Quest™

Rapid Recovery 6.2

Benutzerhandbuch

Inhaltsverzeichnis

Einführung in Rapid Recovery....14
Core Console....16
Zugriff auf die Rapid Recovery Core Console....16
Grundlegende Informationen zur Kurzanleitung....16
Ausblenden der Kurzanleitung....18
Navigieren der Rapid Recovery Core Console....19
Grundlegendes zum linken Navigationsbereich....20
Anzeigen der Startseite der Rapid Recovery Core Console....21
Grundlegende Informationen zur Startseite (Übersichtstabellenansicht)....21
Grundlegende Informationen zu Core-Dashboard-Berichten....24
Anzeigen des Menüs "Geschützte Maschinen"....25
Anzeigen von zusammenfassenden Informationen für eine geschützte Maschine....25
Anzeigen des Bereichs „Zusammenfassung“....26
Anzeigen von Volumes auf einer geschützten Maschine....26
Anzeigen von Replikationsinformationen....26
Anzeigen des Fensterbereichs „Exchange Server-Informationen“....26
Anzeigen des SQL Server-Informationsbereichs....27
Anzeigen von zusammenfassenden Informationen für einen Host....27
Anzeigen von Wiederherstellungspunkten für eine Maschine....27
Anzeigen von Ereignissen für eine geschützte Maschine....28
Anzeigen von Berichten für eine geschützte Maschine....30
Anzeigen von replizierten Maschinen über das Navigationsmenü....30
Anzeigen des Menüs „Nur Wiederherstellungspunkte“....31
Anzeigen des Menüs für benutzerdefinierte Gruppen....32
Verwendung des Fehlerdialogfelds....32
Core-Einstellungen....33
Hauptfunktionen von Core-Einstellungen....33
Sichern und Wiederherstellen der Core-Einstellungen....34
Neustarten oder Herunterfahren des Core-Dienstes....36
Rapid Recovery Core-Einstellungen....36
Konfigurieren von allgemeinen Core-Einstellungen....41
Konfigurieren von Updateeinstellungen....43
Grundlegende Informationen zu nächtlichen Jobs....45
Konfigurieren nächtlicher Jobs für den Core....48
Ändern der Einstellungen für die Übertragungswarteschlange....49
Anpassen der Client-Zeitlimiteinstellungen....49

Grundlegende Informationen zu Deduplizierungscache und Speicherorten....51
Konfigurieren von DVM-Deduplizierungscache-Einstellungen....52
Konfigurieren von Replay Engine-Einstellungen....54
Konfigurieren von Bereitstellungseinstellungen....55
Konfigurieren von Datenbankverbindungseinstellungen....56
Ändern der lokalen Einstellungen für Datenbankverbindung....58
Verwalten von SMTP-Servereinstellungen....59
Konfigurieren von Verbindungseinstellungen des Cloud-Kontos....59
Arbeiten mit Azure Management-Zertifikaten, die mit Ihrem Core verknüpft sind....60
Abrufen der Veröffentlichungseinstellungendatei für Ihr Azure Konto....60
Laden eines Azure Management-Zertifikats....61
Aktualisieren oder Löschen von Azure Management-Zertifikaten....61
Verwalten von Berichteinstellungen....62
Verwalten von Core-SQL-Anfügbarkeitseinstellungen....63
Grundlegende Informationen zu Core-Jobs....65
Core-Jobeinstellungen....69
Hinzufügen von Core-Jobs zu Einstellungen....70
Bearbeiten von Core-Jobeinstellungen....70
Verwalten von Lizenzen....71
Aktualisieren oder Ändern einer Lizenz....74
Hinzufügen einer Lizenz....75
Kontaktaufnahme mit dem Rapid Recovery Lizenzportal-Server....76
Grundlegende Informationen zu SNMP-Einstellungen....76
Konfigurieren der SNMP-Einstellungen....77
Herunterladen der SNMP MIB-Datei....78
Konfigurieren von vSphere-Einstellungen....79
Verwalten der VMware Proxy-Einstellungen....80
Konfigurieren von vFoglight-Einstellungen....81
Tools auf Core-Ebene....81
Grundlegende Informationen über Systeminformationen für den Core....82
Anzeigen von Systeminformationen für den Core....83
Zugriff auf Core-Protokolle....84
Herunterladen und Anzeigen der Core-Protokolldatei....84
Repositorys....85
Grundlegende Informationen zu Repositorys....85
Deduplizierung in Rapid Recovery....88
Verwalten eines DVM-Repositorys....89
Erstellen eines DVM-Repository....90

Hinzufügen eines Speicherorts zu einem vorhandenen DVM-Repository....93
Informationen über das Überprüfen der Integrität der DVM Repositorys....95
Ausführen einer Integritätsprüfung auf einem DVM-Repository....96
Informationen über DVM Repository-Optimierung....97
Optimierung eines DVM-Repositorys....98
Unterbrechen oder Wiederaufnehmen der DVM-Repository-Optimierung....99
Verwalten eines Tiering-Repository....99
Erstellen eines Tiering-Repositorys....100
Überprüfen eines Repositorys....102
Ändern der Repository-Einstellungen....103
Verbinden mit einem vorhandenen Repository....104
Anzeigen oder Ändern von Details zu einem Repository....106
Trennen eines Repository....109
Löschen eines Repositorys....109
Datenschutzverwaltung....110
Einhaltung der Datenschutz-Grundverordnung....110
Verwendung von personenbezogenen Daten durch Rapid Recovery....111
Einschränkungen der Non-Phone-Home-Lizenz....112
Erhalten und Verwenden von Non-Phone-Home-Lizenzen....113
Verschlüsselung....115
Grundlegende Informationen zu Verschlüsselungsschlüsseln....115
Verschlüsseln von Daten, die über ein Netzwerk transportiert werden....116
Anwenden oder Entfernen von Verschlüsselungsschlüsseln....117
Zuordnen eines Verschlüsselungsschlüssels zu einer geschützten Maschine....117
Anwenden eines Verschlüsselungsschlüssels auf der Seite „Geschützte Maschinen“....118
Aufheben der Verschlüsselungsschlüsselzuordnung für eine geschützte Maschine....120
Verwalten von Verschlüsselungsschlüsseln....120
Hinzufügen eines Verschlüsselungsschlüssels....122
Importieren eines Verschlüsselungsschlüssels....123
Entsperren eines Verschlüsselungsschlüssels....124
Sperren eines Verschlüsselungscodes....125
Bearbeiten eines Verschlüsselungsschlüssels....126
Ändern der Passphrase für einen Verschlüsselungsschlüssel....126
Exportieren eines Verschlüsselungsschlüssels....127
Entfernen eines Verschlüsselungsschlüssels....128
Ändern von Verschlüsselungsschlüsseltypen....128
Schützen von Maschinen....130
Informationen über den Schutz von Maschinen mit Rapid Recovery....130

Faktoren bei der Wahl zwischen agentenbasiertem und agentenlosem Schutz..... 131
Informationen über den Schutz von Linux-Computern mit Rapid Recovery.....133
Informationen zum Schützen von Oracle Datenbankservern..... 134
Eingeben oder Bearbeiten der Anmeldeinformationen für Oracle Datenbanken..... 135
Aktivieren des Archivprotokoll-Modus und Hinzufügen von VSS Writer für geschützte Oracle Datenbanken..... 137
Informationen zum Kürzen von Oracle Protokollen..... 138
Manuelles Kürzen der Oracle Datenbankprotokolle..... 138
Informationen über das Verwalten von Anwendungsservern in Rapid Recovery Core..... 139
Schützen von Server-Clustern.....140
Grundlegende Informationen zu Rapid Snap for Virtual.....141
Vorteile der Installation von Hypervisor-Tools für agentenlosen Schutz.....145
Grundlegende Informationen zu absturzsicheren und anwendungskonsistenten Sicherungen.....146
Grundlegende Informationen zum Installationsprogramm der Rapid Recovery Agentensoftware..... 146
Herunterladen des Rapid Recovery Agent Installers..... 147
Bereitstellen des Agenten auf mehreren Maschinen gleichzeitig aus der Core Console..... 147
Verwendung des Bereitstellungsassistenten für die Agentensoftware zum Bereitstellen einer oder mehrerer Maschinen..... 148
Bereitstellung auf Maschinen in einer Active Directory-Domäne.....149
Bereitstellung auf Maschinen auf einem virtuellen VMware vCenter/ESXi-Host..... 150
Bereitstellung einer Erweiterung der Rapid Recovery-Agentensoftware auf geschützten Maschinen..... 152
Manuelles Bereitstellen auf Maschinen..... 152
Überprüfen der Bereitstellung auf mehreren Maschinen.....153
Ändern von Bereitstellungseinstellungen.....154
Grundlegende Informationen zu Schutzzeitplänen.....155
Schützen einer Maschine..... 156
Schützen eines Clusters..... 162
Schützen von Knoten in einem Cluster..... 167
Erstellen von benutzerdefinierten Schutzzeitplänen im einfachen Modus.....168
Erstellen mehrerer Schutzzeitplan-Zeiträume im erweiterten Modus..... 169
Vorübergehendes Deaktivieren und erneutes Aktivieren der Schutzfunktion.....171
So schützen Sie mehrere Maschinen..... 173
Schutz mehrerer Maschinen in einer Active Directory-Domäne.....174
Schutz von mehreren Maschinen auf einem virtuellen VMware vCenter/ESXi-Host.....179
Schutz von virtuellen vCenter/ESXi-Maschinen mit agentenlosem Schutz..... 184
Schutz von mehreren Maschinen auf einem virtuellen Hyper-V-Host..... 189
Schutz von virtuellen Hyper-V-Maschinen mit agentenlosem Schutz..... 195

Manuelles Schützen mehrerer Maschinen..... 200
Überwachen des Schutzes von mehreren Maschinen..... 204
Aktivieren des Anwendungssupports..... 205
Einstellungen und Funktionen für geschützte Exchange-Server..... 206
Festlegen der Anmeldeinformationen für eine Exchange Server-Maschine..... 207
Erzwingen einer Protokollkürzung für eine Exchange-Maschine..... 207
Informationen über Überprüfungen der Bereitstellungsfähigkeit..... 208
Erzwingen einer Bereitstellbarkeitsprüfung für eine Exchange-Datenbank..... 208
Erzwingen einer Prüfsummen-Überprüfung von Exchange-Datenbank-Dateien..... 209
Einstellungen und Funktionen für geschützte SQL-Server..... 210
Festlegen der Anmeldeinformationen für eine SQL Server-Maschine..... 211
Erzwingen einer Protokollkürzung für eine SQL-Maschine..... 211
Über die SQL-Anfügbarkeit..... 212
Erzwingen einer SQL Server-Anfügbarkeitsprüfung..... 213
Verwalten geschützter Maschinen..... 214
Informationen über das Verwalten geschützter Maschinen..... 214
Anzeigen geschützter Maschinen..... 214
Anzeigen von Cluster-Übersichtsinformationen..... 215
Konfigurieren von Maschineneinstellungen..... 215
Anzeigen und Ändern von geschützten Maschineneinstellungen..... 216
Ändern der Einstellungen für einen Hyper-V-Host oder -Knoten..... 221
Ändern der Einstellungen für eine geschützte virtuelle Hyper-V-Maschine..... 222
Ändern der vSphere-Einstellungen für eine geschützte virtuelle VMware-Maschine..... 223
Informationen über das Ändern von Übertragungseinstellungen..... 224
Einschränkung der Übertragungsrate..... 224
Anpassen der nächtlichen Jobs für eine geschützte Maschine..... 226
Anzeigen von Systeminformationen für eine geschützte Maschine..... 226
Verwalten von Maschinen..... 227
Entfernen einer Maschine..... 227
Aufheben des Cluster-Schutzes..... 228
Aufheben des Schutzes von Cluster-Knoten..... 228
Aufheben des Schutzes aller Knoten in einem Cluster..... 228
Anzeigen von Lizenzinformationen für eine Maschine..... 229
Herunterladen und Anzeigen der Protokolldatei für eine geschützte Maschine..... 229
Konvertieren eines geschützten Cluster-Knotens in eine geschützte Maschine..... 230
Grundlegende Informationen zu benutzerdefinierten Gruppen..... 230
Erstellen von benutzerdefinierten Gruppen..... 231
Ändern der Namen von benutzerdefinierten Gruppen..... 232

Entfernen von benutzerdefinierten Gruppen....232
Durchführen von Gruppenaktionen....233
Anzeigen aller Maschinen in einer benutzerdefinierten Gruppe auf einer Seite....234
Snapshots und Wiederherstellungspunkte....235
Verwalten von Snapshots und Wiederherstellungspunkten....235
Anzeigen der Seite „Wiederherstellungspunkte“ einer geschützten Maschine....235
Grundlegende Informationen zu Statusanzeigen für Wiederherstellungspunkte....237
Bereitstellen eines Wiederherstellungspunkts....238
Aufheben der Bereitstellung von Wiederherstellungspunkten....239
Arbeiten mit Linux-Wiederherstellungspunkten....240
Bereitstellen eines Wiederherstellungspunkt-Volumes für eine Linux-Maschine....241
Aufheben der Bereitstellung eines Wiederherstellungspunkts auf einer Linux-Maschine....242
Erzwingen eines Snapshots....243
Entfernen von Wiederherstellungspunkten....244
Löschen einer verwaisten Wiederherstellungspunktkette....244
Migrieren von Wiederherstellungspunkten in ein anderes Repository....245
Replikation....247
Replikation mit Rapid Recovery....247
Wiederherstellungspunkt-Ketten und -Waisen....251
Wenn die Replikation startet....252
Bestimmen der Seeding-Anforderungen und -Strategie....252
Überlegungen zur Übertragungsleistung für Replikationsdaten....255
Informationen zu Replikation und verschlüsselten Wiederherstellungspunkten....256
Informationen zu Aufbewahrungsrichtlinien für die Replikation....256
Anzeigen von ein- und ausgehender Replikation....256
Konfigurieren der Replikation....259
Replikation auf einen selbstverwalteten Ziel-Core....260
Replikation auf den Ziel-Core eines externen Anbieters....264
Senden einer Replikationsanforderung an einen externen Dienstanbieter....264
Überprüfen einer Replikationsanforderung von einem Kunden....267
Genehmigen einer Replikationsanforderung....267
Ablehnen einer Replikationsanforderung....268
Ignorieren einer Replikationsanforderung von einem Kunden....269
Hinzufügen einer Maschine zu einer bestehenden Replikation....269
Konsumieren des Seed-Laufwerks auf einem Ziel-Core....272
Entfernen eines Seed-Laufwerks....273
Verwalten der Replikationseinstellungen....274
Planen der Replikation....274

Erstellen eines Seed-Laufwerks mit der Kopierfunktion....275
Überwachen der Replikation....277
Anhalten und Fortsetzen der Replikation....279
Erzwingen einer Replikation....280
Verwalten der Einstellungen für die ausgehende Replikation....281
Ändern der Ziel-Core-Einstellungen....282
Festlegen der Replikationspriorität für eine geschützte Maschine....282
Entfernen einer ausgehenden Replikation vom Quell-Core....283
Eingehende Replikation vom Ziel-Core entfernen....284
Wiederherstellen von replizierten Daten....285
Ereignisse....286
Anzeigen von Ereignissen mithilfe von Aufgaben, Warnungen und Journalseiten....286
Anzeigen von Aufgaben....287
Anzeigen von laufenden Tasks von einer beliebigen Core Console-Seite....289
Unterbrechen oder Wiederaufnehmen geplanter Aufgaben....289
Anzeigen von Benachrichtigungen....290
Anzeigen eines Journals aller protokollierten Ereignisse....291
Navigieren zwischen Aufgaben, Warnungen und dem Ereignisjournal....293
Grundlegendes zu Ereignisbenachrichtigungen in Rapid Recovery....294
Konfigurieren von Benachrichtigungsgruppen....295
Grundlegende Informationen zu E-Mail-Benachrichtigungen....299
Konfigurieren eines E-Mail-Servers....299
Konfigurieren einer E-Mail-Benachrichtigungsvorlage....301
Konfigurieren von Ereigniseinstellungen....304
Informationen zur Reduzierung von Wiederholungen....304
Konfigurieren der Reduzierung der Wiederholungen....305
Konfigurieren der Ereignisaufbewahrung....305
Berichterstellung....306
Informationen über Berichte von Rapid Recovery....306
Erstellen eines Berichts von der Core Console....308
Bedarfsweise Generierung eines Core-Berichts....308
Generieren eines bedarfsorientierten Berichts zu einer geschützten Maschine....311
Verwalten von geplanten Berichten über die Core Console....313
Planen eines Berichts....313
Ändern eines Berichtszeitplans....317
Anhalten, Wiederaufnehmen oder Löschen eines geplanten Berichts....317
Verwendung des Bericht-Menüs....318
Verwendung der Symbolleiste für Berichte....319

Grundlegende Informationen zu Jobberichten..... 320
Grundlegende Informationen zu Jobübersichtsberichten..... 321
Grundlegende Informationen zu Fehlerberichten..... 322
Grundlegende Informationen zu Zusammenfassungsberichten..... 322
Grundlegende Informationen zu Repositoryberichten..... 324
Grundlegende Informationen zu klassischen Übersichtsberichten..... 324
VM-Export..... 325
Exportieren auf virtuelle Maschinen mit Rapid Recovery..... 325
Exportieren von Daten in eine virtuelle ESXi-Maschine..... 327
Durchführen eines einmaligen ESXi-Exports..... 327
Einrichten eines fortlaufenden Exports zu ESXi..... 329
Exportieren von Daten in eine virtuelle VMware Workstation-Maschine..... 331
Durchführen eines einmaligen VMware Workstation-Exports..... 331
Einrichten eines fortlaufenden Exports zu VMware Workstation..... 333
Exportieren von Daten in eine virtuelle Hyper-V-Maschine..... 335
Durchführen eines einmaligen Hyper-V-Exports..... 335
Einrichten eines fortlaufenden Exports zu Hyper-V..... 337
Exportieren von Daten in eine virtuelle VirtualBox-Maschine..... 339
Durchführen eines einmaligen VirtualBox-Exports..... 339
Einrichten eines fortlaufenden Exports zu VirtualBox..... 340
Exportieren von Daten in eine virtuelle Azure Maschine..... 342
Arbeiten mit Microsoft Azure..... 343
Haftungsausschluss für Azure-Schnittstelle..... 343
Erstellen eines Containers in einem Azure Speicherkonto..... 343
Microsoft Azure Dokumentation..... 344
Vor dem virtuellen Export auf Azure..... 345
Exportieren und Bereitstellen von VMs für Azure..... 345
Durchführen eines einmaligen Azure Exports..... 346
Einrichten eines fortlaufenden Exports zu Azure..... 350
Bereitstellen einer virtuellen Maschine in Azure..... 352
Verwalten von Exporten..... 354
Wiederherstellen von Daten..... 358
Informationen zur Wiederherstellung von Daten mit Rapid Recovery..... 358
Grundlegendes zu Live Recovery..... 358
Wiederherstellen von Daten aus Wiederherstellungspunkten..... 359
Über die Dateisuch- und Wiederherstellungsfunktion..... 360
Suchen und Wiederherstellen einer Datei..... 361
Informationen über das Wiederherstellen von Volumes aus Wiederherstellungspunkten..... 363

Wiederherstellen von Volumes aus einem Wiederherstellungspunkt....364
Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer....367
Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer und Beibehalten der Berechtigungen....367
Wiederherstellen von Clustern und Cluster-Knoten....368
Wiederherstellen von einem angehängten Archiv....369
E-Mail-Wiederherstellung in Rapid Recovery....370
Voraussetzungen der E-Mail-Wiederherstellung....370
Öffnen einer Exchange-Datenbank in Rapid Recovery....371
Wiederherstellen eines E-Mail-Elements in Rapid Recovery....372
Bare-Metal-Wiederherstellung....376
Bare-Metal-Wiederherstellung für Windows-Computer....376
Durchführen einer BMR-Wiederherstellung für Windows-Computer....377
Voraussetzungen für eine Bare-Metal-Wiederherstellung für einen Windows-Computer....378
Durchführen einer Bare-Metal-Wiederherstellung von Daten unter Verwendung des Assistenten zum Wiederherstellen eines Computers....379
Grundlegendes zum Erstellen einer Start-CD für Windows-Computer....383
Grundlegendes zur Treiberinjektion in eine Start-CD....384
Erstellen eines ISO-Image für die Start-CD....384
Übertragen des ISO-Image der Start-CD auf Datenträger....386
Laden der Start-CD und Starten der Zielmaschine....386
Verwendung der Universal Recovery Console für eine BMR....387
Die Universal Recovery Console-Tools....387
Laden von Treibern mit der Universal Recovery Console....388
Laden von Treibern in der Universellen Wiederherstellungskonsole unter Verwendung tragbarer Medien....389
Laden eines Treibers mit URC Chromium....389
Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung....390
Informationen über die Zuweisung der Laufwerke für eine Bare-Metal-Wiederherstellung (BMR)....391
Automatisches Datenträgermapping für eine BMR-Wiederherstellung....392
Manuelles Datenträgermapping für eine BMR-Wiederherstellung....392
Eine BMR aus einem Archiv durchführen....393
Laden von Treibern in das Betriebssystem....396
Durchführen einer BMR-Wiederherstellung für Linux-Maschinen....397
Voraussetzungen für eine BMR-Wiederherstellung für Linux-Maschinen....398
Verwalten eines Linux-Startimage....399
Informationen über das ISO-Startimage für Linux....399

Speichern des Live DVD ISO-Image auf Datenträger 400
Laden der Live DVD und Starten der Zielmaschine 400
Herstellen einer Verbindung mit dem Ziel der BMR-Wiederherstellung vom Rapid Recovery Core aus 401
Verwalten von Linux-Partitionen 401
Erstellen von Partitionen auf dem Ziellaufwerk 401
Formatieren von Partitionen auf dem Ziellaufwerk 402
Breitstellen von Partitionen über die Befehlszeile 403
Starten einer BMR-Wiederherstellung für Linux 404
Starten des Dienstprogramms „Screen“ 404
Starten einer BMR-Wiederherstellung für Linux-Maschinen über die Befehlszeile 405
Wiederherstellen von Volumes einer Linux-Maschine über die Befehlszeile 407
Überprüfen einer BMR-Wiederherstellung 408
Anzeigen des Wiederherstellungsfortschritts 409
Starten eines wiederhergestellten Zielservers 409
Beheben von Universal Recovery Console-Verbindungsproblemen 409
Beheben von Problemen beim Starten 410
Überprüfen der BMR-Wiederherstellung über die Befehlszeile 410
Durchführen einer Dateisystemprüfung für das wiederhergestellte Volume 410
Startbarmachen einer wiederhergestellten Linux-Maschine über die Befehlszeile 411
Verwalten der Alterung von Daten 414
Datenaufbewahrung, Verknüpfen mit einem sekundären Speicher und Archivierung 414
Verwalten von Aufbewahrungsrichtlinien 415
Konfigurieren der Standardeinstellungen für die Aufbewahrungsrichtlinie des Core 416
Anpassen der Aufbewahrungsrichtlinieneinstellungen für eine geschützte Maschine 418
Erzwingen eines Rollup für alle geschützten Maschinen 421
Archivierung 423
Grundlegende Informationen zu Archiven 423
Erstellen eines Archivs und Speicheroptionen 423
Amazon Speicheroptionen und Archivierung 424
Wiederherstellungspunktkettenoptionen für Archive 425
Methoden für den Zugriff auf ein Archiv 426
Verwendungen für Archive 426
Erstellen eines Archivs 426
Archivieren in einer Cloud 430
Bearbeiten einer geplanten Archivierung 431
Deaktivieren oder Aktivieren einer geplanten Archivierung 433
Erzwingen eines Archivierungs-Jobs 433
Überprüfen eines Archivs 434

Anfügen eines Archivs....435
Importieren eines Archivs....436
Cloud-Konten....440
Informationen zu Cloud-Konten....440
Überlegungen zu Cloud-Speicheroptionen....441
Hinzufügen eines Cloud-Kontos....442
Bearbeiten eines Cloud-Kontos....445
Entfernen eines Cloud-Kontos....445
Das Local Mount Utility....447
Informationen zum Local Mount Utility....447
Arbeiten mit Rapid Recovery Kern-Computern im Local Mount Utility....447
Hinzufügen einer Core-Maschine zum Local Mount Utility....448
Verändern der Optionen des Local Mount Utility....449
Bearbeiten von Core-Verbindungseinstellungen im Local Mount Utility....450
Erneut verbinden mit einem Core....451
Verschieben einer Rapid Recovery Core-Maschine zum Local Mount Utility....451
Arbeiten mit geschützten Maschine im Local Mount Utility....452
Bereitstellen eines Wiederherstellungspunkts mit dem Local Mount Utility....452
Untersuchen eines bereitgestellten Wiederherstellungspunktes mit dem Local Mount Utility....453
Aktualisieren von Wiederherstellungspunkten....453
Aufheben der Bereitstellung von Wiederherstellungspunkten in der Local Mount Utility....454
Core Console-Referenzen....455
Anzeigen der Benutzeroberfläche der Core Console....455
Anzeigen geschützter Maschinen....464
Anzeigen von Ereignissen für eine geschützte Maschine....465
Anzeigen des Menüs „Mehr“ für eine geschützte Maschine....467
Third-party contributions....468
Apache 2.0....474
Chromium BSD License N/A....476
Code Project Open License (CPOL) 1.02....477
Far Manager BSD License N/A....480
GNU AFFERO GENERAL PUBLIC LICENSE....480
GPL (GNU General Public License) 2.0....488
LGPL (GNU Lesser General Public License) 2.1....492
OpenSSL 1.0....497
Über uns....500
Glossar....501

Copyright © 2018 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, Alisa 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

WARNING: Das Symbol WARNUNG weist auf mögliche Personen- oder Sachschäden oder Schäden mit Todesfolge hin.

CAUTION: Das Symbol VORSICHT weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: Ein Informationssymbol weist auf Begleitinformationen hin.

Einführung in Rapid Recovery

Rapid Recovery ist eine Sicherungs-, Replikations- und Wiederherstellungs-Lösung, die Nahe-Null-Wiederherstellungszeit-Ziele und Wiederherstellungspunkt-Ziele bietet. Rapid Recovery bietet Datenschutz, Notfallwiederherstellung, Datenmigration und Datenverwaltung. 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. Rapid Recovery kann auch in die Cloud, in eine DL Serie Sicherungs- und Wiederherstellungs-Appliance oder in ein unterstütztes System Ihrer Wahl archivieren. Mit Rapid Recovery können Sie auf ein oder mehrere Ziele für zusätzliche Redundanz und Sicherheit replizieren.

