Quest™

DL1300 Appliance

Versionshinweise

Inhaltsverzeichnis

Einführung:

Dieses Dokument enthält wichtige Produktinformationen und zusätzliche Informationen für die Quest DL1300 Appliance.

HINWEIS: Weitere Informationen über die neuen Funktionen in dieser Version finden Sie im Quest DL1300 Appliance-Bereitstellungshandbuch unter quest.com/support/manuals.

Über Rapid Recovery Software

Die Rapid Recovery Software bietet gegen Null tendierende Wiederherstellungszeiten und Wiederherstellungspunkte. Die Rapid Recovery Software bietet nicht nur Datenrettung, sondern Datenlösungen für die Datenmigration und -verwaltung. Es bietet Ihnen die Flexibilität für die Durchführung von Bare-Metal-Wiederherstellung (auf ähnliche oder unterschiedliche Hardware), und Sie können Sicherungen auf physischen oder virtuellen Maschinen, unabhängig von ihrem Ursprung, wiederherstellen. Die Rapid Recovery Software kann ebenfalls eine Archivierung in der Cloud, in einer Quest DL Series Backup and Recovery Appliance oder in einem unterstützten System Ihrer Wahl vornehmen. Mit der Rapid Recovery Software können Sie auf ein oder mehrere Ziele für zusätzliche Redundanz und Sicherheit replizieren.

Weitere Informationen hierzu finden Sie unter: https://support.quest.com/de-de.

Weitere nützliche Informationen

HINWEIS: Wenn auf der Website support.quest.com/de-de aktualisierte Dokumente vorliegen, lesen Sie diese immer zuerst, denn frühere Informationen werden damit gegebenenfalls ungültig.

HINWEIS: Lesen Sie für sämtliche Dokumentation im Zusammenhang mit Dell OpenManage Server Administrator die Seite dell.com/support.

Die Produktdokumentation beinhaltet:

Handbuch zum Einstieg

Stellt eine Übersicht über die Systemfunktionen, das Einrichten des Systems und die technischen Spezifikationen bereit. Dieses Dokument ist auch im Lieferumfang Ihres Systems enthalten.

Benutzerhandbuch

Bietet Informationen zu Systemfunktionen, zur Fehlerbehebung am System und zur Installation oder zum Austausch von Systemkomponenten.

Bereitstellungshandbuch

Enthält Informationen zur Hardwarebereitstellung und zur Erstbereitstellung der Appliance.

Benutzerhandbuch

Enthält Informationen über die Konfiguration und die Verwaltung des Systems.

OpenManageServer Administrator Benutzerhandbuch

Enthält Informationen über die Verwendung von Dell OpenManage Server Administrator zur Verwaltung des Systems.

System-Platzset

Enthält Informationen zum Einrichten der Hardware und Installieren der Software auf Ihrer Lösung.

HINWEIS: Die System-Platzsetinformationen finden Sie im Handbuch zum Einstieg.

Resource-Medium

Alle im Lieferumfang des Systems enthaltenen Medien mit Dokumentationen und Hilfsmitteln zur Konfiguration und Verwaltung des Systems, insbesondere in Bezug auf Betriebssystem, Systemverwaltungssoftware, System-Updates und mit dem System erworbene Komponenten.

Interoperabilitätshandbuch

Enthält Informationen zu unterstützter Software und Hardware für die DL1300 Appliance sowie Überlegungen, Empfehlungen und Richtlinien zur Nutzung.

Bekannte Probleme und Einschränkungen

Bekannte Probleme und Einschränkungen

Folgende Tabelle führt bekannte Probleme, Problemumgehungen, alte Problem-IDs, neue Problem-IDs, Funktionsbereiche und Siebel-IDs auf.

Bekanntes Problem	Alte Problem-ID	Neue Problem-ID	Funktionsbereich	Siebel-ID
Die Schaltflächen VM starten/Netzwerkadapter sollten deaktiviert sein, wenn der ESX(i)-/Hyper-V-Export der Maschine auf der Appliance gestartet wurde. Problemumgehung: Klicken Sie keine dieser Schaltflächen an, bis der entsprechende VM-Export abgeschlossen ist.	30989	96366	Verwaltung der virtuellen Maschine	--
In einigen Fällen wird die Fehlermeldung Ungültiger Status; bereits geöffnet auf der Registerkarte für virtuelles Standby für DL4x00 Appliances angezeigt. Problemumgehung: Schließen Sie die Fehlermeldung. Wenn das Problem weiterhin besteht, laden Sie die Seite durch Klicken auf F5 neu.	31477	96797	Verwaltung der virtuellen Maschine	--
Die VD-Festplattenbereitstellung schlägt fehl	34937	99967	Speicherbereitstellung	3882937-1

