierung auf eine Exchange Server Version durchzuführen, die von Microsoft unterstützt wird.

Behobene Probleme

In dieser Version behobene kundenseitige Probleme sind nachfolgend aufgeführt.

Tabelle 1. Behobene Probleme für Core und Windows

Beschreibung des behobenen Problems	Problem- ID	Funktionsbereich
Nach dem Upgrade auf Version 5.4.3 oder 6.0.x der Agentensoftware auf einem Windows Server 2012 R2 oder Windows Server 2016 Computer wird statt eines inkrementellen Snapshots ein Basisimage erstellt.	102561	Aktualisieren
In einem Fall einer fehlerhaften Replikation wurden Daten, die vor dem Fehler erfolgreich repliziert werden konnten, aus dem Staging-Bereich (Ziel) gelöscht, wodurch der nächste Replikationsjob von vorne beginnen musste, statt an dem Punkt fortzufahren, an dem der Fehler auftrat.	102578	Replikation
Bereitstellung für Volumes mit ReFS-Dateisystem funktionierte nicht auf Windows Server 2016.	102437	Bereitstellung
Die zweimalige oder häufigere Anforderung der Löschung des gleichen Snapshots in einer bestimmten Sequenz in einem DVM-Repository führte zuweilen zu Dateninkonsistenzen und spamte das Core-Protokoll mit folgendem Fehler: "unmanagedDvm.storageSubsystem."	102286	Repository
Nach der White Labeling-Implementierung war die Volume-Seite für agentlos geschützte VM leer.	101891	Seite „Volumes“
Bei der Durchführung von Bereitstellbarkeitsprüfungen auf geschützten Exchange Servern mit großen Datenbanken oder Servern unter hoher Last traten zuweilen Lücken zwischen untergeordneten Jobs auf, was zu einer Leistungsverschlechterung auf dem Server führte und dazu, dass einige Prüfungen Stunden dauerten.	101797	Exchange Server Prüfungen
Das PowerShell-Skript für Berichte wurde aufgrund der Verlagerung eines Vertrags während des Refactorings nicht ausgeführt. Der Code wurde aktualisiert, um das Problem zu beheben.	101678	PowerShell
Die Arcserve Unified Data Protection Software wurde nicht als inkompatibles Produkt identifiziert.	35798	Validierung
Im Protokoll „Add New Account“ (Neues Konto hinzufügen) war kein Bereich für die Eingabe des Service-Endpunkts für ein S3-kompatibles Cloud-Konto vorhanden.	35736	Archivierung
Die Archivierung in Amazon schlug mit dem Fehler fehl „The authorization mechanism you have provided is not supported. Please use AWS4-HMAC-SHA256“ (Der von Ihnen angegebene Autorisierungsmechanismus wird nicht unterstützt. Verwenden Sie AWS4-HMAC-SHA256) für Buckets in den Regionen Ohio, Mumbai und Seoul.	35733	Archivierung
Die koreanische Übersetzung in den Replikationsplaneinstellungen war falsch.	35726	Internationalisierung, Replikation
Die Spalte „State“ (Status) wies die falsche koreanische Übersetzung der Verschlüsselungsschlüssel auf.	35716	Internationalisierung, Verschlüsselung

Beschreibung des behobenen Problems	Problem-ID	Funktionsbereich
Im Rapid Recovery Softwareentwicklungskit funktionierte das AppRecoveryAPI Muster AddClusterUnderProtectionSample nicht.	35694	SDK
Der virtuelle Export schlug nach bestimmten Schritten mit der Fehlermeldung „No physical extents have been found for cluster offset '19626746' cluster length '520.“ (Es wurden keine Physical Extents für Cluster-Offset '19626746' Cluster-Länge '520' gefunden.) fehl. Extent disk # '1' LCL '19627264' LCF '0' PSF '264192' (Es wurden keine physischen Erweiterungen für Cluster-Offset '19626746' Cluster-Länge '520' gefunden. Erweiterung Datenträger # '1' LCL '19627264' LCF '0' PSF '264192') fehl.	35626	VM Export
Auf der Einstellungsseite der Core Console funktionierte die Validierung in den Timeout-Feldern zuweilen nicht ordnungsgemäß, und es wurde die Fehlermeldung „Uncaught Error“ (Nicht aufgefangener Fehler) angezeigt.	35572	GUI, Kerneinstellungen
In der koreanischen Übersetzung der Benutzeroberfläche trug die Pause-Taste fälschlicherweise die Übersetzung statt.	35557	Lokalisierung, Schutz anhalten
Auf der Seite „Schedule“ (Zeitplan) des Archivassistenten war der Tooltip-Text bei allen Übersetzungen falsch.	35556	Lokalisierung, geplantes Archiv
In den Assistenten zum Schutz von Maschinen war die Option „Daten mit einer Core-basierten Verschlüsselung mit vorhandenem Schlüssel verschlüsseln“ hervorgehoben, wenn sie nicht ausgewählt war.	35554	Schutz, GUI
Volumes waren nach einem Wiederherstellungspunkt von einem angehängten Archiv, das von einem geschützten, agentenlosen Windows Server 2008 R2-Computer erstellt wurde, nicht verfügbar.	35542	Archivierung, agentenloser Schutz
Die E-Mail-Benachrichtigungsvorlage wird auf die Standardeinstellungen zurückgesetzt, nachdem der Core-Dienst neu gestartet wird.	35483	Email-Benachrichtigungsvorlage, GUI
Die Replikation auf einen zweiten Ziel-Core begann nicht, wenn Volumes auf dem Quell-Core fehlten.	35358	Replikation
In einer bestimmten Umgebung konnte das GPT-Volume auf einer agentenlos geschützten virtuellen Maschine nicht von einem im schreibgeschützten Modus bereitgestellten Bereitstellungspunkt geöffnet werden.	35100	Agentenloser Schutz
Bei der Suche nach allen Übertragungsereignissen mithilfe des "Transfer Job per Machine"-Widgets (Job pro Maschine übertragen, in der Dashboard-Ansicht der Core Console) wurde die Textfolge "Transfer" (Übertragung) nicht übersetzt.	34774	Lokalisierung
Auf der Seite "Ereignisse" im Fenster "Löschen von Wiederherstellungspunkten innerhalb des Bereichs" funktionierten die Datums- und Uhrzeit-Picker nicht ordnungsgemäß, bis die Benutzer die Seite aktualisierten.	34347	Ereignisse, GUI
Die Größe der Festplattenmetadaten versetzt den Fortschritt bei der Archivierung. Wenn beispielsweise viele Datenbanken auf einem Volume	32044	Archivierung, Metadaten

Beschreibung des behobenen Problems	Problem- Funktionsbereich ID	
vorhanden sind, bleibt die Statusanzeige zu lange bei 1 % stehen und wird dann schneller.		
Datenbanken von Wiederherstellungspunkten konnten nicht geöffnet werden, wenn die Protokolle und Datendateien sich in unterschiedlichen Repositories befanden.	23285	Wiederherstellung, Anwendungsunterstützung

Tabelle 2. Behobene Probleme für DocRetriever for SharePoint

Beschreibung des behobenen Problems	Problem- Funktionsbereich ID	
DocRetriever Agent funktionierte nicht auf einem Computer, auf dem Microsoft Office SharePoint Server 2007 (32-Bit) installiert war.	102522	Wiederherstellung
Beim Abrufen von Listenelementen von einer SharePoint 2010 Datenbank war eine Wiederherstellung nicht möglich, wenn der gespeicherte Wert ein in XML unzulässiges Zeichen war.	102062	Wiederherstellung
Die Fehlermeldung "Cannot find the original destination..." (Ursprüngliches Ziel wurde nicht gefunden) wird angezeigt, nachdem der Versuch unternommen wurde, eine direkte Wiederherstellung eines Standorts von der "Farm"-Sicherung durchzuführen.	35614	Wiederherstellung

Tabelle 3. Behobene Linux-Probleme

Beschreibung des behobenen Problems	Problem- Funktionsbereich ID	
Das Skript zum Herunterladen von Paketen konnte das Mono-Paket für Debian 8 aufgrund eines unterbrochenen Links, der anschließend repariert wurde, nicht herunterladen.	102366	Debian 8
Benutzer mit SafeNet-verschlüsselten Partitionen konnten Linux-Computer nicht mithilfe der Rapid Recovery Agent-Software schützen.	35226	Schutz

Tabelle 4. Behobene Probleme für Local Mount Utility

Beschreibung des behobenen Problems	Problem- Funktionsbereich ID	
Volume-Image mit aktivierter Datendeduplizierung (Funktion in Windows Server 2012) konnte nicht bereitgestellt werden.	101472	Bereitstellung
Wenn der Benutzer versuchte, Wiederherstellungspunkte für mehrere Agenten in der LMU abzurufen, blieb der Fortschrittsbalken "Connecting in progress" (Verbindung wird hergestellt) hängen.	100635	GUI

Tabelle 5. Mailbox Restore, behobene Probleme

Beschreibung des behobenen Problems	Problem- Funktionsbereich ID
Nachrichten von einer Archiv-Mailbox wurden nach der Wiederherstellung am ursprünglichen Speicherort in der üblichen Mailbox des Benutzers wiederhergestellt.	35654 Wiederherstellung

Bekannte Probleme

Im Anschluss finden Sie eine Liste mit kundenbezogenen Problemen, einschließlich solcher Problemen bei Drittanbieterprodukten, die zum Zeitpunkt der Veröffentlichung bekannt waren.

Tabelle 6. Bekanntes Problem der Central Management Console

Beschreibung des bekannten Problems	Problem- Funktionsbereich ID
Autorisierung auf Central Management Console in einer einzelnen Kundenumgebung aufgrund einer spezifischen Konfiguration von Domänen-Controller, Gruppen und Konten nicht möglich. Problemumgehung: Keine. Ein erneutes Auftreten dieses Problems ist nicht zu erwarten, es sei denn, es bestehen exakt die gleichen Umstände.	101227 Authentifizierung

Tabelle 7. Bekannte Probleme bei Core und Windows

Beschreibung des bekannten Problems	Problem- Funktionsbereich ID
Ein auf einem freigegebenen CIFS-Volume gespeichertes DVM-Repository wird unwillkürlich offline geschaltet, und es tritt folgender Fehler auf: "Multiple connections error occurred while trying to map share." (Beim Versuch, die Freigabe zuzuordnen, ist ein mehrfacher Verbindungsfehler aufgetreten.) Problemumgehung: Wenden Sie sich an den Support, um einen Patch anzufordern, der dieses Problem behebt.	103240 Repository
Archivkomprimierungsgeschwindigkeit für in 6.1.x gespeicherte Archive hat sich im Vergleich zur erreichten Geschwindigkeit in AppAssure Version 5.4.3 um 50 % verringert. Problemumgehung: Keine.	103229 Archiv
Wenn sich Datenbankdateien auf einer Quorum-Disk für ein geschütztes SQL-Servercluster befinden, findet keine Protokollkürzung statt, und es tritt folgender Fehler auf: "SQL log truncation for the protected has been skipped, because there aren't any SQL databases in protection group." (SQL-Protokollkürzung für das geschützte Cluster wurde übersprungen, da sich keine SQL-Datenbanken in der Schutzgruppe befinden.) Problemumgehung: Verschieben Sie die SQL-Datenbank auf ein anderes Volume. Alternativ können Sie die SQL-Protokollkürzung mithilfe eines Skripts nach der Übertragung oder eines geplanten Jobs separat planen.	103225 SQL-Protokollkürzung
In Rapid Recovery Core ab Version 6.0.2 erstellte Archive weisen eine geringere Leistung auf als in früheren Versionen erstellte Archive, sowohl in Bezug auf	103212 Archiv

Beschreibung des bekannten Problems**Problem- Funktionsbereich
ID**

die Geschwindigkeit als auch auf die Komprimierungsrate. Kein Fehler in 6.0.1. Dieser Fehler trat erstmals in Version 6.02 auf und kommt in den Versionen 6.1.0, 6.1.1 und 6.1.2 erneut vor.

Problemumgehung: Wenden Sie sich an den Support, um einen Patch für dieses Problem zu erhalten, sobald er verfügbar ist.

Validierung liegt nicht vor, um Benutzer daran zu hindern, Linux-Systemordner als Zielorte für die standardmäßige Wiederherstellung auszuwählen, und es tritt dieser Fehler auf: "System.ApplicationException: We do not support rollback to system folders at [destination]." (Der Rollback auf Systemordner unter [Ziel] wird von uns nicht unterstützt.)

103178 Wiederherstellung,
Validierung

Problemumgehung: Verwenden Sie Standardprozeduren zur Wiederherstellung eines System-Volumes, oder führen Sie einen virtuellen Export durch. Um das System-Volume wiederherzustellen (für Linux- oder Windows-Computer), führen Sie eine Bare Metal-Wiederherstellung durch, wie im *Rapid Recovery Benutzerhandbuch* beschrieben.

Die Aufbewahrungsrichtlinienlogik berücksichtigt keine spezifischen Fälle, die zum Überspringen der Erstellung eines monatlichen Wiederherstellungspunktes beim Rollup führen könnten. Wenn beispielsweise bei der Erfassung eines inkrementellen Snapshots ein Fehler auftritt oder wenn nächtliche Jobs weiterlaufen und das Ausführen des Rollups verhindern und wenn die Rollup-Richtlinie die Logik erzwingt, einen Wiederherstellungspunkt pro Monat beizubehalten, kann in seltenen Fällen der monatliche Wiederherstellungspunkt ggf. nicht erstellt werden.

103165 Aufbewahrungsrichtlinie

Problemumgehung: Wenn ein übersprungenes Rollup die Ursache ist, besteht die Problemumgehung darin, die Arbeit zu ändern, die die Ausführung des Rollups verzögert.

Datenträger und Volumes werden für agentlos geschützte VM nicht erkannt, wenn das Protokoll FIPS 140-2 auf dem Core aktiviert ist.

102508 Agentenloser
Schutz

Problemumgehung: Deaktivieren Sie FIPS 140-2, oder wenden Sie sich an den Support.

Der Core kann kein DVM-Repository mit einer Größe von mehr als 16 TB erstellen, wenn Schreib-Caching aktiviert ist.

102507 DVM-
Repository

Problemumgehung: Erstellen Sie mehrere Speicherorte mit einer Größe von bis zu 16 TB in einem einzigen Repository.

Bei der Verwendung von Replikation kann der Core keinen Platz auf einem Seed-Laufwerk mit dem Namen "AABackup" belegen.

102506 Replikation,
Seed-
Laufwerk

Problemumgehung: Der Ordnername AABackup ist reserviert. Wenn Sie den Namen AABackup für Ihr Seed-Laufwerk angegeben haben, benennen Sie ihn in einen anderen Wert ohne unzulässige Zeichen oder Ausdrücke um, wie im Glossar für das *Rapid Recovery Benutzerhandbuch* beschrieben.

Für Volumes mit spezifischer Schreibaktivität werden langsame inkrementelle Images erstellt.

102493 Sicherungen

Problemumgehung: Wenden Sie sich an den Support, und fragen Sie nach dem benutzerdefinierten Binär, der dieses Problem behebt.