Rapid Recovery bietet:

- **Flexibilität.** Sie können Universal-Wiederherstellung auf mehreren Plattformen durchführen, darunter Wiederherstellen von physisch auf virtuell, von virtuell auf physisch, von virtuell auf virtuell und physisch auf physisch.
- **Cloud-Integration**. Sie können eine VM exportieren, archivieren und in die Cloud replizieren und eine Bare-Metal-Wiederherstellung aus Archiven in der Cloud durchführen. Kompatible Cloud-Dienste sind Microsoft Azure, Amazon Web Services (AWS), jeder OpenStack-basierte Anbieter (einschließlich Rackspace) und Google Cloud. US-Regierungsspezifische Plattformen umfassen AWS GovCloud (US) und Azure Government.
- **Intelligente Deduplizierung**. Sie können Speicherplatz-Anforderungen reduzieren durch Speicherung der Daten nur einmal und späterer Referenzierung (einmal pro Repository oder Verschlüsselungsdomain).
- **Sofortige Wiederherstellung**. Unsere Live Recovery-Funktion ermöglicht Ihnen zuerst den Zugriff auf kritische Daten, während Wiederherstellungsvorgänge parallel abgeschlossen werden.
- **Wiederherstellung auf Dateiebene**. Sie können Daten auf Dateiebene vor Ort, von einem entfernten Standort oder aus der Cloud wiederherstellen.
- **Suche auf Dateiebene**. Mithilfe von Kriterien, die Sie angeben, können Sie eine Reihe von Wiederherstellungspunkten für eine oder mehrere Dateien suchen. Aus den Suchergebnissen können Sie dann die Dateien auswählen und wiederherstellen, die Sie direkt aus dem Core Console auf dem lokalen Computer wiederherstellen möchten.
- **Virtuelle Unterstützung**. Rapid Recovery unterstützt einen einmaligen virtuellen Export, sodass Sie eine startbare VM aus einem Wiederherstellungspunkt erzeugen können, und Virtual Standby, in dem die startbare VM, die Sie generieren, kontinuierlich nach jedem Backup aktualisiert wird. Sie können den virtuellen Export auch auf Microsoft freigegebene Hyper-V-Cluster-Volumes durchführen.
- **Unterstützung für Rapid Snap for Virtual**. Erweiterte Unterstützung für Virtualisierung umfasst den agentenlosen Schutz von vCenter-/ESXi-VMs und von Hyper-V-VMs. Rapid Snap for Virtual beinhaltet Schutz und AutoErmittlung für VMware ESXi 5.5 und höher ohne installierte Agenten-Software. Host-basierter Schutz unterstützt die Installation des Rapid Recovery Agenten nur auf einem Microsoft Hyper-V-Host, sodass Sie alle zugehörigen Gast-VMs agentenlos schützen können.
- **Anwendungsunterstützung**. Rapid Recovery Agent bietet Anwendungsunterstützung für Microsoft Exchange, SQL-Server und Oracle. Wenn Sie diese Anwendungsserver im Core schützen, sind Backup-Snapshots automatisch anwendungskonsistent; offene Transaktionen und laufenden Transaktionsprotokolle werden abgeschlossen und Caches werden auf der Festplatte abgelegt, bevor Snapshots erstellt werden. Spezifische Anwendungsfunktionen werden unterstützt, einschließlich SQL-Anfügbarkeit (für SQL-Server) und Datenbankintegritätsprüfungen mit DBVERIFY (für Oracle). Die Anwendungskonsistenz erstreckt sich auch auf den agentenlosen Schutz für SQL-Server und Exchange Server.

Weitere Informationen zu Rapid Recovery finden Sie in den folgenden Ressourcen.

- Rapid Recovery Produkt-Support-Website unter https://support.quest.com/rapid-recovery/.
- Dokumentationswebsite unter https://support.quest.com/rapid-recovery/technical-documents/.

Core Console

In diesem Kapitel werden die verschiedenen Elemente der Benutzeroberfläche der Rapid Recovery Core Console beschrieben.

Zugriff auf die Rapid Recovery Core Console

Führen Sie die folgenden Schritte aus, um die Rapid Recovery Core Console zu öffnen.

- Führen Sie einen der folgenden Schritte aus, um die Rapid Recovery Core Console zu öffnen:
    1. Melden Sie sich lokal bei Ihrem Rapid Recovery Core Server an, und doppelklicken Sie dann auf das Symbol der Core Console.
    2. Sie können auch eine der folgenden URLs im Webbrowser eingeben:
    - https://<yourCoreServerName>:8006/apprecovery/admin/ oder
    - https://<yourCoreServerIPaddress>:8006/apprecovery/admin/

NOTE: Da die Rapid Recovery Core Console-UI JavaScript verwendet, muss im Webbrowser, mit dem Sie auf die Core Console zugreifen, JavaScript aktiviert sein.

NOTE: Wenn der Standardport für den Rapid Recovery-Dienst geändert wurde, muss der Port in der obigen URL entsprechend geändert werden.

Grundlegende Informationen zur Kurzanleitung

In der Kurzanleitung finden Sie Workflows zu vorgeschlagenen Aufgaben für die Konfiguration und die Verwendung von Rapid Recovery Core.

Wenn Sie nach dem Hochstufen oder der Installation des Rapid Recovery Core zum ersten Mal zur Core Console navigieren, wird automatisch die Kurzanleitung angezeigt. Klicken Sie auf auf **Kurzanleitung** in der **Startseite** der Kurzanleitung, um die verschiedenen vorgeschlagenen Konfigurationsaufgaben anzuzeigen. Über die Optionen **Schritt überspringen** und **Zurück** können Sie durch die Kurzanleitung navigieren. Klicken Sie auf **Fertigstellen**, um die Anleitung zu schließen, wenn die letzte vorgeschlagene Aufgabe angezeigt wird.

Sie können das Schnellstarthandbuch jederzeit wieder über das Hilfemenü in der Core Console aufrufen. Sie können die **Startseite** in der Kurzanleitung auch ausblenden.

Die Kurzanleitung wird bei jeder Anmeldung bei der Rapid Recovery Core Console angezeigt, sobald Sie die **Startseite** aufrufen (sofern Sie sie nicht ausblenden). Weitere Informationen hierzu finden Sie unter Ausblenden der Kurzanleitung.

Sie müssen die in der Anleitung vorgeschlagenen Schritte nicht durchführen. Sie können die vorgeschlagenen Aufgaben lediglich anzeigen und mit den Optionen **Schritt überspringen** und **Zurück** zwischen den Aufgaben navigieren. Sie können jederzeit auf **Anleitung beenden** klicken, um die Anleitung auszublenden.

Wenn Sie eine in der Kurzanleitung vorgeschlagene Konfigurationsaufgabe durchführen möchten, folgen Sie den Eingabeaufforderungen in den einzelnen Schritten der Anleitung und dem entsprechenden Assistenten bzw. im relevanten Bereich, der in der Benutzeroberfläche angezeigt wird. Die Vorgehensweise für die Durchführung der einzelnen, in der Anleitung vorgeschlagenen Aufgaben wird in diesem Dokument beschrieben (siehe folgende Tabelle).

NOTE: Nicht alle in der Kurzanleitung vorgeschlagenen Konfigurationsaufgaben sind für alle Benutzer erforderlich. Sie müssen wissen, welche Aufgaben Sie für die jeweiligen Anforderungen durchführen müssen.

Die Kurzanleitung deckt die folgenden Konfigurationsaufgaben ab:

Tabelle 1. Konfigurationsaufgaben der Kurzanleitung

Function	Kurzbeschreibung	Ergebnis der Ausgabenauswahl, Link zur Vorgehensweise
Schutz	Schützen einer einzelnen Maschine, Schützen eines Server-Clusters oder Schützen mehrerer Maschinen mit „Massenschutz“	Klicken Sie auf „Schützen“ oder wählen Sie **Maschine schützen** im Dropdown-Menü aus, um den Assistenten zum Schützen einer Maschine zu öffnen. Informationen zum Ausführen des Assistenten zum Schützen einer Maschine finden Sie unter Schützen einer Maschine. Wählen Sie **Cluster schützen** im Dropdown-Menü aus, um das Dialogfeld „Mit Cluster verbinden“ zu öffnen. Weitere Informationen über das Schützen eines Clusters finden Sie unter Schützen eines Clusters. Wählen Sie im Dropdown-Menü **Massenschutz** aus, um den Assistenten zum Schützen mehrerer Maschinen zu öffnen. Informationen zum Ausführen des Assistenten zum Schützen mehrerer Maschine finden Sie unter So schützen Sie mehrere Maschinen.
Replikation	Einrichten der Replikation von einem primären Core (Quell-Core) zu einem sekundären Core (Ziel-Core)	Klicken Sie auf **Replikation**, um die Seite „Replikation“ zu öffnen. Daraufhin werden Sie aufgefordert, mit dem Replikationsassistenten einen Ziel-Core hinzuzufügen. Informationen zum Einrichten der Replikation auf einem selbstverwalteten Core mit dem Replikationsassistenten finden Sie unter Replikation auf einen selbstverwalteten Ziel-Core. Allgemeine Informationen über Replikation finden Sie unter Konfigurieren der Replikation.
Virtueller Export	Durchführen eines einmaligen Exports oder Einrichten eines fortlaufenden Exports von einer geschützten Maschine in eine virtuelle Maschine	Klicken Sie auf **Export**, um einen Datenexport von einer geschützten Maschine in eine virtuelle Maschine durchzuführen. Sie können einen einmaligen Export durchführen oder die Virtual Standby-Funktion so einrichten, dass kontinuierlich ein Export in eine VM erfolgt. Informationen über virtuelle Exporte finden Sie unter Exportieren auf virtuelle Maschinen mit Rapid Recovery.
Verwalten und Konfigurieren	Bietet die Möglichkeit weitere Konfigurationseinstellungen für den Rapid Recovery Core einzurichten.	Klicken Sie auf **Mehr**, um weitere Funktionen zu sehen, die Sie konfigurieren oder verwalten können. Funktionen umfassen Archive; Bereitstellungen; Start-CDs; Repositorys; Verschlüsselungsschlüssel; Cloud-Konten; Dateisuche; Aufbewahrungsrichtlinien; Benachrichtigungen; Berichte; Protokolle und vieles mehr.
Verschlüsselung konfigurieren	Hinzufügen oder Importieren von	Klicken Sie auf **Verschlüsselungsschlüssel** zur Verwaltung der Sicherheit geschützter

Function	Kurzbeschreibung	Ergebnis der Ausgabenauswahl, Link zur Vorgehensweise
	Verschlüsselungsschlüsseln, die Sie für ein oder mehrere geschützten Maschinen verwenden können	Daten durch Hinzufügen oder Importieren von Verschlüsselungsschlüsseln. Sie können Verschlüsselungsschlüssel auf eine oder mehreren geschützte Maschinen anwenden. Die Verschlüsselung wird unter Verschlüsselung behandelt.
Benachrichtigungen konfigurieren	Einrichten von E-Mail-Benachrichtigungen für Ereignisse, Warnungen und Benachrichtigungen	Klicken Sie auf **Ereignisse**, um Benachrichtigungsgruppen für Ereignisse, Warnungen und Benachrichtigungen anzugeben. Wenn diese per E-Mail gesendet werden sollen, müssen Sie auch SMTP-Servereinstellungen angeben. Weitere Informationen zum Verwalten von Ereignissen finden Sie unter Ereignisse sowie unter Konfigurieren von Benachrichtigungsgruppen und Konfigurieren eines E-Mail-Servers.
Aufbewahrung verwalten	Anzeigen oder Ändern der Standardaufbewahrungsrichtlinie für den Core	Klicken Sie auf **Aufbewahrungsrichtlinie**, um die Seite „Aufbewahrungsrichtlinie“ für den Core zu öffnen. Dort können Sie angeben, wie lang ein Wiederherstellungspunkt beibehalten werden soll, bevor ein Rollup erfolgt. Konzeptionelle Informationen zu Aufbewahrungsrichtlinien finden Sie unter Verwalten der Alterung von Daten. Informationen zur Vorgehensweise finden Sie unter Verwalten von Aufbewahrungsrichtlinien.
Wiederherstellung	Wiederherstellen von Daten aus einem Wiederherstellungspunkt auf dem Core	Klicken Sie auf **Wiederherstellen**, um den Assistenten zum Wiederherstellen einer Maschine zu öffnen. Informationen zum Wiederherstellen von Daten finden Sie im Abschnitt Informationen über das Wiederherstellen von Volumes aus Wiederherstellungspunkten.

Ausblenden der Kurzanleitung

Nach der ersten Aktualisierung oder Installation des Rapid Recovery Core wird automatisch die Kurzanleitung angezeigt.

Sie wird auch angezeigt, wenn Sie im Dropdown-Menü „Hilfe“ die Option „Kurzanleitung“ auswählen und wenn Sie die Registerkarte „Startseite“ der Core Console öffnen.

Gehen Sie folgendermaßen vor, um die Kurzanleitung auszublenden.

- Führen Sie in der Rapid Recovery Core Console auf der Seite **Willkommen** der Kurzanleitung die folgenden Schritte durch:
  - Wählen Sie **Dieses Fenster nicht erneut anzeigen** aus, wenn die Seite **Willkommen** der Kurzanleitung ausgeblendet werden soll.

    NOTE: Dadurch wird die Seite **Willkommen** beim Öffnen der Kurzanleitung ausgeblendet, bis der Rapid Recovery Core aktualisiert wird.

    NOTE: Wählen Sie im Assistenten **Zurück** aus, wenn diese Seite zukünftig ausgeblendet werden soll und erweiterte Optionen angezeigt werden, um diese verborgene Seite anzuzeigen.
  - Klicken Sie auf **Schließen**, wenn Sie die Kurzanleitung in dieser Sitzung ausblenden möchten.

    Die Kurzanleitung wird geschlossen. Wenn Sie das nächste Mal die Registerkarte „Startseite“ der Core Console öffnen, wird wieder die Kurzanleitung angezeigt.
    Sie können die Kurzanleitung auch im Hilfemenü öffnen.

- Klicken Sie auf einer beliebigen Seite der Kurzanleitung auf **Beenden**.

  Die Kurzanleitung wird geschlossen. Bei Auswahl dieser Option können Sie die Kurzanleitung weiterhin im Menü „Hilfe“ öffnen.

Navigieren der Rapid Recovery Core Console

Wenn Sie sich bei der Core Console anmelden oder auf das Symbol **Startseite** klicken, wird die **Startseite** angezeigt. Die **Startseite** zeigt eine Übersicht von Rapid Recovery Core mit zwei Optionen an. Im Hauptanzeigebereich ist der Standardinhalt das neue Core Dashboard, in dem eine Reihe von Echtzeitberichten auf Ihrem System angezeigt wird. Standard-Dashboard-Berichte enthalten den letzten Übertragungs-Jobstatus pro Maschine, eine Repository-Übersicht und den Verbindungsstatus für geschützte, replizierte und Nur Wiederherstellungspunkte-Maschinen. Oder Sie können in die klassische Zusammenfassungstabellen-Anzeige wechseln. In dieser Ansicht zeigt der Titel der Seite den Anzeigenamen von Rapid Recovery Core an sowie Übersichtstabellen, die geschützte Maschinen, Repositorys und Warnungen anzeigen. Weitere Informationen finden Sie unter Grundlegende Informationen zur Startseite (Übersichtstabellenansicht) bzw. Grundlegende Informationen zu Core-Dashboard-Berichten.

Auf der **Startseite** (und auf jeder Seite in der Core Console) zeigt der linke Navigationsbereich die Elemente, die auf dem Core geschützt werden an. Sie können in der Benutzeroberfläche auf andere Seiten navigieren. Wählen Sie dazu eine der folgenden Methoden:

- Durch Klicken auf das entsprechende Symbol in der Symbolleiste im linken Navigationsbereich. Die Optionen, die über die Symbolleiste verfügbar sind, umfassen Replizieren, Virtual Standby, Ereignisse, Einstellungen und Mehr.
- Erweitern Sie das Menü (Mehr) auf der Symbolleiste und wählen Sie dann ein Ziel.
- Klicken Sie auf eine Schaltfläche oder Menüoption in der Schaltflächenleiste. Zu den Schaltflächen gehören Schützen, Wiederherstellen, Archivieren und Replizieren.

Wenn Sie ein Element aus dem linken Navigationsbereich wählen, wechselt der Fokus der Core Console zur Anzeige der zusammenfassenden Informationen zu diesem Element. Wenn Sie beispielsweise auf den Namen einer geschützten Maschine klicken, zeigt die Core Console nur Informationen über diese Maschine, anstatt den Core an. In diesem Beispiel wird der Anzeigenamen der geschützten Maschine als Titel der Seite angezeigt. Ein Untermenü wird rechts angezeigt, so können Sie bestimmte Informationen zu der geschützten Maschine anzeigen. Zur Auswahl stehen folgende Optionen:: Zusammenfassung, Wiederherstellungspunkte, Ereignisse, Einstellungen, Berichte und Mehr.

Um wieder zur Anzeige von Informationen über den Core, einschließlich Dashboard-Berichten oder einer Übersichtsansicht für mehrere geschützte oder replizierte Maschinen, zurückzukehren, klicken Sie auf das Symbol **Startseite** oben links in der Benutzeroberfläche. Auf der **Startseite** können Sie zwischen der Dashboardanzeige und der Seite „Zusammenfassung“ wechseln, indem Sie auf den roten Link oben rechts auf der Seite klicken.

Sie können mit dem Titel an der Oberseite der Core Console für die Informationen, die Sie im Core anzeigen, einen Kontext bereitstellen. Beispiel:

- Jedes Mal, wenn Sie den Anzeigenamen oder die IP-Adresse des Core als Seitenüberschrift sehen, sehen Sie zusammenfassende Informationen über den Core.
- Wenn der Titel „Dashboard“ ist, sehen Sie das Core Dashboard.
- Wenn Sie den Anzeigenamen oder die IP-Adresse einer geschützten Maschine oder einem zusammenfassenden Fensterbereich oben auf einer Seite sehen, werden Ihnen Informationen zu einem einzelnen System, das vom Core geschützt oder repliziert ist, im Core angezeigt.
- Wenn Sie den Titel „Geschützte Maschinen“ sehen, werden Ihnen Informationen zu allen geschützten Maschinen in Rapid Recovery Core angezeigt.
- Wenn Sie den Titel „Maschinen repliziert von...“ sehen, werden Ihnen Informationen zu allen replizierten Maschinen in Rapid Recovery Core angezeigt.
- Wenn Sie die Seitenüberschrift „Nur Wiederherstellungspunkte“ sehen, werden Ihnen Informationen zu allen Nur Wiederherstellungspunkte-Maschinen auf diesem Core angezeigt.

Informationen zu den verfügbaren Eigenschaften und Funktionen jeder Seite finden Sie im entsprechend Abschnitt weiter unten.

Weitere Informationen zum Anzeigen von geschützten Maschinen finden Sie unter Anzeigen des Menüs "Geschützte Maschinen". Weitere Informationen zum Verwalten von geschützten Maschinen finden Sie unter Verwalten geschützter Maschinen.

Weitere Informationen zum Anzeigen von replizierten Maschinen finden Sie unter Anzeigen von ein- und ausgehender Replikation.

Weitere Informationen über das Anzeigen von Nur Wiederherstellungspunkte-Maschinen finden Sie unter Anzeigen des Menüs „Nur Wiederherstellungspunkte“.

Grundlegendes zum linken Navigationsbereich

Der linke Navigationsbereich der Core Console wird auf der linken Seite der Benutzeroberfläche angezeigt. Der Inhalt dieses Navigationsbereichs kann je nach Typ der geschützten Objekte in Ihrem Rapid Recovery Core variieren.

Der linke Navigationsbereich enthält immer Folgendes:

- **Symbolleiste.** Für die Navigation zu den wichtigsten Seiten der Core Console.
- **Textfilter.** Der Textfilter ist ein Textfeld, mit dem Sie die Elemente in den unterschiedlichen darunter angezeigten Menüs filtern können. Durch Klicken auf den Pfeil rechts neben dem Textfilter werden die einzelnen darunter angezeigten Menüs erweitert oder reduziert.

Nach diesen Elementen werden im linken Navigationsbereich typischerweise Menüs angezeigt, die Ihnen bei der Navigation, Filterung und Anzeige der in Ihrem Core geschützten Objekte helfen. Dazu gehören geschützte Maschinen, replizierte Maschinen und so weiter.

Jedes Menü ist kontextsensitiv. Das bedeutet, dass sie einzelnen Menüs nur in der Core Console angezeigt werden, wenn sie relevant sind. Wenn Sie zum Beispiel mindestens eine Maschine schützen, wird das Menü „Protected Machines“ (Geschützte Maschinen) angezeigt und so weiter.

Weitere Informationen finden Sie in den Tabellen im linken Navigationsbereich in Anzeigen der Benutzeroberfläche der Core Console.

See also: Anzeigen von zusammenfassenden Informationen für eine geschützte Maschine
See also: Anzeigen von zusammenfassenden Informationen für einen Host
See also: Replikation
See also: Grundlegende Informationen zu benutzerdefinierten Gruppen

Anzeigen der Startseite der Rapid Recovery Core Console

Jedes Mal, wenn Sie sich bei der Rapid Recovery Core Console anmelden, oder jedes Mal, wenn Sie auf das Symbol **Startseite**  in der Symbolleiste klicken, wird die **Startseite** angezeigt. Die **Startseite** bietet eine **Dashboard**-Anzeige und die vertraute Anzeige der **Zusammenfassungstabellen.** Die Zusammenfassungstabellen sind die Standardansicht.

Sie können zwischen Ansichten auf der **Startseite** wechseln, indem Sie auf das Symbol zum Umschalten des Dashboards  oben rechts auf der **Startseite** klicken.

Über die **Startseite** und jede andere Seite der Core Console können Sie durch Verwendung des linken Navigationsbereichs zu den gewünschten Funktionen navigieren.

Weitere Informationen erhalten unter den folgenden Themen:

- Grundlegendes zum linken Navigationsbereich
- Grundlegende Informationen zu Core-Dashboard-Berichten
- Grundlegende Informationen zur Startseite (Übersichtstabellenansicht)
- Anzeigen der Benutzeroberfläche der Core Console

Grundlegende Informationen zur Startseite (Übersichtstabellenansicht)

Die **Startseite** betrifft ausschließlich den Core. In der Dashboard-Ansicht werden Grafik-Berichte in Echtzeit angezeigt. Bei Wechseln zur Übersichtstabellenansicht zeigt die **Startseite** alle Maschinen an, die der Core schützt oder repliziert sowie die dem Core zugeordneten Repositorys und Warnungen für Maschinen auf diesem Core.

Jeder Fensterbereich auf der **Startseite** kann vergrößert oder verkleinert werden. Wenn Sie beispielsweise auf das Symbol  (Ansicht verkleinern) oben rechts vom Fensterbereich der geschützten Maschinen klicken, wird die Ansicht der geschützten Maschinen verkleinert und nur der Name des Fensterbereichs ist sichtbar. Um die Ansicht zu erweitern und wieder alle geschützten Maschinen anzuzeigen, klicken Sie auf das Symbol  (Ansicht erweitern).

Die folgende Tabelle beschreibt die verschiedenen Elemente auf der **Startseite** in der Übersichtstabellenansicht.

Tabelle 2. Optionen auf der Startseite

UI-Element	Description
Geschützte Maschinen	Im Fensterbereich "Geschützte Maschinen" werden die vom Core geschützten Maschinen aufgeführt. Dieser Fensterbereich wird unabhängig davon angezeigt, ob eine Maschine dem Core zum Schutz hinzugefügt wurde.

UI-Element	Description
	Der Abschnitt enthält die folgenden Informationen für jede geschützte Maschine: • **Maschinentyp** Ein Symbol zeigt an, ob die Maschine ein physischer Computer, eine virtuelle Maschine oder ein geschütztes Cluster ist. • **Status.** Farbige Kreise in der Statusspalte zeigen an, ob auf die geschützte Maschine zugegriffen werden kann und ob sie vorübergehend deaktiviert oder offline und nicht erreichbar ist. • **Anzeigename.** Der Anzeigename oder die IP-Adresse der geschützten Maschine. • **Repository-Name.** Der Name des Repositorys, in dem die Wiederherstellungspunkte für die betreffende Maschine gespeichert sind. • **Letzter Snapshot.** Das Datum und die Uhrzeit, zu der Rapid Recovery den aktuellsten Wiederherstellungspunkt-Snapshot für diese Maschine aufgenommen hat. • **Wiederherstellungspunkte.** Die Anzahl der Wiederherstellungspunkte, die im Repository gespeichert sind und der Speicherplatz für jede geschützte Maschine. • **Version**. Die Version der Rapid Recovery Agentensoftware, die auf der Maschine installiert ist. Wenn Sie in diesem Fensterbereich auf einen bestimmten Maschinennamen klicken, wird eine Zusammenfassungsseite mit den zusammenfassenden Informationen für die ausgewählte Maschine angezeigt. Weitere Informationen zu den Aktionen, die Sie auf der Seite "Zusammenfassung" durchführen können, finden Sie unter Anzeigen von zusammenfassenden Informationen für eine geschützte Maschine.
Replizierte Maschinen	Im Fensterbereich "Replizierte Maschinen" sind alle Maschinen aufgeführt, die dieser Core von einem anderen Core repliziert. Dieser Fensterbereich wird nicht angezeigt, es sei denn, Ihr Core repliziert Maschinen von einem anderen Core. Der Abschnitt enthält die folgenden Informationen für jede replizierte Maschine: • **Maschinentyp** Ein Symbol zeigt an, ob die Maschine ein physischer Computer, eine virtuelle Maschine oder ein geschütztes Cluster ist. • **Status.** Farbige Kreise in der Statusspalte zeigen an, ob auf die replizierte Maschine zugegriffen werden kann und ob sie vorübergehend deaktiviert oder offline und nicht erreichbar ist. • **Anzeigename.** Der Anzeigename oder die IP-Adresse der replizierten Maschine. • **Replikationsname.** Der Anzeigename des ursprünglichen Quell-Core für alle Maschinen, die Sie auf diesen Ziel-Core replizieren. Sie können diesen Namen beim Einrichten der Replizierung festlegen. • **Repository-Name.** Der Name des Repositorys, in dem die Wiederherstellungspunkte für die betreffende Maschine gespeichert sind. • **Letzter replizierter Snapshot.** Das Datum und die Uhrzeit, zu der Rapid Recovery das aktuellste Replikat der ursprünglichen geschützten Maschine vorgenommen hat. • **Wiederherstellungspunkte.** Die Anzahl der Wiederherstellungspunkte, die im Repository gespeichert sind und der Speicherplatz für jede replizierte Maschine. • **Version**. Die Version der Rapid Recovery Agentensoftware, die auf der Maschine installiert ist. Wenn Sie in diesem Fensterbereich auf einen bestimmten Maschinennamen klicken, wird die Seite „Zusammenfassung“ mit den zusammenfassenden Informationen für die replizierte Maschine angezeigt.