Bekanntes Problem	Alte Problem-ID	Neue Problem-ID	Funktionsbereich	Siebel-ID
und gibt Code 4 zurück, wenn der Speicherpool nicht über einheitlich leeren Speicherplatz verfügt Problemumgehung: Wenden Sie sich an den Support.				
Falsche Übersetzung von „State“ in einigen Lokalisierungen der Tabelle (Abschnitt Gesicherte Elemente) auf der Registerkarte Sicherung. Problemumgehung: Keine Problemumgehung.	35031	100061	Lokalisierung	--
Die Überwachung der aktiven Aufgabe bleibt während der Erstellung eines RASR USB-Auftrags bei 95 % hängen. Problemumgehung: Der Auftrag hat sich nicht aufgehängt. Er wird erfolgreich abgeschlossen. Die GUI gibt jedoch in einigen Fällen nicht an, dass der Auftrag bereits abgeschlossen wurde. Aktualisieren Sie die GUI.	35531	100551	RASR	--
Nach Bestätigung der erneuten Bereitstellung sollte die GUI umgehend deaktiviert werden. Problemumgehung: Warten Sie ein paar Minuten und	35579	100599	Speicherbereitstellung	--

Bekanntes Problem	Alte Problem-ID	Neue Problem-ID	Funktionsbereich	Siebel-ID
aktualisieren Sie die Seite für die Core Console.				
Es stehen VMM-Aktionen zur Verfügung, wenn der ESXi-Host sich im Wartungsmodus befindet. Problemumgehung: Führen Sie keine VM-Vorgänge über die Registerkarte Virtual Standby aus, wenn der ESXi-Host sich im Wartungsmodus befindet.	35740	100758	Verwaltung der virtuellen Maschine	--
Falsches Verhalten der Logik zum Ermitteln der Bereitstellungsgröße. Problemumgehung: Geben Sie bei der Bereitstellung für die Größe einige GB weniger an, als tatsächlich an Speicherplatz zur Verfügung stehen.	35770	100787	Speicherbereitstellung	--
Die Core-Schnittstelle ist nicht mehr verfügbar, wenn die Erfassung von Core- und Appliance-Protokollen erzwungen wird. Problemumgehung: Aktualisieren Sie die Seite, damit die GUI wieder verfügbar ist.	keine Angabe	100904	Benutzeroberfläche	--
Die Aufträge „Speicherbereitstellung“ und „Bereitstellungskonfiguration wiederherstellen“ können gleichzeitig gestartet werden,	keine Angabe	100907	Speicherbereitstellung	--

Bekanntes Problem	Alte Problem-ID	Neue Problem-ID	Funktionsbereich	Siebel-ID
obwohl das gleichzeitige Starten dieser Aufträge inkompatibel ist. Problemumgehung: 1) Entfernen Sie die erstellte virtuelle Festplatte Repository 2 mithilfe von OMSA. 2) Starten Sie den Core-Dienst neu.				
Es kann kein Windows-Backup erstellt werden, da die notwendigen Volumenelemente für eine Sicherung nicht richtig festgelegt werden, wenn Volumenbuchstaben geändert wurden. Problemumgehung: Entfernen Sie die aktuelle Richtlinie zu gemischten/ geänderten Buchstaben für Partitionen und erstellen Sie eine neue Richtlinie.	keine Angabe	100985	Windows-Backup	--
Der Status von Volumen wird als Ungültig angezeigt, wenn der Wiederherstellungspartition ein Buchstabe zugewiesen ist. Problemumgehung: Warten Sie, bis die RASR USB-Erstellung abgeschlossen ist.	keine Angabe	101224	Speicherbereitstellung	--
Aufträge auf der DL Appliance schlagen nach einiger Zeit mit der Meldung Ausnahme:	keine Angabe	101246	Virtueller Export	3830465-1, 3791536-1, 3825434-1