Beschreibung des bekannten Problems	Problem- ID	Funktionsbereich
<p>Die verzögerte Löschung wird nach dem Rollup-Job abgebrochen, wenn ein französisches Betriebssystem eingestellt ist.</p> <p>Problemumgehung: Wenden Sie sich an den Support, und fragen Sie nach dem benutzerdefinierten Binär, der dieses Problem behebt.</p>	102436	Lokalisierung, Löschen
<p>Zuweilen verwenden exportierte Maschinen andere Laufwerksbuchstaben als die Quellmaschinen. Implementieren Sie eine Funktion zur Zuweisung von Laufwerksbuchstaben an exportierte Maschinen, die mit den Laufwerksbuchstaben übereinstimmen, die den ursprünglichen Quellmaschinen zugewiesen wurden.</p> <p>Problemumgehung: Wenden Sie sich an den Support, und fragen Sie nach dem benutzerdefinierten Binär, der dieses Problem behebt.</p>	102390	Virtueller Export
<p>In einer eindeutigen Umgebung überträgt die Replikation alle Daten auf einmal anstatt inkrementell, da "Deduplizierungs-Cache für Repository neu berechnen" fehlgeschlagen ist.</p> <p>Problemumgehung: Wenden Sie sich an den Support.</p>	102297	Replikation
<p>Lokaler Hyper-V-Export schlägt auf Windows Server 2016 fehl, und es tritt folgender Fehler auf: "WMI class 'MsvmVirtualSystemGlobalSettingData' der Fehler 'properties in class 'MsvmVirtualSystemGlobalSettingData' was not found."</p> <p>Problemumgehung: Keine provisorische Lösung für Hyper-V-Server. Der Remote-Hyper-V-Export funktioniert wie vorgesehen.</p>	102223	Virtueller Export
<p>Hyper-V-Schutz ohne Agent für alle Knoten in einem Cluster schlägt fehl, und es tritt folgender Fehler auf: "Unrecognized Guid Format" (Unbekanntes Guid-Format) aufgrund des spezifischen Status einer VM, die auf einem Cluster gehostet wird.</p> <p>Problemumgehung: Wenden Sie sich an den Support, und fragen Sie nach dem benutzerdefinierten Binär, der dieses Problem behebt.</p>	102221	Hyper-V ohne Agent
<p>Die Überprüfung des Archiv-Jobs wird abgebrochen, wenn der Speicher beschädigt ist, statt mit einer entsprechenden aussagekräftigen Fehlermeldung fehlzuschlagen.</p> <p>Problemumgehung: Keine.</p>	102207	Archivierung
<p>Bei replizierten geschützten Computern wird die nächtliche Job-Einstellung für "Check recovery points integrity" (Wiederherstellungspunkt-Integrität überprüfen) auf die standardmäßige Einstellung (aktiviert) gesetzt, selbst wenn die Einstellung in der Quelle vor der Replikation deaktiviert wird.</p> <p>Problemumgehung: Keine.</p>	102105	Replikation
<p>Beim Versuch, einen einmaligen Export auf einen Wiederherstellungspunkt auf einem geschützten Computer zu Azure durchzuführen, treten Fehler auf, wenn Sie versuchen, einen neuen Cloud-Dienstnamen auf der Seite "Deploy" (Bereitstellen) des Assistenten zum Exportieren virtueller Maschinen anzugeben. Der Fehler lautet "Object reference not set to an instance of an object." (Objektverweis wurde nicht auf eine Instanz oder ein Objekt festgelegt.)</p> <p>Problemumgehung: Erstellen Sie den Cloud-Dienst mithilfe des Verwaltungsmodells "Classic" (Klassisch) direkt über Ihr Azure-Konto in</p>	101819	VM Export

Beschreibung des bekannten Problems	Problem-ID	Funktionsbereich
der gleichen Ressourcengruppe wie Ihre anderen Ressourcen. Geben Sie anschließend über den Assistenten im Core den vorhandenen Cloud-Dienstnamen an.		
Auf der Seite "Recovery Points" (Wiederherstellungspunkte) der Core Console würden Benutzer von einem zusätzlichen Menü für das Wechseln zwischen den Seiten profitieren. Problemumgehung: Verwenden Sie die vorhandene Navigation.	101736	Benutzeroberfläche
Seed-Laufwerk-Jobs schlagen fehl, und es tritt folgender Fehler auf: "Write data task has failed." (Aufgabe zum Schreiben von Daten ist fehlgeschlagen.)	101617	Replikation
Wenn die Option zum sicheren Start auf Windows Server 2016 aktiviert ist, wird die Installation einiger Treiber bei der Agent-Installation blockiert, und es wird folgende Fehlermeldung angezeigt: "The transfer failed." (Die Übertragung ist fehlgeschlagen.)	101573	Installationsprogramm
Nach einigen Wochen schlägt der VM-Export fehl. TCP/IP-Ereignis 4227 wird im Systemprotokoll angezeigt mit der Meldung "TCP/IP failed to establish an outgoing connection because the selected local endpoint was recently used to connect to the same remote endpoint." (TCP/IP konnte keine ausgehende Verbindung herstellen, da der ausgewählte lokale Endpunkt kürzlich für die Verbindung mit dem gleichen Remote-Endpunkt verwendet wurde.) Dieser Fehler tritt typischerweise auf, wenn ausgehende Verbindungen häufig geöffnet und geschlossen werden. Dadurch werden alle verfügbaren lokalen Ports verwendet und TCP/IP dazu gezwungen, einen lokalen Port für eine ausgehende Verbindung erneut zu verwenden. Problemumgehung: Erhöhen Sie vorübergehend den dynamischen Portbereich, und starten Sie den Server regelmäßig neu.	101485	Virtueller Export
ESXi-Exports beginnen, mit folgender Fehlermeldung fehlzuschlagen: "System.OutOfMemoryException" auf DL-Sicherungs- und Wiederherstellungs-Appliances bei starker Belastung nach mehreren Tagen.	101246	Virtueller Export
ESXi Virtual Standby schlägt mit folgender Fehlermeldung fehl: "An entry with the same key already exists" (Ein Eintrag mit dem gleichen Schlüssel ist bereits vorhanden) in einer Systemtestumgebung.	100868	Virtueller Export
Es wird keine Warnmeldung angezeigt, dass das Rollup für Wiederherstellungspunkte auf einem Seed-Laufwerk, das noch nicht belegt wurde, nicht durchgeführt wird. Dies ist nur für Umgebungen relevant, die Replikation mit einem ausstehenden Seed-Laufwerk verwenden. Problemumgehung: Es ist keine provisorische Lösung erforderlich, da der Defekt nur das Nichtvorhandensein einer Benachrichtigung beschreibt.	35823	Replikation
Die Felder "Maximum connection pooling size" (Maximale Connection Pooling-Größe) und "Minimum connection pooling size" (Minimale Connection Pooling-Größe) für die MongoDB-Verbindung sind nicht validiert, sodass die Benutzer einen Maximalwert unter dem Minimalwert festlegen können. Problemumgehung: Legen Sie angemessene Werte fest.	35607	Core-Einstellungen
Statt eines inkrementellen Images wird ein Basis-Image auf einem geschützten Windows Server 2012 R2 Computer erstellt, wenn die NTFS-Bootsektorkopie	34981	Sicherungen

Beschreibung des bekannten Problems**Problem- Funktionsbereich
ID**

geändert wird. Dieser Fehler betrifft nur Benutzer, die Drittanbietersoftware installiert haben, die sich in der NTFS Bootsektorkopie geändert hat.

Problemumgehung: Es gibt keine Problemumgehung.

Es werden unerwartete Basis-Images in ESXi-VMs generiert, die Snapshots mit aktivierter Stilllegung haben. Der Fehler betrifft Benutzer, die virtuelle vCenter-Maschinen schützen, die SAN-Snapshots mit aktivierter Stilllegung haben.
Problemumgehung: Deaktivieren Sie die Stilllegung.

34916 Virtueller Export

Bei der Suche nach allen Übertragungsereignissen mithilfe des "Transfer Job per Machine"-Widgets (in der Dashboard-Ansicht der Core Console) wird die Textfolge "Transfer" nicht übersetzt.

34774 Lokalisierung

Die Exportrate für Wiederherstellungspunkte von Repositories, die eine hohe Fragmentierung aufweisen, ist langsam.

Problemumgehung: Es sind zwei Optionen verfügbar. Option 1: Deaktivieren Sie vorübergehend den Schutz, archivieren Sie alle Wiederherstellungspunkte für diesen Computer, entfernen Sie das Repository, erstellen Sie ein neues Repository, weisen Sie den geschützten Computer dem neuen Repository zu, importieren Sie das Archiv in das neue Repository und reaktivieren Sie anschließend den Schutz. Option 2: Wenden Sie sich an den Support, und fragen Sie nach dem benutzerdefinierten Binär, der dieses Problem behebt.

34758 Virtueller Export, Repository

Die virtuelle Standby-Leistung ist langsam, wenn mehrere gleichzeitig geschützte Computer exportiert werden (zum Beispiel 36).

Problemumgehung: Verringern Sie die maximal zulässige Anzahl gleichzeitig ausgeführter Exportjobs.

34434 Virtueller Export

Warnmeldung: "Informationen über zugewiesenen Speicherplatz ist für einige Volumes nicht verfügbar..." wird auf der Seite "Zusammenfassung" für eine geschützte Maschine angezeigt, wenn die VM sich im NFS-Datenspeicher (Network File System) befindet.

Problemumgehung: Es gibt keine Problemumgehung. Hierbei handelt es sich um eine Beschränkung von auf einem NFS-Datenspeicher gespeicherten VM.

33551 Zusammenfassende Informationen

Die Replikationsrate wird extrem langsam, wenn ein virtueller Exportjob gleichzeitig mit dem Replikationsjob gestartet wird.

Problemumgehung: Verwenden Sie einen Zeitplan, um die gleichzeitige Ausführung von Replikation und Export zu verhindern.

33230 Virtueller Export, Replikation, Ressourcenbelegung

Bei der gleichzeitigen Archivierung von zwei oder mehr Jobs schlagen alle aktiven Archivierungsjobs mit folgendem Fehler fehl, wenn der Speicherplatz des Ziel-Netzwerkspeichergeräts nicht mehr ausreicht. "Nicht genügend Platz auf Festplatte".

Problemumgehung: Erstellen Sie unterschiedliche Zeitpläne für die Ausführung der einzelnen Archive, sodass die Archive nicht gleichzeitig in der Netzwerkfreigabe ausgeführt werden.

31827 Archivierung

Nach dem virtuellen Export eines ohne Agent geschützten WinXPx86-Computers oder dem virtuellen Export einer beliebigen Maschine auf einem ESXi-Host lässt sich die daraus resultierende VM nicht starten. Das Problem

31705 Virtueller Export

Beschreibung des bekannten Problems	Problem- Funktionsbereich ID	
<p>betrifft die Controller-Treiber für SCSI- und IDE-Controller, die in der exportierten VM fehlen.</p> <p>Problemumgehung: Es gibt derzeit keine Problemumgehung.</p>		
<p>Nach dem virtuellen Export von RHEL 6 oder 7 von einem ESXi-Host lässt sich die daraus resultierende VM nicht starten.</p> <p>Problemumgehung: Keine.</p>	31277	Virtueller Export
<p>agentenlose ESXi-Wiederherstellung oder virtueller Export unter Verwendung des SaN-Transportmodus schlägt mit der Fehlermeldung "One of the parameters was invalid." (Einer der Parameter ist ungültig.) fehl.</p> <p>Problemumgehung: Verwenden Sie den Netzwerk-Transportmodus für die Wiederherstellung von Daten.</p>	29508	VMware ohne Agent, Datenwiederherstellung
<p>Bei der Nutzung der automatischen Datenträgerzuweisung für den VM-Export von ESXi tritt in seltenen Fällen ein Fehler mit einer nicht aussagekräftigen Fehlermeldung auf: "Aufgabe 'ReconfigVM_Task' ist fehlgeschlagen: Ungültige Konfiguration für Gerät '0'."</p> <p>Problemumgehung: Versuchen Sie, den Vorgang erneut auszuführen. Er sollte erfolgreich sein.</p>	27309	Virtueller Export

Tabelle 8. DL-Appliance, bekannte Probleme

Beschreibung des bekannten Problems	Problem- Funktionsbereich ID	
<p>In einer spezifischen Kundenumgebung ist die Appliance-Seite "Provisionierung" nicht verfügbar, und es wird ein Fehler gemeldet: "CIM Chassis-Fehler", da ein Speicherpool ein Gehäuse referenziert, das nicht existiert.</p> <p>Problemumgehung: Wenden Sie sich an den Support, und fragen Sie nach dem benutzerdefinierten Binär, der dieses Problem behebt.</p>	102495	GUI
<p>Zuweilen wird "Interner Serverfehler" auf der Seite "Sicherung" angezeigt.</p> <p>Problemumgehung: Ignorieren und schließen Sie diese Fehlermeldung.</p>	102379	Speicherbereitstellung
<p>Repository-Wartung schlug nach der Wiederherstellung der Provisionierungskonfiguration nach dem Upgrade auf 6.1.2 fehl.</p> <p>Problemumgehung: Wenden Sie sich an den Support.</p>	102340	Windows-Backup
<p>Der Benutzer kann mehrere Jobs zur erneuten Bereitstellung gleichzeitig auf der DL-Appliance starten.</p> <p>Problemumgehung: Starten Sie einen Job zur erneuten Bereitstellung nicht mehrmals, bevor Sie sichergestellt haben, dass keine anderen Jobs ausgeführt werden. Wenn dieses Problem auftritt, wenden Sie sich für die erneute Bereitstellung des Repositories an den Support von Quest.</p>	102322	Speicherbereitstellung
<p>Falscher Standardwert des Felds "Repository-Name" im Assistenten "Neues Repository hinzufügen".</p> <p>Problemumgehung: Geben Sie manuell einen Repository-Namen ein, der den Feldvalidierungsregeln entspricht.</p>	101348	Speicherbereitstellung

Beschreibung des bekannten Problems	Problem-ID	Funktionsbereich
<p>Durch eine erneute Bereitstellung des Auftrags wird die Core-Lokalisierung nicht wiederhergestellt.</p> <p>Problemumgehung: Ändern Sie die Core-Lokalisierung manuell in den Core-Einstellungen.</p>	101316	Speicherbereitstellung
<p>Jobs schlagen mit dem Fehler „System.OutOfMemoryException“ auf DL-Appliances fehl, nachdem sie eine gewissen Zeit ausgeführt wurden.</p> <p>Problemumgehung: Installieren Sie die aktuellsten Windows-Updates, und starten Sie die Appliance neu. Wenden Sie sich an den Support, wenn dieses Problem weiterhin besteht.</p>	101246	Speicherbereitstellung
<p>Der Status von Volumen wird als „Ungültig“ angezeigt, wenn der Wiederherstellungspartition ein Buchstabe zugewiesen ist.</p> <p>Problemumgehung: Warten Sie, bis die RASR USB-Erstellung abgeschlossen ist.</p>	101224	Virtueller Export
<p>Der Start von RASR schlägt mit einem Ausnahmefehler auf DL1300 und DL4300 mit neuen ID-Modulen fehl.</p> <p>Problemumgehung: Wenden Sie sich an den Support.</p>	101051	Speicherbereitstellung
<p>Es kann kein Windows-Backup erstellt werden, da die notwendigen Volumenelemente für eine Sicherung nicht richtig festgelegt werden, wenn Volumenbuchstaben geändert wurden.</p> <p>Problemumgehung: Entfernen Sie die aktuelle Richtlinie zu gemischten/ geänderten Buchstaben für Partitionen, und erstellen Sie eine neue Richtlinie mit heterogenen Volume-Buchstaben.</p>	100985	RASR
<p>Parameter im Popup-Fenster „Vorhandenes Repository erweitern“ geben nach einer Aktualisierung über RUU#3.1 nicht den tatsächlich verfügbaren Speicherplatz für die Repository-Erweiterung auf dem internen Controller auf der DL1300 an.</p> <p>Problemumgehung: Erweitern Sie das Repository über die Repository-Konfigurationsseite.</p>	100908	Windows-Backup
<p>Die Aufträge „Speicherbereitstellung“ und „Bereitstellungskonfiguration wiederherstellen“ können gleichzeitig gestartet werden, obwohl das gleichzeitige Starten dieser Aufträge inkompatibel ist.</p> <p>Problemumgehung: 1) Entfernen Sie die erstellte virtuelle Festplatte Repository 2 mithilfe von OMSA. 2) Starten Sie den Core-Dienst neu.</p>	100907	Speicherbereitstellung
<p>RASR USB kann nach einer Aktualisierung über RUU nicht auf dem Server erstellt werden, wenn der Server aus einem Windows-Backup wiederhergestellt wurde.</p> <p>Problemumgehung: Führen Sie eine RASR-Wiederherstellung über folgende Orte durch: 1) Zuvor erstelltes RASR USB; 2) RECOVERY-Partition durch Drücken von F8 während des POST-Vorgangs; 3) virtuelles RASRdisk-Laufwerk; 4) IDSDM (nur DL4300).</p>	100905	Speicherbereitstellung
<p>Die Core-Schnittstelle ist nicht mehr verfügbar, wenn die Erfassung von Core- und Appliance-Protokollen erzwungen wird.</p>	100904	RASR

Beschreibung des bekannten Problems**Problem- Funktionsbereich
ID**

Problemumgehung: Aktualisieren Sie die Seite, damit die GUI wieder verfügbar ist.