UI-Element	Description
Nur-Wiederherstellungspunkte-Maschinen	Im Fensterbereich "Nur-Wiederherstellungspunkte-Maschinen" sind alle Maschinen aufgeführt, die aus dem Schutz oder der Replikation entfernt wurden, wenn die Wiederherstellungspunkte gespeichert wurden. Die Maschinen können für die Wiederherstellung auf Dateiebene, aber nicht für eine BMR-Wiederherstellung, die Wiederherstellung ganzer Volumes oder das Hinzufügen von Snapshot-Daten verwendet werden. Dieser Fensterbereich wird nicht angezeigt, wenn keine Maschine dieser Definition entspricht. Dieser Abschnitt enthält die folgenden Informationen für jede „Nur Wiederherstellungspunkte“-Maschine: • **Maschinentyp** Ein Symbol zeigt an, ob die Maschine ein physischer Computer, eine virtuelle Maschine oder ein geschütztes Cluster ist. • **Status.** Farbige Kreise in der Statusspalte zeigen an, ob auf die Nur-Wiederherstellungspunkte-Maschine zugegriffen werden kann und ob sie vorübergehend deaktiviert oder offline und nicht erreichbar ist. • **Anzeigename.** Der Anzeigename oder die IP-Adresse der Maschine, für die Wiederherstellungspunkte gespeichert sind. • **Repository-Name.** Der Name des Repositorys, in dem die verbleibenden Wiederherstellungspunkte für die betreffende Maschine gespeichert sind. • **Wiederherstellungspunkte.** Die Anzahl der Wiederherstellungspunkte, die im Repository gespeichert sind und der Speicherplatz für jede Nur-Wiederherstellungspunkte-Maschine. Wenn Sie in diesem Fensterbereich auf einen bestimmten Maschinennamen klicken, wird die Seite „Zusammenfassung“ für die Nur-Wiederherstellungspunkte-Maschine angezeigt.
DVM-Repositorys	Dieser Fensterbereich wird für DL1000 angezeigt, unabhängig davon, ob Deduplication Volume Manager (DVM)-Repositorys erstellt wurden. Dieser Fensterbereich wird nicht angezeigt, es sei denn, Ihr Core weist mindestens ein DVM-Repository auf. Er enthält die folgenden Informationen für jedes DVM-Repository: • **Type.** Ein Symbol zeigt ein Repository an. • **Status.** Farbige Kreise in der Statusspalte zeigen an, ob das Repository bereitgestellt wurde und Übertragungen von Wiederherstellungspunkten annehmen kann oder nicht erreichbar oder im Fehlerzustand ist. • **Repository-Name.** Der Anzeigename des Repositorys. • **Speicherplatz.**Die Größe des Speicherplatzes, der im Repository verwendet wird, und die Größe des Speicher-Volumes bzw. der Erweiterung. • **Geschützte Daten.** Der genutzte Speicherplatz im Repository. • **Maschinen.** Die Anzahl der Maschinen, für die im Repository Wiederherstellungspunkte gespeichert sind. • **Wiederherstellungspunkte.** Die Anzahl der Wiederherstellungspunkte, die im Repository gespeichert sind. • **Komprimierungsverhältnis.** Das Komprimierungsverhältnis der geschützten Daten im Repository, um Speicherplatz zu sparen. Weitere Informationen hierzu finden Sie unter Grundlegende Informationen zu Repositorys.

UI-Element	Description
Warnungen	In diesem Abschnitt werden wichtige Benachrichtigungen für den Core und alle davon geschützten Maschinen aufgelistet. Der Abschnitt enthält folgende Informationen: • **Symbole.** Die Symbolspalte zeigt die Art der Benachrichtigung an. Hierzu gehören Informationsmeldungen, Fehler. • **Datum.** Zeigt den Zeitpunkt (Datum und Uhrzeit) an, zu dem die Benachrichtigung von Rapid Recovery erstellt wurde. • **Meldung.** Beschreibt die Benachrichtigung. Diese Details werden auch auf der Registerkarte "Ereignisse" für den Core angezeigt. Weitere Informationen hierzu finden Sie unter Anzeigen von Ereignissen mithilfe von Aufgaben, Warnungen und Journalseiten.

Grundlegende Informationen zu Core-Dashboard-Berichten

Das Core-Dashboard zeigt einen Satz von Echtzeit-Grafik-Berichten mit Daten, die für Ihren Core, die von Ihnen geschützten Maschinen und die Snapshots, die in Ihrem Repository gespeichert sind, relevant sind. Dashboard-Berichte umfassen:

- Core-Systemberichte
  - **Fehler-Überwachung**. Dieser Bericht zeigt Job-Aktivität, Verbindungen mit dem Lizenzportal und Übertragungsaktivität zur frühen Erkennung von Störungen auf Ihrem System. Klicken Sie auf das Uhr-Widget, um alle verfolgten Aktivitäten zu löschen und zur Überwachung neuer Ereignisse.
  - **Repository**. Dieser Bericht zeigt die mit dem Core verknüpften Repositorys an. Es werden die Anzahl von Repositorys angezeigt, wie viele Maschinen jeweils geschützt werden, die Anzahl der Wiederherstellungspunkte und den Prozentsatz der Komprimierung oder Deduplizierung. Dieser Bericht wird jede Minute aktualisiert.
- Maschinenberichte
  - **Maschinen-Konnektivität**. Dieser Bericht zeigt den Verbindungsstatus von auf Ihrem Core geschützten und replizierten Maschinen. Darüber hinaus zeigt er die Konnektivität für Daten auf einem Wiederherstellungspunkte-nur Maschine.
- Snapshot-Berichte
  - **Übertragungs-Job**. Dieser Bericht zeigt alle Snapshot-Datenübertragungen (einschließlich Basisabbilder und inkrementelle Snapshots), die in den letzten 24 Stunden abgeschlossen wurden. Snapshots umfassen Basisabbilder und inkrementelle Snapshots. Dieser Dashboard-Bericht wird als Kreis-Diagramm angezeigt.
  - **Transfer-Job pro Maschine**. Dieser Job zeigt für die einzelnen geschützten Maschinen die Anzahl der erfolgreichen und fehlgeschlagenen Übertragungs-Jobs der letzten 24 Stunden an. Dieser Dashboard-Bericht wird in einem Liniendiagramm angezeigt.

Am oberen Rand des Dashboards können Sie auf das Widget  (Erweitern) klicken, um eine Liste der im Dashboard angezeigten Berichte in den drei weiter oben beschriebenen Kategorien einzublenden. Jede Berichtskategorie und jeder Bericht verfügt über ein Kontrollkästchen. Wenn das Kontrollkästchen aktiviert ist, erscheint der Bericht bzw. die Kategorie auf dem Dashboard. Wenn Sie die Option deaktivieren, wird der Bericht nicht angezeigt. Auf diese Weise können Sie die Anzeige von Berichten auf dem Dashboard schnell ändern.

Wenn Sie auf  (Reduzieren) klicken, wird das Menü ausgeblendet.

Sie können auch die Ansicht beliebiger Berichte auf dem Dashboard ein- oder ausblenden, indem Sie auf den Nach-oben- oder Nach-unten-Pfeil in der Kopfzeile des Berichts klicken. Einige Dashboard-Berichte (Maschinen-Konnektivität und Repository) haben ein Pluszeichen neben dem Pfeil, von dem aus Sie eine weitere geschützte Maschine oder entsprechend ein anderes Repository hinzufügen können.

Sie können auch per Drag-and-Drop den Speicherort von einem der Berichte an eine beliebige andere Stelle auf dem Dashboard verschieben, um die Berichte in einer für Ihre Verwendung effektivsten Weise zu sortieren.

Anzeigen des Menüs "Geschützte Maschinen"

Auf der Rapid Recovery-Benutzeroberfläche enthält der linke Navigationsbereich das Menü "Geschützte Maschinen". Wie bei allen Menüs im Navigationsbereich wird die Menübeschriftung in Großbuchstaben angezeigt. Dieses Menü ist standardmäßig vollständig erweitert und zeigt eine Liste aller Maschinen an, die von diesem Core geschützt werden. Werden Servercluster geschützt, sind diese ebenfalls in der Liste enthalten.

Sie können die Ansicht für geschützte Maschinen und Server-Cluster im Core reduzieren oder erweitern, indem Sie auf den Pfeil auf der linken Seite dieses Menüs klicken.

Das Menü „Geschützte Maschinen“ enthält auf der rechten Seite ein Dropdown-Menü mit den Funktionen, die für die geschützten Maschinen durchgeführt werden können. Klicken Sie auf den Pfeil rechts neben **Geschützte Maschine**, um das Menü anzuzeigen.

Jede im Menü „Geschützte Maschinen“ aufgelistete Maschine verfügt ebenfalls über ein Dropdown-Menü, das lediglich Funktionen für die jeweilige Maschine steuert.

Wenn Sie Servercluster im Rapid Recovery Core verwalten, wird der Cluster ebenfalls im linken Navigationsmenü angezeigt. Sie können vom Drop-Down-Menü eines beliebigen Clusters aus auch zur Seite **Geschützte Knoten** für den ausgewählten Cluster navigieren.

Wenn Sie auf den Pfeil links neben dem Menü „Geschützte Maschinen“ klicken, wird die Liste der geschützten Maschinen und Server-Cluster ausgeblendet, sodass keine Maschinen mehr aufgelistet werden. Wenn Sie erneut auf diesen Pfeil klicken, wird die Liste der Maschinen wieder eingeblendet.

Wenn Sie auf einen Maschinennamen im Menü "Geschützte Maschinen" klicken, wird die Seite "Zusammenfassung" für die betreffende Maschine geöffnet. Weitere Informationen zu den Aktionen, die Sie auf der Seite "Zusammenfassung" durchführen können, finden Sie unter Anzeigen von zusammenfassenden Informationen für eine geschützte Maschine.

Durch Klicken direkt auf das Menü **Geschützte Maschinen** können Sie die Seite **Geschützte Maschinen** im Hauptinhaltsbereich in einem einzigen Fensterbereich mit den geschützten Maschinen auf diesem Core anzeigen. Weitere Informationen über Aktionen im Fensterbereich **Geschützte Maschinen** auf der Seite "Geschützte Maschinen" finden Sie unter .

NOTE: Von der Seite **Geschützte Maschinen** können Sie durch Anklicken des Symbols **Startseite** in der Symbolleiste zu einer Ansicht aus der Core-Perspektive zurückkehren.

Anzeigen von zusammenfassenden Informationen für eine geschützte Maschine

Wenn Sie auf den Namen einer geschützten Maschine in der Core Console klicken, wird die Seite **Zusammenfassung** angezeigt. Die Seite umfasst mindestens einen Fensterbereich Zusammenfassung und einen Fensterbereich Volumes. Wenn eine Maschine der Replikation hinzugefügt wird, wird auch ein Fensterbereich Replikation angezeigt.

Wenn mindestens ein geschützter Exchange Server vorhanden ist, gibt es darüber hinaus auch einen Fensterbereich Exchange Server-Informationen mit Informationen zu den geschützten Exchange Servern.

Wenn mindestens ein geschützter SQL Server vorhanden ist, gibt es darüber hinaus auch einen Fensterbereich SQL Server-Informationen mit Informationen zu den geschützten SQL Servern.

Oben auf der Seite befindet sich ein Menü mit Aktionen, die Sie auf der geschützten Maschine ausführen können. Darunter befindet sich mindestens ein Fensterbereich "Zusammenfassung" und ein Fensterbereich "Volumes". Wenn eine Maschine der Replikation hinzugefügt wird, wird auch ein Fensterbereich "Replikation" angezeigt.

Beim Anzeigen von Informationen für eine geschützte Maschine auf der Seite "Zusammenfassung" und in allen anderen Ansichten befindet sich am oberen Seitenrand ein Menü mit Funktionen, die Sie ausführen können. Dieses Menü wird unmittelbar unter dem Namen der geschützten Maschine angezeigt.

See also: Anzeigen des Bereichs „Zusammenfassung“
See also: Anzeigen von Volumes auf einer geschützten Maschine
See also: Anzeigen von Replikationsinformationen
See also: Anzeigen des Fensterbereichs „Exchange Server-Informationen“
See also: Anzeigen des SQL Server-Informationsbereichs
c_Viewing_summary_information_for_a_host.xml

Anzeigen des Bereichs „Zusammenfassung“

Der Fensterbereich **Zusammenfassung** enthält zusammenfassende Informationen zur geschützten Maschine, z. B. Hostname, Datum und Uhrzeit des letzten Snapshots, Datum und Uhrzeit des nächsten geplanten Snapshots, Informationen zum Verschlüsselungsschlüssel sowie Version der Rapid Recovery-Agentensoftware. Darüber hinaus gibt es einen Link zu einer Seite mit detaillierten Systeminformationen für die Maschine.

Anzeigen von Volumes auf einer geschützten Maschine

Für jede geschützte Maschine können Sie im Fensterbereich „Volumes“ der Registerkarte „Zusammenfassung“ die folgenden Aktionen für die aufgelisteten Volumes ausführen:

- Schutzzeitplan für ein ausgewähltes Volume festlegen. Die Schutzzeitpläne werden normalerweise eingerichtet, wenn eine Maschine erstmals unter Schutz gestellt wird. Weitere Informationen zur Änderung eines Schutzzeitplans finden Sie unter Erstellen von benutzerdefinierten Schutzzeitplänen im einfachen Modus.
- Erstellung eines Basisimage oder eines Snapshots erzwingen. Snapshots werden normalerweise gemäß Schutzzeitplan erstellt. Sie können jedoch jederzeit die Erstellung eines Basisimage oder eines inkrementellen Snapshots für ausgewählte Volumes erzwingen. Weitere Informationen finden Sie unter Erzwingen eines Snapshots.

Anzeigen von Replikationsinformationen

Der Fensterbereich **Replikation** enthält zusammenfassende Informationen zu der replizierten Maschine, einschließlich Replikationsname, Status der Replikation, Fortschritt sowie verfügbarer Speicherplatz.

Anzeigen des Fensterbereichs „Exchange Server-Informationen“

Der Fensterbereich **Exchange Server-Informationen** wird nur für geschützte Maschinen angezeigt, die Exchange Server sind.

Dieser Bereich enthält zusammenfassende Informationen zum geschützten Exchange-Server, einschließlich der installierten Version von Microsoft Exchange, des Pfads, auf dem Exchange installiert ist, und des Pfads, der für Exchange Mailbox-Daten definiert ist.

Das Mailspeicher-Raster zeigt den Namen der Exchange-Datenbank (EDB), den Pfad der EDB-Datei, den Pfad der Protokolldateien, das Protokoll-Präfix, den Systempfad, die Database Availability Group (AG) und den Typ des Mailspeichers an.

Anzeigen des SQL Server-Informationsbereichs

Der Bereich **SQL Server Information** (SQL Server-Informationen) wird nur für geschützte Maschinen angezeigt, die SQL-Server sind.

Dieser Bereich enthält zusammenfassende Informationen zu den geschützten SQL-Servern. Sie können die Datenbankinformationen erweitern, um Details für jede Tabelle in der Datenbank anzuzeigen. Sie können auch den Datenbank- oder Tabellennamen sowie den Datenbankpfad anzeigen.

Anzeigen von zusammenfassenden Informationen für einen Host

Wenn Sie auf den Namen einer Hypervisor- oder Cluster-Hostmaschine in der Core Console klicken, wird die Seite **Zusammenfassung** angezeigt. Die Seite umfasst mindestens eine Aktionsleiste mit Funktionen, einen Fensterbereich „Zusammenfassung“ und einen Fensterbereich „Prozessoren“. Die Aktionsleiste wird am oberen Rand aller Seiten für den Host angezeigt. Der Fensterbereich „Zusammenfassung“ enthält Informationen wie den Hostnamen und die Virtualisierungssoftware. Der Fensterbereich „Prozessoren“ enthält eine Tabelle, in der Architektur, Anzahl der Cores, Anzahl der Threads, die Taktfrequenz und eine Beschreibung jedes Prozessors aufgeführt sind.

Je nach Art des Host werden möglicherweise auch die folgenden weiteren Fensterbereiche angezeigt:

- **SMB-Server.** Wenn ein Hyper-V-Host einen oder mehrere SMB-Server verwendet, werden in diesem Abschnitt die Hostnamen für jeden SMB-Server aufgelistet.
- **Knoten.** Die Seite **Zusammenfassung** eines Cluster-Host umfasst einen Abschnitt zum Auflisten des Hostnamens und der Rapid Recovery Versionsnummer jedes Knotens.
- **Volumes.** Bei Verwendung von agentenlosem Schutz umfasst die Seite **Zusammenfassung** für einen Hyper-V-Host diesen Abschnitt, um den Namen, das Dateisystem, die Speicherplatznutzung, den aktuellen und nächsten Snapshot für jedes geschützte Volume aufzulisten.
- **Gemeinsame Festplatten.** Wenn ein Hyper-V-Host, der agentenlosen Schutz verwendet, über ein oder mehrere freigegebene VHDX-Volumes verfügt, werden in diesem Abschnitt der Name und der Pfad jeder virtuellen Festplatte aufgelistet.

Weitere Informationen über CSV-Cluster finden Sie unter „Unterstützung für freigegebene Clustervolumes“ im *Rapid Recovery Systemanforderungen-Handbuch.* Weitere Informationen zu verwandten Themen finden Sie unter den folgenden Links:

- Anzeigen von zusammenfassenden Informationen für eine geschützte Maschine
- Grundlegende Informationen zu Rapid Snap for Virtual

Anzeigen von Wiederherstellungspunkten für eine Maschine

Auf der Seite „Wiederherstellungspunkte“ wird eine Liste der erfassten Wiederherstellungspunkte für die jeweils ausgewählte Maschine mit den zugehörigen Maschinen- und Repositorydaten angezeigt. Auf dieser Seite können Sie bestimmte Wiederherstellungspunkte bereitstellen, exportieren und wiederherstellen sowie Wiederherstellungspunkte löschen.

Die Seite ist in zwei Bereiche unterteilt: Zusammenfassung der Wiederherstellungspunkte und Wiederherstellungspunkte. Der Bereich „Zusammenfassung“ enthält keine Links für durchführbare Aktionen. Er enthält die folgenden Daten für die Maschine.

Tabelle 3. Daten im Bereich „Zusammenfassung der Wiederherstellungspunkte“

UI-Element	Description
Wiederherstellungspunkte, gesamt	Die Anzahl der Wiederherstellungspunkte, die für die jeweilige geschützte Maschine erfasst wurden.
Geschützte Daten, gesamt	Der Umfang der Daten der geschützten Maschine, der im Repository gespeichert ist.
Repository	Der Name des Repositorys, in dem Rapid Recovery die Wiederherstellungspunkte für die betreffende geschützte Maschine speichert.
Repositorystatus	Die Statusanzeige zeigt den belegten Speicherplatz im Repository in Prozent an. Unter der Statusanzeige werden das genutzte Datenvolumen und die Gesamtgröße des Repositorys angezeigt.

Weitere Informationen finden Sie unter .

Anzeigen von Ereignissen für eine geschützte Maschine

Auf der Seite **Ereignisse** können Sie die Jobs anzeigen, die auf der ausgewählten geschützten Maschine durchgeführt wurden oder werden. Über die Schaltflächen oben auf der Seite können Sie zu Joblisten in den folgenden drei Aktivitätskategorien navigieren:

- **Aufgaben.** Ein Job, den Rapid Recovery durchführen muss, damit die einwandfreie Funktionsweise gewährleistet ist.
- **Warnungen.**Eine Benachrichtigung für eine Aufgabe oder ein Ereignis mit Fehlern oder Warnungen.
- **Journal.**Eine Zusammenstellung aller Aufgaben und Ereignisse der geschützten Maschine.

Die folgende Tabelle enthält Beschreibungen der Schaltflächen auf der Seite **Ereignisse**.

Tabelle 4. Elemente der Seite „Ereignisse“

UI-Element	Description
Stichwortsuche	Bietet die Möglichkeit, ein bestimmtes Element in der jeweiligen Kategorie zu suchen. Nur für Tasks verfügbar.
Von	Um die Suchergebnisse einzugrenzen, können Sie ein Datum eingeben, an dem die Suche beginnen soll. Nur für Tasks verfügbar.
Bis	Um die Suchergebnisse einzugrenzen, können Sie ein Datum eingeben, an dem die Suche enden soll. Nur für Tasks verfügbar.
Statussymbole	Jedes Symbol stellt einen anderen Jobstatus dar. Für Tasks und Warnungen können Sie durch Klicken auf eines der Symbole die Liste anhand dieses Status filtern und so einen Bericht erzeugen. Wenn Sie ein zweites Mal auf das Symbol klicken, wird der Filter

UI-Element	Description
	für den betreffenden Status entfernt. Sie können nach mehr als einem Status filtern. Die Status umfassen: • **Aktiv.**Ein Job, der gerade durchgeführt wird. • **In Warteschlange.** Ein Job, der auf den Abschluss eines anderen Jobs wartet, damit er eingeleitet werden kann. • **Wartend.**Ein Job der auf eine Genehmigung oder den Abschluss eines Vorgangs wartet, z. B. Bereitstellung eines Seed-Laufwerks. (Weitere Informationen zu Seed-Laufwerken finden Sie unter Replikation.) • **Abgeschlossen.**Ein Job, der erfolgreich durchgeführt wurde. • **Fehlgeschlagen.** Ein fehlgeschlagener Job, der nicht abgeschlossen wurde.
Dienstsymbol	Über diese Schaltfläche wird die Jobliste um Dienstjobs erweitert. Wenn Sie auf dieses Symbol klicken, wird in jedem Statussymbol ein kleineres Dienstsymbol angezeigt, damit Sie nach Dienstjobs mit dem jeweiligen Status filtern können (sofern vorhanden). Beispiele für Dienstjobs sind das Löschen von Indexdateien oder das Entfernen einer Maschine aus der Schutzfunktion.
Dropdown-Liste „Exporttyp“	Die Dropdown-Liste enthält die Formate, in die der Ereignisbericht exportiert werden kann. Nur für Tasks verfügbar. Sie umfasst folgende Formate: • PDF • HTML • CSV • XLS • XLSX
(Exportsymbol)	Konvertiert den Ereignisbericht in das ausgewählte Format. Nur für Tasks verfügbar.
Seitenauswahl	Ereignisberichte können verschiedene Jobs auf mehreren Seiten enthalten. Mit den Zahlen und Pfeilen unten in der Seite **Ereignisse** können Sie zu den Seiten des Berichts navigieren.

Auf der Seite **Ereignisse** werden alle Ereignisse in einer Tabelle angezeigt. Die folgende Tabelle führt die angezeigten Informationen zu jedem Element auf.

Tabelle 5. Detaillierte Informationen zur Übersichtstabelle „Ereignisse“

UI-Element	Description
Status	Zeigt den Status der Task, Warnung oder des Journalelements an. Verfügbar für Warnungen oder Journalelemente. Kicken Sie auf die Kopfzeile, um die Ergebnisse nach Status zu filtern.
Name	Nur für Tasks verfügbar. Dieses Textfeld gibt den Tasktyp an, der für diese geschützte Maschine abgeschlossen wurde. Beispiele sind die Übertragung von Volumes, die Wartung des Repository, Durchführen eines Rollups, Überprüfung der Bereitstellungsfähigkeit, Durchführen von Prüfsummen-Überprüfungen usw.
Startzeit	Verfügbar für Tasks, Warnungen und Journalelemente. Zeigt das Datum und die Uhrzeit an, an dem bzw. zu der der Job oder die Task begann.

UI-Element	Description
Endzeit	Nur für Tasks verfügbar. Zeigt das Datum und die Uhrzeit an, an dem bzw. zu der die Task beendet wurde.
Jobdetails	Nur für Tasks verfügbar. Öffnet das Dialogfeld**Aktive Task überwachen**, so dass Sie Details des spezifischen Job oder der Task anzeigen können. Diese Details umfassen eine ID für den Job, die Geschwindigkeit, mit der die Daten vom Core übertragen wurden (falls relevant), die zum Abschluss des Jobs verwendete Zeit, der Gesamtaufwand in Anzahl an Gigabyte sowie alle untergeordneten Aufgaben im Zusammenhang mit dem Job.
Meldung	Verfügbar für Warnungen und Journalelemente. Dieses Textfeld enthält einen beschreibenden Inhalt der Warnung oder des Journalelements.

Anzeigen von Berichten für eine geschützte Maschine

Über das Dropdown-Menü **Berichte** können Sie bei Bedarf für die ausgewählte geschützte Maschine Berichte generieren.

- Der Jobbericht bietet einen Bericht über den Status erfolgreicher und fehlgeschlagener Jobs für die ausgewählte Maschine. Fehlgeschlagene Jobs können im Fehlerbericht genauer angezeigt werden. Weitere Informationen zu dieser Berichtsart, siehe Grundlegende Informationen zu Jobberichten.
- Der Fehlerbericht enthält Informationen zu fehlgeschlagenen und abgebrochenen Core-Jobs für die angegebene Maschine. Weitere Informationen zu dieser Berichtsart, siehe Grundlegende Informationen zu Fehlerberichten.

Weitere Informationen zum Erstellen dieser Berichte finden Sie unter Bedarfsweise Generierung eines Core-Berichts.

Anzeigen von replizierten Maschinen über das Navigationsmenü

Wenn Ihr Core Maschinen von einem anderen Rapid Recovery Core repliziert, wird der Anzeigename des Quell-Core als reduzierbares Menü im linken Navigationsbereich der Core Console angezeigt. Wie bei allen Menübezeichnungen im Navigationsbereich wird der Menüname dieser replizierten Maschine in Großbuchstaben unterhalb des Menüs „Geschützte Maschinen“ angezeigt. Standardmäßig ist das Menü der replizierten Maschinen vollständig erweitert und es sind alle von diesem Quell-Core stammenden Maschinen, die auf Ihren Ziel-Core repliziert werden, aufgelistet.

Sie können die Ansicht der replizierten Maschinen von diesem Quell-Core reduzieren oder erweitern, indem Sie auf den Pfeil auf der linken Seite dieses Menüs klicken.

Jedes Menü replizierter Maschinen enthält auf der rechten Seite ein Dropdown-Menü mit den Funktionen, die gleichzeitig für alle von diesem Core stammenden replizierten Maschinen durchgeführt werden können.

Klicken Sie auf den Pfeil rechts neben dem Menü replizierter Maschinen, um eine Dropdownliste der Funktionen anzuzeigen, die Sie ausführen können. Folgende Aktionen sind verfügbar:

- Replikation vorübergehend deaktivieren Wenn die Replikation derzeit aktiv ist, wird die Aktion gestoppt, bis Sie sie wieder aufnehmen.
- Replikation wieder aufnehmen Wenn die Replikation angehalten wurde, wird die Replikation wieder begonnen.
- Replikation erzwingen. Repliziert bei Bedarf, anstatt zu einem festgelegten Zeitpunkt.
- Replikation aufheben. Entfernt die Replikationsbeziehung zwischen Quell-Core und Ihren Ziel-Core. Optional können Sie die in diesem Core gespeicherten Wiederherstellungspunkte löschen. Weitere Informationen finden Sie unter Entfernen einer ausgehenden Replikation vom Quell-Core bzw. Eingehende Replikation vom Ziel-Core entfernen.

Durch direktes Klicken auf den Namen des Quell-Core im Navigationsmenü wird die Seite **Machines replicated from [Source Core Name]** (Von [Quell-Core-Name] replizierte Maschinen) im Hauptinhaltsbereich angezeigt. Weitere Informationen zu den Aktionen, die Sie auf der Seite ausführen können, finden Sie unter Anzeigen von ein- und ausgehender Replikation.