Bekanntes Problem	Alte Problem-ID	Neue Problem-ID	Funktionsbereich	Siebel-ID
Systemspeicher voll fehl. Problemumgehung: Wenden Sie sich an den Support.				
Eine erneute Bereitstellung des Auftrags wird die Core-Lokalisierung nicht wiederhergestellt. Problemumgehung: Ändern Sie die Core-Lokalisierung manuell in den Core-Einstellungen.	keine Angabe	101316	Speicherbereitstellung	-
Das Wiederherstellen des Bereitstellungskonfigurationsauftrags schlägt mit dem nicht informativen Fehler „Volumen kann nicht in Ordner ‚I:\‘ bereitgestellt werden, da er Dateien oder Ordner enthält“ fehl, wenn die virtuelle Festplatte denselben Buchstaben trägt, der bereits vor der erneuten Bereitstellung verwendet wurde. Problemumgehung: Entfernen Sie mithilfe des Festplatten-Managers zugewiesene Buchstaben von verbundenen virtuellen Medien. Führen Sie die erneute Volumenbereitstellung über die Appliance-Bereitstellungsseite erneut durch.	35805	100822	Speicherbereitstellung	-

Bekanntes Problem	Alte Problem-ID	Neue Problem-ID	Funktionsbereich	Siebel-ID
Beim Versuch der Anmeldung mit den Anmeldeinformationen des lokalen Administrators wird der Fehler „Einschränkungen“ angezeigt, nachdem die Appliance in die Domain integriert und FTBU abgeschlossen wurde. Problemumgehung: Melden Sie sich mit den Anmeldeinformationen des Domain-Administrators beim Betriebssystem an.	35828	100845	DL Appliance-Konfigurationsassistent	--
Der Bereitstellungsauftrag schlägt mit einem Fehler fehl, wenn der Repository-Name drei aufeinanderfolgende Punkte enthält. Problemumgehung: Verwenden Sie im Repository-Namen nicht drei aufeinanderfolgende Punkte.	keine Angabe	100913	Speicherbereitstellung	--
Der erste Start von Core nach FTBU ist aufgrund des Kompatibilitätsmodus im Browser nicht erfolgreich, wenn der Server während FTBU neu gestartet wurde. Problemumgehung: Schließen Sie den Browser und starten Sie Core erneut.	keine Angabe	101313	DL Appliance-Konfigurationsassistent	--
FTBU stürzt beim Start ab, wenn ein bootfähiges	keine Angabe	101457	DL Appliance-Konfigurationsassistent	--

Bekanntes Problem	Alte Problem-ID	Neue Problem-ID	Funktionsbereich	Siebel-ID
Medium mit einer System-EFI-Partition verwendet wird, die mit einem Server verbunden ist. Problemumgehung: Verbinden Sie keine externen Medien mit dem Appliance-Server, bis FTBU erfolgreich abgeschlossen wurde.				
Core wird mit einem Fehler geöffnet, der angibt, dass einige Dienste nach FTBU auf DL1300 nicht initialisiert werden konnten. Problemumgehung: Starten Sie den Server neu.	keine Angabe	101487	DL Appliance-Konfigurationsassistent	--
Beim Versuch, den Core-Dienst zu starten, der sich bereits im Status „Wird gestartet“ befindet, schlägt FTBU fehl. Problemumgehung: Starten Sie den Server erneut.	keine Angabe	101554	DL Appliance-Konfigurationsassistent	--

Rapid Recovery Systemanforderungen

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

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 Empfehlungen beruhen auf typischen Netzwerkanforderungen einer Netzwerkinfrastruktur zur Unterstützung der gesamten Geschäftsprozesse zusätzlich zu Sicherungs-, Replikations- und Wiederherstellungsfunktionen, die Rapid Recovery bietet.

Unterstützung für UEFI und ReFS

Unified Extensible Firmware Interface (UEFI - Vereinheitlichte erweiterbare Firmware-Schnittstelle) ist ein Ersatz für Basic Input/Output System (BIOS). UEFI wird in Windows 8 und Windows 8.1, Windows 10, Windows Server® 2012 und Windows Server 2012 R2 sowie Windows Server 2016 verwendet. 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.

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

Rapid Recovery unterstützt auch UEFI für geschützte Maschinen mit den Linux® Distributionen, die wir unterstützen. Hierzu zählen Red Hat® Enterprise Linux® (RHEL®), CentOS™, Debian ®, Ubuntu®, SUSE® Enterprise Linux (SLES®) und Oracle® Linux.