Wenn das Windows-Backup auf dem Server mit einem alten Winbackups-Volumen mit einer Größe von 75 GB und ohne freien Speicherplatz auf dem internen Controller erzwungen wurde, wird für die Haupt-Appliance ein roter Status ohne Möglichkeit zur Problemlösung angezeigt.

100887 Benutzeroberfläche

Problemumgehung: Löschen Sie die Protokolle des Windows-Backups wie folgt: 1) Öffnen Sie die Ereignisanzeige. 2) Gehen Sie zu „Anwendungs- und Dienstprotokolle“. 3) Navigieren Sie zu Microsoft -> Windows -> Backup. 4) Klicken Sie mit der rechten Maustaste auf „Betriebsbereit“ und wählen Sie „Speichern und Löschen“ oder, wenn Sie keine Speicherung wünschen, nur „Löschen“.

Wiederherstellen des Bereitstellungskonfigurationsauftrags schlägt mit einer nicht aussagekräftigen Fehlermeldung fehl: „Cannot mount volume to the folder 'I:\' because it contains files or folders“ (Volumen kann nicht an Ordner 'I:\' bereitgestellt werden, da er Dateien oder Ordner enthält), wenn dem virtuellen Laufwerk ein Buchstabe zugewiesen ist, der bereits vor der erneuten Bereitstellung verwendet wurde.

35805 Provisionierung

Problemumgehung: Entfernen Sie mithilfe des Festplatten-Managers zugewiesene Buchstaben von verbundenen virtuellen Medien. Führen Sie die erneute Volumenbereitstellung über die Appliance-Bereitstellungsseite erneut durch.

Falsches Verhalten der Logik zum Ermitteln der Bereitstellungsgröße.

35770 Windows-Backup

Problemumgehung: Geben Sie bei der Bereitstellung für die vorgesehene Größe einige GB weniger an, als tatsächlich an Speicherplatz zur Verfügung stehen.

Es stehen VMM-Aktionen zur Verfügung, wenn sich der ESXi-Host im Wartungsmodus befindet.

35740 Speicherbereitstellung

Problemumgehung: Führen Sie keine VM-Vorgänge über die Seite Virtual Standby aus, wenn sich ein ESXi-Host im Wartungsmodus befindet.

Nach Bestätigung der erneuten Bereitstellung sollte die GUI umgehend deaktiviert werden.

35579 Verwaltung der virtuellen Maschine

Problemumgehung: Warten Sie ein paar Minuten und aktualisieren Sie die Seite für die Core Console.

Überwachung der aktiven Aufgabe bleibt während der Erstellung eines RASR USB-Jobs bei 95 % hängen.

35531 Speicherbereitstellung

Problemumgehung: Aktualisieren Sie die GUI. Typischerweise wird der Job erfolgreich abgeschlossen, zeigt aber in einigen Fällen nicht den korrekten Status an, bis Sie die GUI aktualisieren.

Der Job „Wiederherstellen des Bereitstellungskonfiguration“ schlägt in einer spezifischen Umgebung fehl.

35137 RASR

Problemumgehung: Entfernen Sie alle physischen und virtuellen Medien vom Server, bevor Sie Vorgänge des Typs „Bereitstellung wiederherstellen“ ausführen.

Beschreibung des bekannten Problems	Problem-ID	Funktionsbereich
<p>Auf der Seite „Sicherungen“ wird eine falsche Übersetzung von „Status“ im Bereich „Gesicherte Elemente“ für eine Sprache (nicht Englisch) angezeigt.</p> <p>Problemumgehung: Keine.</p>	35031	Speicherbereitstellung
<p>Die VD-Festplattenbereitstellung schlägt fehl und gibt Code 4 zurück, wenn der Speicherpool nicht über einheitlich leeren Speicherplatz verfügt.</p> <p>Problemumgehung: Wenden Sie sich an den Support.</p>	34937	Lokalisierung
<p>In einigen Fällen wird der Fehler „Ungültiger Status; bereits geöffnet“ auf der Seite „Virtual Standby“ für DL4x00 Appliances angezeigt.</p> <p>Problemumgehung: Schließen Sie die Fehlermeldung. Wenn das Problem weiterhin besteht, laden Sie die Seite durch Klicken auf F5 neu.</p>	31477	Speicherbereitstellung
<p>Die Schaltflächen „VM starten“ und „Netzwerkadapter“ sollten deaktiviert sein, wenn der ESXi-/Hyper-V-Export der Maschine auf Appliances gestartet wurde. Problemumgehung: Klicken Sie keine dieser Schaltflächen an, bis der entsprechende VM-Export abgeschlossen ist.</p>	30989	Verwaltung der virtuellen Maschine

Tabelle 9. Bekannte Dokumentationsprobleme

Beschreibung des bekannten Problems	Problem-ID	Funktionsbereich
<p>Die Komponente Microsoft Windows Azure Storage 7.2.1 wird nicht in der Liste der im Produkt gefundenen Drittanbieterkomponenten angezeigt. Eine veraltete Version der Komponente wird an ihrer Stelle angezeigt.</p> <p>Problemumgehung: Microsoft Windows Azure Storage 7.2.1 verwendet die Apache 2.0 Lizenz, die in der Liste „Beiträge von Drittanbietern“ in der Produkthilfe aufgeführt ist und über einen Hyperlink von der Seite „Über Rapid Recovery“ zugänglich ist.</p>	102504	Kontextsensitive Hilfe
<p>Die Komponente DataGridViewImageAnimator 1.0 wird in der Liste der im Produkt gefundenen Drittanbieterkomponenten angezeigt, obwohl sie in Rapid Recovery 6.1.2 nicht verwendet wurde.</p> <p>Problemumgehung: Die Komponente wird in einer zukünftigen Version aus der Liste „Beiträge von Drittanbietern“ entfernt.</p>	102503	Kontextsensitive Hilfe
<p>Die Komponente SimpleRestServices 1.3.0.3 wird nicht in der Liste der im Produkt gefundenen Drittanbieterkomponenten angezeigt. Eine veraltete Version der Komponente wird an ihrer Stelle angezeigt.</p> <p>Problemumgehung: SimpleRestServices 1.3.0.3 wird in Rapid Recovery 6.1.2 verwendet. Die Komponente verwendet die MIT N/A Lizenz. Eine Kopie der Lizenz finden Sie unter http://quest.com/legal/third-party-licenses.aspx.</p>	102502	Kontextsensitive Hilfe
<p>Die Komponente OpenStack.NET 1.4.0.2 wird nicht in der Liste der im Produkt gefundenen Drittanbieterkomponenten angezeigt. Eine veraltete Version der Komponente wird an ihrer Stelle angezeigt.</p> <p>Problemumgehung: OpenStack.NET 1.4.0.2 wurde in Rapid Recovery 6.1.2 verwendet. Die Komponente verwendet die MIT N/A Lizenz. Eine Kopie der Lizenz finden Sie unter http://quest.com/legal/third-party-licenses.aspx.</p>	102501	Kontextsensitive Hilfe

Beschreibung des bekannten Problems	Problem- Funktionsbereich ID	
<p>Die Komponente NLog 3.2.1 wird nicht in der Liste der im Produkt gefundenen Drittanbieterkomponenten angezeigt. Eine veraltete Version der Komponente wird an ihrer Stelle angezeigt.</p> <p>Problemumgehung: NLog 3.2.1 wurde in Rapid Recovery 6.1.2 verwendet. Die Komponente verwendet die BSD - Kowalski 2011 Lizenz, Copyright (c) 2004-2011 Jaroslaw Kowalski <jaak@jkowwalski.net>. Eine Kopie der Lizenz finden Sie unter http://quest.com/legal/third-party-licenses.aspx.</p>	102500	Kontextsensitive Hilfe
<p>Die Komponente AWS SDK für .NET 3.3.1.2 wird nicht in der Liste der im Produkt gefundenen Drittanbieterkomponenten angezeigt. Eine veraltete Version der Komponente wird an ihrer Stelle angezeigt.</p> <p>Problemumgehung: AWS SDK für .NET 3.3.1.2 verwendet die Apache 2.0 Lizenz, die in der Liste „Beiträge von Drittanbietern“ in der Produkthilfe aufgeführt ist und über einen Hyperlink von der Seite „Über Rapid Recovery“ zugänglich ist.</p>	102499	Kontextsensitive Hilfe
<p>Die kontextsensitive Produkthilfe für Rapid Recovery Core wurde ab Version 6.1.2 umbenannt, um Quest Software als ihren Eigentümer widerzuspiegeln. Außer der Umbenennung wurden in dieser Version keine Änderungen am Inhalt der Hilfedateien vorgenommen.</p>	70130	Kontextsensitive Hilfe
<p>Das im <i>Rapid Recovery Benutzerhandbuch</i> unter „Deploying a virtual machine in Azure“ (Bereitstellen einer virtuellen Maschine in Azure) für Version 6.1.x beschriebene Verfahren enthält unnötige Schritte. Künftige Versionen der Dokumentation werden entsprechend angepasst.</p> <p>Problemumgehung: Ignorieren Sie beim Ausführen des Verfahrens die Schritte 4 bis 8. Der aktuelle Schritt 9 sollte beginnen mit „Wählen Sie auf der Seite ‚Destination‘ (Ziel)...“.</p>	101859	Exportieren nach Azure
<p>Das im <i>Rapid Recovery Benutzerhandbuch</i> unter „Setting up continual export to Azure“ (Konfigurieren kontinuierlicher Exporte nach Azure) für die Version 6.1.x beschriebene Verfahren enthält überflüssige Schritte. Künftige Versionen der Dokumentation werden entsprechend angepasst.</p> <p>Problemumgehung: Ignorieren Sie beim Ausführen des Verfahrens die Schritte 4 und 5. Da Sie kontinuierliche Exporte konfigurieren, werden Sie nicht zur Auswahl eines Wiederherstellungspunktes aufgefordert. Ebenfalls gibt es am Ende des Assistenten keine Seite „Summary“ (Übersicht). Klicken Sie auf der Seite „Volumes“ des Assistenten auf Fertig stellen (statt auf Weiter).</p>	101858	Exportieren nach Azure
<p>In Azure erstellte Container werden verwendet, um virtuelle Maschinen zu speichern, die aus Rapid Recovery Core in Ihr zugehöriges Azure-Konto exportiert werden. Wenn Sie vor der Durchführung eines virtuellen Exports einen bestimmten Container erstellen, wird der betreffende Container im Assistenten zum Exportieren virtueller Maschinen in der Regel im Fenster „Destination“ (Ziel) im Feld „Container name“ (Containername) als eine der Auswahlmöglichkeiten angezeigt. Wenn Sie den Container erstellen, indem Sie beim Konfigurieren eines virtuellen Exports einen gültigen Containernamen in das Feld „Container name“ (Containername) eingeben, wird der Container unter Umständen nicht sofort im Assistenten angezeigt. Dieses Verhalten wird in den zugehörigen Verfahren im <i>Rapid Recovery Benutzerhandbuch</i> nicht beschrieben.</p> <p>Problemumgehung: Wenn Sie einen Container mit dem Assistenten für den Export von virtuellen Maschinen erstellen und auf diesen Container in der Benutzeroberfläche des Assistenten nicht zugegriffen werden kann,</p>	101853	Exportieren nach Azure

Beschreibung des bekannten Problems	Problem- Funktionsbereich ID	
<p>schließen Sie einfach den Assistenten und starten Sie ihn erneut, und Sie sollten anschließend auf den neu erstellten Container zugreifen können. Künftige Versionen der Dokumentation werden entsprechend angepasst.</p>		
<p>Rapid Recovery Core greift für virtuelle Exporte nach Azure auf Speicherplatz und Container in Azure zurück, die mithilfe des Verwaltungsmodells „Classic“ (Klassisch) erstellt wurden. Container, die in Azure mit dem neueren Bereitstellungsmodell „Resource Manager“ (Ressourcenmanager) erstellt wurden, werden von Core nicht erkannt. In dem im <i>Rapid Recovery Benutzerhandbuch</i> unter „Creating a container in an Azure storage account“ (Erstellen eines Containers in einem Azure-Speicherkonto) für die Version 6.1.x beschriebenen Verfahren wird nicht auf die Notwendigkeit des Verwaltungsmodells „Classic“ (Klassisch) hingewiesen. Künftige Versionen der Dokumentation werden entsprechend angepasst.</p> <p>Problemumgehung: Verwenden Sie bei virtuellen Exporten das Verwaltungsmodell „Classic“ (Klassisch) zur Erstellung von Speicherkonten und Containern. Wenn Sie bereits ein Speicherkonto mithilfe des Verwaltungsmodells „Classic“ (Klassisch) erstellt haben, wird für alle dafür angelegten neuen Container automatisch das richtige Modell („Classic“ (Klassisch)) verwendet.</p>	101837	Exportieren nach Azure

Tabelle 10. Kaseya Add-On, bekannte Probleme

Beschreibung des bekannten Problems	Problem- Funktionsbereich ID	
<p>In einigen Fällen werden die Anmeldedaten für Kerne und Agenten im Kaseya Server in unverschlüsseltem Text in der Datei „AppRecoveryParams.json“ gespeichert.</p>	102096	Authentifizierung

Tabelle 11. Linux Schutz – bekannte Probleme

Beschreibung des bekannten Problems	Problem- Funktionsbereich ID	
<p>Ein Ubuntu Linux Agent kann nicht geschützt werden, wenn er eine Partition vom Typ „non fs data“ enthält.</p>	102284	Metadaten
<p>Transport Layer Security (TLS) 1.2 Protokoll kann nicht mit Linux Agent verwendet werden.</p> <p>Problemumgehung: Deaktivieren Sie TLS.</p>	101279	Sicherheit
<p>Es wird keine Warnmeldung angezeigt, die darauf hinweist, dass der Agentendienst nicht gestartet werden kann, wenn er auf einer Linux Maschine mithilfe eines anderen ini-Systems als dem ursprünglich installierten System installiert wurde. Beispielsweise verwendet Debian 8 standardmäßig SysD. Wenn SysD entfernt und SysV installiert wird, wird der Agent nicht gestartet.</p> <p>Problemumgehung: Es ist keine provisorische Lösung erforderlich, da der Defekt nur das Nichtvorhandensein einer Benachrichtigung beschreibt.</p>	35818	Benachrichtigungen
<p>Bestimmte Volumes werden nach dem virtuellen Export einer Linux Maschine nicht bereitgestellt. Dieser Fehler betrifft nur Benutzer mit LVM-Volumes auf einer iSCSI Dell EqualLogi Maschine.</p>	35288	Virtuelle Exporte (ESXi)