Anhalten und Fortsetzen der Replikation
Erzwingen einer Replikation
Entfernen einer ausgehenden Replikation vom Quell-Core
Eingehende Replikation vom Ziel-Core entfernen

Anzeigen des Menüs „Nur Wiederherstellungspunkte“

Das Menü „Nur Wiederherstellungspunkte“ wird im linken Navigationsbereich angezeigt, wenn eine der folgenden Bedingungen zutrifft:

- Wenn Ihr Rapid Recovery Core einige Wiederherstellungspunkte von einer Maschine, die zuvor geschützt wurde, beibehält.
- Wenn Sie die Replikation entfernt aber die Wiederherstellungspunkte beibehalten haben.

Wie bei allen Menüs im Navigationsbereich wird die Menübeschriftung in Großbuchstaben angezeigt.

Sie können die Ansicht für „Nur Wiederherstellungspunkte“-Maschinen reduzieren oder erweitern, indem Sie auf den Pfeil auf der linken Seite dieses Menüs klicken.

Das Menü enthält auf der rechten Seite ein Dropdown-Menü mit den Funktionen, die für alle „Nur Wiederherstellungspunkte“-Maschinen durchgeführt werden können. In diesem Fall ist nur eine Funktion verfügbar, mit der Sie Wiederherstellungspunkte vom Core entfernen können.

CAUTION: Diese Aktion entfernt alle „Nur Wiederherstellungspunkte-Maschinen“ im Rapid Recovery **Core. Die Wiederherstellungspunkte werden dadurch unwiderruflich gelöscht, sodass die betreffenden Wiederherstellungspunkte auf diesem Core nicht mehr wiederhergestellt werden können.**

Anzeigen des Menüs für benutzerdefinierte Gruppen

Das Menü für benutzerdefinierte Gruppen wird nur dann im linken Navigationsbereich angezeigt, wenn mindestens eine benutzerdefinierte Gruppe erstellt wurde. Wie bei allen Menüs im Navigationsbereich wird die Menübeschriftung in Großbuchstaben angezeigt.

Sie können die Ansicht für Elemente in diesem Menü reduzieren oder erweitern, indem Sie auf den Pfeil auf der linken Seite klicken.

Das Menü für benutzerdefinierte Gruppen enthält auf der rechten Seite ein Dropdown-Menü mit den Funktionen, die gleichzeitig für alle gleichartigen Elemente in der jeweiligen Gruppe durchgeführt werden können.

Weitere Informationen finden Sie unter Grundlegende Informationen zu benutzerdefinierten Gruppen.

Verwendung des Fehlerdialogfelds

Wenn in der Benutzeroberfläche der Rapid RecoveryRapid Recovery Core Console ein Fehler festgestellt wird, z. B. beim Versuch, einen ungültigen Parameter einzugeben, wird ein Fehlerdialogfeld angezeigt. Im Dialogfeld werden normalerweise die Fehlerursache sowie Links mit weiteren Informationen zum Fehler sowie die Schaltfläche „Schließen“ angezeigt. Sie müssen das Fehlerdialogfeld schließen, damit Sie fortfahren können. Sie sollten jedoch ggf. weitere Informationen zum Fehler anzeigen.

Im Fehlerdialogfeld sind die folgenden Optionen verfügbar:

Benutzeroberflächenfehler, die zur Anzeige des Fehlerdialogfelds führen, werden auf der Rapid Recovery-Seite für Ereignisse nicht angezeigt, da es sich lediglich um Validierungs- oder Dateneingabefehler handelt. Wenn Sie jedoch auf die Option „Knowledge Base durchsuchen“ für einen Fehler klicken, wird der für den Fehler zurückgegebene URL-Link in der Datei „CoreAppRecovery.log“ protokolliert. Sie können in der Protokolldatei die Textzeichenfolge „KB article url generated“ suchen, um die in einem Browser angezeigte URL der Fehler zu ermitteln. Weitere Informationen zum Herunterladen oder Anzeigen von Core-Fehlerprotokollen finden Sie unter Herunterladen und Anzeigen der Core-Protokolldatei bzw. Zugriff auf Core-Protokolle.

Core-Einstellungen

In diesem Abschnitt wird beschrieben, wie Sie die Einstellungen für Ihre Rapid Recovery Core verwalten und ändern, und die wichtigsten Funktionstasten und Tools in der Core Console.

Die Rapid Recovery Core-Einstellungen sind standardmäßig so konfiguriert, dass sie für die meisten Benutzer optimale Leistung bringen. Nach diesen Einstellungen richtet sich, welche Informationen in der Core Console angezeigt werden, und sie beeinflussen die Leistung derRapid Recovery Core. Klicken Sie auf der Symbolleiste auf (Einstellungen) für den Zugriff auf Core-Einstellungen.

Eine Reihe wichtiger Funktionen werden als Schaltflächen entlang des oberen Randes der Seite angezeigt. Für den Zugriff auf eine der folgenden Funktionen klicken Sie auf die entsprechende Schaltfläche. Weitere Informationen zu diesen Schaltflächen finden Sie unter Hauptfunktionen von Core-Einstellungen.

Unter den Tasten-Funktionstasten befinden sich die konfigurierbaren Einstellungen des Core. Um alle Konfigurationsoptionen für eine Einstellung zu sehen, klicken Sie auf eine Verknüpfung auf der linken Seite des Fenster „Einstellungen“ oder blättern Sie nach unten zum rechten Rand der Seite. Weitere Informationen zu sämtlichen Core-Einstellungen finden Sie unter Rapid Recovery Core-Einstellungen.

Sie können auch auf Core-Tools zugreifen, wie z. B. die Anzeige einer Zusammenfassung von Systeminformationen und Core-Protokolldateien herunterladen. Weitere Informationen finden Sie unter Tools auf Core-Ebene.

Hauptfunktionen von Core-Einstellungen

Eine Reihe wichtiger Funktionen sind als Schaltflächen entlang des oberen Randes der Seite (Einstellungen) angeordnet. Für den Zugriff auf eine der folgenden Funktionen klicken Sie auf die entsprechende Schaltfläche.

Die auf der Seite „Einstellungen“ angezeigten Felder werden in der folgenden Tabelle beschrieben.

Tabelle 6. Hauptfunktionen von Core-Einstellungen

Hauptfunktionstaste	Description
Sicherungseinstellungen	Sichert die Core-Konfigurationseinstellungen in einer von Ihnen benannten XML-Datei. Geben Sie einen vollqualifizierten, lokalen Pfad für den Core-Server ein.
Wiederherstellungseinstellungen	Wenn Sie über eine XML-Sicherungskopie der Core-Einstellungen verfügen, können Sie mit dieser Option den Namen und lokalen Pfad der Datei angeben, aus der Sie die Core-Einstellungen wiederherstellen. Verwenden Sie diese Funktion zum Wiederherstellen der Core-Einstellungen oder zum Migrieren von einem anderen Core. Optional können Sie auch Repositorys wiederherstellen.
Core-Dienst neu starten	Mit dieser Option wird der Dienst ordnungsgemäß heruntergefahren und dann wieder gestartet.
Core-Dienst herunterfahren	Mit dieser Option wird der Dienst ordnungsgemäß heruntergefahren.

Weitere Informationen zum Sichern und Wiederherstellen von Core-Einstellungen finden Sie unter Sichern und Wiederherstellen der Core-Einstellungen.

Weitere Informationen zum Herunterfahren und Neustarten des Core-Dienstes finden Sie unter Neustarten oder Herunterfahren des Core-Dienstes.

Sichern und Wiederherstellen der Core-Einstellungen

Sie können Core-Einstellungsinformation in einer Datei speichern und diese Einstellungen später wiederherstellen, wenn es Probleme mit der Core-Maschine gibt oder die Einstellungen auf eine andere Maschine migriert werden sollen. Die Informationen, die gesichert werden, umfassen Repositorymetadaten (z. B. Repositoryname, Datenpfad und Metadatenpfad), im Core geschützte Maschinen, Replikationsbeziehungen (Ziele und Quellen), für Virtual Standby konfigurierte Maschinen und Informationen zu Verschlüsselungsschlüsseln.

Dabei werden nur die Konfigurationseinstellungen und nicht die Daten wiederhergestellt. In der Konfigurationsdatei werden keine Sicherheitsinformationen gespeichert (z. B. Authentifizierungsinformationen). Durch das Speichern einer Konfigurationsdatei entsteht daher kein Sicherheitsrisiko.

NOTE: Sie müssen zuerst die Core-Einstellungsinformationen gesichert haben, damit die Core-Einstellungen wie nachstehend beschrieben wiederhergestellt werden können.

Gehen Sie folgendermaßen vor, um Core-Einstellungen wiederherzustellen.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen).

   Die Seite **Einstellungen** wird angezeigt. Im oberen Fensterbereich der Seite „Einstellungen“ sehen Sie über den Kategorien von Einstellungen die Schaltflächen, **Einstellungen sichern** und **Einstellungen wiederherstellen**.
3. Gehen Sie zu Schritt 4, wenn die Core-Einstellungen gesichert werden sollen. Gehen Sie zu Schritt 6, um Einstellungen wiederherzustellen.
4. Um die aktuellen Einstellungen in einer XML-Datei zu sichern, klicken Sie von der Gehäuseoberseite aus der Seite **Einstellungen** auf **Einstellungen sichern**.

   Das Dialogfeld „Core-Konfiguration sichern“ wird angezeigt.
5. Geben Sie im Textfeld „Lokaler Pfad“ einen Verzeichnispfad ein, der lokal auf der Core-Maschine zugänglich ist, auf der Core-Einstellungen als XML-Datei gespeichert werden sollen und klicken Sie dann auf **Sicherung**.

   Geben Sie z. B. `C:\Users\Your_User_Name\Documents\RRCoreSettings` ein und klicken Sie dann auf **Sichern**.

   Daraufhin wird eine Datei namens AppRecoveryCoreConfigurationBackup.xml im angegebenen lokalen Verzeichnis gespeichert.
6. Führen Sie die folgenden Schritte aus, um die Core-Einstellungen aus einer XML-Sicherungsdatei wiederherzustellen, die zuvor mit der beschriebenen Methode gespeichert wurde.

   NOTE: Bei der Wiederherstellung der Core-Konfigurationseinstellungen wird der Rapid Recovery Core-Dienst neu gestartet.

   a. Klicken Sie auf der Seite **Einstellungen** oben auf **Wiederherstellungseinstellungen**.

   Das Dialogfeld **Core-Konfiguration wiederherstellen** wird angezeigt.

   b. Geben Sie im Textfeld **Lokaler Pfad** den lokalen Pfad zum Speicherort der Core-Konfigurationseinstellungen ein.

   Geben Sie z. B. `C:\Users\Your_User_Name\Documents\RRCoreSettings` ein.

c. Gehen Sie zu Schritt g, wenn keine Repositoryinformationen wiederhergestellt werden sollen.

d. Wählen Sie ggf. **Repositorys wiederherstellen** aus und klicken Sie dann auf **Wiederherstellen**, wenn Sie in der Sicherungsdatei konfigurierte Repositoryinformationen wiederherstellen möchten.

Das Dialogfeld **Repositorys wiederherstellen** wird angezeigt.

Wenn Repositoryinformationen aus den gesicherten Konfigurationsdaten wiederhergestellt werden sollen, werden alle Repositorys, die beim Sichern der Core-Einstellungen konfiguriert waren, zur Überprüfung angezeigt. Standardmäßig sind alle vorhandenen Repositorys ausgewählt.

e. Überprüfen Sie die Repositoryinformationen, die wiederhergestellt werden sollen. Falls mehrere Repositorys zur Überprüfung in der Liste angezeigt werden und nur Informationen einiger Repositorys wiederhergestellt werden sollen, können Sie die nicht erwünschten Repositorys abwählen.

f. Wenn Sie zufrieden sind mit der Auswahl von Repositorys, die Sie wiederherstellen möchten, klicken Sie auf **Speichern**.

Das Dialogfeld **Repositorys wiederherstellen** wird geschlossen.

g. Klicken Sie im Dialogfeld **Repositorys wiederherstellen** auf **Wiederherstellung**.

Das Dialogfeld **Restore Repositorys** wird geschlossen, und der Wiederherstellungsvorgang beginnt. Es wird eine Benachrichtigung mit dem Hinweis angezeigt, dass die Konfiguration des Repositorydienstes geändert wurde.

h. Wenn Konfigurationseinstellungen nicht wiederhergestellt werden konnten, wird eine Fehlermeldung angezeigt. Überprüfen Sie die Fehlerdetails, um festzustellen, ob Maßnahmen ihrerseits erforderlich sind. Weitere Informationen hierzu finden Sie unter Anzeigen von Ereignissen mithilfe von Aufgaben, Warnungen und Journalseiten. Klicken Sie auf **Schließen**, um fortzufahren und das Fehlerdialogfeld zu schließen.

i. Nach der Wiederherstellung der Konfiguration, stellen Sie sicher, dass die folgenden Bedingungen zutreffen:

- Alle Verschlüsselungsschlüssel entsperren. Weitere Informationen hierzu finden Sie unter Entsperren eines Verschlüsselungsschlüssels.
- Wenn Virtual Standby so konfiguriert ist, ständig eine VM auf ein Netzwerk-Ziel zu aktualisieren, müssen Sie die Anmeldeinformationen für das Netzwerk in den virtuellen Standby-Einstellungen vor der erfolgreichen Synchronisierung angeben. Weitere Informationen hierzu finden Sie unter VM-Export.
- Wenn die geplante Archivierung so konfiguriert ist, dass in ein Cloud-Konto archiviert wird, müssen Sie die Anmeldeinformationen angeben, sodass der Core eine Verbindung zum Cloud-Konto herstellen kann. Weitere Informationen über die Verknüpfung des Core mit einem Cloud-Konto finden Sie unter Hinzufügen eines Cloud-Kontos.
- Überprüfen Sie die Einstellungen für den Ziel-Core im Quell-Core (insbesondere den Host), wenn eine Replikation eingerichtet ist und Sie auf einem Ziel-Core wiederherstellen möchten. Weitere Informationen zum Verwalten Ihres eigenen Core finden Sie unter Replikation auf einen selbstverwalteten Ziel-Core. Informationen zum Replizieren auf einen von einem Drittanbieter verwalteten Core finden Sie unter Replikation auf den Ziel-Core eines externen Anbieters.
- Wenn die SQL-Anfügbarkeitsprüfung konfiguriert ist, und wenn die SQL Server-Instanz, die die Prüfung durchführt, auf der Core-Maschine ist, geben Sie anschließend die SQL-Anmeldeinformationen in-Anfügbarkeitseinstellungen ein. Weitere Informationen hierzu finden Sie unter Verwalten von Core-SQL-Anfügbarkeitseinstellungen.

Stellen Sie sicher, dass die Replay-Engine-Konfiguration wiederhergestellt wurde, und aktualisieren Sie die Einstellungen (falls nicht geschehen), um eine effektiven Kommunikation sicherzustellen. Weitere Informationen hierzu finden Sie unter Konfigurieren von Replay Engine-Einstellungen.

Neustarten oder Herunterfahren des Core-Dienstes

Ein Maschine, auf der Rapid Recovery Core ausgeführt wird, wird unweigerlich heruntergefahren oder muss neu gestartet werden. In Version 6.2 wurde Rapid Recovery Core verbessert, damit die Core-Dienste jetzt ordnungsgemäß heruntergefahren und neu gestartet werden können.

Die Core-UI bietet jetzt UI-Funktionen, um den Core-Dienst mit einem Klick herunterzufahren oder neu zu starten. Diese Funktion ist nützlich, wenn eine geplante Wartung des Core-Servers (einschließlich Neustart) erforderlich ist. Benutzer erhalten eine Benachrichtigung, wenn die entsprechenden Dienste heruntergefahren wurden. Der Zugriff auf diese Funktionen erfolgt über den oberen Rand der Seite „Core-Einstellungen“.

NOTE: Eine weitere nützliche Funktion, die ein ordnungsgemäßes Herunterfahren unterstützt, ist die Möglichkeit, den Core zu deaktivieren, damit er keine zukünftigen Aufgaben plant. Weitere Informationen dazu finden Sie unter Unterbrechen oder Wiederaufnehmen geplanter Aufgaben.

Verwenden Sie dieses Verfahren zum Starten oder Herunterfahren des Core-Dienstes.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen).

   Die Seite **Einstellungen** wird angezeigt. Im oberen Fensterbereich der Seite „Einstellungen“ sehen Sie über den Kategorien von Einstellungen die Optionen **Core-Dienst neu starten** oder **Core-Dienst herunterfahren**.
3. Wenn Sie den Core-Dienst neu starten möchten, klicken Sie am oberen Rand des Fensterbereichs „Einstellungen“ auf **Core-Dienst neu starten**.

   Eine Liste der einzelnen Aufgaben, die vor einem Neustart ausgeführt werden müssen, wird angezeigt, darunter eine Anzeige des Aufgabenfortschritts.
4. Optional können Sie einen der folgenden Schritte ausführen:
   a. Um einen Neustart zu erzwingen (kein ordnungsgemäßer Prozess, bei dem Aufgaben explizit angehalten werden, bevor sie abgeschlossen sind), klicken Sie auf **Neustart erzwingen**.
   b. Um den Neustart des Core-Dienstes abzubrechen, klicken Sie auf **Abbrechen**.
5. Wenn Sie den Core-Dienst herunterfahren möchten, ohne ihn sofort wieder neu zu starten, klicken Sie am oben Rand des Fensterbereichs „Einstellungen“ auf **Core-Dienst herunterfahren**.
6. Optional können Sie einen der folgenden Schritte ausführen:
   a. Um ein Herunterfahren zu erzwingen (kein ordnungsgemäßer Prozess, bei dem Aufgaben explizit angehalten werden, bevor sie abgeschlossen sind), klicken Sie auf **Herunterfahren erzwingen**.
   b. Um den Neustart des Core-Dienstes abzubrechen, klicken Sie auf **Abbrechen**.

Zugehörige Tasks

See also: Unterbrechen oder Wiederaufnehmen geplanter Aufgaben

Rapid Recovery Core-Einstellungen

Das Fenster „Einstellungen“ enthält eine Navigationsspalte auf der linken Seite, in der jede Core-Einstellung aufgelistet ist. Klicken Sie auf einen Link in der Liste, oder blättern Sie nach unten auf der rechten Seite, um alle Konfigurationsoptionen für jeden Core zu sehen.

Wenn Sie auf eine Einstellung klicken, die Sie ändern möchten, kann diese Einstellung nun bearbeitet werden. Führen Sie eine der folgenden Aktionen aus:

- Wenn das Bedienelement ein Drop-Down-Menü ist, klicken Sie auf den nach unten gerichteten Pfeil, um die Optionen anzuzeigen, und wählen Sie die gewünschte Option aus dem Menü aus.
- Wenn das Bedienelement ein Textfeld ist, geben Sie einen Wert ein.
- Wenn als Option „Ja“ oder „Nein“ angezeigt wird, klicken Sie auf den Wert, der durch ein Kontrollkästchen ersetzt wird. Für die Einstellung von „Ja“ aktivieren Sie das Kontrollkästchen. Für den Wert „Nein“ deaktivieren Sie das Kontrollkästchen.
- Wenn die Option einen Zeitwert anzeigt (zum Beispiel Stunden, Minuten und Sekunden), klicken Sie auf jede Komponente und geben Sie einen neuen Wert ein oder verwenden Sie die Aufwärts- und Abwärtspfeile, um die neuen Werte zu wählen.

Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf ✔, um die Änderungen zu bestätigen und zu speichern, und verlassen Sie den Bearbeitungsmodus oder klicken Sie auf ✖, um den Bearbeitungsmodus ohne Speichern zu beenden.

Die Rapid Recovery Core Einstellungen, die Sie erstellen können, sind in der folgenden Tabelle beschrieben. Jede Einstellung verfügt über einen Link zu einem relevanten Thema mit weiteren Informationen.

Tabelle 7. Rapid Recovery konfigurierbare Core-Einstellungen

Konfigurationseinstellung	Beschreibung
Allgemein	Allgemeine Einstellungen sind Konfigurationsoptionen, die allgemein für Rapid Recovery Core gelten, z. B. Anzeigeoptionen und Ports für den Webserver und den Rapid Recovery Dienst. Weitere Informationen zu den allgemeinen Einstellungen für Rapid Recovery Core sowie zum Konfigurieren dieser Einstellungen finden Sie unter Konfigurieren von allgemeinen Core-Einstellungen.
Aktualisierungen	Die Aktualisierungseinstellungen steuern Aspekte der automatischen Updatefunktion, die aktualisierte Versionen der Rapid Recovery Software sucht. Weitere Informationen zu den Einstellungen zum Aktualisieren von Rapid Recovery Core sowie zum Konfigurieren dieser Einstellungen finden Sie unter Konfigurieren von Updateeinstellungen.
Nächtliche Jobs	Die Einstellungen für nächtliche Jobs umfassen automatisierte Aufgaben, die der Core täglich ausführt. Sie können festlegen, wann die Jobs gestartet und welche Jobs durchgeführt werden. Quest empfiehlt, die Jobs außerhalb der normalen Geschäftszeiten zu planen, um eine mögliche Belastung des Systems zu verringern, wenn die Nachfrage nach Ressourcen hoch ist. Weitere Informationen finden Sie unter Grundlegende Informationen zu nächtlichen Jobs, Konfigurieren nächtlicher Jobs für den Core und Anpassen der nächtlichen Jobs für eine geschützte Maschine.
Übertragungswarteschlange	Die Einstellungen für die Übertragungswarteschlange überwachen die Anzahl der Wiederholungen von Übertragungsvorgängen, wenn Jobs fehlschlagen, weil Ressourcen nicht verfügbar sind. Sie können die maximale Anzahl gleichzeitiger Übertragungen sowie die maximale Anzahl von Wiederholungsversuchen für die Übertragung von Daten festlegen. Weitere Informationen zu den Einstellungen für die Übertragungswarteschlange finden Sie unter Ändern der Einstellungen für die Übertragungswarteschlange.

Konfigurationseinstellung	Beschreibung
Zeitlimiteinstellungen für Client	Die Zeitlimiteinstellungen für Clients bestimmen das zulässige Zeitlimit, in dem bestimmte Verbindungsanforderungen bzw. Lese- und Schreibvorgänge durchgeführt werden müssen. Weitere Informationen zu den Zeitlimiteinstellungen für Clients finden Sie unter Anpassen der Client-Zeitlimiteinstellungen.
DVM-Deduplizierungs-Cache	Die Deduplizierung sorgt dafür, dass einzigartige Informationsblöcke nur einmal im Repository gespeichert und Verweise auf mehrmals vorkommende Datenblöcke erstellt werden. Die Verweise werden in einem Deduplizierungscache gespeichert. Werden Verschlüsselungsschlüssel verwendet, wird die Deduplizierung in den einzelnen Verschlüsselungsdomänen durchgeführt. Mit den DVM-Deduplizierungscacheeinstellungen können Sie Cachegröße und Speicherort für den primären und sekundären Cache sowie den Speicherort für den Metadatencache konfigurieren. Weitere Informationen zum Deduplizierungscache finden Sie unter Grundlegende Informationen zu Deduplizierungscache und Speicherorten. Informationen zum Anpassen der Einstellungen finden Sie unter Konfigurieren von DVM-Deduplizierungscache-Einstellungen.
Replay Engine	Replay Engine-Einstellungen steuern Informationen bezüglich des Kommunikationskanals für die Replay Engine, wie z. B. IP-Adressen und Timeout-Einstellungen, um Sie beim Anpassen der Leistung für Ihre spezifischen Netzwerkanforderungen zu unterstützen. Weitere Informationen zu diesen Engine-Einstellungen für Rapid Recovery finden Sie unter Konfigurieren von Replay Engine-Einstellungen.
Bereitstellung	Mit den Bereitstellungseinstellungen können Sie Optionen für die Bereitstellung der Rapid Recovery Agenten-Software vom Core aus auf die zu schützenden Maschinen festlegen. Weitere Informationen zum Konfigurieren der Bereitstellungseinstellungen finden Sie unter Konfigurieren von Bereitstellungseinstellungen.
Datenbankverbindung	Rapid Recovery speichert diese Transaktionsinformationen in einer MongoDB-Dienstdatenbank, die standardmäßig lokal auf der Core-Maschine installiert ist. Sie können diese Einstellungen konfigurieren, um die Aufbewahrungsdauer der Informationen in der Datenbank oder die Größe des Verbindungspools zu ändern, damit mehr oder weniger gleichzeitige Verbindungen möglich sind. Weitere Informationen zum Festlegen oder Ändern der Datenbankverbindungseinstellungen finden Sie unter Konfigurieren von Datenbankverbindungseinstellungen.
Lokale Datenbankeinstellungen	Rapid Recovery zeigt Informationen zu Core-Aufgaben, Ereignissen und Benachrichtigungen auf der Registerkarte „Ereignisse“ an. Rapid Recovery speichert diese Transaktionsinformationen in einer MongoDB-Dienstdatenbank, die lokal auf derselben Maschine wie der Rapid Recovery Core installiert ist. Sie können die Anmeldeinformationen (Benutzername und Kennwort) für die lokale Mongo-Dienstdatenbank über die Einstellungen für die lokale Datenbank konfigurieren. Informationen zum Anpassen der Einstellungen der lokalen Datenbank finden Sie unter Ändern der lokalen Einstellungen für Datenbankverbindung.
SMTP-Server	Konfigurieren Sie SMTP-Servereinstellungen (Simple Mail Transfer Protocol) für den Core, um diese Core-Ereignisinformationen auch per E-Mail zu senden.