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.

  > **!** VORSICHT: 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 Repositorys auf komplexen dynamischen Volumes (Stripeset-Volumes, gespiegelte Volumes, übergreifende Volumes oder RAID 1-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 ermöglicht Ihnen den Schutz, die Wiederherstellung, das Replizieren und Archivieren von virtuellen Maschinen, die auf freigegebenen Clustervolumes (CSVs) gehostet werden, die auf Windows

Server 2012, Windows Server 2012 R2 und Windows Server 2016 mit der Agenten-Software Rapid Recovery ausgeführt werden.

Bei CSVs, die auf Windows Server 2008 R2 ausgeführt werden, unterstützt Rapid Recovery natives Backup. Sie können CSVs von einem Wiederherstellungspunkt aus wiederherstellen oder einen virtuellen Export zu einem Hyper-V-CSV ausführen. Es gibt keinen Support für freigegebene Clustervolumes, die auf früheren Windows-Betriebssystemen wie Windows 2008 ausgeführt werden.

Rapid Recovery unterstützt den virtuellen Export eines geschützten freigegebenen Clustervolumes unter Verwendung des Rapid Recovery-Agents.

Im Gegensatz dazu besteht in Rapid Recovery Version 6.1 die Möglichkeit, einen virtuellen Export zu einem Hyper-V-CSV, der auf Windows Server 2012, Windows Server 2012 R2 oder Windows Server 2016 ausgeführt wird, durchzuführen.

Bei anderen Betriebssystemen kann der Rapid Recovery-Agentendienst auf allen Knoten in einem Cluster ausgeführt werden und das Cluster kann als Cluster im Rapid Recovery Core geschützt werden. Freigegebene Clustervolumes werden jedoch nicht in der Core Console angezeigt und können nicht geschützt werden. Alle lokalen Datenträger (z. B. das Betriebssystemvolume) können geschützt werden.

Die folgende Tabelle veranschaulicht die derzeitige Unterstützung im Rapid Recovery Core für freigegebene Clustervolumes, die mit dem Rapid Recovery-Agent geschützt werden.

Die Unterstützung von Rapid Recovery für freigegebene Clustervolumes auf geschützten Computern mit dem Rapid Recovery-Agent

Die folgende Tabelle veranschaulicht die derzeitige Unterstützung im Rapid Recovery Core für freigegebene Clustervolumes, die mit dem Rapid Recovery-Agent geschützt werden.

Rapid Recovery Unterstützung für freigegebene Cluster-Volumes	Schutz, Replikation, Rollup, Einbinden und Archivbereitstellung		Wiederherstellung von freigegebenen Clustervolumes		Virtueller Export in freigegebenes Hyper-V-CSV	
Rapid Recovery-Version	6.0.x	6.1	6.0.x	6.1	6.0.x	6.1
Windows Server 2008 R2	Ja	Ja	Ja	Ja	Ja	Ja
Windows Server 2012	Nein	Nein	Nein	Nein	Ja	Ja
Windows Server 2012 R2	Nein	Nein	Nein	Nein	Ja	Ja
Windows Server 2016	Nein	Nein	Nein	Nein	Nein [1]	Ja

[1] Windows Server 2016 wurde nicht für die Rapid Recovery-Version 6.0.x getestet und wird daher nicht unterstützt.

Bei der Verwendung des Hyper-V-basierten Schutzes unterstützt Rapid Recovery Version 6.1 den Schutz von VMs auf freigegebenen Clustervolumes, auf denen Windows Server 2012, Windows Server 2012 R2 und Windows Server 2016 ausgeführt werden. Es werden nur die VMs, nicht die Volumes geschützt.

Unterstützung für freigegebene Clustervolumes unter Verwendung eines Host-basierten Schutzes auf Hyper-V

Die folgende Tabelle veranschaulicht die derzeitige Unterstützung im Rapid Recovery Core für freigegebene Clustervolumes, die über einen Host-basierten Schutz auf den Hyper-V-Gästen geschützt werden.