Beschreibung des bekannten Problems	Problem- Funktionsbereich ID	
Problemumgehung: Es gibt derzeit keine Problemumgehung.		
Agentenlos geschützte Ubuntu-Maschine ist nach BMR nicht startfähig. Problemumgehung: Verwenden Sie Rapid Recovery Agent auf Ubuntu statt den agentenlosen Schutz.	31206	BMR Startfähigkeit

Tabelle 12. Bekannte Probleme für Local Mount Utility

Beschreibung des bekannten Problems	Problem- Funktionsbereich ID	
Bei bereitgestellten Wiederherstellungspunkte auf einer Windows Server 2016 Maschine sind die „Explore“-Schaltflächen deaktiviert. Problemumgehung: Verwenden Sie Windows Explorer, um Daten in bereitgestellten Wiederherstellungspunkten zu finden.	101860	Bereitstellungen

Tabelle 13. Mailbox Restore, bekannte Probleme

Beschreibung des bekannten Problems	Problem- Funktionsbereich ID	
MailboxRestore kann eine Nachricht mit Emoticon-Symbolen wie einem unzufriedenen Gesicht (ASCII-Symbol „😒“) nicht wiederherstellen. Problemumgehung: Wenden Sie sich an den Support, und fragen Sie nach dem benutzerdefinierten Binär, der dieses Problem behebt.	102360	Wiederherstellung
Bei der Wiederherstellung von Berechtigungen für einen öffentlichen Ordner wird eine nicht aussagekräftige Fehlermeldung angezeigt, wenn der Benutzer nicht in der globalen Adressliste gefunden wurde. Problemumgehung: Es ist keine provisorische Lösung erforderlich, da der Fehler nur eine Fehlermeldung beschreibt, die ignoriert werden kann.	102018	Wiederherstellung

Rapid Recovery Systemanforderungen

In diesem Abschnitt werden die System- und Lizenzvoraussetzungen für die Installation von Rapid Recovery Core, Rapid Recovery Agent und Rapid Recovery Central Management Console beschrieben.

Folgende Themen werden behandelt:

- [Empfohlene Netzwerkinfrastruktur](#)
- [Unterstützung für UEFI und ReFS](#)
- [Unterstützung für dynamische und Basis-Volumes](#)
- [Unterstützung für freigegebene Clustervolumes](#)
- [Anforderungen für Rapid Recovery Core-Installation](#)
- [Rapid Recovery Version 6.1 Betriebssystem-Installations- und Kompatibilitätsmatrix](#)
- [Anforderungen für Rapid Recovery Core und Central Management Console](#)
- [Rapid Recovery Agent-Softwareanforderungen](#)
- [Rapid Recovery Local Mount Utility Softwareanforderungen](#)
- [Agentenloser Schutz Rapid Snap for Virtual](#)
- [Hypervisor-Anforderungen](#)
- [DVM-Repository-Anforderungen](#)
- [Lizenzierungsanforderungen](#)
- [Quest Support-Richtlinien](#)

Empfohlene Netzwerkinfrastruktur

Für die Ausführung von Rapid Recovery benötigt Quest mindestens eine Netzwerkinfrastruktur von 1 GbE für eine effiziente Leistung. Quest empfiehlt 10-GbE-Netzwerke für stabile Umgebungen. 10-GbE-Netzwerke werden auch für den Schutz von Servern mit großen Volumes (5 TB oder mehr) empfohlen.

Wenn mehrere Netzwerkschnittstellenkarten (NICs) auf der Core-Maschine vorhanden sind, die eine Netzwerkkartengruppierung (Gruppierung mehrerer physischer Netzwerkkarten in eine einzelne logische Netzwerkkarte) unterstützen und die Switches im Netzwerk dies zulassen, kann die Leistung durch eine Netzwerkkartengruppierung im Core weiter gesteigert werden. In solchen Fällen kann die Einbindung von Ersatznetzwerkkarten, die eine Netzwerkkartengruppierung unterstützen, auf geschützten Maschinen (sofern möglich) ebenfalls zu einer Steigerung der Gesamtleistung führen.

Falls der Core iSCSI oder NAS (Network Attached Storage) verwendet, empfiehlt Quest, getrennte Netzwerkschnittstellenkarten für Speicher- und Netzwerkdatenverkehr zu verwenden.

Verwenden Sie Netzwerkkabel mit der entsprechenden Nennleistung zum Abrufen der erwarteten Bandbreite. Quest empfiehlt das regelmäßige Testen Ihrer Netzwerkleistung und das entsprechende Anpassen der Hardware.

Diese Empfehlung basiert auf den typischen Anforderungen an eine Netzwerkinfrastruktur, die neben sämtlichen Geschäftsabläufen auch die von Rapid Recovery bereitgestellten Sicherungs-, Replikations- und Wiederherstellungsmöglichkeiten unterstützen soll.

Unterstützung für UEFI und ReFS

Unified Extensible Firmware Interface (UEFI - Vereinheitlichte erweiterbare Firmware-Schnittstelle) ist ein Ersatz für Basic Input/Output System (BIOS). Für Windows verwendet UEFI die EFI-Systempartitionen (Extensible Firmware Interface), die wie einfache FAT32-Volumes behandelt werden.

Rapid Recovery bietet Schutz- und Wiederherstellungsmöglichkeiten für EFI-Systempartitionen bei Verwendung der folgenden Betriebssysteme:

- **Windows:** Windows 8, Windows 8.1, Windows 10, Windows Server 2012, Windows Server 2012 R2 und Windows Server 2016.
- **Linux:** Alle unterstützten Versionen von Linux.

Außerdem unterstützt Rapid Recovery Schutz- und Wiederherstellungsfunktionen für ReFS-Volumes (Resilient File System) für Windows Server 2012, Windows Server 2012 R2 und Windows Server 2016.

Unterstützung für dynamische und Basis-Volumes

Rapid Recovery unterstützt die Erstellung von Snapshots aller dynamischer Volumes und Basis-Volumes. Darüber hinaus unterstützt Rapid Recovery den Export von einfachen dynamischen Volumes, die sich auf einem einzelnen physischen Datenträger befinden. Wie der Name impliziert, sind einfache dynamische Volumes keine Stripeset-Volumes, gespiegelte Volumes, übergreifende Volumes oder RAID-Volumes.

Das Verhalten für den virtuellen Export der dynamischen Datenträger unterscheidet sich je nachdem, ob das Volume, das Sie exportieren möchten, geschützt ist durch die Rapid Recovery-Agentensoftware oder eine VM ist, die agentenlosen Schutz verwendet. Dies ist der Fall, da nicht einfache oder komplexe dynamische Volumes willkürliche Festplattengeometrien haben, die nicht vollständig durch den Rapid Recovery Agenten interpretiert werden.

Wenn Sie versuchen, einen komplexen dynamischen Datenträger von einer Maschine mit Rapid Recovery Agentensoftware zu exportieren, wird eine Benachrichtigung in der Benutzerschnittstelle angezeigt, die Sie darauf hinweist, dass Exporte begrenzt sind und auf einfache dynamische Volumes beschränkt sind. Wenn Sie versuchen, etwas anderes als ein einfaches dynamisches Volume mit dem Rapid Recovery Agenten zu exportieren, wird der Exportvorgang jedoch fehlschlagen.

Im Gegensatz dazu werden dynamische Volumes für virtuelle Maschinen, die Sie agentenlos schützen, unterstützt für den Schutz, virtuellen Export, die Wiederherstellung von Daten und BMR und für Repository-Storage, bis auf einige wichtige Einschränkungen. Beispiel:

- **Schutz** Schutz: Für den Fall dass ein dynamisches Volume sich über mehrere Laufwerke erstreckt, müssen Sie diese Laufwerke zusammen schützen, um die Integrität des Volumes zu bewahren.
- **Virtueller Export:** Virtueller Export: Sie können komplexe dynamische Volumes von einem ESXi- oder Hyper-V-Host exportieren, z. B. Stripeset-Volumes, gespiegelte Volumes, übergreifende Volumes oder RAID-Volumes – und zwar mithilfe von agentenlosem Schutz. Die Volumes werden jedoch auf Datenträgerebene exportiert, ohne Volume-Parsing. Wenn zum Beispiel das Exportieren einer dynamischen Speicherlaufwerks auf zwei Laufwerke übergreift, umfasst der Exportvorgang zwei getrennte Datenträgervolumes.



CAUTION: Beim Exportieren eines dynamischen Datenträgers, der sich über mehrere Laufwerke erstreckt, müssen Sie die dynamischen Datenträger mit den Originalsystemvolumes zum Erhalten der Festplattentypen exportieren.

- **Wiederherstellen von Daten:** Beim Exportieren eines dynamischen Datenträgers, der sich über mehrere Laufwerke erstreckt, müssen Sie die dynamischen Datenträger mit den Originalsystemvolumes zum Erhalten der Festplattentypen exportieren. Wenn Sie nur einen Datenträger wiederherstellen, verursachen Sie eine Unterbrechung der Festplattenkonfiguration.

Repository-Speicher: Darüber hinaus unterstützt Rapid Recovery die Erstellung von Repositories auf komplexen dynamischen Volumes (Stripeset-Volumes, gespiegelte Volumes, übergreifende Volumes oder RAID-Volumes). Das Dateisystem der Maschine für das Hosting des Repository muss NTFS oder ReFS oder xfs sein.

Unterstützung für freigegebene Clustervolumes

Rapid Recovery Version 6.1 und höher enthält die Funktion „Rapid Snap for Virtual“. Wenn Rapid Recovery Agent auf jedem Knoten installiert ist, können Sie unterstützte virtuelle Maschinen schützen und wiederherstellen, die in freigegebenen Clustervolumes (CSVs) auf Hyper-V gehostet und unter Windows Server 2012 R2 und Windows Server 2016 ausgeführt werden.

Darüber hinaus unterstützt Rapid Recovery Version 6.1 und höher den virtuellen Export nach auf Hyper-V gehosteten CSVs, die unter Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 und Windows Server 2016 ausgeführt werden. Weitere Informationen zu unterstützten Hypervisoren finden Sie unter [Hypervisor-Anforderungen](#).

Rapid Recovery bietet nur Unterstützung für den Schutz und die Wiederherstellung von CSVs, die unter Windows Server 2008 R2 ausgeführt werden.

Die folgende Tabelle veranschaulicht die derzeitige Unterstützung in Rapid Recovery für freigegebene Clustervolumes.

Tabelle 14. Unterstützung in Rapid Recovery für freigegebene Clustervolumes

Betriebssystem	Schützen ¹ und Wiederherstellen ² von VMs auf in Hyper-V gehosteten CSVs		Virtueller Export in freigegebenes Hyper-V-CSV		Schützen ¹ und Wiederherstellen ³ von CSVs	
	6.0.x	6.1.x	6.0.x	6.1.x	6.0.x	6.1.x
CSV-Betriebssystem	Rapid Recovery Version	Rapid Recovery Version	Rapid Recovery Version	Rapid Recovery Version	Rapid Recovery Version	Rapid Recovery Version
Windows Server 2008 R2	Nein	Nein	Ja	Ja	Ja	Ja
Windows Server 2012	Nein	Nein	Ja	Ja	Nein	Nein
Windows Server 2012 R2	Nein	Ja	Ja	Ja	Nein	Nein
Windows Server 2016	Nein	Ja	Nein	Ja	Nein	Nein

¹ Der Begriff „Schützen“ umfasst in diesem Kontext den Schutz, die Replikation, das Rollup, die Bereitstellung und die Archivierung.

² Der Begriff „Wiederherstellen“ umfasst in diesem Kontext die Wiederherstellung auf Datei- und Volume-Ebene, die Bare-Metal-Wiederherstellung und den virtuellen Export.

³ Der Begriff „Wiederherstellen“ umfasst in diesem Kontext die Wiederherstellung auf Datei- und Volume-Ebene sowie die Bare-Metal-Wiederherstellung.

Anforderungen für Rapid Recovery Core-Installation

Sie müssen den Rapid Recovery Core auf einem dedizierten Windows 64-Bit-Server installieren. Auf Servern sollten keine anderen Anwendungen, Rollen, oder Funktionen installiert sein, die nicht in Bezug zu Rapid

Recovery stehen. Beispiel: Verwenden Sie nicht die Core-Maschine als Hypervisor-Host (außer wenn der Server ein entsprechend dimensioniertes Quest DL Series Sicherungs- und Wiederherstellungs-Gerät ist).

Ein weiteres Beispiel wäre, nicht den Core-Server als umfassenden Datenverkehrs-Web-Server zu verwenden. Wenn möglich, installieren Sie nicht Microsoft Exchange Server, SQL Server oder Microsoft SharePoint auf der Core-Maschine und führen Sie diese auch nicht aus. Wenn SQL Server auf der Core-Maschine erforderlich ist – wenn Sie beispielsweise Rapid RecoveryDocRetriever for SharePoint verwenden – stellen Sie sicher, dass Sie mehr Ressourcen zuweisen, und zwar zusätzlich zu denen, die für effiziente Core-Vorgänge benötigt werden.

Abhängig von Ihrer Lizenz und den umgebungsspezifischen Anforderungen müssen Sie mehrere Cores eventuell jeweils auf einem dedizierten Server installieren. Optional können Sie für die Remote-Verwaltung mehrerer Cores die Rapid Recovery Central Management Console auf einem 64-Bit-Windows-Computer installieren.

Für jede Maschine, die Sie in einem Rapid Recovery Core schützen möchten, müssen Sie die entsprechende Version der Rapid Recovery Agent-Software für das Betriebssystem der jeweiligen Maschine installieren. Optional können Sie Schutz von virtuellen Maschinen auf einem VMware ESXi Host ohne vorherige Installation des Rapid Recovery Agent ausführen. Dieser agentenlose Schutz hat gewisse Einschränkungen. Weitere Informationen finden Sie unter „Grundlegende Informationen zu Rapid Snap for Virtual“ im *Rapid Recovery Benutzerhandbuch*.

Vergewissern Sie sich vor der Installation von Rapid RecoveryVersion 6.1, dass das System die folgenden Mindestanforderungen für Hardware und Software erfüllt. Weitere Informationen zur Auslegung von Hardware-, Software-, Arbeitsspeicher-, Speicher- sowie Netzwerkanforderungen finden Sie im Knowledge Base-Artikel 185962, "[Sizing Rapid Recovery Deployments](#)" (Auslegung der Rapid Recovery-Bereitstellungen).

CAUTION: Die Ausführung des Rapid Recovery Core unter Windows Core-Betriebssystemen, die nur eingeschränkte Serverrollen bieten, wird von Quest nicht unterstützt. Dies umfasst alle Editionen von Windows Server 2008 Core, Windows Server 2008 R2 Core, Windows Server 2012 Core, Windows Server 2012 R2 Core und Windows Server 2016 Core. Außer Windows Server 2008 Core, werden diese Core Edition Betriebssysteme für die Ausführung der Rapid Recovery Agent-Software unterstützt.