Konfigurationseinstellung	Beschreibung
	Weitere Informationen zum Konfigurieren eines SMTP-E-Mail-Servers finden Sie unter Konfigurieren eines E-Mail-Servers. **NOTE:** Um Ereignisinformationen per E-Mail senden zu können, müssen Sie auch Benachrichtigungsgruppeneinstellungen konfigurieren. Weitere Informationen zum Angeben von Ereignissen, für die E-Mail-Benachrichtigungen erstellt werden sollen, finden Sie unter Konfigurieren von Benachrichtigungsgruppen.
Cloud-Konten	Über die Cloud-Konto-Einstellungen können Sie Konfigurationseinstellungen für unterstützte Cloud-Konten angeben. Mit diesen Einstellungen können keine Cloud-Konten erstellt werden. Stattdessen verknüpfen Sie vorhandene externe Cloud-Speicher- oder Cloud-Dienstanbieter-Konten mit Ihrem Rapid Recovery Core, um Aktionen, wie z. B. die Archivierung von Rapid Recovery Informationen zu erleichtern. Informationen zum Einstellen der Zeitüberschreitungseinstellungen für Cloud-Konten finden Sie unter Konfigurieren von Verbindungseinstellungen des Cloud-Kontos. Weitere Informationen zum Definieren eines Cloud-Kontos im Rapid Recovery Core Console finden Sie unter Cloud-Konten.
Azure Management-Zertifikate	Damit Informationen über Ihre Azure Abonnements für die Core Console verfügbar sind, müssen Sie ein Azure Management-Zertifikat laden, das dem Core zugeordnet werden kann. In der Core Console können Sie neue Zertifikate laden, die Ansicht der Zertifikate, die derzeit Ihrem Core zugeordnet sind, aktualisieren oder ein derzeit Ihrem Core zugeordnetes Azure Zertifikat löschen. Weitere Informationen zur Verwendung von Azure Management-Zertifikaten mit dem Core finden Sie unter Arbeiten mit Azure Management-Zertifikaten, die mit Ihrem Core verknüpft sind.
Berichte	Die Berichtseinstellungen umfassen Konfigurationsparameter, mit denen Sie die Schriftart auswählen können, die für mit Rapid Recovery Core generierte Berichte verwendet wird. Sie können auch das Papierformat und die Seitenausrichtung für Berichte festlegen. Weitere Informationen zu den Berichteinstellungen finden Sie unter Verwalten von Berichteinstellungen.
Anfügbarkeit	Mit den Einstellungen für die Anfügbarkeit können Sie angeben, dass auf dem geschützten Rechner SQL-Anfügbarkeits-Checks ausgeführt werden oder ob die SQL Serverinstanz auf dem Core verwendet wird. Bei der Angabe von SQL auf dem Core müssen Sie Anmeldeinformationen bereitstellen. Weitere Informationen wie die Einstellungen der SQL-Anfügbarkeit für den Core verwaltet werden, finden Sie unter Verwalten von Core-SQL-Anfügbarkeitseinstellungen.
Jobs	Core-Jobs werden automatisch erstellt, wenn Vorgänge eingeleitet werden, z. B. eine Replikation. Sie können mit den Jobs-Core-Einstellungen für jeden Job Einstellungen festlegen. Sie können die Anzahl der Jobs konfigurieren, die gleichzeitig ausgeführt werden können. Falls Netzwerk- oder andere Kommunikationsprobleme verhindern, dass ein Job beim ersten Mal erfolgreich ausgeführt wird, können Sie mit der Einstellung für die Wiederholungsversuchsanzahl die Anzahl der Wiederholungsversuche für den Job festlegen. Weitere Informationen zu Core-Jobs, den verfügbaren Jobs sowie zum Konfigurieren der Jobs finden Sie unter Core-Jobeinstellungen.

Konfigurationseinstellung	Beschreibung
Lizenzierung	Rapid Recovery bietet die Möglichkeit, in der Core Console die Lizenz für den Core zu ändern, die Anzahl der täglichen Snapshots zu begrenzen, Lizenzpoolinformationen anzuzeigen und eine Verbindung zum Lizenzserver herzustellen. Weitere Informationen zur Verwaltung von Lizenzen auf dem Core finden Sie unter Verwalten von Lizenzen. Weitere Informationen zur Lizenzverwaltung finden Sie unter *Rapid Recovery Lizenzportal - Benutzerhandbuch*. **NOTE:** Das Rapid Recovery Lizenzportal hat einen anderen Versionszyklus als die Rapid Recovery Software. Die neueste Produktdokumentation finden Sie auf der Quest Technical Documentation-Website.
SNMP-Konfiguration	Das SNMP-Protokoll (Simple Network Management Protocol) ermöglicht die Verwaltung von Geräten in einem IP-Netzwerk. Sie können den Rapid Recovery Core als einen SNMP-Agenten konfigurieren. Der Core kann Informationen wie Benachrichtigungen, Repositorystatus und geschützte Maschinen melden. Weitere Informationen zur Verwendung von SNMP mit Rapid Recovery finden Sie unter Grundlegende Informationen zu SNMP-Einstellungen.
vSphere	Die vSphere Core-Einstellungen gelten nur für Benutzer des agentenlosen Schutz von virtueller Maschinen. Bei der Verwendung eines vSphere Hosts beinhalten diese Einstellungen Verbindungseinstellungen, die für die VMs gelten. Weitere Informationen über die Einstellungen von vSphere für agentenlosen Schutz von VMware oder ESXi finden Sie unter Konfigurieren von vSphere-Einstellungen.
VMware-Proxy	Wenn ein VMware-Proxy-Dienst mit dem Core installiert ist, können Benutzer Dienst-Zeitüberschreitungen im Zusammenhang mit VMware Disk Storage festlegen. Weitere Informationen zu diesen Einstellungen finden Sie unter Verwalten der VMware Proxy-Einstellungen.
Datenschutz-Portal	Wenn Sie zwei oder mehr Cores haben, können Sie Ihren Core-Server mit dem Quest Datenschutzportal integrieren. Mit dieser Funktion, die besonders nützlich für Managed Service-Anbieter ist, können Sie mehrere Cores verwalten, haben Sie Zugriff auf ein Dashboard, in dem Sie Aufgaben und Ereignisse überwachen, Repository-Status anzeigen und die Systemintegrität prüfen können, können Sie Berichte erstellen und eine immer größere Liste anderer Funktionen aus einer einzigen Web-basierten Benutzeroberfläche heraus durchführen. Verwenden Sie diese Einstellung, um den Zugriff auf das Portal zu aktivieren oder zu deaktivieren.
vFoglight	Quest Foglight for Virtualization (vFoglight) unterstützt Administratoren bei der Überwachung, Analyse und Optimierung von Hypervisoren, einschließlich VMware, Hyper-V und OpenStack-Umgebungen. Für Kunden, die VMs mit vFoglight verwalten und sie auf einer Rapid Recovery Console schützen, ermöglicht diese Core-Einstellung, die Navigation für beide Produkte zu integrieren. Nach erfolgreicher Eingabe der vFoglight Einstellungen durch Klicken auf die vFoglight-URL auf der Seite **Zusammenfassung** für VM in der Core Console können Benutzer zur entsprechenden Seite für diese virtuelle Maschine in vFoglight navigieren. Weitere Informationen zu den vFoglight Core-Einstellungen finden Sie unter Konfigurieren von vFoglight-Einstellungen. Weitere Informationen zu vFoglight finden Sie auf der vFoglight - Produktseite auf der Quest Website.

Sie können auch auf Core-Tools zugreifen, wie z. B. die Anzeige einer Zusammenfassung von Systeminformationen und Core-Protokolldateien herunterladen. Weitere Informationen hierzu finden Sie unter Tools auf Core-Ebene.

Konfigurieren von allgemeinen Core-Einstellungen

Die allgemeinen Einstellungen für den Rapid Recovery Core umfassen den Anzeigenamen des Core, den Webserverport, den Dienstport, das Gebietsschema (die Anzeigesprache der Core Console) sowie das Farbthema der Anzeige.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite "Einstellungen" auf **Allgemein**.
   - Scrollen Sie auf der rechten Seite der Seite "Einstellungen" bis zur Überschrift "Allgemein".
3. Klicken Sie auf die allgemeine Einstellung, die Sie ändern möchten.

   Die ausgewählte Einstellung kann nun in einem Textfeld oder in einem Drop-Down-Menü bearbeitet werden.
4. Geben Sie die Konfigurationsinformationen ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 8. Informationen zu allgemeinen Einstellungen

Textfeld	Description
Core-ID	Jeder Core hat eine einzigartige Core-ID. Diese ID wird zum Beispiel für die Integration Ihres Core mit dem Datenschutz-Portal verwendet, um Berichterstattung oder Verwaltung von zwei oder mehr Cores zu ermöglichen. Der Core-ID ist jetzt unter „Allgemeine Einstellungen“ aufgeführt. **NOTE:** Dieses Feld kann nicht konfiguriert werden.
Anzeigename	Geben Sie einen neuen Anzeigenamen für den Core ein. Dies ist der Name, der in Rapid Recovery Core Console und (sofern aktiviert) in Datenschutz-Portal angezeigt wird. Sie können bis zu 64 Zeichen eingeben.
Webserverport	Geben Sie eine Portnummer für den Webserver ein. Der Standardport ist 8006. **NOTE:** Quest empfiehlt die Verwendung des Standard-Ports.
Dienstport	Geben Sie eine Portnummer für den Rapid Recovery Core Dienst ein. Der Standardport ist 8006. **NOTE:** Quest empfiehlt die Verwendung des Standard-Ports.
Gebietsschema	Wählen Sie in der Drop-Down-Liste **Gebietsschema** die gewünschte Anzeigesprache aus. Sie haben die Auswahl zwischen Englisch, Französisch, Deutsch, Japanisch, Koreanisch, Portugiesisch, vereinfachtes Chinesisch und Spanisch.

Textfeld	Description
	NOTE: Nach einer Änderung der Sprache muss der Rapid Recovery Core Dienst neu gestartet werden, damit die geänderte Sprache in der Core Console angezeigt wird. Sie können den Dienst mit Hilfe der Schaltfläche **Core-Dienst neu starten** oben auf der Core-Einstellungsseite neu starten.
Thema	Wählen Sie aus der Drop-Down-Liste **Thema** den Stil aus, den Sie auf die Core Console anwenden möchten. Drei Themen stehen zur Verfügung: • **Dunkel**. Dieses Thema bietet einen durchgehenden dunkelgrauen Hintergrund auf der gesamten Oberfläche (im Menü des linken Navigationsbereichs, der oberen Schaltflächenleiste und dem primären Bereich). Textelemente und Textschaltflächen werden grauweiß angezeigt, wenn sie nicht im Fokus sind, oder weiß, wenn sie im Fokus sind. Klickbare Links werden in einem mittleren Blau angezeigt. Gelegentliche Tasten haben weißen Text auf einem mittelblauen Hintergrund. • **Hybrid**. Dieses Thema bietet den bekannten dunkelgrauen Hintergrund für das Menü des linken Navigationsbereichs und die Symbolleiste am oberen Rand der Core Console. Textelemente in diesen Bereichen sind weiß. Der primäre Bereich hat einen weißen Hintergrund mit weißen Highlights. Textelemente und Textschaltflächen werden schwarz angezeigt. Klickbare Links werden in einem dunklen Blau angezeigt. Gelegentliche Tasten haben weißen Text auf einem blauen Hintergrund. • **Hell**. Dieses Thema bietet einen sauberen, weißen Hintergrund auf der gesamten Oberfläche (im Menü des linken Navigationsbereichs, der oberen Schaltflächenleiste und dem primären Bereich). Das Quest Logo und einige Designelemente sind orange. Textelemente sind dunkelgrau, mit Titeln in Schwarz. Klickbare Links werden beim Darüberfahren blau angezeigt. Gelegentliche Tasten haben weißen Text auf einem mittelblauen Hintergrund.
Nutzung persönlicher Daten zustimmen	Um die Einstellung zum Berechtigen der Anwendung, personenbezogene Daten zu nutzen, in der Drop-Down-Liste **Nutzung persönlicher Daten zustimmen** zu ändern, wählen Sie **Ja** bzw. **Nein**. Wählen Sie im angezeigten Dialogfeld die entsprechende Lizenzdatei aus und registrieren Sie sie. Beim Upgrade oder Installieren von Rapid Recovery Core haben Sie die Möglichkeit, der Weitergabe von personenbezogenen Daten zuzustimmen. Wenn Sie mit der Weitergabe von personenbezogenen Daten durch Quest einverstanden sind, können Sie Funktionen wie automatisches Update und Datenschutz-Portal (dann standardmäßig aktiviert) verwenden. Wenn Sie der Weitergabe von personenbezogenen Daten durch Quest bei Installation nicht zustimmen, werden Sie aufgefordert, eine Non-Phone-Home-Lizenz zu registrieren. Sie müssen Zugriff auf die Non-Phone-Home-Lizenz haben, um die Änderung zu bestätigen. Unabhängig von der Option, die Sie während der Installation gewählt haben, können Sie die Einstellung **Nutzung persönlicher Daten zustimmen** in den allgemeinen Core-Einstellungen ändern. Stellen Sie sicher, dass Sie Zugang zu der Non-Phone-Home-Lizenz haben, da Sie bei dieser Aktion aufgefordert werden, die Non-Phone-Home-Lizenz hochzuladen. Wenn Sie diese Einstellung in Version 6.2 von „Ja“ auf „Nein“ ändern, gilt Folgendes: a. Sie werden aufgefordert, die Non-Phone-Home-Lizenzdatei hochzuladen.

Textfeld	Description
	b. Nach der Bestätigung der Non-Phone-Home-Lizenz werden die Update-Einstellungen für den Core automatisch so angepasst, dass nie nach Core-Updates gesucht wird oder diese installiert werden. c. Die Einstellung im Datenschutz-Portal „Verbindung mit Datenschutzportal aktivieren“ wird auf „Nein“ gesetzt. Das Gegenteil trifft jedoch nicht zu. Wenn Sie diese Einstellung von „Nein“ zu „Ja“ ändern, stimmen Sie der Weitergabe von personenbezogenen Daten durch den Core zu, es werden aber keine Daten weitergegeben, bis sie explizit die Lizenz zum Phone-Home-Modus geändert und die entsprechende Core-Einstellungen aktualisiert haben. Beispiel: a. Der Non-Phone-Home-Schlüssel bleibt registriert, bis Sie explizit einen Standard-Phone-Home-Schlüssel (den Sie vom Lizenzportal erhalten) hochladen. b. Um das automatische Update zu nutzen, ändern Sie „Neue Aktualisierungen suchen“ von „Nie“ auf „Täglich“, „Wöchentlich“ oder „Monatlich“. Ändern Sie ggf. „Updates installieren“ auf „Benachrichtigen“ oder „Updates automatisch installieren“. c. Um Informationen an Datenschutz-Portal weiterzugeben, setzen Sie „Verbindung mit Datenschutzportal aktivieren“ auf „Ja“. **NOTE:** Wenn Sie dies zuerst konfigurieren, werden Sie aufgefordert, eine Phone-Home-Lizenz hochzuladen. Grundlegende Informationen zu den Auswirkungen der Weitergabe von personenbezogenen Daten finden Sie in Datenschutzverwaltung, einschließlich Thema Verwendung von personenbezogenen Daten durch Rapid Recovery. Weitere Informationen zu den Funktionen, die Sie nicht ausführen können, wenn Sie den Non-Phone-Home-Modus verwenden, finden Sie im Thema Einschränkungen der Non-Phone-Home-Lizenz. Informationen, um eine Lizenz für den **Non-Phone-Home-Modus** anzufordern, finden Sie unter Erhalten und Verwenden von Non-Phone-Home-Lizenzen.

5. Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf ✓, um die Änderungen zu speichern und den Bearbeitungsmodus zu beenden, oder klicken Sie auf ✕, um den Bearbeitungsmodus ohne Speichern zu beenden.

Konfigurieren von Updateeinstellungen

Rapid Recovery umfasst die Funktion für automatische Updates. Bei der Installation des Rapid Recovery Core können Sie auswählen, ob die Rapid Recovery Core-Software automatisch aktualisiert werden soll, wenn Updates verfügbar sind, und wie oft das System nach Updates suchen soll.

NOTE: Die Funktion zur automatischen Aktualisierung erfordert eine Lizenz mit dem Standard-Phone-Home-Modus. Wenn Sie eine Softwarelizenz im Non-Phone-Home-Modus verwenden, ist Ihr Core nicht berechtigt, mit Rapid Recovery Lizenzportal zu kommunizieren und kann den Core nicht aktualisieren oder Sie über verfügbare Updates informieren. Weitere Informationen hierzu finden Sie unter Datenschutzverwaltung.

Rapid Recovery Releasenummern enthalten in der Regel vier Informationsblöcke, die durch Punkte getrennt sind: die Nummer für Haupt- und Neben-Release, Revision und die Build-Nummer. Beispiel: das erste Release mit dem neuen Markennamen von Rapid Recovery war 6.0.1.609. Die nächste Version war 6.0.2.142.

Die automatische Aktualisierungsfunktion vergleicht alle Ziffern in einer Releasenummer. Wenn Sie die automatische Aktualisierung aktivieren, wird die Core-Software nur dann ohne Benutzereingriff aktualisiert, wenn die Nummer für Haupt- und Neben-Release identisch sind. Es würde beispielsweise eine automatische Aktualisierung von Core Version 6.0.1.609 auf 6.0.2.142 stattfinden (beide beginnen mit 6.0). Auf dem gleichen Computer würde der Core nicht automatisch von 6.0.2.142 auf 6.1.1.XXX aktualisiert werden, da die Ziffern nach

dem ersten Punkt nicht gleich sind. Stattdessen werden Sie benachrichtigt (durch ein Banner am oberen Rand der Core Console), dass eine Aktualisierung der Core-Software verfügbar ist. Diese Benachrichtigung bietet Ihnen Gelegenheit, die Versionshinweise zu prüfen und festzustellen, ob die Aktualisierung auf die neueste Core-Version für Ihre Bedürfnisse geeignet ist.

NOTE: Informationen zum Installieren der Rapid Recovery Core-Software finden Sie im *Rapid Recovery-Installations- und Aktualisierungshandbuch*.

Sie können die vom System verwendeten Einstellungen für die Suche nach Updates jederzeit anzeigen und ändern.

CAUTION: Bei Verwendung der Replikationsfunktion kann die Konfiguration des Systems für die automatische Installation von Updates dazu führen, dass der Quell-Core vor dem Ziel-Core aktualisiert wird, sodass die Replikation fehlschlagen oder keine neue Replikation zwischen Cores eingerichtet werden kann. Quest **empfiehlt, dass Administratoren für Benutzer, die die Replikationsfunktion verwenden, automatische Updates nur auf dem Ziel-Core installieren und erst danach die Quell-Cores und anschließend die geschützten Maschinen manuell aktualisieren.**

Führen Sie die folgenden Schritte aus, um Updateeinstellungen zu konfigurieren.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite **Einstellungen** auf **Updates**.
   - Führen Sie einen Bildlauf nach unten auf der rechten Seite der Seite **Einstellungen** durch, bis Sie die Updates-Überschrift sehen können.
3. Klicken Sie auf die Einstellung, die Sie ändern möchten.

   Die ausgewählte Einstellung wird bearbeitbar.
4. Geben Sie die Konfigurationsinformationen ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 9. Informationen zu Updateeinstellungen

Textfeld	Description
Auf neue Aktualisierungen überprüfen	Wählen Sie aus, wie häufig Rapid Recovery nach Updates sucht und sie installiert. Sie können zwischen folgenden Optionen wählen: • Nie • Täglich • Wöchentlich • Monatlich Wenn Sie sich nach der ausgewählten Schwelle der vergangenen Zeit für automatische Updates entscheiden, wenn ein Update verfügbar ist, wird es installiert nachdem nächtliche Jobs abgeschlossen sind.
Updates installieren	Geben Sie an, wie verfügbare Updates verarbeitet werden sollen. Wählen Sie dazu eine der folgenden Optionen aus: • Niemals Updates suchen • Benachrichtigung über Updates anzeigen, Updates aber nicht automatisch installieren • Updates automatisch installieren
Status	Der Status zeigt an, ob neue Updates zur Verfügung stehen.

Textfeld	Description
Letzte Prüfung	Das Feld „Letzte Prüfung“ zeigt Datum und Uhrzeit an, zu dem/der das System zuletzt auf ein Update überprüft wurde. Klicken Sie auf **Jetzt prüfen**, um sofort zu überprüfen, ob ein Software-Update verfügbar ist. Diese Überprüfung erfolgt unabhängig von der Häufigkeit, die Sie festgelegt haben.

5. Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf ✓, um die Änderungen zu speichern und den Bearbeitungsmodus zu beenden, oder klicken Sie auf ✕, um den Bearbeitungsmodus ohne Speichern zu beenden.

Grundlegende Informationen zu nächtlichen Jobs

Nächtliche Jobs sind täglich ausgeführte, automatisierte Aufgaben, die zu einem vorgegebenen Zeitpunkt außerhalb der normalen Geschäftszeiten durchgeführt werden. Diese Jobs sind speicherintensiv und umfassen verschiedene Integritätsprüfungen und Datenkonsolidierungsaufgaben, die am besten durchgeführt werden, wenn der Rapid Recovery Core weniger stark ausgelastet ist.

Eine Beschreibung der nächtlichen Jobs mit dem jeweiligen Anwendungsbereich finden Sie in der folgenden Tabelle. Nächtliche Jobs können auf Core-Level verwaltet werden (das gilt für alle Maschinen, die auf dem Core geschützt sind). Die nächtlichen Jobs, die auch für eine Liste bestimmter geschützter Maschinen angewendet werden können, ist der Anwendungsbereich „geschützte Maschine“.

Tabelle 10. Informationen über nächtliche Jobs

Jobname	Bereich	Description
Ändern	k. A.	Diese Steuerung öffnet das Dialogfeld **Nächtliche Jobs**, dort können Sie Einstellungen für jede nächtliche Aufgabe aktivieren, deaktivieren oder ändern.
Uhrzeit für nächtliche Jobs	Alle	Diese Einstellung zeigt die Zeit an, wann der Start der Ausführung nächtlicher Jobs geplant ist. Quest empfiehlt, Ihren Core so zu konfigurieren, dass nächtliche Aufgaben in einer Zeit mit geringer Aktivität ausgeführt werden. Die Standardeinstellung ist 00:00 Uhr.
Überprüfen Sie Anfügbarkeit von SQL-Datenbanken	Geschützte Maschine	Prüft die Integrität von Wiederherstellungspunkten, die SQL-Datenbanken enthalten. Weitere Informationen hierzu finden Sie unter Verwalten von Core-SQL-Anfügbarkeitseinstellungen.
Überprüfen Sie bei Exchange-Datenbanken die Prüfsumme	Geschützte Maschine	Prüft die Integrität von Wiederherstellungspunkten, die EDB-Dateien, Exchange-Datenbankdateien, enthalten. **NOTE:** Diese Option wird nicht angezeigt, wenn kein Exchange Server im Core geschützt wird.
Integrität der Oracle-	Core oder geschützte Maschine	Überprüft die Integrität von Oracle Datenbanken mit dem Dienstprogramm DBVERIFY.

Jobname	Bereich	Description
Datenbanken prüfen		Ablauf: • Letzten Wiederherstellungspunkt für jede Schutzgruppe bereitstellen. • Dateien und Ordner für jedes Volumes auflisten. • Untersucht die Wiederherstellungspunkte, um sicherzustellen, dass Datendateien gültig und Datenblöcke nicht beschädigt sind. • Bereitstellung des Wiederherstellungspunktes aufheben.
Prüfen Sie die Integrität der Wiederherstellungspunkte	Core oder geschützte Maschine	Prüft die Integrität von Wiederherstellungspunkten aller geschützten Maschinen. Standardmäßig ist die Option `Check integrity of recovery points` nicht aktiviert. Ablauf: • Letzten Wiederherstellungspunkt für jede Schutzgruppe bereitstellen. • Dateien und Ordner für jedes Volumes auflisten. • Wiederherstellungspunkte überprüfen, um deren Gültigkeit sicherzustellen. • Bereitstellung des Wiederherstellungspunktes aufheben.
Verwaiste Registrierungsschlüssel auf Hyper-V-Agenten bereinigen		Für Hyper-V-Hosts, die agentenlosen Schutz in Rapid Recovery Version 6.1.x verwenden, werden durch diesen nächtlichen Job verwaiste Schlüssel, die in der Windows-Registrierung für jede Anfügen- und Trennvorgang erstellt werden, bereinigt. Die Registrierungseinträge sind harmlos, sammeln sich aber im Laufe der Zeit an und verlangsamen die Leistung. **NOTE:** Ab Rapid Recovery Version 6.2 verhindert eine verbesserte Vorgehensweise bei der Beschaffung von Speicher-Metadaten für agentenlosen Schutz durch Hyper-V das Erstellen von Registrierungseinträgen.
Konsolidieren Sie VMware Snapshots für geschützte virtuelle Maschinen	Core oder geschützte Maschine	Diese nächtliche Aufgabe ist relevant, wenn Sie native VMware-APIs zum Schutz von Maschinenverwenden, ohne die Software Rapid Recovery Agent. Sie sollten VMware Snapshots regelmäßig konsolidieren. Das Aktivieren dieser nächtlichen Aufgabe lässt Sie diese Konsolidierungen täglich ausführen. Dieser nächtliche Job enthält nur einen Parameter, Maximum der gleichzeitigen Konsolidierungen, er muss auf eine Zahl zwischen 1 und 100 eingestellt werden.
Zurückgestellte Löschjobs	Core	Mit dieser Einstellung können Sie das Entfernen von Wiederherstellungspunkten aus dem Repository bis zu der im Core für nächtliche Jobs angegebenen Zeit hinausschieben. Wenn diese Option aktiviert ist, schaltet die Core-Verarbeitung nach der Ausführung anderer nächtlicher Jobs auf den Job „Löschen von Datensätzen, die zuvor zum Löschen markiert wurden“ um. Mit diesem Job werden markierte Wiederherstellungspunkte aus dem Repository entfernt, bis sie entweder alle entfernt wurden oder bis vier Stunden seit der Durchführung der nächtlichen Jobs abgelaufen sind. Nächtliche Jobs werden dann beendet, und andere in der Warteschlange stehende Jobs werden wieder aufgenommen. Alle übrigen Löschungen finden, gleichzeitigen mit anderen Aufgaben, im Hintergrund statt bis zum nächsten Durchgang nächtlicher Jobs am folgenden Tag.

Jobname	Bereich	Description
		Standardmäßig ist die Option `Deferred Delete` nicht aktiviert. Quest empfiehlt, diesen nächtlichen Job deaktiviert zu lassen, solange Sie nicht auf Probleme mit der Übertragungsleistung im Zusammenhang mit der Löschung gesicherter Wiederherstellungspunkte stoßen. Wenn Sie diese neue Option aktivieren, empfiehlt Quest, dass Sie die Core-Jobs überprüfen, um sicherzugehen, dass die meisten Wiederherstellungspunkte, die zum Löschen markiert wurden, innerhalb einer Woche aus dem Repository gelöscht werden. Dieser Ansatz hilft dabei, ein ausgewogenes Verhältnis zwischen maximaler Übertragungsleistung und maximaler Wiedergewinnung von Repository-Speicherplatz zu wahren.
Löschen Sie alte Ereignisse und Jobs	Core	Sorgt dafür, dass die Ereignisdatenbank nicht zu groß wird, indem alte Ereignisse entfernt werden. Die Anzahl Tage ist konfigurierbar (Standardeinstellung: 30 Tage).
Protokollkürzung für Exchange	Geschützte Maschine	Sorgt dafür, dass Exchange-Protokolle nicht zu groß werden, indem das Exchange-Datenbanktransaktionsprotokoll dem letzten Wiederherstellungspunkt entsprechend gekürzt wird. **NOTE:** Diese Option wird nicht angezeigt, wenn kein Exchange Server im Core geschützt wird.
Protokollkürzung für Oracle	Geschützte Maschine	Steuert die Kürzung von Oracle Protokollen. Sofern diese Option nicht deaktiviert ist, findet die Kürzung einmal täglich bei den nächtlichen Jobs statt. • Sie können die Core-Löschrichtlinie **Automatisch** (standardmäßig aktiviert) verwenden, mit der alle lokal gespeicherten Oracle Protokolle im Rahmen der nächtlichen Jobs gelöscht werden. Protokolle für den aktuellen Tag sind bis zur Ausführung der nächtlichen Jobs weiterhin in den Sicherungs-Snapshots vorhanden. • Sie können eine benutzerdefinierte Löschrichtlinie für einen bestimmten geschützten Oracle Server auswählen. Mit der Löschrichtlinie **Neueste behalten** können Sie den Zeitraum festlegen, nach dem Oracle Protokolle gekürzt werden, während mit der Löschrichtlinie **Angegebene Anzahl behalten** eine bestimmte Anzahl von Protokolldateien behalten werden, bevor die älteren gekürzt werden. • Sie können den nächtlichen Job deaktivieren, was jedoch zu erheblichen Ansammlungen von Protokolldateien führen kann. In solchen Fällen können Benutzer Protokolldateien auch manuell kürzen, wie im Thema Manuelles Kürzen der Oracle Datenbankprotokolle beschrieben.
Protokollkürzung für SQL	Geschützte Maschine	Sorgt dafür, dass SQL Server-Protokolle nicht zu groß werden, indem das Datenbanktransaktionsprotokoll dem letzten Wiederherstellungspunkt entsprechend gekürzt wird. **NOTE:** Diese Option wird nicht angezeigt, wenn kein SQL Server im Core geschützt wird.