	Windows Server 2012	Windows Server 2012 R2	Windows Server 2016
Schutz, Replikation, Rollup, Einbinden und Archivieren von VMs auf CSV	Nein [1]	Ja	Ja
Wiederherstellen von VMs, die auf CSV gehostet sind	Nein [1]	Ja	Ja
Virtueller Export aus freigegebenem Hyper-V-CSV	Nein [1]	Ja	Ja
Virtueller Export in freigegebenes Hyper-V-CSV	Nein [1]	Ja	Ja

[1] Windows Server 2012 wird in diesem Szenario nicht unterstützt. Der komplette Support (und zukünftige Funktionen) für CSVs unter Verwendung des Host-basierten Hyper-V-Schutzes ist vorerst für Windows Server 2012 und höhere Betriebssysteme geplant.

Hypervisor-Unterstützung in Rapid Recovery

Im Allgemeinen schützt Rapid Recovery Gastsysteme virtueller Computer (wie KVM oder XenServer) mithilfe der Rapid Recovery Agent-Software.

Jeder geschützte Computer, der auf einem Hypervisor gehostet wird, muss die dokumentierten Systemanforderungen erfüllen oder übertreffen. Unter finden Sie die Anforderungen an Betriebssystem, Architektur, Speicher, Prozessor, Serveranwendung, Storage, Netzwerk und Netzwerk-Hardware.

Einzelne Hypervisoren können ebenfalls zu Einschränkungen bei der Unterstützung bestimmter Betriebssysteme führen. Siehe die entsprechende Dokumentation für die einzelnen relevanten Hypervisoren.

Für eine erfolgreiche Nutzung von Rapid Recovery ist die übergeordnete Anforderung, dass Cores korrekt dimensioniert sind und über ausreichend Ressourcen und Infrastruktur verfügen, um die Sicherung, Replikation und andere von Ihnen benötigte Funktionen zu unterstützen. Diese Ressourcen sind zusätzlich zu allen Anforderungen für den ursprünglichen Zweck der Computer zu sehen. Informationen zur Auslegung von Hardware-, Software-, Arbeitsspeicher-, Speicher-, Netzwerk- und Netzwerkhardware finden Sie im Knowledge Base-Artikel 185962, "Sizing Rapid Recovery Deployments" (Auslegung der Rapid Recovery-Bereitstellungen).

Die agentenlose Unterstützung für Hypervisoren in Rapid Recovery Version 6.0.2 ist auf VMware/ESXi beschränkt. Gast-Computer müssen andere Anforderungen erfüllen, z. B. die Installation von VMware Tools. Die agentenlose Unterstützung von Rapid Recovery Version 6.1 umfasst Host-basierte Unterstützung für Hyper-V, wo die Agenten-Software nur auf dem Host erforderlich ist. Weitere Informationen zur agentenlosen Unterstützung finden Sie unter Agentenloser Schutz Rapid Snap for Virtual.

Der virtuelle Export wird nur für VMware/ESXI-, Hyper-V- und VirtualBox-Hypervisoren und auf der Azure-Plattform unterstützt.

Lizenzanforderungen für den virtuellen Export-Hypervisor

Rapid Recovery Core unterstützt den virtuellen Export auf mehrere Hypervisor-Plattformen. Beim Export auf ESXi, Hyper-V oder VMware Workstation müssen Sie die Versionen mit vollem Lizenzumfang dieser Hypervisoren verwenden, nicht die kostenlosen Versionen.

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 die Core-Maschine nicht als Hypervisor-Host (außer wenn der Server eine entsprechend dimensionierte Quest DL Series Backup and Recovery Appliance 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 diese auch nicht aus. Wenn ein SQL Server auf dem Kern-Computer 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 Kern-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 Agentenloser Schutz Rapid Snap for Virtual.

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).

VORSICHT: 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.

HINWEIS: 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.

VORSICHT: Quest rät davon ab, den Rapid Recovery Core auf der derselben physischen Maschine zu installieren, die als Hyper-V-Host dient. (Diese Empfehlung gilt nicht für Backup and Recovery Appliances 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.

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

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

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

Windows-Betriebssystem	Core/ Central Management Console	Agent	Agentenlos	LMU	MR	DR	URC-Wiederherstellung	VM-Export 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 [3]
Windows 7 SP1	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja [3]
Windows 8	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja [3]
Windows 8,1	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja [3]
Windows 10	Ja [2]	Ja [2]	Ja [2]	Ja	Ja	Ja	Ja	Ja [3]
Windows Server 2003	Nein	Nein	Ja	Nein	Nein	Nein	Ja [1]	Nein