NOTE: Quest rät davon ab, Rapid Recovery Core auf einer All-in-One Server Suite, wie Microsoft Small Business Server oder Microsoft Windows Server Essentials, zu installieren.

CAUTION: Quest rät davon ab, den Rapid Recovery Core auf derselben physischen Maschine zu installieren, die als Hyper-V-Host dient. (Diese Empfehlung gilt nicht für Sicherungs- und Wiederherstellungsappliances der Quest DL Series.)

Rapid RecoveryVersion 6.1 Betriebssystem-Installations- und Kompatibilitätsmatrix

Microsoft Windows-Betriebssysteme

Rapid Recovery Core muss auf einem entsprechend dimensionierten Server installiert werden, auf dem ein unterstütztes 64-Bit-Microsoft Windows-Betriebssystem ausgeführt wird. Die folgende Tabelle und die Anmerkungen listen jedes Windows-Betriebssystem auf und beschreiben Kompatibilität der einzelnen Rapid Recovery Komponenten oder deren Funktion.

NOTE: Diese Informationen werden zur Verfügung gestellt, um Nutzer über Kompatibilität zu informieren. Quest unterstützt keine Betriebssysteme, die das Ende ihres Lebenszyklus erreicht haben.

Tabelle 15. Rapid Recovery-Komponenten und -Funktionen, die mit Windows-Betriebssystemen kompatibel sind

Diese Tabelle führt jedes unterstützte Windows Betriebssystem und die damit kompatiblen Rapid Recovery Komponenten auf.

Windows-Betriebssystem	Core/ Central Management Console	Agent	Agentenlos	MMU	MR	DR	URC- Wiederherstellung	VM- Exportierung nach Azure
Windows XP SP3	Nein	Nein	Ja	Nein	Nein	Nein	Ja ¹	Nein
Windows Vista	Nein	Nein	Ja	Nein	Nein	Nein	Ja ¹	Nein
Windows Vista SP2	Nein	Ja	Ja	Ja	Ja	Ja	Ja ¹	Nein
Windows 7	Nein	Nein	Ja	Nein	Nein	Nein	Ja	Ja ²
Windows 7 SP1	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja ²
Windows 8	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja ²
Windows 8,1	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja ²
Windows 10	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja ²
Windows Server 2003	Nein	Nein	Ja	Nein	Nein	Nein	Ja ¹	Nein
Windows Server 2008	Nein	Nein	Ja	Nein	Nein	Nein	Ja ¹	Ja ²
Windows Server 2008 SP2	Ja	Ja	Ja	Ja	Ja	Ja	Ja ¹	Ja ²
Windows Server 2008 R2	Nein	Nein	Ja	Nein	Nein	Nein	Ja	Ja ²
Windows Server 2008 R2 SP1	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja ²
Windows Server 2012	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja ²
Windows Server 2012 R2	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja ²
Windows Server 2016	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Windows-Installations- und -Support-Hinweise:

¹ Die Start-CD unterstützt Bare-Metal-Wiederherstellung, aber nicht Treiberinjektion.

² Virtuelle Maschinen können nur bei Verwendung der 64-Bit-Versionen der aufgelisteten Betriebssysteme nach Azure exportiert werden.

Linux-Betriebssysteme

Linux-Betriebssysteme werden als geschützte Maschinen in einem Rapid Recovery Core unterstützt. Sie können agentenlosen Schutz verwenden oder den Rapid Recovery Agent installieren. Die folgende Tabelle und die Anmerkungen listen jedes unterstützte Linux-Betriebssystem und -Verteilung auf und beschreiben die Unterstützung der einzelnen Rapid Recovery-Komponenten oder deren Funktion.

Tabelle 16. Kompatible Rapid Recovery-Komponenten und Funktionen durch Linux-Betriebssystem

Diese Tabelle führt jede unterstützte Linux-Verteilung und die damit kompatiblen Rapid Recovery Komponenten auf.

Windows-Betriebssystem	Core/Central Management Console	Agent	Agentenlos
Linux Betriebssystem oder Verteilung	Agent	Agentenlos	Live DVD
Red Hat Enterprise Linux 6.3 - 6.8	Ja	Ja	Ja
Red Hat Enterprise Linux 7.0 - 7.3	Ja	Ja	Ja
CentOS Linux 6.3 - 6.8	Ja	Ja	Ja
CentOS Linux 7.0 - 7.3	Ja	Ja	Ja
Debian Linux 7, 8	Ja	Ja	Ja
Oracle Linux 6.3 - 6.8	Ja	Ja	Ja
Oracle Linux 7.0 - 7.3	Ja	Ja	Ja
Ubuntu Linux 12.04 LTS, 12.10	Ja	Ja	Ja
Ubuntu Linux 13.04, 13.10	Ja	Ja	Ja
Ubuntu Linux 14.04 LTS, 14.10	Ja ¹	Ja ¹	Ja ¹
Ubuntu Linux 15.04, 15.10	Ja ¹	Ja ¹	Ja ¹
Ubuntu Linux 16.04 LTS	Ja ¹	Ja ¹	Ja ¹
SUSE Linux Enterprise Server (SLES) 11 SP2 oder höher	Ja	Ja	Ja
SLES 12	Ja ¹	Ja ¹	Ja ¹

Linux-Installation und Support-Hinweise:

¹ Das B-tree-Dateisystem (Btrfs) wird nur mit Betriebssystemen mit der Kernel-Version 4.2. oder höher unterstützt. Kompatible Betriebssysteme umfassen derzeit die Ubuntu-Versionen 14.04.4, 15.10, und 16.04. Die SLES-Versionen 12 und 12 SP1 haben ältere Kernel-Versionen, entsprechend bietet Rapid Recovery keine Unterstützung für ihre Implementierungen von BTRFS.

Anforderungen für Rapid Recovery Core und Central Management Console

Anforderungen für den Rapid Recovery Core und die Central Management Console (CMC) werden in der folgenden Tabelle beschrieben.

Betriebssystemanforderungen für die Central Management Console sind identisch mit den Anforderungen für den Rapid Recovery Core. Diese Komponenten können auf dem gleichen Computer oder auf unterschiedlichen Maschinen, mit Ihren Anforderungen installiert werden.

Tabelle 17. Anforderungen für Rapid Recovery Core und Central Management Console

Anforderung	Details
Betriebssystem	<p>Die Rapid Recovery Core und Central Management Console erfordern eine der folgenden 64-Bit-Windows Betriebssysteme (BS). Sie laufen nicht auf 32-Bit-Windows-Systemen oder auf Linux-Verteilungen. Der Rapid Recovery Core setzt eines der folgenden x64-Windows-Betriebssysteme voraus:</p> <ul style="list-style-type: none"> • Microsoft Windows 7 SP1 • Microsoft Windows 8, 8.1* • Microsoft Windows 10 • Microsoft Windows Server 2008 SP2, 2008 R2 SP1 (außer Core-Editionen) • Microsoft Windows Server 2012, 2012 R2* (außer Core-Editionen) • Microsoft Windows Server 2016* (außer Core-Editionen) <p>Auf Windows-Betriebssystemen muss .NET Framework 4.5.2 installiert sein, damit der Rapid Recovery Core-Dienst ausgeführt werden kann. Darüber hinaus muss auf Betriebssystemen, die mit * markiert sind, die ASP .NET 4.5x-Rolle/Funktion installiert sein. Bei der Installation oder Aktualisierung des Core überprüft das Installationsprogramm abhängig vom Betriebssystem des Core-Servers, ob diese Komponenten vorhanden sind. Die Komponenten werden dann bei Bedarf automatisch installiert oder aktualisiert.</p> <p>Der Rapid Recovery Core unterstützt alle x64-Editionen der aufgeführten Windows-Betriebssysteme, sofern keine anderen Angaben gemacht werden. Der Rapid Recovery Core unterstützt keine Windows Server Core-Editionen.</p> <p>Wenn für aufgeführte Betriebssysteme ein Service Pack angegeben ist (z. B. Windows 7 SP1), dann ist das Betriebssystem des angegebenen Service Packs die Mindestanforderung. Wenn ein Betriebssystem ohne Service Pack aufgeführt ist (z. B. Windows 8), dann wird das Basis-Betriebssystem unterstützt. Alle nachfolgenden SP für ein aufgeführtes BS werden ebenfalls unterstützt, sofern nicht ausdrücklich ausgeschlossen.</p> <p>Für eine optimale Leistung wird empfohlen, den Rapid Recovery Core unter Windows 8.1 (oder höher) oder Windows Server 2012 (oder höher) zu installieren.</p>
Architektur	Nur 64-Bit-Version
Arbeitsspeicher	<p>Mindestens 8GB RAM</p> <p>Quest empfiehlt dringend, ECC-Speicher zu verwenden, um eine optimale Leistung der Rapid Recovery Core-Server sicherzustellen.</p>
Prozessor	Quad-Core oder höher

Anforderung	Details
Speicher	<p>Quest empfiehlt das Ausfindigmachen des Repository auf Direct Attached Storage(DAS)-, Storage Area Network(SAN)- oder Network Attached Storage(NAS)-Geräten (aufgeführt in der bevorzugten Reihenfolge).</p> <p>i NOTE: Quest empfiehlt bei der Installation eines NAS die Beschränkung der Repository-Größe auf 6 TB. Alle Speichergeräte müssen die Mindest-Input/Output-Anforderungen erfüllen. Eine Anleitung zur Dimensionierung von Hardware, Software, Arbeitsspeicher, Speicher und Netzwerkanforderungen finden Sie im Quest Knowledge Base-Artikel 185962, „Sizing Rapid Recovery Deployments“ (Dimensionierung von Rapid Recovery Bereitstellungen).</p>
Netzwerk	<p>mind. 1-GB-Ethernet (GbE)</p> <p>i NOTE: Für stabile Umgebungen empfiehlt Quest ein 10-GbE-Backbonenetzwerk.</p>
Netzwerkhardware	<p>Verwenden Sie Netzwerkkabel mit der entsprechenden Nennleistung zum Abrufen der erwarteten Bandbreite.</p> <p>i NOTE: Quest empfiehlt das regelmäßige Testen Ihrer Netzwerkleistung und das entsprechende Anpassen der Hardware.</p>

Rapid Recovery Agent-Softwareanforderungen

Anforderungen für die Rapid Recovery-Agent-Software werden in der folgenden Tabelle beschrieben.

i **NOTE:** Der Rapid Recovery Agent kann nicht für einen Computer bereitgestellt werden, auf dem ein Linux-Betriebssystem installiert ist, wenn das Add-on für Kaseya verwendet werden soll. Bei Verwendung dieses Add-ons auf einem Linux-Computer müssen Sie den Agenten manuell installieren. Weitere Informationen finden Sie im *Rapid Recovery Benutzerhandbuch*.

Tabelle 18. Rapid Recovery Agent-Softwareanforderungen

In der ersten Spalte der folgenden Tabelle werden die Anforderungen der Agenten-Software einschließlich Betriebssystem, Architektur, Speicher, Prozessor, Exchange-Server, SQL Server, SharePoint, Storage, Netzwerk und Netzwerk-Hardware aufgelistet. In der zweiten Spalte befinden sich bestimmte Details zu jeder einzelnen Anforderung.

Anforderung Details

Betriebssystem	<p>Die Rapid Recovery Agent-Software unterstützt 32-Bit- und 64-Bit-Windows- und Linux-Betriebssysteme. Dazu gehören:</p> <ul style="list-style-type: none">• Microsoft Windows Vista SP2• Microsoft Windows 7 SP1• Microsoft Windows 8, 8.1*• Microsoft Windows 10• Microsoft Windows Server 2008 SP2, 2008 R2 SP1 (alle Editionen außer Windows Server 2008 Core)• Microsoft Windows Server 2012, 2012 R2*• Microsoft Windows Server 2016*• Red Hat Enterprise Linux (RHEL) 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2, 7.3• CentOS Linux 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2, 7.3• Oracle Linux 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2, 7.3• Debian Linux 7, 8• Ubuntu Linux 12.04 LTS, 12.10, 13.04, 13.10, 14.04 LTS, 14.10, 15.04, 15.10, 16.04 LTS• SUSE Linux Enterprise Server (SLES) 11 (SP2 und höher), 12
----------------	---



NOTE: Auf Windows-Betriebssystemen muss Microsoft .NET Framework Version 4.5.2 installiert sein, damit der Rapid Recovery Core-Dienst ausgeführt werden kann. Die oben aufgeführten Betriebssysteme, die mit einem * gekennzeichnet sind, benötigen darüber hinaus die ASP .NET 4.5.x-Rolle oder -Funktion. Bei der Installation oder Aktualisierung der Rapid Recovery Agent-Software überprüft das Installationsprogramm, ob diese Komponenten vorhanden sind. Die Komponenten werden dann bei Bedarf automatisch installiert oder aktualisiert.

Zusätzliche Betriebssysteme werden nur für agentenlosen Schutz unterstützt. Weitere Informationen finden Sie unter [Agentenloser Schutz Rapid Snap for Virtual](#).

Wenn für aufgeführte Betriebssysteme ein Service Pack angegeben ist (z. B. Windows 7 SP1), dann ist das Betriebssystem des angegebenen Service Packs die Mindestanforderung. Wenn ein Betriebssystem ohne Service Pack aufgeführt ist (z. B. Windows 8), dann wird das Basis-Betriebssystem unterstützt. Alle nachfolgenden SP für ein aufgeführtes BS werden ebenfalls unterstützt, sofern nicht ausdrücklich ausgeschlossen.

Die Rapid Recovery Agent-Software unterstützt die Installation von Windows Server Core-Editionen für Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 und Windows Server 2016. Lediglich bei Windows Server 2008 R2 Core muss SP1 oder höher installiert sein. Windows Server 2008 Core-Edition wird nicht unterstützt.

Die Rapid Recovery Agent-Software unterstützt die in der Liste aufgeführten Linux-Verteilungen. Die meisten freigegebenen Kernel-Versionen wurden getestet. Zu den unterstützten Dateisystemen zählen ext2, ext3, ext4 und xfs. BTRFS wird auch unterstützt (nur bei bestimmten Linux Betriebssystemen mit Kernel-Version 4.2. Weitere Informationen finden Sie unter [Rapid Recovery Version 6.1 Betriebssystem-Installations- und Kompatibilitätsmatrix](#).

Agenten, die unter Microsoft Hyper-V Server 2012 installiert sind, arbeiten im Core Edition-Modus von Windows Server 2012.