Jobname	Bereich	Description
Rollup	Core oder geschützte Maschine	Wendet die Aufbewahrungsrichtlinie auf die gesicherten Daten an, indem Wiederherstellungspunkte im Zeitplan, der in der Richtlinie vorgegeben ist, kombiniert oder „aufgerollt“ werden. Sie können die Richtlinie auf Core anpassen, sie gilt standardmäßig für alle geschützten Maschinen. Standardmäßig wird der Rollup-Job für den ganzen Core ausgeführt; oder klicken Sie auf [Erweitern], um die Anzeige der geschützten Maschinen zu erweitern. Sie können dann die Gruppe von geschützten Maschinen definieren, die Sie mit der Core-Richtlinie zurücksetzen möchten. Weitere Informationen zur Verwendung einer Aufbewahrungsrichtlinie auf einer geschützten Maschine, die sich von den Standardrichtlinien unterscheidet, finden Sie im Core unter Anpassen der Aufbewahrungsrichtlinieneinstellungen für eine geschützte Maschine.

Konfigurieren nächtlicher Jobs für den Core

Wenn eine Option für nächtliche Jobs im Rapid Recovery Core aktiviert ist, wird der ausgewählte Job einmal täglich zum angegebenen Zeitpunkt für alle Maschinen ausgeführt, die vom Core geschützt werden. Wenn Sie einen nächtlichen Job auf der Core-Ebene deaktivieren, wird der angegebene Job folglich nicht mehr für die durch den Core geschützten Maschinen ausgeführt.

NOTE: Wenn der Umfang eines nächtlichen Jobs, wie unter Grundlegende Informationen zu nächtlichen Jobs beschrieben, geschützte Maschinen umfasst, können Sie den nächtlichen Job auf bestimmte einzelne geschützte Maschinen einschränken. Weitere Informationen zur Verwendung nächtlicher Jobeinstellungen für eine geschützte Maschine finden Sie unter Anpassen der nächtlichen Jobs für eine geschützte Maschine.

Da nächtliche Jobs speicherintensiv sind, empfiehlt Quest, den Core so zu konfigurieren, dass diese Jobs in Zeiten mit geringer Auslastung durchgeführt werden. Nächtliche Jobs werden standardmäßig um 00:00 Uhr ausgeführt. Führen Sie die folgenden Schritte aus, wenn ein anderer Zeitraum besser geeignet ist, um diese Einstellung im Feld „Uhrzeit für nächtliche Jobs“ zu ändern.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite **Einstellungen** auf **Nächtliche Jobs**.
   - Scrollen Sie auf der rechten Seite der Seite **Einstellungen** bis zur Überschrift "Nächtliche Jobs".
3. Um einen nächtlichen Job zu ändern oder den Zeitpunkt zu ändern, zu dem nächtliche Jobs gestartet werden, klicken Sie auf **Ändern**.

   Das Dialogfeld **Nächtliche Jobs** wird angezeigt.
4. Geben Sie im Feld **Uhrzeit für nächtliche Jobs** eine neue Zeit ein, wenn Sie den Zeitpunkt für die Ausführung nächtlicher Jobs ändern möchten.
5. Klicken Sie in der ersten Spalte die gewünschten Optionen für nächtliche Jobs an, die Sie für den Core einstellen möchten. Klicken Sie auf eine ausgewählte Option, um sie zu löschen.
6. Klicken Sie auf **OK**.

   Das Dialogfeld **Nächtliche Jobs** wird geschlossen und die Einstellungen für nächtliche Jobs für den Core werden gespeichert.

Ändern der Einstellungen für die Übertragungswarteschlange

Die Einstellungen für die Übertragungswarteschlange sind Einstellungen auf Core-Ebene, die die maximale Anzahl gleichzeitiger Übertragungen sowie die maximale Anzahl von Wiederholungsversuchen für die Übertragung von Daten festlegen.

Führen Sie die nachstehend beschriebenen Schritte durch, um die Einstellungen für die Übertragungswarteschlange zu ändern.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite „Einstellungen“ auf **Übertragungswarteschlange** .
   - Führen Sie einen Bildlauf nach unten auf der rechten Seite der Seite Einstellungen durch, bis Sie die Übertragungswarteschlangen-Überschrift sehen können.
3. Klicken Sie auf die Einstellung, die Sie ändern möchten.

   Die ausgewählte Einstellung wird bearbeitbar.
4. Geben Sie die Konfigurationsinformationen ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 11. Einstellungsinformationen für die Übertragungswarteschlange

Textfeld	Description
Maximale Anzahl gleichzeitiger Übertragungen	Geben Sie einen Wert ein, um die Anzahl gleichzeitiger Übertragungen zu aktualisieren. Sie können eine Zahl zwischen 1 und 60 eingeben. Je kleiner die Zahl ist, desto geringer ist die Belastung von Netzwerkressourcen und anderen Systemressourcen. Mit steigender Anzahl verarbeiteter Agenten steigt auch die Belastung des Systems.
Maximale Anzahl der Wiederholungen	Geben Sie einen Wert ein, um die maximale Anzahl der Versuche vor dem Abbrechen des Übertragungsvorgangs einzustellen. Sie können eine Zahl zwischen 1 und 60 eingeben.

5. Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf , um die Änderungen zu speichern und den Bearbeitungsmodus zu beenden, oder klicken Sie auf , um den Bearbeitungsmodus ohne Speichern zu beenden.

Anpassen der Client-Zeitlimiteinstellungen

Die Client-Zeitlimiteinstellungen steuern den zulässigen Zeitraum, in dem verschiedene Vorgänge durchgeführt werden sollen.

NOTE: Quest empfiehlt, die Standardzeitlimiteinstellungen beizubehalten, sofern in der jeweiligen Umgebung keine speziellen Probleme auftreten und Sie von einem Quest Support-Mitarbeiter aufgefordert werden, die Einstellungen zu ändern.

Führen Sie die nachstehend beschriebenen Schritte aus, um die Einstellungen für das Client-Zeitlimit anzupassen.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite "Einstellungen" auf **Zeitlimiteinstellungen für Client**.
   - Scrollen Sie auf der rechten Seite der Seite "Einstellungen" bis zur Überschrift "Zeitlimiteinstellungen für Client".
3. Klicken Sie auf die Einstellung, die Sie ändern möchten.

   Die ausgewählte Einstellung wird bearbeitbar.
4. Geben Sie die Konfigurationsinformationen ein (siehe Beschreibung in der folgenden Tabelle).
5.

Tabelle 12. Informationen über Zeitlimiteinstellungen für Client

Einstellung	Description
Zeitüberschreitung Verbindung	Steuert das Zeitlimit für die Verbindung zwischen dem Core und geschützten Maschinen beim Senden von Daten über HTTP. Geben Sie die Zeitdauer ein, die vor einer Zeitüberschreitung der Verbindung verstreichen soll. Das Format ist HH:MM:SS (Stunden:Minuten:Sekunden). **NOTE:** Die Standardeinstellung ist 0:05:00 bzw. fünf Minuten.
Zeitüberschreitung Lesen/ Schreiben	Steuert das Zeitlimit für die Verbindung zwischen dem Core und geschützten Maschinen beim Lesen oder Schreiben von Streamdaten über HTTP. Ein Beispiel dafür ist der Empfang von geänderten Datenblöcken einer geschützten Maschine auf dem Core für einen inkrementellen Snapshot. Geben Sie die Zeitdauer ein, die bei einem Lese-/Schreibvorgang vor einer Zeitüberschreitung verstreichen soll. Das Format ist HH:MM:SS (Stunden:Minuten:Sekunden). **NOTE:** Die Standardeinstellung ist 0:05:00 bzw. fünf Minuten.
UI-Zeitlimit für Verbindung	Steuert die Zeitüberschreitung für die Verbindung zwischen der grafischen Benutzeroberfläche und dem Rapid Recovery Core-Dienst über HTTP. Geben Sie die Zeitdauer ein, die vor einer UI-Zeitüberschreitung der Verbindung verstreichen soll. Das Format ist HH:MM:SS (Stunden:Minuten:Sekunden). **NOTE:** Die Standardeinstellung ist 0:05:00 bzw. fünf Minuten.
UI-Zeitlimit für Lesen/ Schreiben	Steuert die Zeitüberschreitung für die Verbindung für Lese- oder Schreib-Datenströme zwischen der grafischen Benutzeroberfläche und dem Rapid Recovery Core-Dienst über HTTP. Geben Sie die Zeitdauer ein, die bei Lese-/Schreibvorgängen vor einer Zeitüberschreitung verstreichen soll. Das Format ist HH:MM:SS (Stunden:Minuten:Sekunden).

Einstellung	Description

NOTE: Die Standardeinstellung ist 0:05:00 bzw. fünf Minuten.

6. Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf ✓, um die Änderungen zu speichern und den Bearbeitungsmodus zu beenden, oder klicken Sie auf ✕, um den Bearbeitungsmodus ohne Speichern zu beenden.

Grundlegende Informationen zu Deduplizierungscache und Speicherorten

Durch die globale Deduplizierung wird der erforderliche Speicherplatz auf den Datenträgern für die über den Core gesicherten Daten verringert. Jedes Repository wird dedupliziert. Dabei werden alle einzigartigen Blocks nur ein Mal physisch auf den Datenträgern gespeichert. In nachfolgenden Sicherungen werden virtuelle Verweise oder Zeiger auf die betreffenden Blöcke verwendet. Zur Identifizierung von Duplikatblöcken enthält Rapid Recovery einen Deduplizierungscache für Deduplizierungs-Volume-Manager (DVM)-Repositorys. Der Cache enthält Verweise auf einzigartige Blöcke.

Standardmäßig umfasst dieses Deduplizierungscache für DVM-Repositorys 1,5 GB. Diese Größe ist für viele Repositorys ausreichend. Solange dieser Cache nicht überschritten wird, werden die Daten im ganzen Repository dedupliziert. Ist der Umfang der redundanten Informationen so umfangreich, dass der Deduplizierungscache voll ist, können die Vorteile der Deduplizierung für neu hinzugefügte Daten nicht vollständig genutzt werden. Der Umfang der im Repository gespeicherten Daten bevor der Deduplizierungscache voll ist hängt von der Art der gesicherten Daten ab und ist für jeden Benutzer unterschiedlich.

Sie können den DVM-Deduplizierungscache vergrößern, indem Sie die Einstellung des Deduplizierungscache im Rapid Recovery Core ändern. Weitere Informationen über eine Vergrößerung des Cache finden Sie unter Konfigurieren von DVM-Deduplizierungscache-Einstellungen.

Bei eine Vergrößerung des DVM-Deduplizierungscache müssen zwei Faktoren berücksichtigt werden: Speicherplatz und RAM-Nutzung.

Speicherplatz. Zwei Exemplare des DVM-Deduplizierungscache werden auf Datenträgern gespeichert: ein primärer Cache und ein sekundärer Cache, der eine parallele Kopie ist. Bei Verwendung der Standard-Cachegröße von 1,5 GB für ein DVM-Repository werden also 3 GB Festplattenspeicher im System verwendet. Wenn Sie den Cache vergrößern, steigt der Umfang des benötigten Speicherplatzes doppelt proportional zur Cachegröße. Um eine einwandfreie und störungsfreie Leistung sicherzustellen, ändert der Core die Priorität dieser Cachespeicher dynamisch. Beide sind erforderlich. Der einzige Unterschied besteht darin, dass der primäre Cache zuerst gespeichert wird.

RAM-Nutzung. Beim Start des Rapid Recovery Core wird der Deduplizierungscache in den Arbeitsspeicher geladen. Die Größe des Cache wirkt sich daher auf die Speicherauslastung Ihres Systems aus. Der Gesamtumfang des vom Core verwendeten Arbeitsspeichers hängt von mehreren Faktoren ab. Zu diesen Faktoren gehört, welche Vorgänge ausgeführt werden, die Anzahl der Benutzer, die Anzahl der geschützten Maschinen und die Größe des Deduplizierungscache. Jeder Vorgang, der vom Core durchgeführt wird (Übertragung, Replikation, Rollup usw.), belegt zusätzlichen Arbeitsspeicher. Sobald ein Vorgang beendet wurde, sinkt die Speicherbelegung entsprechend. Administratoren müssen jedoch die maximal erforderliche RAM-Nutzung berücksichtigen, damit ein effizienter Betrieb möglich ist.

Gemäß den Standardeinstellungen für den Rapid Recovery Core befinden sich der primärer Cache, der sekundäre Cache und der Metadatencache für DVM-Repositorys im Verzeichnis "AppRecovery". Dieser Ordner ist auf der Core-Maschine installiert.

NOTE: Abhängig von den jeweiligen Einstellungen ist das Verzeichnis "AppRecovery" auf dem Rapid Recovery Core möglicherweise nicht sichtbar. Damit das Verzeichnis sichtbar ist, müssen Sie u. U. die Ordneroptionen so ändern, dass versteckte Dateien, Ordner und Laufwerke angezeigt werden.

Sofern der Rapid Recovery Core auf dem Laufwerk C: installiert ist, werden standardmäßig die folgenden Speicherorte verwendet:

Tabelle 13. Standardspeicherorte für DVM-Deduplizierungscache-Einstellungen

Einstellung	Standardspeicherort
Speicherort primärer Cache	C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache
Speicherort sekundärer Cache	C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache
Speicherort Metadaten-Cache	C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata

Sie können den Speicherort dieser Caches ändern. Um die Fehlertoleranz zu erhöhen, können Sie beispielsweise den Speicherort des sekundären Cache auf ein anderes physisches Laufwerk als den primären Cache verlagern, vorausgesetzt, der Rapid Recovery Core kann auf den Speicherort zugreifen.

Weitere Informationen zum Ändern der Speicherorte für diese Einstellungen finden Sie unter Konfigurieren von DVM-Deduplizierungscache-Einstellungen.

Quest empfiehlt, dass Sie Deduplizierungsspeicher separat planen. Deduplizierung tritt nur in einem einzelnen Repository (nicht über mehrere Repositorys) auf. Bei Verwendung von Core-basierter Verschlüsselung ist die Deduplizierung auf die von einem einzigen Schlüssel geschützten Daten begrenzt, da aus Sicherheitsgründen jeder Schlüssel für eine einzige Verschlüsselungsdomäne gilt.

Weitere Informationen zur Replikation finden Sie unter Deduplizierung in Rapid Recovery.

Konfigurieren von DVM-Deduplizierungscache-Einstellungen

Führen Sie die folgenden Schritte aus, um Deduplizierungscache-Einstellungen für DVM-Repositorys zu konfigurieren.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite "Einstellungen" auf **DVM-Deduplizierungscache**. Diese Einstellung wird nur angezeigt, wenn Ihr Core ein oder mehrere DVM-Repositorys aufweist.
   - Scrollen Sie auf der rechten Seite der Seite "Einstellungen" bis zur Überschrift "DVM-Deduplizierungscache".
3. Wenn Sie die Standardeinstellung für den DVM-Deduplizierungscache wiederherstellen möchten, gehen Sie wie folgt vor:
   a. Klicken Sie am oberen Rand des Einstellungsbereichs des Deduplizierungscache auf **Standardeinstellungen wiederherstellen**.

   Das Dialogfeld "Standardeinstellungen wiederherstellen" wird angezeigt.

   b. Klicken Sie auf **Ja**, um den Wiederherstellungsvorgang zu bestätigen.
4. Klicken Sie auf die Einstellung, die Sie ändern möchten.

Die ausgewählte Einstellung wird bearbeitbar.

5. Zur Änderung individueller Deduplizierungscache-Einstellungen geben Sie die in der folgenden Tabelle beschriebenen Konfigurationsinformationen ein.

Tabelle 14. Informationen über DVM-Deduplizierungscache-Einstellungen

Einstellung	Description
Standardeinstellung wiederherstellen	Diese Steuerung setzt den Standardspeicherort des DVM-Cache auf die Standardeinstellungen zurück, die für jede Einstellung beschrieben werden.
Speicherort primärer Cache	Geben Sie zum Ändern des Speicherorts für den primären Cache für DVM-Repositorys im Textfeld "Speicherort primärer Cache" den Pfad zu einem Speicherort ein, auf den der Core Zugriff hat. Der Standardspeicherort ist: `C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache` Da der primäre und der sekundäre Cache gleich groß sind, ist zum Speichern dieser beiden Cachespeicher doppelt so viel Speicherplatz erforderlich wie die zugewiesene Deduplizierungscache-Größe. Wenn Sie beispielsweise die Standardgröße von 1,5 GB für den Deduplizierungscache angeben, müssen Sie sicherstellen, dass jeder der beiden Speicherorte über einen Speicherplatz von mindestens 1,5 GB verfügt. Wenn sich beide Speicherorte auf einem Laufwerk befinden (z. B. dem Laufwerk C:), muss mindestens 3,0GB freier Speicherplatz vorhanden sein.
Speicherort sekundärer Cache	Geben Sie zum Ändern des Speicherorts für den sekundären Cache für DVM-Repositorys im Textfeld "Speicherort sekundärer Cache" den Pfad zu einem Speicherort ein, auf den der Core Zugriff hat. Der Standardspeicherort ist: `C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache`
Speicherort für Cache-Metadaten:	Geben Sie zum Ändern des Speicherorts für Cache-Metadaten für DVM-Repositorys im Textfeld "Speicherort für Cache-Metadaten" den Pfad zu einem Speicherort ein, auf den der Core Zugriff hat. Der Standardspeicherort ist: `C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata`
Größe des Deduplizierungscache (GB)	Wenn Sie die Größe des Deduplizierungscache für DVM-Repositorys ändern möchten, geben Sie im Textfeld "Größe des Deduplizierungscache" eine neue Größe ein (in GB). Der Standardspeicherort ist: `C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache` Die minimale Cachegröße beträgt 1,5GB. Darüber hinaus darf die Cachegröße nicht größer sein als 50 Prozent des installierten Arbeitsspeichers.

6. Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf ✓, um die Änderungen zu speichern und den Bearbeitungsmodus zu beenden, oder klicken Sie auf ✕, um den Bearbeitungsmodus ohne Speichern zu beenden.

Konfigurieren von Replay Engine-Einstellungen

Sie können Informationen zur Replay Engine konfigurieren. Dabei handelt es sich um den Kommunikationskanal für Rapid Recovery. Diese Einstellungen legen Core-Einstellungen für eine effektive Kommunikation fest.

Quest empfiehlt, im Normalfall die Standardeinstellungen zu verwenden. In einigen Fällen werden Sie u. U. vom Quest Support angewiesen, diese Einstellungen zu ändern, um das Leistungsverhalten an die jeweiligen Netzwerkanforderungen anzupassen.

Führen Sie die folgenden Schritte aus, um die Replay Engine-Einstellungen zu konfigurieren.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite „Einstellungen“ auf **Replay Engine**.
   - Führen Sie einen Bildlauf nach unten auf der rechten Seite der Seite Einstellungen durch, bis Sie die Replay Engine-Überschrift sehen können.
3. Klicken Sie auf die Einstellung, die Sie ändern möchten.

   Die ausgewählte Einstellung wird bearbeitbar.
4. Geben Sie die Konfigurationsinformationen ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 15. Informationen zu Replay Engine-Einstellungen

Textfeld	Description
IP-Adresse	Der Core verwendet diese IP-Adresse beim Bereitstellen und Wiederherstellen für einen Wiederherstellungspunkt, damit Feedback zwischen geschützten Maschinen und dem Core möglich wird. Die IP-Adresse für die Replay Engine wird mit der IP-Adresse der Core-Maschine automatisch befüllt. Wenn Sie die Server-IP-Adresse manuell eingeben, wird dieser Wert in Fällen verwendet, in denen die geschützte Maschine nicht die automatisch angegebene IP-Adresse auflösen kann. Sie müssen diesen Wert nicht manuell einstellen, außer Sie haben Probleme mit geschützten Maschinen, die zur Kommunikation mit dem Core in der Lage sind.
Bevorzugter Port	Geben Sie eine Portnummer ein oder übernehmen Sie die Standardeinstellung. Der Standardport ist 8007. Der Port wird zur Festlegung des Kommunikationskanals für die Replay Engine verwendet.
Verwendeter Port	Stellt den Port dar, der für die Replay Engine-Konfiguration verwendet wird.
Automatische Portzuweisung zulassen	Wählen Sie diese Option aus, um eine automatische TCP-Portzuweisung zuzulassen.
Admin-Gruppe	Geben Sie einen neuen Namen für die Administratorgruppe ein. Der Standardname ist BUILTIN\Administrators.

Textfeld	Description
Minimale asynchrone-E/A-Länge	Geben Sie einen Wert ein oder wählen Sie die Standardeinstellung aus. Dieser Wert beschreibt die minimale asynchrone Eingabe-/Ausgabelänge. Die Standardeinstellung ist 65536.
Zeitüberschreitung beim Lesen	Geben Sie einen Wert für die Zeitüberschreitung beim Lesen ein oder wählen Sie die Standardeinstellung aus. Die Standardeinstellung ist 00:05:00.
Zeitüberschreitung beim Schreiben	Geben Sie einen Wert für die Zeitüberschreitung beim Schreiben ein oder wählen Sie die Standardeinstellung aus. Die Standardeinstellung ist 00:05:00.
Größe des Empfangspuffers	Geben Sie eine Puffergröße für eingehende Daten ein oder übernehmen Sie die Standardeinstellung. Die Standardeinstellung ist 8192.
Größe des Sendepuffers	Geben Sie eine Puffergröße für ausgehende Daten ein oder übernehmen Sie die Standardeinstellung. Die Standardeinstellung ist 8192.
Keine Verzögerung	Es wird empfohlen, dieses Kontrollkästchen deaktiviert zu lassen, da andernfalls die Netzwerkleistung beeinträchtigt wird. Falls Sie feststellen, dass diese Einstellung geändert werden muss, wenden Sie sich an den Quest Support, um entsprechende Anweisungen zu erhalten.

5. Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf ✓, um die Änderungen zu speichern und den Bearbeitungsmodus zu beenden, oder klicken Sie auf ✕, um den Bearbeitungsmodus ohne Speichern zu beenden.

Konfigurieren von Bereitstellungseinstellungen

Rapid Recovery bietet die Möglichkeit, Installationsprogramme vom Rapid Recovery Core auf die zu schützenden Maschinen herunterzuladen.

Sie können Einstellungen für die Bereitstellung der Rapid Recovery Agentensoftware vom Core auf die zu schützenden Maschinen konfigurieren.

Führen Sie die folgenden Schritte aus, um Bereitstellungseinstellungen zu konfigurieren.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite "Einstellungen" auf **Bereitstellen**.
   - Scrollen Sie auf der rechten Seite der Seite "Einstellungen" bis zur Überschrift "Bereitstellen".
3. Klicken Sie auf die Einstellung, die Sie ändern möchten.

   Die ausgewählte Einstellung wird bearbeitbar.
4. Geben Sie die Konfigurationsinformationen ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 16. Informationen zu Bereitstellungseinstellungen

Textfeld	Description
Agent Installer-Name	Der Standarddateiname ist „Agent-Web.exe“. Wenn Sie diesen Dateinamen aus irgendeinem Grund ändern möchten, können Sie diese Einstellung verwenden, um

Textfeld	Description
	der ausführbaren Datei des Core Web-Installationsprogramms einen neuen Namen zu geben. Mit dieser Datei wird die aktuellste Version des Installationsprogramms des Rapid Recovery Core direkt aus dem Internet als Stream heruntergeladen. Dieser Vorgang kann nach Bedarf angehalten und fortgesetzt werden.
Core-Adresse	Geben Sie die Adresse des Core-Servers ein. Diese besteht normalerweise aus dem Protokoll, dem Namen des Core-Servers und dem Port sowie dem Verzeichnis, in dem sich die Core-Dateien befinden. Wenn der Server beispielsweise „Sample“ heißt, lautet diese Einstellung „https://sample:8006/apprecovery/admin/Core“.
Zeitüberschreitung Empfang fehlgeschlagen	Das zulässige Zeitlimit für die Bereitstellung der Agent-Software. Die Standardeinstellung ist 00:25:00 bzw. fünfundzwanzig Minuten. Wenn Sie diese Einstellung ändern möchten, geben Sie die Zeitdauer ein, in der das System versucht, die Bereitstellung der Agentensoftware auszuführen, bevor bei Lese-/Schreibvorgängen eine Zeitüberschreitung auftritt. Das Format ist HH:MM:SS (Stunden:Minuten:Sekunden).
Maximale Anzahl paralleler Installationen	Diese Einstellung steuert die maximale Anzahl von Bereitstellungen der Agent-Software, die der Core gleichzeitig durchführen kann. Die Standardeinstellung ist 100.

5. Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf ✓, um die Änderungen zu speichern und den Bearbeitungsmodus zu beenden, oder klicken Sie auf ✕, um den Bearbeitungsmodus ohne Speichern zu beenden.

Konfigurieren von Datenbankverbindungseinstellungen

Rapid Recovery zeigt Informationen über Core-Aufgaben, -Ereignisse und -Alarme auf der Seite „Ereignisse an“. Rapid Recovery speichert diese Informationen zu Transaktionen in einem MongoDB-Service-Datenbank, die standardmäßig lokal auf der Core-Maschine installiert ist. Sie können diese Einstellungen konfigurieren, um die Aufbewahrungsdauer der Informationen in der Datenbank oder die Größe des Verbindungspools zu ändern, damit mehr oder weniger gleichzeitige Verbindungen möglich sind.

Wenn ein zweiter Rapid Recovery Core verwendet wird, können Sie die Datenbankverbindungseinstellungen des ersten Core so konfigurieren, dass auf die zweite Core-Maschine verwiesen wird. Auf diese Weise werden die Ereignisdaten beider Cores in der MongoDB auf dem zweiten Core gespeichert.