Windows-Betriebssystem	Core/Central Management Console	Agent	Agentenlos	LMU	MR	DR	URC-Wiederherstellung	VM-Export nach Azure
Windows Server 2008	Nein	Nein	Ja	Nein	Nein	Nein	Ja [1]	Ja [3]
Windows Server 2008 SP2	Ja	Ja	Ja	Ja	Ja	Ja	Ja [1]	Ja [3]
Windows Server 2008 R2	Nein	Nein	Ja	Nein	Nein	Nein	Ja	Ja [3]
Windows Server 2008 R2 SP1	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja [3]
Windows Server 2012	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja [3]
Windows Server 2012 R2	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja [3]
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] Im Allgemeinen funktionieren die Komponenten von AppAssure 5.4.x und Rapid Recovery 6.x unter Windows 10, es gibt jedoch zwei Ausnahmen:

- SCSI Controller-Treiber fehlen bei Computern mit Windows 10, die nach VirtualBox-Hypervisor exportiert wurden.

[3] 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.

Kompatible Rapid Recovery-Komponenten und Funktionen durch Linux-Betriebssystem

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

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 - 7.2	Ja	Ja	Ja
CentOS Linux 6.3 - 6.8	Ja	Ja	Ja
CentOS Linux 7.0 - 7.2	Ja	Ja	Ja
Debian Linux 7, 8	Ja	Ja	Ja
Oracle Linux 6.3 - 6.8	Ja	Ja	Ja
Oracle Linux 7.0 - 7.2	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 11 SP2 oder höher	Ja	Ja	Ja
SUSE Linux Enterprise Server 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 SUSE Linux Enterprise Server-Versionen 12 und 12 SP1 haben ältere Kernel-Versionen, entsprechend bietet Rapid Recovery keine Unterstützung für ihre Implementierungen von BTRFS.

Anforderungen für Rapid Recovery Kern 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.

Anforderungen für Rapid Recovery Core und Central Management Console

In der ersten Zeile der folgenden Tabelle werden die Anforderungen wie Betriebssystem, Architektur, Speicher, Prozessor, Storage, Netzwerk und Netzwerk-Hardware aufgeführt. In der zweiten Spalte befinden sich bestimmte Details zu jeder einzelnen Anforderung.

Anforderung	Details
Betriebssystem	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: • 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) 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. 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.

Anforderung	Details
	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. Für eine optimale Leistung wird empfohlen, den Rapid Recovery Core unter Windows 8.1 (oder höher) oder Windows Server 2012 (oder höher) zu installieren.
Architektur	Nur 64-Bit-Version
Arbeitsspeicher	Mindestens 8GB RAM Quest empfiehlt dringend, ECC-Speicher zu verwenden, um eine optimale Leistung der Rapid Recovery Core-Server sicherzustellen.
Prozessor	Quad-Core oder höher
Speicher	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). HINWEIS: Quest empfiehlt bei der Installation eines NAS die Beschränkung der Repository-Größe auf 6 TB. Alle Speichergeräte müssen die Mindes-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).
Netzwerk	mind. 1-GB-Ethernet (GbE) HINWEIS: Für stabile Umgebungen empfiehlt Quest ein 10-GbE-Backbonenetzwerk.
Netzwerkhardware	Verwenden Sie Netzwerkkabel mit der entsprechenden Nennleistung zum Abrufen der erwarteten Bandbreite. HINWEIS: Quest empfiehlt das regelmäßige Testen Ihrer Netzwerkleistung und das entsprechende Anpassen der Hardware.

Rapid Recovery Agent-Softwareanforderungen

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

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	Die Rapid Recovery Agenten-Software unterstützt 32-Bit- und 64-Bit-Windows- und Linux-Betriebssysteme. Dazu gehören: • 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 • CentOS Linux 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2 • Oracle Linux 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2 • 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

Anforderung	Details
	HINWEIS: 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 RecoveryVersion 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. HINWEIS: Native Sicherungen von freigegebenen Cluster-Volumes werden nur auf geschützten Windows 2008 R2-Maschinen (SP2 und höher) unterstützt.
Architektur	32-Bit- oder 64-Bit-Version