Anforderung	Details
	<p>i NOTE: Native Sicherungen von freigegebenen Cluster-Volumes werden nur auf geschützten Windows 2008 R2-Maschinen (SP2 und höher) unterstützt.</p>
Architektur	32-Bit- oder 64-Bit-Version
Arbeitsspeicher	Mind. 4GB
Prozessor	Einzelprozessor oder höher
Unterstützung für Microsoft Exchange Server	Microsoft Exchange Server 2007 SP1 Rollup 5 oder höher, Exchange Server 2010, Exchange Server 2013 oder Exchange Server 2016
Unterstützung für Microsoft SQL Server	Microsoft SQL Server 2008 oder höher
Unterstützung für Microsoft SharePoint Server	<p>Microsoft SharePoint 2007, 2010, 2013, 2016</p> <p>i NOTE: Unterstützung für „SharePoint“ bezieht sich auf vollständig lizenzierte Versionen von Microsoft SharePoint Server für die oben aufgelisteten Versionen.</p>
Speicher	Direkt angeschlossener Speicherplatz, Speicherbereichsnetzwerk oder Network Attached Storage
Netzwerk	<p>mind. 1-GB-Ethernet (GbE)</p> <p>i NOTE: Für stabile Umgebungen empfiehlt Quest ein 10-GbE-Backbonenetzwerk.</p> <p>Quest rät davon ab, Maschinen über ein Wide Area Network (WAN) zu schützen. Wenn Sie über mehrere vernetzte Standorte verfügen, empfiehlt Quest die Installation eines Core an jedem Standort. Um Informationen auszutauschen, können Sie eine Replikation zwischen den Cores an unterschiedlichen Standorten durchführen. Die Replikation zwischen Cores ist WAN-optimierter. Die übermittelten Daten sind während der Übertragung komprimiert, dedupliziert und verschlüsselt.</p>
Netzwerkhardware	<p>Verwenden Sie Netzkabel mit der entsprechenden Nennleistung zum Abrufen der erwarteten Bandbreite.</p> <p>i NOTE: Quest empfiehlt das regelmäßige Testen Ihrer Netzwerkleistung und das entsprechende Anpassen der Hardware.</p>

Rapid Recovery Local Mount Utility Softwareanforderungen

Das Local Mount Utility (LMU) ist im Lieferumfang Rapid Recovery enthalten. Sie können das LMU-Installationsprogramm von der Seite **Downloads** entweder von der Core Console oder dem [Rapid Recovery-Lizenzportal](#) abrufen.

Tabelle 19. Local Mount Utility Softwareanforderungen

Anforderung	Details
Betriebssystem	<p>Die Rapid Recovery Local Mount Utility Software unterstützt 32-Bit- und 64-Bit-Windows Betriebssysteme, einschließlich der Folgenden:</p> <ul style="list-style-type: none"> • Microsoft Windows Vista SP2 • Microsoft Windows 7 SP1 • Microsoft Windows 8, 8.1* • Microsoft Windows 10 • Microsoft Windows Server 2008 SP2, 2008 R2 SP1 (alle Editionen außer Windows Server 2008 Core und Windows Server 2008 R2 Core) • Microsoft Windows Server 2012, 2012 R2* • Microsoft Windows Server 2016*
	<p>i NOTE: Auf Windows-Betriebssystemen muss Microsoft .NET Framework Version 4.5.2 installiert sein, damit der Dienst Local Mount Utility ausgeführt werden kann. Die oben aufgeführten Betriebssysteme, die mit einem * gekennzeichnet sind, benötigen darüber hinaus die ASP .NET 4.5.x-Rolle oder -Funktion. Bei der Installation oder Aktualisierung des LMU überprüft das Installationsprogramm, ob diese Komponenten vorhanden sind. Die Komponenten werden dann bei Bedarf automatisch installiert oder aktualisiert.</p> <p>Wenn für aufgeführte Betriebssysteme ein Service Pack angegeben ist (z. B. Windows 7 SP1), dann ist das Betriebssystem des angegebenen Service Packs die Mindestanforderung. Wenn ein Betriebssystem ohne Service Pack aufgeführt ist (z. B. Windows 8), dann wird das Basis-Betriebssystem unterstützt. Alle nachfolgenden SP für ein aufgeführtes BS werden ebenfalls unterstützt, sofern nicht ausdrücklich ausgeschlossen.</p> <p>Die LMU-Software unterstützt die Installation von Windows Server Core-Editionen für Windows Server 2012, Windows Server 2012 R2 und Windows Server 2016. Windows Server 2008 Core Edition und Windows Server 2008 R2 Core Edition werden nicht unterstützt.</p>
Architektur	32-Bit- oder 64-Bit-Version
Arbeitsspeicher	Mind. 4GB
Prozessor	Einzelprozessor oder höher
Netzwerk	<p>mind. 1-GB-Ethernet (GbE)</p> <p>i NOTE: Für stabile Umgebungen empfiehlt Quest ein 10-GbE-Backbonenetzwerk.</p>
Netzwerkhardware	<p>Verwenden Sie Netzkabel mit der entsprechenden Nennleistung zum Abrufen der erwarteten Bandbreite.</p> <p>i NOTE: Quest empfiehlt das regelmäßige Testen Ihrer Netzwerkleistung und das entsprechende Anpassen der Hardware.</p>

Agentenloser Schutz Rapid Snap for Virtual

Mit der Funktion Rapid Snap for Virtual von Rapid Recovery können Sie virtuelle Maschinen (VMs) auf bestimmten Hypervisor-Plattformen schützen, ohne vorherige Installation des Rapid Recovery-Agents auf allen Gast-Computern.

Bei der Verwendung dieser Funktion auf einer Hyper-V-Hypervisor-Plattform installieren Sie den Agenten ausschließlich auf dem Hyper-V-Host. Bei der Verwendung dieser Funktion auf VMware ESXi nutzt der ESXi-Host native APIs für den erweiterten Schutz seiner Gast-Computer.

Da die Agenten-Software nicht auf allen virtuellen Maschinen installiert werden muss, ist diese Funktion branchenweit als agentenloser Schutz bekannt. In Bezug auf Hyper-V wird diese Funktion auch als Host-basierter Schutz bezeichnet.

Rapid Snap for Virtual bietet verschiedene Vorteile, es gibt jedoch auch einige Einschränkungen. Beispiel: Sie können auf Volume-Ebene von dynamischen Volumes kein Snapshots erfassen (wie z. B. verteilt, gespiegelt übergreifend oder RAID). Dennoch können Snapshots auf dynamischen Volumes auf Datenträgerebene erfasst werden. Stellen Sie sicher, dass Sie sowohl die Vorteile als auch die Nachteile verstehen, bevor Sie diese Funktion nutzen. Weitere Informationen finden Sie unter Grundlegende Informationen zu Rapid Snap for Virtual im *Rapid Recovery Benutzerhandbuch*.

Bei der Verwendung von agentenlosem oder Host-basiertem Schutz verfügen Ihre VMs über die gleichen Mindestanforderungen für das zugrundeliegende Betriebssystem, den RAM, den Speicherplatz und die Netzwerkinfrastruktur wie mit der mit Rapid Recovery Agent-Software geschützten Maschinen. Ausführliche Informationen hierzu finden Sie unter [Rapid Recovery Agent-Softwareanforderungen](#).

Agentenlose Unterstützung für andere Betriebssysteme

Rapid Recovery Version 6.x verwendet Microsoft .NET Framework 4.5.2, das nicht von Windows XP SP3, Windows Vista (vor SP2), Windows Server 2003 und Windows Server 2008 unterstützt wird. Wenn Sie Maschinen mit diesen Betriebssystemen in einer früheren Core-Version geschützt haben (wie z. B. AppAssure Core 5.4.3), wurde die entsprechende Version von AppAssure Agent (verwendete eine frühere Version von .NET) unterstützt.

Sie können weiterhin diese Maschinen in einem Rapid Recovery Core schützen und dabei die frühere Agent-Version verwenden.

Geschützte Maschinen mit diesen Betriebssysteme können jedoch nicht mit Rapid Recovery Agent Version 6.x aktualisiert werden.

Maschinen mit diesen Windows-Betriebssystemen können jedoch in einem Rapid Recovery Version 6.x Core mit einer der folgenden Methoden geschützt werden:

- Schutz von virtuellen Maschinen auf einem VMware ESXi-Host mithilfe von agentenlosem Schutz.
- Installieren und Ausführen einer früheren kompatiblen Version von Agent auf einer physischen oder virtuellen Maschine, die Sie schützen möchten. Für Version 6.0.2 ist die einzige unterstützte kompatible Agent Version für dieses BS ist AppAssure Agent 5.4.3.

VMware ESXi Umgebungen sind mit einigen Betriebssystemen kompatibel, die Quest nicht unterstützt. z. B. Windows XP SP3, Windows Vista (vor SP2), Windows Server 2003 und Windows Server 2008 haben alle ihr End of Life mit Microsoft erreicht.

Während eines Tests hat die gesamte Palette von Rapid Recovery-Funktionen (Sicherung, Wiederherstellung, Replikation und Export) mit diesen bestimmten Betriebssystemen korrekt funktioniert.

Trotzdem verwenden Sie diese Betriebssysteme auf eigenes Risiko. Quest Support ist nicht in der Lage, Ihnen bei Problemen mit Betriebssystemen, die das Ende ihres Lebenszyklus erreicht haben, oder die als nicht unterstützt für einen Rapid Recovery Agent aufgeführt waren, zu helfen.

Einschränkungen der Unterstützung von Rapid Snap for Virtual (agentenloser Schutz)

Die Liste unterstützter Betriebssysteme steht unter [Rapid Recovery Version 6.1 Betriebssystem-Installations- und Kompatibilitätsmatrix](#) zur Verfügung. Alle bekannten Einschränkungen sind in diesen Matrizen oder als

Anmerkungen in den Tabellen mit den Anforderungen an die Core- oder Agenten-Software enthalten. Falls ein Fehler die Verwendung spezifischer Funktionen vorübergehend ausschließt, werden diese Informationen in der Regel in den Versionshinweisen für eine bestimmte Version gemeldet. Quest empfiehlt Benutzern die Überprüfung von Systemanforderungen und Versionshinweisen vor der Installation von Software-Versionen.

Quest führt keine vollständigen Tests mit nicht unterstützten Betriebssystemen durch. Wenn agentenloser Schutz zum Schutz von virtuellen Maschinen mit einem OS verwendet wird, das nicht von Rapid Recovery Agent-Software unterstützt wird, tun Sie dies auf eigenes Risiko. Benutzer werden gewarnt, dass möglicherweise einige Beschränkungen gelten. Diese Einschränkungen können Folgendes umfassen:

- Die fehlende Möglichkeit, einen virtuellen Export durchzuführen (einmalig oder dauernd)
- Die fehlende Möglichkeit, auf ein Archiv zu speichern oder aus einem Archiv wiederherzustellen
- Die fehlende Möglichkeit, eine Wiederherstellung auf einem System-Volumen mit Bare-Metal-Wiederherstellung durchzuführen

Wenn z. B. eine Maschine mit Windows 95 agentenlos, geschützt wird und einen virtuellen Export auf Hyper-V versucht, schlägt dies fehl. Dieser Fehler geschieht aufgrund von Einschränkungen in Hyper-V-Unterstützung dieses älteren Betriebssystems.

Zur Meldung spezifischer Probleme können Sie Kontakt mit Ihrem Quest Support-Vertreter aufnehmen. Das Melden solcher Schwierigkeiten ermöglicht es Quest, potenziell spezifische Inkompatibilitäten zu Knowledge Base-Artikeln oder künftigen Versionen dieser Versionshinweise hinzuzufügen.

Hypervisor-Anforderungen

Ein Hypervisor erstellt virtuelle Maschinen (Gäste) und führt diese auf einem Hostcomputer aus. Jeder Gast hat ein eigenes Betriebssystem.

Unter Verwendung der virtuellen Exportfunktion von Rapid Recovery können Sie einen einmaligen virtuellen Export durchführen oder Anforderungen für einen kontinuierlichen virtuellen Export, bekannt als Virtual Standby, definieren. Dieser Vorgang kann von jeder geschützten Maschine, physisch oder virtuell durchgeführt werden. Sollte eine geschützte Maschine ausfallen, können Sie die virtuelle Maschine starten, um Vorgänge wiederherzustellen, und anschließend die Wiederherstellung durchführen.

Mit Rapid Recovery können Sie einen virtuellen Export auf VM-Hosts durchführen, wie in der folgenden Tabelle beschrieben.

Tabelle 20. Hypervisor-Anforderungen mit Unterstützung für virtuellen Export

Die nachfolgende Tabelle listet die Hypervisor-Anforderungen auf. In der ersten Spalte werden alle Anforderungen aufgelistet: Host für virtuelle Maschinen, Gast-BS, Speicher und Architektur. Die zweite Spalte gibt Details für jede Anforderung an.

Anforderung	Details
Host für virtuelle Maschinen	<p>VMware:</p> <ul style="list-style-type: none"> • VMware Workstation 7.0, 8.0, 9.0, 10, 11, 12 • VMware vSphere auf ESXi 5.0, 5.1, 5.5, 6.0, 6.5 <p>i NOTE: Quest empfiehlt die Ausführung auf der neuesten unterstützten VMware Version. Zukünftige Haupt-Releases unserer Software werden voraussichtlich ESXi 5.0 und 5.1 nicht unterstützen.</p> <p>i NOTE: ESXi 6.5 wurde um die neue Funktion „Secure Boot“ (Sicherer Start) erweitert. Diese Funktion wird demnächst von Rapid Recovery unterstützt. Zurzeit unterstützt Rapid Recovery keine virtuellen Exporte nach vCenter/ESXi 6.5, wenn auf dem Quellcomputer die Option „Secure Boot“ (Sicherer Start) verwendet wird.</p> <p>Microsoft Hyper-V:</p>

Anforderung	Details
	<p>i NOTE: Für den virtuellen Export auf den Hyper-V-Host, sind .NET 4.5.2 und .NET 2.0 auf dem Hyper-V-Host erforderlich.</p> <ul style="list-style-type: none"> • Erste Generation: <ul style="list-style-type: none"> ◦ Hyper V, ausgeführt auf Microsoft Server-Versionen 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016 ◦ Hyper-V mit Ausführung auf Microsoft Windows 8 und 8.1 mit Hyper-V, Windows 10 ausgeführt wird • Zweite Generation: <ul style="list-style-type: none"> ◦ Hyper-V, ausgeführt auf Microsoft Server 2012 R2, 2016 ◦ Hyper-V, ausgeführt auf Microsoft Windows 8.1, Windows 10 <p>i NOTE: Lediglich geschützte Maschinen mit den folgenden UEFI-Betriebssystemen (Unified Extensible Firmware Interface) unterstützen einen Export auf Hyper-V-Hosts der zweiten Generation:</p> <ul style="list-style-type: none"> • Windows 8 (UEFI) • Windows 8,1 (UEFI) • Windows Server 2012 (UEFI) • Windows Server 2012 R2 (UEFI) • Windows Server 2016 (UEFI) <p>NOTE: Der Hyper-V-Export in eine VM der zweiten Generation kann fehlschlagen, wenn auf dem Hyper-V-Host nicht genügend RAM für die Durchführung des Exports zugewiesen wurde.</p> <p>Oracle VirtualBox:</p> <ul style="list-style-type: none"> • VirtualBox 4.2.18 und höher
Gast (exportiert) Betriebssystem	<p>Volumes unter 2 TB. Für geschützte Volumes unter 2 TB kann die VM (Gast) die gleichen unter dem Thema Rapid Recovery Agent-Softwareanforderungen beschriebenen unterstützten Betriebssysteme verwenden.</p> <p>Volumes über 2 TB. Wenn Sie einen virtuellen Export auf einem System durchführen möchten, bei dem die geschützten Volumes 2 TB überschreiten, verwenden Sie Windows 2012 R2, Windows Server 2016, VMware ESXi 5.5 oder VMware ESXi 6.0. Frühere Betriebssysteme werden aufgrund einer mangelnden Fähigkeit des Hosts, eine Verbindung mit dieser virtuellen Festplatte (VHD) herzustellen, nicht unterstützt.</p> <p>Hyper-V Generation 1 und Generation 2 VMs werden unterstützt.</p> <p>i NOTE: Nicht alle Betriebssysteme werden auf allen Hypervisoren unterstützt.</p>
Speicher	Der reservierte Speicher auf dem Host muss gleich oder größer als der Speicher in den Gast-VMs sein.
Architektur	32-Bit- oder 64-Bit-Version

Mit Rapid Recovery können Sie VM-Hosts ohne vorherige Installation der Rapid Recovery Agent-Software auf jedem einzelnen Gast schützen. Dies ist bekannt als agentenloser Schutz. Weitere Informationen, einschließlich

Ausnahmen für agentenlosen Schutz, finden Sie im *Rapid Recovery Benutzerhandbuch* unter „Grundlegendes zu Rapid Snap for Virtual“.