Alternativ können Sie die Datenbankverbindungseinstellungen des Core so konfigurieren, dass auf eine andere Maschine mit einer separat installierten MongoDB verwiesen wird, auf die der Rapid Recovery Core über das Netzwerk zugreifen kann. Die Ereignistransaktionsdaten für den Core werden dann in dieser Dienstdatenbank und nicht lokal gespeichert. Weitere Informationen zum Festlegen oder Ändern der Datenbankverbindungseinstellungen finden Sie unter Konfigurieren von Datenbankverbindungseinstellungen.

NOTE: Weitere Informationen über das Anzeigen von Ereignisinformationen des Rapid Recovery Core finden Sie unter Anzeigen von Ereignissen mithilfe von Aufgaben, Warnungen und Journalseiten.

Es besteht die Möglichkeit, die MongoDB-Dienstdatenbank auf einer anderen Maschine zu installieren, auf die der Rapid Recovery Core zugreifen kann. Wenn die Dienstdatenbank für den Rapid Recovery Core auf einer anderen Maschine als der Hostmaschine für den Rapid Recovery Core installiert ist, müssen Sie die Datenbankanmeldeinformationen (Benutzername und Kennwort) hier angeben.

Führen Sie die Schritte dieses Verfahrens durch, um die Datenbankverbindungseinstellungen für die Dienstdatenbank zu ändern, die vom Rapid Recovery Core verwendet wird.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite „Einstellungen“ auf **Datenbankverbindung**.
   - Führen Sie einen Bildlauf nach unten auf der rechten Seite der Seite Einstellungen durch, bis Sie die Datenbankverbindungs-Überschrift sehen können.
3. Von der Oberseite des Einstellungsbereichs „Datenbankverbindung“ können Sie Folgendes tun:
   - Klicken Sie auf **Verbindung testen**, um die Einstellungen zu prüfen.

     Testen der Verbindung wird empfohlen, wenn Sie Änderungen an den Datenbankverbindungseinstellungen vornehmen.
   - Klicken Sie auf **Standardeinstellungen wiederherstellen** zur Wiederherstellung aller Standard-Datenbankverbindungseinstellungen.

     Sie werden aufgefordert, diese Maßnahme zu bestätigen, was dazu führt die besonderen Datenbankverbindungseinstellungen aufzugeben.
4. Klicken Sie auf die Einstellung, die Sie ändern möchten.

   Die ausgewählte Einstellung wird bearbeitbar.
5. Geben Sie die Konfigurationsinformationen ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 17. Informationen zu Datenbankverbindungseinstellungen

Beschreibungen der Verbindungseinstellungen, die auf der Seite „Einstellungen“ für den Rapid Recovery Core verfügbar sind.

Textfeld	Description
Hostname	Geben Sie einen Hostnamen für die Datenbankverbindung ein. **NOTE:** Wenn „localhost“ als Parameter für den Host angegeben wird, ist die MongoDB lokal auf der Hostmaschine des Core installiert.
Port	Geben Sie eine Portnummer für die Datenbankverbindung ein. **NOTE:** Die Standardeinstellung ist 27017.
Benutzername	Geben Sie den Namen eines Benutzers mit Administratorberechtigungen für die MongoDB-Dienstdatenbank ein. **NOTE:** Wenn „localhost“ als Parameter für den Host angegeben wurde, muss dieses Feld nicht ausgefüllt werden.
Kennwort	Geben Sie das Kennwort für den angegebenen Benutzernamen ein. **NOTE:** Wenn „localhost“ als Parameter für den Host angegeben wurde, muss dieses Feld nicht ausgefüllt werden.
Aufbewahrungszeiten (Tag)	Geben Sie die Anzahl an Tagen ein, für die der Ereignis- und Jobverlauf in der Dienstdatenbank aufbewahrt werden soll.
Max. Verbindungspoolgröße	Legt die maximale Anzahl von zwischengespeicherten Datenbankverbindungen fest, um eine dynamische Wiederverwendung zu ermöglichen.

Textfeld	Description
	NOTE: Die Standardeinstellung ist 100.
Min. Verbindungspoolgröße	Legt die minimale Anzahl von zwischengespeicherten Datenbankverbindungen fest, um eine dynamische Wiederverwendung zu ermöglichen. **NOTE:** Die Standardeinstellung ist 0.

6. Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf ✓, um die Änderungen zu speichern und den Bearbeitungsmodus zu beenden, oder klicken Sie auf ✕, um den Bearbeitungsmodus ohne Speichern zu beenden.

Ändern der lokalen Einstellungen für Datenbankverbindung

Sie können Systemereignisse in Bezug auf den Rapid Recovery Core auf der Seite „Ereignisse“ anzeigen. Der Rapid Recovery Core speichert diese Transaktionsinformationen in einer MongoDB-Dienstdatenbank. Standardmäßig ist diese Datenbank lokal auf der Core-Maschine installiert und der Hostname in den Einstellungen für Datenbankverbindung ist standardmäßig Localhost. In dieser Situation umgeht die Loopback-Schnittstelle lokale Netzwerkschnittstellenhardware und Anmeldeinformationen für die Datenbank sind nicht erforderlich.

Optional können Sie zur Erhöhung der Sicherheit Anmeldeinformationen für die Datenbank (einen Benutzernamen und ein Kennwort) für die vom Rapid Recovery Core verwendete MongoDB-Datenbank explizit angeben.

NOTE: Weitere Informationen über das Anzeigen von Ereignisinformationen des Rapid Recovery Core finden Sie unter Anzeigen von Ereignissen mithilfe von Aufgaben, Warnungen und Journalseiten. Informationen über Einstellungen für Datenbankverbindungen finden Sie unter Konfigurieren von Datenbankverbindungseinstellungen.

Führen Sie die nachstehend beschriebenen Schritte durch, um den lokalen Einstellungen für Datenbankverbindungen Anmeldeinformationen für die Datenbank hinzuzufügen.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf ⚙ (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite "Einstellungen" auf **Lokale Datenbankeinstellungen**.
   - Scrollen Sie auf der rechten Seite der Seite "Einstellungen" bis zur Überschrift "Lokale Datenbankeinstellungen".
3. Klicken Sie auf die Einstellung, die Sie ändern möchten.

   Die ausgewählte Einstellung wird bearbeitbar.
4. Geben Sie die entsprechenden Anmeldeinformationen für die Verbindung mit der Dienstdatenbank ein, wie in der folgenden Tabelle beschrieben.

Tabelle 18. Informationen über lokale Datenbankeinstellungen

Textfeld	Description
Benutzername	Geben Sie den Namen eines Benutzers mit Administratorberechtigungen für die MongoDB-Dienstdatenbank ein.
Kennwort	Geben Sie das Kennwort für den angegebenen Benutzernamen ein.

5. Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf ✓, um die Änderungen zu speichern und den Bearbeitungsmodus zu beenden, oder klicken Sie auf ✕, um den Bearbeitungsmodus ohne Speichern zu beenden.

Verwalten von SMTP-Servereinstellungen

Wenn Sie SMTP-Servereinstellungen (Simple Mail Transfer Protocol) für den Core konfigurieren, können Sie Aufgaben-, Ereignis- und Warn-Benachrichtigungen auch per E-Mail senden.

Informationen über das Konfigurieren eines SMTP-E-Mail-Servers finden Sie unter Konfigurieren eines E-Mail-Servers.

NOTE: Um Ereignisinformationen per E-Mail senden zu können, müssen Sie auch Benachrichtigungsgruppeneinstellungen konfigurieren. Weitere Informationen zum Angeben von Ereignissen, für die E-Mail-Benachrichtigungen erstellt werden sollen, finden Sie unter Konfigurieren von Benachrichtigungsgruppen.

Konfigurieren von Verbindungseinstellungen des Cloud-Kontos

Über Konto-Verbindungseinstellungen können Sie bestimmen, wie viel Zeit zwischen Rapid Recovery-Versuchen, eine Verbindung zu Ihrem Cloud-Konto herzustellen, verstreichen sollte, bevor eine Zeitüberschreitung eintritt. Führen Sie die folgenden Schritte aus, um die Verbindungseinstellungen für das Cloud-Konto zu konfigurieren.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf **Einstellungen**.

   Die Seite „Einstellungen“ wird angezeigt.
3. Klicken Sie im linken Menü auf **Cloud-Konten**.
4. Klicken Sie in der Tabelle „Cloud-Konten“ auf das Drop-Down-Menü neben dem Cloud-Konto, das Sie konfigurieren möchten, und führen Sie dann eine der folgenden Aktionen durch:
   - Um die Cloud-Konfiguration wieder auf die folgenden Standardeinstellungen zurückzusetzen, klicken Sie auf **Zurücksetzen**.
     - **Anforderungszeitüberschreitung**: 01:30 (Minuten und Sekunden)
     - **Schreibpuffergröße**: 8388608 (Byte)
     - **Lesepuffergröße**: 8388608 (Byte)
   - Klicken Sie zum Ändern der Cloud-Konto-Verbindungseinstellungen auf **Bearbeiten** und führen Sie im Dialogfeld **Cloud-Konfiguration** eine der folgenden Aktionen aus:
     - Unter **Zeitüberschreitung für Anforderung** bestimmen Sie mithilfe der Pfeile nach oben und unten die Zeitspanne (in Minuten und Sekunden), die Rapid Recovery für einen Versuch

aufwenden sollte, eine Verbindung zum Cloud-Konto herzustellen, falls es zu einer Verzögerung kommt. Die Verbindungsversuche werden nach dem eingegebenen Zeitraum eingestellt.

- Geben Sie für **Schreibpuffergröße** die Puffergröße für das Schreiben von archivierten Daten in die Cloud ein.
- Geben Sie für **Lesepuffergröße** die Blockgröße ein, die für das Lesen archivierter Daten aus der Cloud reserviert ist.

Arbeiten mit Azure Management-Zertifikaten, die mit Ihrem Core verknüpft sind

Über die Rapid Recovery Core-Einstellungen können Sie Azure Management-Zertifikate mit Ihren Core verknüpfen. Auf diese Weise ist der Core in der Lage, auf Informationen zu Ihren Azure Abonnements zuzugreifen und diese Informationen über die Core Console verfügbar zu machen.

Wenn Sie beispielsweise einen virtuellen Export nach Azure durchführen, können Sie nach dem Laden der Zertifikatinformationen das entsprechende Azure Abonnement aus einem Dropdown-Feld auswählen. Auf die mit dem Abonnement verbundenen Objekte kann dann auch über andere Steuerelemente in der Core Console-UI, wie Speicherkonten, Container usw. zugegriffen werden.

Azure Management-Zertifikatinformationen werden in einer Veröffentlichungseinstellungendatei gespeichert, die in Microsoft Azure erstellt wird. Sie können ein oder mehrere Management-Zertifikate zu Ihrem Core hinzufügen. Die Anmeldeinformationen werden im Core sicher gespeichert.

Das Arbeiten mit Azure Management-Zertifikaten von Core-Einstellungen umfasst die folgenden Aufgaben:

- Abrufen der Veröffentlichungseinstellungendatei für Ihr Azure Konto
- Laden eines Azure Management-Zertifikats
- Aktualisieren oder Löschen von Azure Management-Zertifikaten

Abrufen der Veröffentlichungseinstellungendatei für Ihr Azure Konto

Zum Durchführen dieser Aufgabe müssen Sie eine Windows-Maschine verwenden, auf der PowerShell aktiviert ist. Sie müssen außerdem Zugriff auf ein Azure Konto haben, dem die Service-Administrator- oder Service-Co-Administrator-Rolle zugewiesen ist.

Die Veröffentlichungseinstellungendatei ist ein XML-Dokument, das auf Azure generiert wird. Die Datei enthält die AzureServiceManagement API-Definition, und Informationen über Ihr Azure Abonnement, einschließlich sicherer verschlüsselter Anmeldedaten, Ihres Abonnementtyps und eines Azure Management-Zertifikats. Diese Datei enthält eine Datei mit der Endung `.publishsettings`, von der die Beschreibung abgeleitet wird. Ohne die Veröffentlichungseinstellungendatei können Sie Ihren Core nicht mit einem Azure Konto verbinden.

Sie können eine Kopie der Veröffentlichungseinstellungendatei von einer Windows-Maschine abrufen, die bei Ihrem Azure Konto angemeldet ist.

CAUTION: Da die Veröffentlichungseinstellungendatei Ihre Anmeldedaten sowie Informationen zu Ihrem Azure Konto enthält, empfiehlt Microsoft die Speicherung der Veröffentlichungseinstellungendatei an einem sicheren Ort. Sobald Sie das Zertifikat geladen haben, können Sie die Datei von Ihrem lokalen System löschen.

Microsoft begrenzt die Anzahl der Management-Zertifikate pro Abonnement auf 100, mit der zusätzlichen Begrenzung von 100 Management-Zertifikaten für alle Abonnements unter der Benutzer-ID eines bestimmten Service-Administrators. Wenn Sie von mehreren Cores aus auf das gleiche Azure Konto zugreifen müssen, können Sie die Veröffentlichungseinstellungendatei einmal erstellen und dann die gleiche Datei zum Laden des Management-Zertifikats in mehreren Cores verwenden. Auf diese Weise können Sie die Zertifikaterstellungsgrenze überschreiten.

NOTE: Weitere Informationen zu dieser Begrenzung finden Sie im Abschnitt „Einschränkungen“ des Microsoft KB-Artikels „Übersicht über Zertifikate für Azure Cloud Services“ unter https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-certs-create.

Führen Sie die nachstehend beschriebenen Schritte aus, um die Veröffentlichungseinstellungendatei zu erhalten.

1. Von einer Windows-Maschine aus melden Sie sich beim Azure Dashboard an.
2. Während Sie bei Azure angemeldet sind, öffnen Sie ein weiteres Browserfenster.
3. Führen Sie ein PowerShell-Skript aus, um die Datei herunterzuladen, indem Sie folgende Adresse in die Browser-URL eingeben: `https://manage.windowsazure.com/publishsettings/index?client=powershell`.

   Wenn Sie erfolgreich sind, wird die Veröffentlichungseinstellungendatei in Ihrem Standard-Download-Verzeichnis gespeichert.
4. Verschieben Sie diese Datei auf eine Maschine, auf die die Core Console zugreifen kann.

Informationen zum Verknüpfen der Azure Abonnementinformationen mit Ihrem Rapid Recovery Core finden Sie im *Rapid Recovery Benutzerhandbuch* Thema „Laden eines Azure Management-Zertifikats“.

Laden eines Azure Management-Zertifikats

Zum Durchführen dieser Aufgabe müssen Sie über eine Veröffentlichungseinstellungendatei aus dem entsprechenden Azure Konto verfügen. Informationen zum Zugriff auf diese Datei finden Sie unter Abrufen der Veröffentlichungseinstellungendatei für Ihr Azure Konto.

Wenn Sie ein Azure Management-Zertifikat in Ihren Core laden, geben Sie der Core Console Zugriff auf Abonnementinformationen für Ihr Azure Konto. Anschließend können Sie Objekte im Zusammenhang mit Ihrem Azure Abonnement über die Core Console anzeigen.

Führen Sie die Schritte in diesem Verfahren aus, um ein Azure Management-Zertifikat in Ihren Core zu laden.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite „Einstellungen“ auf **Azure Management-Zertifikate**.
   - Scrollen Sie auf der rechten Seite der Seite „Einstellungen“ bis zur Überschrift „Azure Management-Zertifikate“.
3. Klicken Sie unter der Überschrift „Azure Management-Zertifikate“ auf **+Zertifikat laden**.

   Das Dialogfeld **Zertifikat laden** wird angezeigt.
4. Klicken Sie im Dialogfeld **Zertifikat laden** auf **Durchsuchen**.

   Das Fenster **Datei hochladen** wird angezeigt.
5. Navigieren Sie zu dem Speicherort, an dem sich Ihre Veröffentlichungseinstellungendatei befindet, wählen Sie die Datei aus und klicken Sie auf **Öffnen**.

   Das Fenster **Datei hochladen** wird geschlossen und das Azure Management-Zertifikat wird in die Core Console geladen.

Aktualisieren oder Löschen von Azure Management-Zertifikaten

Um ein Azure Management-Zertifikat von der Core Console zu löschen, muss ein Zertifikat in den Core geladen und mit diesem verknüpft sein. Informationen zum Zuordnen von Zertifikaten zu ihrem Core finden Sie unter Laden eines Azure Management-Zertifikats.

Führen Sie die Schritte in diesem Verfahren aus, um die Ansicht der mit Ihrem Core verknüpften Azure Management-Zertifikate zu aktualisieren oder um ein Zertifikat aus dem Core zu löschen.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite „Einstellungen“ auf **Azure Management-Zertifikate**.
   - Scrollen Sie auf der rechten Seite der Seite „Einstellungen“ bis zur Überschrift „Azure Management-Zertifikate“.
3. Um die Ansicht der in der Core Console verfügbaren Zertifikaten zu aktualisieren, klicken Sie unter der Überschrift „Azure Management-Zertifikate“ auf **Aktualisieren**.

   Die Seite **Core-Einstellungen** wird aktualisiert und zeigt aktualisierte Informationen zu den mit Ihrem Core verknüpften Zertifikaten an.
4. Um ein Zertifikat aus dem Core zu löschen, klicken Sie für das entsprechende Zertifikat auf und wählen Sie **Löschen**.
5. Klicken Sie im Bestätigungsdialogfeld, um den Löschvorgang des Zertifikats zu bestätigen.

   Das Dialogfeld wird geschlossen und das ausgewählte Azure Management-Zertifikat wird aus Ihrem Core gelöscht.

Verwalten von Berichteinstellungen

Sie können Berichte für den Rapid Recovery Core oder für geschützte Maschinen generieren. Informationen über generierbare Berichten finden Sie unter Berichterstellung.

Führen Sie die hier beschriebenen Schritte aus, um die Berichteinstellungen für Core-Berichte zu verwalten.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite "Einstellungen" auf **Berichte**.
   - Scrollen Sie auf der rechten Seite der Seite "Einstellungen" bis zur Überschrift "Berichte".

     Die Core-Einstellungen für **Berichte** werden angezeigt. Die Berichteinstellungen werden in der folgenden Tabelle beschrieben.

Option	Description
Standardeinstellungen wiederherstellen	Diese Option setzt alle Berichteinstellungen auf die Standardeinstellungen zurück. Die Standardeinstellungen sind unten für jede Einstellung aufgeführt.
Schriftart	Diese Option legt die Standardschriftart für Berichte fest. Die Standardschriftart ist Trebuchet MS. Sie können jede auf Ihrem System verfügbare Schriftart festlegen.
Papierformat	Diese Option legt das Standardpapierformat für das Drucken von Berichten fest. Die Standardeinstellung

Option	Description
	ist Letter. Sie können zwischen folgenden Papierformaten wählen: • A3 • A4 • B4 • Executive • Ledger • Legal • Letter • Tabloid
Seitenausrichtung	Diese Option legt die Seitenausrichtung für exportierte Berichte fest. Die Standardausrichtung ist Querformat. Sie können zwischen folgenden Layout-Optionen wählen: • Querformat • Hochformat

3. Um Änderungen an den Einstellungen für Berichte vorzunehmen, klicken Sie in das entsprechende Einstellungsfeld.

   Das Einstellungsfeld wird als konfigurierbares Drop-Down-Menü angezeigt.

4. Klicken Sie auf das Drop-Down-Menü und wählen Sie eine der verfügbaren Optionen aus.

   Klicken Sie zum Beispiel im Feld "Schriftart" auf **Times New Roman**.

5. Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf ✓, um die Änderungen zu speichern und den Bearbeitungsmodus zu beenden, oder klicken Sie auf ✕, um den Bearbeitungsmodus ohne Speichern zu beenden.

   Die ausgewählte Option wird nun als neue Einstellung für die ausgewählten Berichtsparameter angezeigt.

Verwalten von Core-SQL-Anfügbarkeitseinstellungen

SQL-Anfügbarkeitsprüfungen werden als Teil der nächtlichen Jobs der Rapid Recovery durchgeführt. Um die Lizenzierungskosten zu senken, stehen Ihnen in Rapid Recovery zwei Optionen zum Ausführen von Anfügbarkeitsprüfungen zur Verfügung: Verwenden einer lizenzierten Instanz des SQL Servers, die auf der Rapid Recovery Core-Maschine installiert ist, oder Verwenden der Instanz des SQL Servers, die bereits auf Ihrer geschützten Maschine installiert ist. Die zweite Option ist nun die Standardeinstellung. Wenn Ihre geschützte Maschine jedoch während des Zeitpunkts, zu dem der nächtlichen Jobs auftritt, bereits verwendet wird, sollten Sie erwägen, die Überprüfungen mit einer Instanz des SQL Servers auf dem Core durchzuführen.

Die Fähigkeit, Anfügbarkeitsprüfungen mithilfe der SQL Server-Instanz auf einer geschützten Maschine durchzuführen, ist eine Funktion derRapid Recovery Agenten-Software. Diese Funktion funktioniert nicht, wenn der SQL-Server ohne Agent geschützt ist. Konfigurieren Sie daher bei der Verwendung von agentenlosem Schutz auf der SQL-Maschine diese Core-Einstellung als **SQL Server des Core verwenden**, wie in Schritt 3 dieses Verfahrens gezeigt.

Zusammenfassend beinhaltet der Prozess der Verwaltung der Core SQL-Anfügbarkeitseinstellungen die folgenden Aufgaben:

- Letzten Wiederherstellungspunkt für Schutzgruppen mit Datenbanken bereitstellen.
- Verbindung vom SQL Server zur Datenbank herstellen.
- Datenbank öffnen.
- Datenbank schließen.
- Bereitstellung des Wiederherstellungspunktes aufheben.

  Um diese nächtliche Prüfung zu ermöglichen, geben Sie eine SQL Server-Instanz an, die für die Durchführung von Anfügbarkeitsprüfungen für SQL Server-Datenbanken auf geschützten Maschinen verwendet werden soll.

  NOTE: Diese Option wird nicht angezeigt, wenn kein SQL Server im Core geschützt wird.

Zum Konfigurieren des Core zum Ausführen der SQL-Anfügbarkeitsprüfungen als Teil der nächtlichen Jobs führen Sie die folgenden Schritte aus.

NOTE: Wenn Sie die Standardoption zum Verwenden der auf der geschützten Maschine installierten Instanz des SQL Servers auswählen, verwaltet die SQL Server-Instanz die SQL-Anfügbarkeit für alle geschützten SQL-Maschinen. Wenn Sie nicht wollen, dass diese Einstellung für alle geschützten SQL-Maschinen gilt, wählen Sie "SQL Server des Core verwenden" aus. Zur Durchführung von Anfügbarkeitsprüfungen auf dem Core, müssen Sie eine lizenzierte Version von SQL Server auf der Core-Maschine installieren oder verwenden.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite "Einstellungen" auf **Anfügbarkeit**.
   - Scrollen Sie auf der rechten Seite der Seite "Einstellungen" bis zur Überschrift "Anfügbarkeit".
3. Wählen Sie zum Verwenden der auf der geschützten SQL Server-Maschine installierten SQL Server-Instanz die Option **SQL Server der geschützten Maschine verwenden**. Dies ist die Standardoption.
4. Wählen Sie zum Verwenden der auf dem Rapid Recovery Core installierten SQL Server-Instanz die Option **SQL Server des Core verwenden** und geben Sie dann die in der folgenden Tabelle beschriebenen Authentifizierungsinformationen ein.

Tabelle 19. SQL Server-Anmeldeinformationen

Beschreibungen der erforderlichen Informationen für die Authentifizierung einer Verbindung zu SQL Server.

Textfeld	Description
SQL Server	Wählen Sie im Drop-Down-Menü des SQL Servers die entsprechende SQL Server-Instanz aus dem Core-Server aus.
Credential Type (Typ der Anmeldeinformationen)	Wählen Sie die passende Authentifizierungsmethode für Ihre Anmeldeinformationen aus den folgenden Optionen aus: • Windows • SQL
Benutzername	Geben Sie einen Benutzernamen für den Zugriff auf den SQL Servers auf dem Core basierend auf der ausgewählten Art der Anmeldeinformationen ein.

Textfeld	Description
Kennwort	Geben Sie ein Kennwort für den Zugriff auf den SQL Servers auf dem Core basierend auf der ausgewählten Art der Anmeldeinformationen ein.

5. Klicken Sie auf **Verbindungstest**.

   NOTE: Wenn Sie die Anmeldeinformationen falsch eingegeben haben, wird eine Meldung mit dem Hinweis angezeigt, dass die Überprüfung der Anmeldeinformationen fehlgeschlagen ist. Korrigieren Sie die Anmeldeinformationen und führen Sie den Verbindungstest erneut aus.

6. Klicken Sie nach Fertigstellen der gewünschten Änderungen auf **Übernehmen**.

Grundlegende Informationen zu Core-Jobs

Core-Jobs sind Prozesse, die der Rapid Recovery Core durchführt zur Unterstützung der Vorgänge, einschließlich Sicherung auf Wiederherstellungspunkte, Replizieren von Daten Archivieren von Daten, Exportieren von Daten auf VMs, Wartung von Repositorys usw. Core-Jobs werden für bestimmte Vorgänge automatisch eingeleitet, wie z. B. Replizierung oder Archivierung eines bestehenden Zeitplans. Sie können auch einige Jobs auf Nachfrage aus verschiedenen Elementen in der Core Console aufrufen.

- Beim Anzeigen oder Bearbeiten von Core-Jobeinstellungen enthält jeder Core-Job zwei Parameter: Maximale Anzahl gleichzeitiger Jobs und Wiederholungsanzahl.
  - Der Parameter der maximalen Anzahl gleichzeitiger Jobs legt fest, wie viele Jobs dieses Typs gleichzeitig ausgeführt werden können.
  - Der Wiederholungsanzahl-Parameter bestimmt, wie oft der Job bis zum Abbrechen des Jobs versucht werden sollte, wenn Netzwerk- oder anderen Kommunikationsfehler den Erfolg der Jobs beim ersten Mal verhindern.
- In der Core Jobs-Tabelle zeigt die Spalte Einstellungen an, ob sich der Job in der Liste in den Core Job-Einstellungen per Vorgabe befindet oder ob sie explizit hinzugefügt werden müssen.

Die folgende Tabelle beschreibt die wichtigsten verfügbaren Core Jobs und deren Funktionen.