Anforderung	Details
Arbeitsspeicher	Mind. 4GB
Prozessor	Einzelprozessor oder höher
Microsoft Exchange Server Support	Microsoft Exchange Server 2007 SP1 Rollup 5 oder höher, Exchange Server 2010, Exchange Server 2013 oder Exchange Server 2016
Microsoft SQL Server Support	Microsoft SQL Server 2008 oder höher
Microsoft SharePoint	Microsoft SharePoint 2007, 2010, 2013, 2016
Speicher	Direkt angeschlossener Speicherplatz, Speicherbereichsnetzwerk oder Network Attached Storage
Netzwerk	mind. 1-GB-Ethernet (GbE) HINWEIS: Für stabile Umgebungen empfiehlt Quest ein 10-GbE-Backbonenetzwerk. 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.
Netzwerkhardware	Verwenden Sie Netzwerkkabel mit der entsprechenden Nennleistung zum Abrufen der erwarteten Bandbreite. HINWEIS: Quest empfiehlt das regelmäßige Testen Ihrer Netzwerkleistung und das entsprechende Anpassen der Hardware.

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.

Local Mount Utility Softwareanforderungen

In der folgenden Tabelle werden Anforderungen für das Local Mount Utility aufgelistet, die Rapid Recovery umfasst. In der ersten Zeile werden die Anforderungen wie Betriebssystem, Architektur, Speicher, Prozessor,

Netzwerk und Netzwerk-Hardware aufgeführt. In der zweiten Spalte befinden sich bestimmte Details zu jeder einzelnen Anforderung.

Anforderung	Details
Betriebssystem	Die Rapid Recovery Local Mount Utility Software unterstützt 32-Bit- und 64-Bit-Windows Betriebssysteme, einschließlich der Folgenden: • 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*
	HINWEIS: 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. 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 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.
Architektur	32-Bit- oder 64-Bit-Version
Arbeitsspeicher	Mind. 4GB
Prozessor	Einzelprozessor oder höher

Anforderung	Details
Netzwerk	mind. 1-GB-Ethernet (GbE) HINWEIS: Für stabile Umgebungen empfiehlt Quest ein 10-GbE-Backbonenetzwerk.
Netzwerkhardware	Verwenden Sie Netzwerkkabel mit der entsprechenden Nennleistung zum Abrufen der erwarteten Bandbreite. HINWEIS: Quest empfiehlt das regelmäßige Testen Ihrer Netzwerkleistung und das entsprechende Anpassen der Hardware.

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 dem Thema 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 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 Betriebssysteme 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 RecoveryVersion 6.1 Betriebssystem-Installations- und Kompatibilitätsmatrix zur Verfügung. Alle bekannten Einschränkungen sind in diesen Matrizen oder als Anmerkungen in den Softwareanforderungs-Tabellen für den Core oder den Agent 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-Volume 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.

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	VMware • VMware Workstation 7.0, 8.0, 9.0, 10, 11, 12 • VMware vSphere auf ESXi 5.0, 5.1, 5.5, 6.0 HINWEIS: 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. Microsoft Hyper-V HINWEIS: Für den virtuellen Export auf den Hyper-V-Host, sind .NET 4.5.2 und .NET 2.0 auf dem Hyper-V-Host erforderlich. • Erste Generation ◦ 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 ◦ Hyper-V, ausgeführt auf Microsoft Server 2012 R2, 2016 ◦ Hyper-V, ausgeführt auf Microsoft Windows 8.1, Windows 10

Anforderung	Details
	HINWEIS: Lediglich geschützte Maschinen mit den folgenden UEFI-Betriebssystemen (Unified Extensible Firmware Interface) unterstützen einen Export auf Hyper-V-Hosts der zweiten Generation: • Windows 8 (UEFI) • Windows 8,1 (UEFI) • Windows Server 2012 (UEFI) • Windows Server 2012 R2 (UEFI) • Windows Server 2016 (UEFI) HINWEIS: 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. Oracle VirtualBox • VirtualBox 4.2.18 und höher
Gast (exportiert) Betriebssystem	Volumes unter 2 TB. Für geschützte Volumes unter 2 TB kann die VM (Gast) die gleichen unter dem Thema beschriebenen unterstützten Betriebssysteme verwenden. 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. Hyper-V Generation 1 und Generation 2 VMs werden unterstützt. HINWEIS: Nicht alle Betriebssysteme werden auf allen Hypervisoren unterstützt.
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 schützen. Dies ist bekannt als agentenloser Schutz. Weitere Informationen, einschließlich Ausnahmen für agentenlosen Schutz, finden Sie im Rapid Recovery Benutzerhandbuch, Thema „Grundlegendes zu Rapid Snap for Virtual“.