Der agentenlose Schutz wird wie in der folgenden Tabelle beschrieben unterstützt.

Tabelle 21. Hypervisor-Anforderungen mit Unterstützung für agentenlosen oder Host-basiertem Schutz

Die folgende Tabelle listet Hypervisor-Anforderungen speziell für den agentenlosen (oder Host-basierten) Schutz auf. In der ersten Spalte werden alle Anforderungen aufgelistet: Host für virtuelle Maschinen, BS, Speicher und Architektur. Die zweite Spalte gibt Details für jede Anforderung an.

Anforderung	Details
Host für virtuelle Maschinen	<p>VMware:</p> <ul style="list-style-type: none"> VMware vSphere auf ESXi 5.0 (Build 623860 oder höher), 5.1, 5.5, 6.0, 6.5. Sie sollten auch die neuesten VMware Tools auf jeden einzelnen Gast installieren. <p>i NOTE: Für den agentenlosen Schutz mit vSphere/ESXi Version 6.5 gelten die folgenden Einschränkungen:</p> <ul style="list-style-type: none"> ESXi 6.5 wurde um die neue Funktion „Secure Boot“ (Sicherer Start) erweitert. Diese Funktion wird demnächst von Rapid Recovery unterstützt. Zurzeit unterstützt Rapid Recovery keine virtuellen Exporte nach vCenter/ESXi 6.5, wenn auf dem Quellcomputer die Option „Sicherer Start“ verwendet wird. In ESXi 6.5 wurde die Unterstützung für verschlüsselte virtuelle Maschinen hinzugefügt. Für diese Funktion ist jedoch Virtual Disk Development Kit (VDDK) Version 6.5 erforderlich. Der agentenlose Schutz mithilfe von VDDK 6.5 wird voraussichtlich ab Rapid Recovery Version 7.0.0 unterstützt. Bis dahin wird der agentenlose Schutz verschlüsselter virtueller Maschinen in ESXi ab Version 6.5 von Rapid Recovery nicht unterstützt. Virtuelle Maschinen, die mit ESXi 6.5 agentenlos geschützt werden, können nicht übertragen werden, wenn der Übertragungsmodus auf „SAN“ (Storage Area Network) eingestellt ist. <p>i NOTE: Quest empfiehlt dringend die Ausführung auf der neuesten unterstützten VMware Version. Zukünftige Haupt-Releases unserer Software werden voraussichtlich ESXi 5.0 und 5.1 nicht unterstützen.</p> <p>Microsoft Hyper-V:</p> <ul style="list-style-type: none"> Windows Server 2012 R2 Windows Server 2016 Windows 8 x64 Windows 8,1 x64 Windows 10 x64
Betriebssystem	Für Sicherheit auf Volumestufe, müssen Volumes auf Gast-VMs müssen über GPT oder MBR Partitionstabellen verfügen. Wenn andere Partitionstabellen gefunden werden, erfolgt Schutz auf Datenträgerebene, nicht auf Volume-Ebene.
Speicher	Der reservierte Speicher auf dem Host muss gleich oder größer als der Speicher in den Gast-VMs sein.
Architektur	32-Bit- oder 64-Bit-Version

DVM-Repository-Anforderungen

Beim Erstellen eines Deduplication Volume Manager (DVM) Repositorys können Sie dessen Speicherort auf einem lokalen Speichervolume bzw. auf einen Datenträger-Volumen auf einem freigegebenen CIFS (Common Internet File System) Speicherort angeben. Wenn Sie das Repository lokal auf dem Core-Server erstellen, müssen Sie Ressourcen entsprechend zuweisen.

DVM-Repositorys müssen auf primären Speichergeräten gespeichert werden. Archivspeichergeräte, z. B. Data Domain-Geräte, werden aufgrund der beschränkten Leistung nicht unterstützt. Ebenso dürfen Repositorys nicht auf NAS-Dateiservern gespeichert werden, die an die Cloud gebunden sind, da diese Geräte zu Leistungseinschränkungen neigen, wenn sie als primärer Speicher verwendet werden.

Quest empfiehlt das Ausfindigmachen des Repository auf Direct Attached Storage(DAS)-, Storage Area Network(SAN)- oder Network Attached Storage(NAS)-Geräten. Sie sind in der bevorzugten Reihenfolge aufgeführt. Quest empfiehlt bei der Installation eines NAS die Beschränkung der Repository-Größe auf 6 TB. Alle Speichergeräte müssen die Mindest-Input/Output-Anforderungen erfüllen. Informationen zu diesen Anforderungen sowie zusätzliche Anleitung für die Dimensionierung von Hardware-, Software-, Arbeitsspeicher-, Speicher- und Netzwerkanforderungen finden Sie in der *Rapid Recovery Größeneinstellungsanleitung*, auf die unten verwiesen wird.

Bei der Erstellung eines DVM-Repository müssen Sie die Repository-Größe auf einem Volume angeben. Jedes DVM-Repository unterstützt bis zu 4096 Repository-Erweiterungen (zusätzliche Speicherplatz-Volumen).

Quest unterstützt keine Installation eines Rapid Recovery Core oder eines Repository für einen Core auf einem freigegebenen Clustervolumen (CSV).

Sie können mehrere DVM-Repositorys auf allen Volumes auf einem unterstützten physischen oder virtuellen Host installieren. Mit dem Installationsprogramm können Sie die Größe eines DVM Repositorys bestimmen.



NOTE: Sie können einen geplanten On-Demand-Bericht zur Überwachung der Größe erstellen, um die Größe und den Funktionszustand Ihres Repository zu überwachen. Weitere Informationen zum Erstellen eines Repository-Berichts finden Sie unter „Erstellen eines Berichts von der Core Console“ im *Rapid Recovery Benutzerhandbuch*.

Erstellen Sie immer das Repository in einem dedizierten Ordner oder Verzeichnis und nicht im Stammordner auf einem Volume. Beispiel: Bei einer Installation auf einem lokalen Pfad verwenden Sie `D:\Repository\` statt `D:\`. Es hat sich bewährt separate Verzeichnisse für Daten und Metadaten zu erstellen. Zum Beispiel `D:\Repository\Data` und `D:\Repository\Metadata`.

Weitere Informationen zur Verwendung von Rapid Recovery finden Sie im *Rapid Recovery Benutzerhandbuch*. Weitere Informationen zum Verwalten von Rapid Recovery Lizenzen finden Sie im *Rapid Recovery Lizenzportal Benutzerhandbuch*. Weitere Informationen zur Dimensionierung von Hardware-, Software-, Arbeitsspeicher-, Speicher- sowie Netzwerkanforderungen finden Sie in der *Rapid Recovery Größeneinstellungsanleitung*, auf die in Knowledge Base-Artikel 185962, „[Sizing Rapid Recovery Deployments](#)“ (Dimensionierung von Rapid Recovery Bereitstellungen), verwiesen wird.

Lizenzierungsanforderungen

Bevor Sie Rapid Recovery Komponenten installieren können, müssen Sie sich im Rapid Recovery Lizenzportal registrieren, ein Konto erstellen und einen Lizenzschlüssel oder eine Lizenzdatei anfordern, damit Sie die Rapid Recovery Core- und Rapid Recovery Agent-Software herunterladen sowie Maschinen konfigurieren und schützen können. Um den Core mit dem Lizenzportal zu registrieren, muss der Server über eine Internetverbindung verfügen und sich auf regelmäßiger Basis in das Lizenzportal einchecken können.

Weitere Informationen zum Rapid Recovery Lizenzportal, zum Abrufen eines Lizenzschlüssels und zur Registrierung für ein Konto finden Sie im *Rapid Recovery Lizenzportal Benutzerhandbuch*.

Quest Support-Richtlinien

Für Kunden mit einem gültigen Supportvertrag bietet Quest Support über Telefon und E-Mail für den aktuellen Haupt- und Neben-Release, sofern dieser auf die aktuelle Wartungsversion gepatcht wurde. Diese Version wird als N bezeichnet. Quest bietet außerdem vollständige Unterstützung für N - 1 und N - 2. Für Zwischenversionen steht nur eingeschränkte Unterstützung zur Verfügung.

Quest beschreibt seine Support-Richtlinien für den Produktlebenszyklus auf seiner Support-Website (rufen Sie <https://support.quest.com/de-de/rapid-recovery/> auf, klicken Sie auf **Richtlinien und Produktlebenszyklus** und erweitern Sie anschließend **Richtlinie für Software-Produktlebenszyklus**). Informationen zur vollständigen, eingeschränkten und eingestellten Unterstützung finden sie in den oben genannten Richtlinien.

Produktlizenzierung

Zum Verwenden und Verwalten einer beliebigen Version von Rapid Recovery, AppAssure oder der Backup and Recovery Gerätesoftware der Quest DL Serie benötigen Sie zwei Elemente:

- **Ein Konto beim Rapid Recovery Lizenzportal.**

Lizenzportal-Konten sind kostenfrei. Wenn Sie ein neuer Benutzer sind, registrieren Sie sich unter <https://licenseportal.com>. Verwenden Sie bei der Registrierung die E-Mail-Adresse, die Ihrem Quest Vertriebsbeauftragten bekannt ist. Wenn Sie ein Upgrade von einer Testversion durchführen, verwenden Sie die E-Mail-Adresse, die der Testversion zugeordnet ist. Wenn Sie eine andere E-Mail-Adresse verwenden müssen, wenden Sie sich an Ihren Quest Vertriebsbeauftragten, um Unterstützung zu erhalten.



NOTE: Dieses Lizenzportal erhielt kürzlich den neuen Markennamen. Wenn Sie bereits ein Lizenzportal-Konto für die Verwendung mit AppAssure oder Rapid Recovery registriert haben, nutzen Sie die Anmeldeinformationen für dieses Konto. Bisherige Benutzer des Lizenzportals müssen sich nicht für ein neues Konto für Rapid Recovery registrieren.

Weitere Informationen über das Lizenzportal finden Sie im *Benutzerhandbuch für das Rapid Recovery Lizenzportal* auf unserer [Dokumentationswebsite](#).

- **Eine Softwarelizenz** Die Verwendung von Rapid Recovery erfordert eine Lizenz. Sie können eine Testlizenz verwenden, sie hat eine begrenzte Laufzeit, oder Sie verwenden eine langfristige Lizenz (keine Testversion). Nach Ablauf des Testzeitraums erstellt der Rapid Recovery Core keine Snapshots mehr, bis Sie eine gültige Lizenz erwerben und registrieren.

Wenn Sie sich für eine Testversion von Rapid Recovery registriert haben, ist das Installationsprogramm mit einer Testlizenz konfiguriert, die Sie sofort verwenden können. Diese temporäre Testlizenz ist 14 Tage gültig und kann vom Gruppenadministrator einmalig auf 28 Tage verlängert werden.

Wenn Sie eine DL Backup and Recovery Appliance erworben haben, ist Ihre Appliance mit einer 30-tägigen temporären Lizenz konfiguriert, die automatisch beim ersten Starten von Core auf der Appliance aktiviert wird.

Nach dem Kauf von Software oder einer DL Appliance erhalten Sie per E-Mail eine langfristig gültige Lizenzdatei oder Lizenznummer (keine Testversion). Wenn dies auf dem Auftrag angegeben wurde, wird die Lizenz an die E-Mail-Adresse des Endbenutzers gesendet. Andernfalls wird die langfristige Lizenz an die Kontakt-E-Mail-Adresse auf dem Auftrag gesendet.

So aktivieren Sie eine Testversion der Softwarelizenz:

Bei der Registrierung für eine Testversion wird in das Rapid Recovery Kernsoftware-Installationsprogramm eine Testlizenz geschrieben. Sie melden sich einfach bei Ihrem Lizenzportalkonto an und laden die Rapid Recovery Kernsoftware. Überprüfen Sie sorgfältig die, und installieren Sie einen Rapid Recovery Core. Sie können sofort damit beginnen, Maschinen zu schützen und zu sichern.

So aktivieren Sie eine erworbene kommerzielle Softwarelizenz (ohne eine Testlizenz):

Wenn Sie eine Softwarelizenz erworben haben und nicht mit einer Testlizenz gestartet haben, werden Sie in der Core Console nach der Installation des Rapid Recovery Core nach der Lizenz gefragt. Geben Sie die

Lizenznummer ein oder suchen Sie nach der Lizenzdatei, die Ihnen bei der Bestellung per E-Mail bereitgestellt wurde. Weitere Informationen dazu finden Sie unter **Aktualisieren oder Ändern einer Lizenz** im *Rapid Recovery Benutzerhandbuch*.

So aktivieren Sie eine DL Appliance Lizenz:

Jede Quest DL Series Appliance enthält eine 30-tägige Lizenz, die automatisch beim ersten Starten von Core auf der Appliance aktiviert wird.

So aktualisieren Sie eine Testlizenz:

Aktualisieren Sie für die ununterbrochene Sicherung auf eine langfristige Lizenz, bevor die Testversion ausläuft. Sobald eine Testlizenz abläuft, hört der Rapid Recovery Core auf, Snapshots zu erstellen. Wenn Sie die Sicherungen wieder aufnehmen wollen, die durch das Fehlen einer Lizenz unterbrochen wurden, erwerben Sie eine langfristige Lizenz und geben Sie die Lizenzinformationen in der Core Console ein.

Core Console wird automatisch aus dem Lizenzpool entfernt, wenn 20 Tage lang nach Ablauf der Toleranzzeit keine Verbindung zwischen Core Console und dem Lizenzportal hergestellt wird. Sobald wieder eine Verbindung zum Lizenzportal besteht, wird Core Console im Lizenzportal automatisch wiederhergestellt.

Um eine Lizenzaktualisierung anzufordern, wenden Sie sich an Ihren Vertriebsmitarbeiter von Dell. Füllen Sie dazu das Online-Formular „Vertrieb kontaktieren“ unter <https://www.quest.com/register/95291/>. Nach der Aktualisierung oder dem Kauf Ihrer langfristigen Rapid Recovery Lizenz durch den Verkaufsberater, erhalten Sie eine E-Mail mit Ihrem neuen Lizenzschlüssel oder einer Lizenzdatei. Geben Sie diese Lizenzinformationen in der Core Console ein. Weitere Informationen dazu finden Sie unter **Aktualisieren oder Ändern einer Lizenz** im *Rapid Recovery Benutzerhandbuch*.

Zum Hinzufügen einer Lizenz zu einer Sicherungs- und Wiederherstellungs-Appliance der DL Serie siehe **Hinzufügen einer Lizenz** im *Rapid Recovery Benutzerhandbuch*.

Erste Schritte mit Rapid Recovery

Diese Themen enthalten Informationen, die Sie verwenden können, um mit dem Schutz Ihrer Daten mit Rapid Recovery zu beginnen.

Folgende Themen werden behandelt:

- [Aktualisierungs- und Installationsanweisungen](#)
- [Weitere Ressourcen](#)

Aktualisierungs- und Installationsanweisungen

Quest empfiehlt Benutzern, das *Rapid Recovery Installations- und Aktualisierungshandbuch* vor Installation oder Aktualisierung sorgfältig zu lesen und zu verstehen. Lesen Sie insbesondere bei der Aktualisierung alle Themen im Kapitel **Upgrade auf Rapid Recovery**. Lesen Sie bei neuen Installationen alle Themen im Kapitel **Installation von Rapid Recovery**.