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

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	VMware • VMware vSphere auf ESXi 5.0 (Build 623860 oder höher), 5.1, 5.5, 6.0. • Sie sollten auch die neuesten VMware Tools auf jeden einzelnen Gast installieren. HINWEIS: 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. Microsoft Hyper-V • 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-Volume 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 Mindes-Input/Output-Anforderungen erfüllen. Informationen zu diesen Anforderungen sowie eine zusätzliche Anleitung zur 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-Volumes).

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

HINWEIS: Sie können einen geplanten On-Demand-Bericht zur Überwachung der Größe erstellen, um die Größe und den Funktionszustand Ihres Repository zu überwachen. Weitere Informationen über das Erstellen eines Repositoryberichts finden Sie unter dem Thema „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.

Registrieren Ihres Geräts am Lizenzportal

1. Navigieren Sie in Ihrem Webbrowser zu dem Lizenzportal unter der Website-URL, die in der E-Mail aufgeführt wurde, die Sie beim Kauf erhalten haben.
2. Geben Sie auf der Seite *Registrieren* in das Textfeld E-Mail-Adresse die E-Mail-Adresse, die Ihrem Vertrag zugeordnet ist, ein.
3. Geben Sie die Lizenznummer für Ihr Gerät ein.

   Wenn Sie über mehrere Geräte verfügen, geben Sie eine Lizenznummer ein, und drücken Sie anschließend die Eingabetaste, um weitere Nummern einzugeben.
4. Klicken Sie auf **Aktivieren**.

   Wenn die E-Mail-Adresse, die Sie eingegeben haben, nicht auf dem Lizenzportal registriert ist (im Falle eines neuen Lizenzportal-Kontos), werden Sie aufgefordert, ein Konto im Lizenzportal unter Verwendung dieser E-Mail-Adresse zu erstellen.
5. Geben Sie die für die Erstellung eines Kontos erforderlichen Informationen im Lizenzportal ein.

   Nach der Registrierung sind Sie beim Lizenzportal angemeldet. Außerdem wird eine Aktivierungs-E-Mail an Ihre E-Mail-Adresse gesendet.
6. Es wird eine Benachrichtigung über die erfolgreiche Registrierung angezeigt, die zudem den Lizenzschlüssel angibt. Diese Benachrichtigung enthält folgende Anweisungen zur Anwendung des Lizenzschlüssels auf Ihre Appliance:
   a. Starten Sie die Core Console für Ihre Appliance.
   b. Gehen Sie zu **Konfiguration** → **Lizenzierung**.
   c. Klicken Sie auf **Lizenz ändern**.
   d. Kopieren und fügen Sie den Software-Lizenzschlüssels aus der Benachrichtigung der erfolgreichen Registrierung ein und speichern Sie die Änderungen.
7. Klicken Sie auf **OK**.

Weitere Informationen finden Sie unter Quest Softwarelizenz- und Produktvereinbarungen auf https://www.quest.com/de-de/legal/license-agreements.aspx.

HINWEIS: Wenn die genutzte Kapazität auf Ihrer DL Appliance die Kapazität übersteigt, für die Sie eine Lizenz erworben haben, wird die Snapshot-Funktion deaktiviert. Wenden Sie sich für weitere Unterstützung an Ihren Kundenbetreuer bei der Quest Software Group.

Wie Sie Hilfe bekommen

Kontaktaufnahme mit Quest

HINWEIS: Wenn Sie über keine aktive Internetverbindung verfügen, finden Sie Kontaktinformationen auf der Eingangsrechnung, dem Lieferschein, der Rechnung oder im Quest Produktkatalog.

Quest bietet verschiedene Optionen für Online- und Telefonsupport an. Wenn Sie über keine aktive Internetverbindung verfügen, finden Sie Kontaktinformationen auf der Eingangsrechnung, dem Lieferschein, der Rechnung oder im Quest Produktkatalog. Die Verfügbarkeit ist abhängig von Land und Produkt und einige Dienste sind in Ihrem Gebiet möglicherweise nicht verfügbar. Um sich mit Quest im Zusammenhang mit Verkauf, technischem Support und Kundendienst in Verbindung zu setzen, rufen Sie die Website support.quest.com/de-de auf.

Anmerkungen, Vorsichtshinweise und Warnungen

HINWEIS: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.

WARNUNG: Durch eine WARNUNG wird auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen kann.