Außerdem empfiehlt Quest, dass Benutzer vor einer Aktualisierung sorgfältig die Versionshinweise für jede Version prüfen sowie die jeweilige Version. Dieser Prozess hilft bei der Identifizierung und schließt potenzielle Probleme aus. Da die Anmerkungen zu jeder Version die letzten Produktdokumente sind, die aktualisiert werden, stellen sie die beste Quelle dar, um die aktualisierten Systemanforderungen zu erfahren.

Führen Sie für eine Aktualisierung von AppAssure Core Version 5.4.3 oder Rapid Recovery Core Version 6.0.x oder 6.1.x die neueste Core-Installationssoftware auf dem Core-Server aus. Wenn Sie mit Replikation arbeiten, aktualisieren Sie immer den Zielkern vor dem Quellkern.

Führen Sie zum Schutz von Maschinen, auf denen die Agenten-Software ausgeführt wird, bei einem Upgrade von AppAssure Core Version 5.4.3 oder Rapid Recovery Core Version 6.0.x oder 6.1.x das neueste Installationsprogramm für Rapid Recovery Agent auf jeder Maschine aus, die Sie schützen möchten. Weitere Informationen dazu finden Sie unter **Schutz**.

Sie können auch die Funktion „Rapid Snap for Virtual“ verwenden, um virtuelle Maschinen auf unterstützten Hypervisor-Plattformen agentenlos zu schützen. Es gelten wichtige Einschränkungen. Weitere Informationen zu Vorteilen oder Einschränkungen für agentenlosen Schutz, finden Sie unter [Grundlegende Informationen zu Rapid Snap for Virtual](#) in der Ausgabe der Version 6.1 des *Rapid Recovery Benutzerhandbuchs*.

Gemäß der Richtlinie für Quest Software werden bei Rapid Recovery die zwei vorherigen/niedrigeren Versionen unterstützt. Beim Upgrade von einer älteren Version hat es sich bewährt, zuerst auf die vollständig unterstützte Version (in diesem Fall Rapid Recovery Core Version 6.0.2) oder die entsprechende Vorgängerversion (in diesem Fall AppAssure Core Version 5.4.3) zu aktualisieren. Anschließend können Sie das Installationsprogramm der Version 6.1.2 für die entsprechende Softwarekomponente von Rapid Recovery ausführen.



NOTE: Die Version 6.0.1 unterstützt keine lokalisierten Instanzen. Bei der Ausführung von AppAssure Core 5.4.3 in einer anderen Sprache als Englisch müssen Sie auf Rapid Recovery Core Version 6.0.2 oder neuer aktualisieren.

Details finden Sie im *Rapid Recovery Installations- und Aktualisierungshandbuch*.

Bei der Aktualisierung einer Linux-Maschine von AppAssure Agent auf Rapid Recovery Agent Version 6.x müssen Sie zuerst die AppAssure Agent-Software deinstallieren. Weitere Informationen und besondere Anweisungen finden Sie im *Rapid Recovery Installations- und Aktualisierungshandbuch*.

Zum Herunterladen der Rapid Recovery Core Software benötigen Sie ein registriertes Konto im [Lizenzportal](#). Eine erfolgreiche Registrierung ermöglicht Ihnen das Herunterladen der Software, eine sorgfältige Prüfung der, und die Installation eines Rapid Recovery Core.

Lizenzierung

Testversionen von Rapid Recovery Core enthalten möglicherweise einen temporären Lizenzschlüssel. Ein Lizenzschlüssel ist erforderlich, um unterbrechungsfreie Sicherungen, Replikation oder Datenwiederherstellung auszuführen. Weitere Informationen stehen zur Verfügung unter:

- Grundlegende Informationen über Lizenzschlüssel finden Sie im [Produktlizenzierung](#) Abschnitt der Versionshinweise.
- Weitere Informationen über die Verwaltung von Lizenzen des Rapid Recovery Core finden Sie unter [Verwalten von Lizenzen](#) im *Rapid Recovery Benutzerhandbuch*.
- Alle Informationen über Lizenzen finden Sie im *Rapid Recovery Lizenzportal-Benutzerhandbuch*.

Schutz

Zum Schutz physischer oder virtueller Maschinen (außer VMs auf VMware vSphere), müssen Sie die Rapid Recovery Agent-Software installieren. Sie können Rapid Recovery Agent im [Lizenzportal](#) für die Installation auf jeder Maschine, die Sie schützen möchten, herunterladen. Sie können für die zu schützenden Maschinen auch Agent bereitstellen, über einen ordnungsgemäß konfigurierten Rapid Recovery Core.

Bei Verwendung eines VMware vSphere Host für Ihren Kern und die geschützten Maschinen haben Sie in vielen Fällen die Möglichkeit, die Maschinen zu schützen, ohne Rapid Recovery Agent zu installieren. Wird der agentenlose Schutz verwendet, gelten einige Einschränkungen (besonders für SQL Server oder Exchange Server). Weitere Informationen zur Verschlüsselung finden Sie unter [Grundlegende Informationen zu agentenlosem Schutz](#) im *Rapid Recovery Benutzerhandbuch*.

Fügen Sie Ihre Maschinen zum Schutz auf dem Rapid Recovery Core mithilfe des Assistenten zum Schützen einer Maschine bzw. zum Schützen mehrerer Maschinen hinzu.



NOTE: Vor dem Schützen eines Clusters, müssen Sie zuerst ein Repository erstellen. Weitere Informationen dazu finden Sie unter [Erstellen eines DVM-Repository](#) im *Rapid Recovery Benutzerhandbuch*. Obwohl ein Repository auch erforderlich ist, um eine Maschine zu schützen, haben Sie die Option ein Repository im Workflow zum Schutz einer Maschine zu erstellen.

Weitere Ressourcen

Zusätzliche Informationen erhalten Sie in den folgenden Ressourcen:

- [Technische Dokumentation](#)
- [Videos und Lernprogramme](#)
- [Knowledge Base](#)
- [Ressourcen für den technischen Support](#)
- [Schulung und Zertifizierung](#)
- [Rapid Recovery Lizenzportal](#)

Globalisierung

Dieser Abschnitt enthält Informationen zum Installieren und Verwenden dieses Produkts in nicht englischsprachigen Konfigurationen (beispielsweise für Kunden außerhalb Nordamerikas). Dieser Abschnitt ersetzt nicht die anderen Angaben zu unterstützten Plattformen und Konfigurationen in der Produktdokumentation.

Diese Version ist für Unicode aktiviert und unterstützt alle Zeichensätze. In dieser Version sollten alle Produktkomponenten für die Verwendung derselben oder kompatibler Zeichenkodierungen konfiguriert und so installiert werden, dass sie dieselben Gebietsschema- und Regionsoptionen verwenden. Diese Version unterstützt die Verwendung in folgenden Regionen: Nordamerika, Westeuropa und Lateinamerika, Mittel- und Osteuropa, Fernost (Asien), Japan. Es wird bidirektionales Schreiben unterstützt (Arabisch und Hebräisch). Diese Version unterstützt komplexe Schriftzeichen (Mittelasien – Indien, Thailand).

Diese Version wurde für die folgenden Sprachen lokalisiert: Chinesisch (vereinfacht), Französisch, Deutsch, Japanisch, Koreanisch, Portugiesisch (Brasilien), Spanisch.

Diese Version umfasst die folgenden bekannten Funktionen oder Einschränkungen:

- Für Rapid Recovery ist Microsoft .NET Framework 4.5.2 erforderlich. AppAssure verwendet eine ältere .NET-Version. Es ist keine Herunterstufungsoption verfügbar. Wenn Sie von AppAssure auf Rapid Recovery aktualisieren und sich anschließend entscheiden eine frühere Version von AppAssure zu verwenden, müssen Sie eine neue Installation von AppAssure Core und Agent durchführen.
- Protokolle und KB-Artikel für Rapid Recovery sind nur auf Englisch verfügbar.
- Das Rapid Recovery Add-On für Kaseya ist nur auf Englisch verfügbar.
- Die technische Produktdokumentation für diese Version ist nur auf Englisch verfügbar, ausschließlich der Versionshinweise, die in allen der oben aufgelisteten Sprachen verfügbar sind.

Über uns

Mehr als nur ein Name

Wir befinden uns auf einer Mission: Informationstechnologie soll Sie bei Ihrer Arbeit noch weiter entlasten. Das ist der Grund dafür, dass wir Community-orientierte Softwarelösungen konzipieren, die Sie unterstützen und dafür sorgen, dass Sie weniger Zeit mit IT-Verwaltung aufwenden müssen und mehr Zeit für Unternehmensinnovationen haben. Wir helfen Ihnen bei der Modernisierung Ihres Rechenzentrums, bringen Sie schneller in die Cloud und bieten Ihnen das Know-how, die Sicherheit und die Barrierefreiheit, die Sie für das Wachstum Ihres datenorientierten Unternehmens benötigen. Zusammen mit der Einladung von Quest an die globale Community, Teil ihrer Innovation zu sein, und mit unserem entschlossenen Engagement, die

Kundenzufriedenheit sicherzustellen, bieten wir weiterhin Lösungen an, die für unsere Kunden heute einen wirklichen Unterschied machen, und wir blicken auf ein Erbe zurück, auf das wir stolz sein können. Wir stellen uns dem Status Quo und entwickeln uns zu einem neuen Software-Unternehmen. Als Ihr Partner arbeiten wir auch unerlässlich daran, dass Ihre Informationstechnologie für Sie und von Ihnen konzipiert wird. Das ist unsere Mission, und wir bringen Sie gemeinsam zu Ende. Willkommen bei einem neuen Quest. Wir möchten Sie zu Join the Innovation™ einladen.

Unsere Marke, unsere Vision. Gemeinsam.

Unser Logo zeigt unsere Geschichte: Innovation, Community und Support. Ein wichtiger Teil dieser Geschichte beginnt mit dem Buchstaben Q. Dabei handelt es sich um einen perfekten Kreis, der unsere Verpflichtung zu technologischer Präzision und Stärke widerspiegelt. Der Freiraum im Q selbst symbolisiert unsere Anforderung, die neue Community, das neue Quest um das fehlende Stück, nämlich Sie, zu ergänzen.

Kontaktaufnahme mit Quest

Für Vertriebs- oder andere Anfragen, besuchen Sie <https://www.quest.com/company/contact-us.aspx> oder wenden sich unter + 1-949-754-8000 telefonisch an uns.

Ressourcen für den technischen Support

Der technische Support steht Quest Kunden mit gültigem Servicevertrag sowie Kunden mit Testversionen zur Verfügung. Auf das Quest Support Portal können Sie unter <https://support.quest.com/de-de/> zugreifen.

Das Support Portal stellt Selbsthilfetools bereit, mit denen Sie Probleme schnell und eigenständig lösen können – 24 Stunden am Tag, 365 Tage im Jahr. Das Support-Portal bietet folgende Möglichkeiten:

- Einreichen und Verwalten einer Serviceanfrage
- Anzeigen von Knowledge Base-Artikeln.
- Registrieren für Produktbenachrichtigungen
- Herunterladen von Software und technischer Dokumentation
- Anzeigen von Anleitungsvideos
- Teilnehmen an Community-Diskussionen.
- Online mit Supporttechnikern chatten
- Anzeigen von Services, die Sie bei der Verwendung unseres Produkts unterstützen

Copyright © 2017 Quest Software Inc.

ALLE RECHTE VORBEHALTEN.

Dieses Handbuch enthält urheberrechtlich geschützte Informationen. Die im vorliegenden Handbuch beschriebene Software unterliegt den Bedingungen der jeweiligen Softwarelizenz oder Geheimhaltungsvereinbarung. Die Software darf nur gemäß den Bedingungen der Vereinbarung benutzt oder kopiert werden. Kein Teil dieses Handbuchs darf ohne schriftliche Genehmigung von Quest Software Inc. in irgendeiner Form oder auf irgendeine Weise vervielfältigt oder übertragen werden. Dies beinhaltet Fotokopien und Aufzeichnungen für einen anderen Zweck als die persönliche Nutzung durch den Käufer.

Die Informationen in diesem Dokument werden in Verbindung mit Quest Software Produkten bereitgestellt. Durch dieses Dokument bzw. in Verbindung mit dem Verkauf von Quest Software Produkten wird keine ausdrückliche oder stillschweigende Lizenz, weder durch Duldung noch anderweitig, für Rechte des geistigen Eigentums von Quest Software gewährt. SOFERN DURCH DIE BEDINGUNGEN UND BESTIMMUNGEN IN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT NICHT ANDERS ANGEGEBEN, ÜBERNIMMT QUEST SOFTWARE KEINERLEI HAFTUNG UND SCHLIESST JEDE VERTRAGLICHE ODER GESETZLICHE GARANTIE ODER GEWÄHRLEISTUNG FÜR IHRE PRODUKTE AUS, WIE UNTER ANDEREM DIE GESETZLICHE GEWÄHRLEISTUNG HINSICHTLICH MARKTGÄNGIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHTVERLETZUNG VON RECHTEN DRITTER. UNTER KEINEN UMSTÄNDEN HAFTET QUEST SOFTWARE FÜR UNMITTELBARE, MITTELBARE, NACHFOLGENDE, BESONDERE ODER BEILÄUFIG ENTSTANDENE SCHÄDEN ODER STRAFSCHADENERSATZ (WIE UNTER ANDEREM SCHÄDEN IN BEZUG AUF ENTGANGENE GEWINNE, GESCHÄFTSUNTERBRECHUNGEN ODER DATENVERLUST), DIE SICH DURCH DIE NUTZUNG ODER UNFÄHIGKEIT DER NUTZUNG DIESES DOKUMENTS ERGEBEN,

SELBST WENN QUEST SOFTWARE ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE. Quest Software macht keine Zusicherungen oder Gewährleistungen bezüglich der Richtigkeit oder Vollständigkeit der Inhalte dieses Dokuments und behält sich das Recht vor, jederzeit und ohne vorherige Ankündigung Änderungen an den Spezifikationen und Produktbeschreibungen vorzunehmen. Quest Software übernimmt keine Verpflichtung zur Aktualisierung der in diesem Dokument enthaltenen Informationen.

Bei Fragen zur möglichen Verwendung dieser Materialien wenden Sie sich an:

Quest Software Inc., Attn: LEGAL Dept., 4 Polaris Way, Aliso Viejo, CA 92656.

Informationen zu regionalen und internationalen Niederlassungen finden Sie auf unserer Website (<https://www.quest.com/de-de>).




Patente

Quest Software ist stolz auf seine fortschrittliche Technologie. Für dieses Produkt gelten möglicherweise Patente und angemeldete Patente. Die aktuellsten Informationen über die entsprechenden Patente zu diesem Produkt finden Sie auf unsere Website unter <https://www.quest.com/de-de/legal/>.

Marken

Quest, das Quest Logo und Join the Innovation sind Marken und registrierte Marken von Quest Software Inc. Eine vollständige Liste der Marken von Quest finden Sie unter <https://www.quest.com/legal/trademark-information.aspx>. Alle anderen Marken und registrierten Marken sind Eigentum ihrer jeweiligen Inhaber.

Legende

-  **CAUTION:** Das Symbol VORSICHT weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.
-  **WARNING:** Das Symbol WARNUNG weist auf mögliche Personen- oder Sachschäden oder Schäden mit Todesfolge hin.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** Ein Informationssymbol weist auf Begleitinformationen hin.