Tabelle 20. Core Jobs

Jobname	Description	Maximale Anzahl gleichzeitiger Jobs	Wiederholungsanzahl	Einstellungen
Anfügbarkeitsprüfung von SQL-Datenbanken in Snapshot	Damit kann der Core die Konsistenz der SQL-Datenbanken prüfen und sicherstellen, dass alle unterstützenden MDF- (Daten) und LDF- (Protokoll) Dateien in der Snapshot-Sicherungskopie verfügbar sind. Ablauf: • Letzten Wiederherstellungspunkt für Schutzgruppen mit SQL-Datenbanken bereitstellen. • Stellen Sie die Datenbank bereit. Wenn Sie Anfügbarkeit vom geschützten SQL Server	1	0	Standardeinstellung

Jobname	Description	Maximale Anzahl gleichzeitiger Jobs	Wiederholungsanzahl	Einstellungen
	durchführen, Bereitstellung über UNC-Pfad. • Verbindung vom SQL Server zur Datenbank herstellen. • Führen Sie die Überprüfung der Bereitstellungsfähigkeit durch. • Führen Sie Cleanup-Vorgänge durch. • Datenbank schließen. • Heben Sie die Bereitstellung der Datenbank auf. • Bereitstellung des Wiederherstellungspunktes aufheben.			
Überprüfen Sie bei Exchange-Datenbanken die Prüfsumme	Prüft die Integrität von Wiederherstellungspunkten, die Exchange-Datenbanken enthalten. Ablauf: • Letzten Wiederherstellungspunkt für Schutzgruppen mit SQL-Datenbanken bereitstellen. • Verbindung vom SQL Server zur Datenbank herstellen. • Datenbank öffnen. • Datenbank schließen. • Bereitstellung des Wiederherstellungspunktes aufheben.	1	0	Standardeinstellung
Überprüfen der Bereitstellungsfähigkeit der Exchange-Datenbanken	Überprüft, ob Exchange-Datenbanken bereitstellbar sind.	1	0	Standardeinstellung
Replizieren geschützter Maschinen Daten von Remotequelle	Überträgt eine Kopie der Wiederherstellungspunkte für eine geschützte Maschine von einem Quell-Core auf einen Ziel-Core. Dieser Job wird auf dem Ziel-Core ausgeführt und empfängt eingehende replizierte Wiederherstellungspunkte.	3	0	Standardeinstellung
Replizieren geschützter Maschinendaten für Remoteziel	Überträgt eine Kopie der Wiederherstellungspunkte für eine geschützte Maschine von einem Quell-Core (auf dem sie ursprünglich gespeichert waren) auf einen Ziel-Core.	1	3	Standardeinstellung

Jobname	Description	Maximale Anzahl gleichzeitiger Jobs	Wiederholungsanzahl	Einstellungen
	Dieser Job läuft auf dem Quell-Core und steuert ausgehende Replikation.			
Rollup-Wiederherstellungspunkte	Wendet die Aufbewahrungsrichtlinie für die gesicherten Daten durch Kombinieren oder Rollup von Wiederherstellungspunkten auf dem definierten Zeitplan in der Aufbewahrungsrichtlinie an.	1	0	Standardeinstellung
Prüfen von Wiederherstellungspunkten	Prüft die Integrität von Wiederherstellungspunkten.	1	0	Hinzufügen
Alle Wiederherstellungspunkte löschen	Löscht den vollen Satz der Wiederherstellungspunkte auf einer geschützten Maschine.	1	0	Hinzufügen
Wiederherstellungspunkte-Kette löschen	Löscht eine vollständige Wiederherstellungspunkt-Kette auf einer geschützten Maschine.	1	0	Hinzufügen
Einen Bereich von Wiederherstellungspunkten löschen	Löscht einen Satz von Wiederherstellungspunkten auf einer geschützten Maschine nach Wiederherstellungspunkt-Kennung oder Datumsbereich.	1	0	Hinzufügen
Agent-Software auf Computern bereitstellen	Stellt Rapid Recovery Agentensoftware auf der angegebenen Maschine oder Maschinen bereit.	1	0	Hinzufügen
Exchange-Bibliotheken herunterladen	Herunterladen von Microsoft Exchange Bibliotheken von der geschützten Maschine auf die Core-Maschine auf den Pfad `C:\ProgramData\AppRecovery\ExchangeLibraries`.	1	0	Hinzufügen
Auf Archiv exportieren	Erstellt Sicherungskopien im angegebenen Pfad mit einem Archiv der ausgewählten Wiederherstellungspunkte. Ablauf: • Wiederherstellungspunkte bereitstellen. • Schreiben von Daten auf Sicherungskopien. • Bereitstellung des Wiederherstellungspunktes aufheben.	1	0	Hinzufügen

Jobname	Description	Maximale Anzahl gleichzeitiger Jobs	Wiederholungsanzahl	Einstellungen
Export auf virtuelle Maschine	Exportiert Daten aus bestimmten Wiederherstellungspunkten der geschützten Maschine auf den Zielpfad als virtuelle Maschine. Ablauf: • Wiederherstellungspunkte bereitstellen. • Erstellt die virtuelle Maschine aus den Wiederherstellungspunktdaten im Zielpfad. • Bereitstellung des Wiederherstellungspunktes aufheben.	1	0	Hinzufügen
Archive importieren	Importiert Wiederherstellungspunkt aus der angegebenen Sicherung auf ein zuvor erstelltes Core-Archiv.	1	0	Hinzufügen
Repository warten	Führt eine Überprüfung des Repositorys durch. Ablauf: • Prüft Repository-Dateisystem. • Wiederherstellungspunkte bereitstellen. • Neu berechnen des Deduplizierungs-Cache für Repository. • Laden der Wiederherstellungspunkte von Repository.	1	0	Hinzufügen
Wiederherstellungspunkt-Snapshots bereitstellen	Führt Bereitstellung des Wiederherstellungspunkts auf einen angegebenen Pfad durch.	1	0	Hinzufügen
Schützen von virtuellen ESX® Maschinen	Fügt alle angegebenen virtuellen Maschinen agentenlosem Schutz hinzu. Job wird sofort ausgeführt nach dem Hinzufügen von agentenlosem Schutz eines oder mehrerer VMs auf den Core über den Assistenten zum Schützen mehrerer Maschinen. Job stellt ID-Nummer für die einzelnen angegebenen VMs ein, schreibt Informationen über den Core in eine Konfigurationsdatei und ruft die Metadaten aus der Datei ab.	1	0	Hinzufügen

Jobname	Description	Maximale Anzahl gleichzeitiger Jobs	Wiederholungen	Einstellungen
Wiederherstellen aus Wiederherstellungspunkt	Führt eine Wiederherstellung aus einem Wiederherstellungspunkt auf eine angegebene Ziel-Maschine durch. Ablauf: • Wiederherstellungspunkte bereitstellen. • Schreibt alle Daten des Wiederherstellungspunkts auf die angegebene Maschine. • Bereitstellung des Wiederherstellungspunktes aufheben.	1	0	Hinzufügen
Hochladen von Protokollen	Lädt Protokolle auf den angegebenen Server hoch.	1	0	Hinzufügen

Einige Core-Jobs sind in „Einstellungen“ enthalten. In den Job-Einstellungen können Sie festlegen, wie viele gleichzeitige Jobs des gleichen Typs der Core ausführen kann, und es wird beschrieben, wie viele Wiederholungsversuche versucht werden sollten, wenn der erste Job-Versuch fehlschlägt.

Weitere Informationen zu diesen Einstellungen finden Sie unter Core-Jobeinstellungen.

Weitere Informationen zum Hinzufügen von Jobs zu Core-Einstellungen finden Sie unter Hinzufügen von Core-Jobs zu Einstellungen.

Weitere Informationen zum Bearbeiten von Einstellungen für Jobs in der Liste „Einstellungen“ finden Sie unter Bearbeiten von Core-Jobeinstellungen.

Core-Jobeinstellungen

Über die Option (Einstellungen) über die Symbolleiste können Sie auf Einstellungen für einige Core-Jobs zugreifen. Im Bereich **Jobs** auf der Seite "Core-Einstellungen" können Sie zwei Einstellungen für jeden Job-Typ festlegen:

1. Die maximale Anzahl an Jobs dieses Typs, die der Core gleichzeitig ausführen soll. Diese Einstellung muss einen Wert zwischen 1 und 50 aufweisen.
2. Die Anzahl an Versuchen zum Ausführen eines Jobs, wenn ein Netzwerk- oder anderer Kommunikationsfehler verhindert, dass der Job beim ersten Versuch korrekt ausgeführt wird. Diese Einstellung muss einen Wert zwischen 0 und 10 aufweisen.

Mehrere Jobs werden automatisch in die Core-Einstellungen eingeschlossen. Diese Jobs weisen den Wert "Standard" in der Spalte "Einstellungen" auf (wie unter Grundlegende Informationen zu Core-Jobs dargestellt).

Sie können den Einstellungen andere Jobs hinzufügen, wenn Sie diese Einstellungen zur Steuerung der maximalen Anzahl der Jobs oder Wiederholungen für diese Funktionen konfigurieren möchten. Diese Jobs weisen den Wert "Hinzufügen" in der Spalte "Einstellungen" auf. Eine Anleitung zum Hinzufügen dieser Jobs zur Tabelle "Einstellungen" finden Sie unter Hinzufügen von Core-Jobs zu Einstellungen.

Bei Core-Jobs, die nicht in den Einstellungen verfügbar sind, besteht keine Möglichkeit zum Einstellen dieser beiden Parameter.

Bei Jobs, die in den Einstellungen aufgeführt sind, können Sie vorhandene Einstellungen bearbeiten. Mit dieser Option können Sie die beiden Parameter anpassen, einen Job-Typ aus der Liste der Jobeinstellungen löschen oder Standardeinstellungen wiederherstellen. Ausführliche Informationen hierzu finden Sie unter Bearbeiten von Core-Jobeinstellungen.

Hinzufügen von Core-Jobs zu Einstellungen

Mit Core Job-Einstellungen können Sie für jeden Jobtyp die maximale Anzahl der Jobs für den Core definieren, die gleichzeitig versucht wird, und wie oft dieser Job wiederholt werden sollte, wenn der erste Versuch fehlgeschlagen ist.

Jeder Core Job-Typ hat Standardwerte für diese beiden Parameter, wie im Thema Core-Jobeinstellungen beschrieben. Diese Liste gibt außerdem an, welche der Job-Typen im Lieferumfang der Kerneinstellungen standardmäßig enthalten sind.

Durch Hinzufügen eines Core-Jobs zu den Einstellungen können Sie diese Parameter für den Job-Typ, den Sie hinzugefügt haben, ändern.

Führen Sie die folgenden Schritte aus, um einen Job zu Core-Einstellungen hinzuzufügen.

1. Navigieren Sie zur Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite „Einstellungen“ auf **Jobs**.
   - Scrollen Sie auf der rechten Seite der Seite „Einstellungen“, bis Sie die Überschrift „Jobs“ sehen können.

     Die Core-Einstellungen der Jobs werden angezeigt.
3. Klicken Sie auf der Seite „Core-Einstellungen“ unter „Jobs“ auf **Hinzufügen**.

   Das Dialogfeld „Jobeinstellungen“ wird angezeigt.
4. Wählen Sie im Dialogfeld **Jobeinstellungen** im Feld **Jobs** den Namen des Jobs aus, den Sie hinzufügen möchten.

   Die betreffenden Jobs werden unter dem Thema Core-Jobeinstellungen behandelt.
5. Geben Sie im Textfeld **Maximale Anzahl gleichzeitiger Jobs** einen neuen Wert zwischen 1 und 50 ein, um die maximale Anzahl von Jobs festzulegen, die der Core gleichzeitig durchführen kann.
6. Geben Sie im Textfeld **Wiederholungsanzahl** einen neuen Wert zwischen 0 und 10 ein, um die Anzahl der Wiederholungsversuche festzulegen, die der Core unternehmen soll, bevor der Job abgebrochen wird.
7. Klicken Sie auf **Speichern**.

   Das Dialogfeld „Jobeinstellungen“ wird geschlossen und die neuen Jobeinstellungen werden übernommen.

Bearbeiten von Core-Jobeinstellungen

Mit Core Job-Einstellungen können Sie für jeden Jobtyp die maximale Anzahl der Jobs für den Core definieren, die gleichzeitig versucht wird, und wie oft dieser Job wiederholt werden sollte, wenn der erste Versuch fehlgeschlagen ist.

Jeder Core Job-Typ hat Standardwerte für diese beiden Parameter, wie im Thema Grundlegende Informationen zu Core-Jobs beschrieben. Diese Liste gibt außerdem an, welche der Job-Typen im Lieferumfang der Kerneinstellungen standardmäßig enthalten sind. Durch Bearbeitung der Core Jobeinstellungen können Sie Folgendes erreichen:

- Sie können die Einstellungen für jeden Core Job-Typ anpassen.
- Sie können einen Job-Typ aus der Liste der Core-Einstellungen löschen. Diese Funktion ist nicht verfügbar, wenn der Job standardmäßig in den Einstellungen vorhanden ist.

NOTE: Durch Löschen eines Jobs aus den Core-Einstellungen wird der Job-Typ einfach aus dieser Liste entfernt. Um die Core-Einstellungen für diesen Job-Typ später erneut zu bearbeiten, können Sie ihn der Liste wie unter Hinzufügen von Core-Jobs zu Einstellungen beschrieben hinzufügen.

- Sie können für jeden Job-Typ die Standardeinstellungen wiederherstellen.

NOTE: Sie können diese Funktion zwar nur für standardmäßig in den Core-Einstellungen vorhandene Job-Typen verwenden, Sie können jedoch die Standardeinstellungen für andere Job-Typen wiederherstellen, indem Sie sie aus der Liste entfernen und anschließend erneut hinzufügen.

Führen Sie die folgenden Schritte aus, um die Einstellungen eines Jobs zu bearbeiten.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite **Einstellungen** auf **Jobs**.
   - Scrollen Sie auf der rechten Seite der Seite **Einstellungen**, bis Sie die Überschrift „Jobs“ sehen können.

   Die Core-Einstellungen der Jobs werden angezeigt.
3. Wählen Sie aus dem Job-Raster einen Job aus, den Sie aus der Liste entfernen möchten. Wählen Sie aus dem Drop-Down-Menü für diesen Job die Option **Löschen** aus.

   Der Job wird aus der Liste entfernt.
4. Wählen Sie in dem Job-Raster einen Job aus der Liste aus, für den Sie die Einstellungen zurücksetzen möchten. Wählen Sie aus dem Drop-Down-Menü für diesen Job die Option **Auf Standardwerte zurücksetzen** aus.

   Die Jobeinstellungen für diesen Job werden auf die Standardeinstellungen zurückgesetzt.
5. Wählen Sie aus dem Job-Raster den Job aus, den Sie ändern möchten. Wählen Sie aus dem Drop-Down-Menü für diesen Job die Option **Bearbeiten** aus.
6. Das Dialogfeld „Job-Einstellungen: [JobName]“ wird geöffnet.
7. Geben Sie im Textfeld „Maximale Anzahl gleichzeitiger Jobs“ einen neuen Wert zwischen 1 und 50 ein, um die maximale Anzahl von Jobs zu ändern, die der Core gleichzeitig durchführen kann.
8. Geben Sie im Textfeld "Wiederholungsanzahl" einen neuen Wert zwischen 0 und 10 ein, um die Einstellung für die Anzahl der Wiederholungsversuche zu ändern, die der Core unternehmen soll, bevor der Job abgebrochen wird.
9. Klicken Sie auf **Speichern**.

   Das Dialogfeld „Jobeinstellungen“ wird geschlossen und die neuen Jobeinstellungen werden übernommen.

Verwalten von Lizenzen

Es gibt drei Arten von Rapid Recovery Softwarelizenzen:

- **Testversion**, die nach 14 Tagen aufhört, Snapshots aufzunehmen.
- **Abonnement**, welche ein Ablaufdatum hat, und
- **Unbefristet**, welche kein Ablaufdatum hat.

Viele Rapid Recovery Core Benutzer beginnen mit einer Testlizenz, die über eingeschränkte Funktionen verfügt. Nach Ablauf der 14 Tage kann ein Gruppenadministrator die Testlizenz um 28 Tage verlängern, wenn die Umstände es erfordern. Andernfalls können Sie eine unbefristete oder Abonnement-Lizenz kaufen und registrieren.

NOTE: Informationen über das Eingeben des Lizenzschlüssels oder Dateiinformationen (z. B. zum Aktualisieren oder Ändern einer Testlizenz auf eine gültige Langzeitlizenz) finden Sie unter Aktualisieren oder Ändern einer Lizenz.

Rapid Recovery liefert Lizenzen in einer Datei. Eine Rapid Recovery Lizenzdatei enthält einen Pool von Lizenzen, die Sie auf die Maschinen verteilen können, die Sie schützen möchten. Dieser Pool wird auf Rapid Recovery Lizenzportal angezeigt. Für jeden der zuvor aufgeführten Lizenztypen gibt es zwei Arten von Lizenzpools:

- **Enterprise.** Jede Lizenz in diesem Pool kann unabhängig vom belegten Speicherplatz auf eine Installation desRapid Recovery Agenten oder eine Buchse auf einem Hypervisor-Host mit agentenlosem Schutz angewendet werden.
- **Kapazität.** Diese Lizenzen werden angewendet, gemessen daran wie viele Daten geschützt werden sollen (in Terabyte (TB)), unabhängig von der Anzahl der installierten Rapid Recovery Agenten oder Buchsen. Wenn Sie den Betrag des Speicherplatzes, der der erworbenen Lizenz zugeordnet ist, überschreiten, müssen Sie eine weitere Lizenz erwerben. Für die Lizenzierung nach Kapazität:
  - DL-Appliances mit einem Backend-Kapazitätslizenzmodell, in dem die Kapazität, die in der Lizenz angegeben wird, die Größe der Repository (in TB) begrenzt, die Sie auf der Appliance verwenden können.
  - Software-Installationen verwenden ein Backend-Kapazitätslizenzmodell, in dem die Kapazität, die in der Lizenz angegeben wird, die Datenmenge (in TB) von den zu schützenden Maschinen begrenzt, die Sie in dem Repository speichern können. Die Frontend-Kapazität wird vor der Komprimierung und Deduplizierung gemessen.

In Version 6.2 kann ein Core nur einen Lizenzpooltyp verwenden. Wenn zum Beispiel Ihr Core einen kapazitätsbasierten Lizenzpool nutzt, kann er nicht gleichzeitig einen Unternehmenslizenzpool verwenden. Auch das Gegenteil trifft zu.

Lizenzpool-Typen können nicht in einer einzigen Lizenzdatei kombiniert werden. Zum Beispiel können Sie nicht einen Enterprise-Lizenzpool und einen Kapazitäts-Lizenzpool in die gleiche unbefristete Lizenz einschließen.

Lizenzdateien sind Textdateien, die mit der Dateierweiterung `.lic` enden. Im Folgenden sind Beispiele von Lizenzdateien gegeben:

- Lizenzdateien können eine Länge von neun Zeichen haben und aus drei Gruppen von Ziffern bestehen, die jeweils durch einen Bindestrich getrennt sind; z. B. `123-456-789.lic`.
- Softwarebasierte Lizenzen können im Format Software-<Group name>.lic angezeigt werden, wobei die Gruppe nach dem Kundennamen oder Konto benannt ist, z. B. `Software-YourCompany.lic`.
- DL-Lizenzen können im Format <Appliance Series>-<Group name>.lic angezeigt werden, wobei die Gruppe nach dem Kundennamen oder Konto benannt ist, z. B. `DL4X00 Series-YourCompany.lic`.

Rapid Recovery unterstützt die folgenden Lizenztypen in zwei Modi: den standardmäßigen Phone-Home-Modus und den Non-Phone-Home-Modus, der einige Einschränkungen aufweist. Abonnement-Lizenzen können nur im Phone-Home-Modus ausgeführt werden. Unbefristete und Testlizenzen können entweder Phone-Home- oder Non-Phone-Home-Lizenzen verwenden. Informationen dazu, wie dieser Modus sich auf die Nutzung von personenbezogenen Daten in Rapid Recovery auswirkt, finden Sie im Thema „Datenschutzverwaltung“. Informationen zu Beschränkungen bei Non-Phone-Home-Lizenzen oder Informationen zum Erwerb einer Lizenz mit diesem Modus finden Sie unter „Obtaining and using non-phone-home licenses“ (Erhalten und Verwenden von Non-Phone-Home-Lizenzen). Diese Themen finden Sie in *Rapid Recovery Benutzerhandbuch*.

Rapid Recovery ermöglicht Ihnen die Verwaltung von Lizenzen oder eine direkte Verbindung mit dem Lizenzserver über die Core Console durch Auswählen von (Einstellungen) auf der Symbolleiste und klicken auf **Lizenzierung**.

Die Lizenzierungseinstellungen enthalten folgende Informationen:

Lizenzdetails:

-  **Lizenz ändern**. Hiermit können Sie eine vorhandene, dem Core zugeordnete Lizenz durch Hochladen einer Lizenzdatei oder Eingeben eines Lizenzschlüssels ändern.
- **Lizenz hinzufügen**. Diese Option ist nur für DL Sicherungs-Appliances verfügbar. Sie ermöglicht das Hochladen einer Lizenzdatei oder Eingeben eines Lizenzschlüssels.
- **Lizenzportalgruppe**. Mit dieser Option kann das Lizenzportal für die Gruppenverwaltung geöffnet werden.
- **Lizenztyp**. Es gibt die folgenden Lizenzarten: „Testversion“, „Abonnement“ oder „Unternehmen“. Weitere Informationen finden Sie im Thema „Understanding software license types“ (Grundlegende Informationen zu Softwarelizenzarten) in *Rapid Recovery Lizenzportal - Benutzerhandbuch*.
- **Lizenzstatus**. Zeigt den Status der Lizenz an. Wenn der Status „Aktiv“ ist, können Snapshots weiter wie geplant erstellt werden. Wenn die Lizenz gesperrt oder abgelaufen ist bzw. der Core über den Toleranzzeitraum hinaus nicht mit dem Rapid Recovery Lizenzportal kommunizieren konnte, wird die Snapshot-Erstellung vorübergehend deaktiviert, bis der Lizenzstatus korrigiert wurde.
- **Lizenzschlüssel läuft ab in**. Diese Option ist nur bei Verwendung einer Abonnement-Lizenz verfügbar und zeigt die Dauer in Tagen an, bis das Abonnement abläuft.

Lizenzbedingungen:

- **Maximale Anzahl Snapshots pro Tag**. Zeigt die maximale Anzahl der Sicherungen für die bestimmte Lizenz an.

Lizenzpool:

- **Poolgröße**. Der Lizenzpool stellt die Anzahl der verfügbaren Lizenzen dar, die keine Testversion sind, die im Rapid Recovery Lizenzportal Gruppen und Untergruppen zugewiesen werden können. Die Größe des Pools gibt an, wie viele Lizenzen zugewiesen werden können. Weitere Informationen finden Sie im Thema „Grundlegende Informationen zu Lizenzpools“ in *Rapid Recovery Lizenzportal - Benutzerhandbuch*.
- **Von diesem Core verwendet**. Zeigt die Anzahl der Maschinen aus dem Lizenzpool an, die durch diesen Core geschützt werden.
- **Insgesamt in Gruppe verwendet**. Zeigt die Gesamtzahl der geschützten Maschinen in derselben Lizenzgruppe wie dieser Core an.
- **Phone-Home deaktiviert**. Wenn sichtbar, zeigt dieser Zustand an, dass der Core nicht mit Rapid Recovery Lizenzportal oder Datenschutz-Portal kommuniziert. Die automatische Aktualisierung ist deaktiviert und keine personenbezogenen Daten werden zwischen Core und Quest Software, Inc. oder einer sonstigen Einrichtung weitergegeben, um die Einhaltung der Datenschutz-Grundverordnung sicherzustellen.

Lizenzserver. Diese Einstellungen gelten für normale Lizenzen (Phone-Home-Lizenzen). Diese Einstellungen gelten nicht für Appliances und andere NPH-Lizenzen:

- **Adresse des Lizenzservers**. Zeigt eine aktive URL für den Lizenzserver für diesen Core an.
- **Letzte Antwort vom Lizenzserver**. Zeigt an, ob der letzte Kommunikationsversuch mit dem Lizenzserverportal erfolgreich war.
- **Letzter Kontakt zum Lizenzserver**. Zeigt Datum und Uhrzeit des letzten erfolgreichen Kontakts mit dem Lizenzserver an.
- **Nächste Kontaktaufnahme zum Lizenzserver**: Zeigt den nächsten planmäßigen Zeitpunkt für eine Verbindung zum Lizenzserver an.
- **Jetzt Kontakt aufnehmen**. Mit dieser Schaltfläche kann bei Bedarf eine Verbindung zum Lizenzserver hergestellt werden. Verwenden Sie diese Option, nachdem Sie Änderungen an Ihrer Lizenzkonfiguration vorgenommen haben, um Änderungen sofort anstatt beim nächsten geplanten Versuch zu registrieren.

Weitere Informationen zu Lizenzen finden Sie unter *Rapid Recovery Lizenzportal - Benutzerhandbuch*.

Weitere Informationen über das Aktualisieren oder Ändern eines Lizenzschlüssels oder einer Lizenzdatei finden Sie unter Aktualisieren oder Ändern einer Lizenz.

Benutzer von DL Sicherungs-Appliances können auch dem Core Lizenzen hinzufügen, falls erforderlich. Weitere Informationen hierzu finden Sie unter Hinzufügen einer Lizenz.

Weitere Informationen zur Kontaktaufnahme mit dem Lizenzportalserver finden Sie unter Kontaktaufnahme mit dem Rapid Recovery Lizenzportal-Server.

Sie können auch Lizenzinformationen für eine einzelne geschützte Maschine anzeigen. Weitere Informationen hierzu finden Sie unter Anzeigen von Lizenzinformationen für eine Maschine.

Aktualisieren oder Ändern einer Lizenz

Nach einem Hochstufen oder Kauf einer Rapid Recovery Langzeitlizenz erhalten Sie per E-Mail entweder eine Lizenzdatei oder einen Lizenzschlüssel.

Führen Sie die Schritte in diesem Verfahren zum Hochstufen Ihrer Testlizenz oder zur Änderung Ihrer vorhandenen Lizenz aus und ordnen Sie sie der Rapid Recovery Core Console zu.

NOTE: Benutzer von DL Sicherungs-Appliances können auch dem Core Lizenzen hinzufügen, falls erforderlich. Weitere Informationen hierzu finden Sie unter Hinzufügen einer Lizenz.

NOTE: Informationen zum Abrufen eines Lizenzschlüssels oder Details zur Verwendung des Lizenzportals zum Herunterladen von Software, Registrieren von Appliances, Verwalten von Lizenzabonnements und Erstellen von Lizenzportal-Berichten erhalten Sie im *Rapid Recovery Lizenzportal - Benutzerhandbuch*.

Wenn Sie gerade einen neuen Core installiert haben und eine Meldung in der Core Console sehen, in der Sie aufgefordert werden, eine Lizenzdatei oder einen Schlüssel auszuwählen, fahren Sie mit Schritt 5.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen).
3. Führen Sie einen Bildlauf nach unten auf der rechten Seite der Seite **Einstellungen** durch, bis Sie die **Lizenzserver**-Überschrift sehen können.

   Die Core-Einstellungen für die Lizenzierung werden angezeigt.
4. Zum Aktualisieren oder Ändern der vorhandenen Lizenz im Zusammenhang mit dem Core klicken Sie im Bereich „Core-Einstellungen“ über den Lizenzdetails auf **Lizenz ändern**.

   Das Dialogfeld **Lizenz ändern** wird angezeigt.
5. Wenn Sie den Lizenzschlüssel manuell eingeben möchten, fahren Sie mit Schritt 6 fort. Führen Sie die folgenden Schritte aus, um eine Lizenzdatei hochzuladen:
   a. Um eine Lizenzdatei hochzuladen, klicken Sie im Feld **Lizenzdatei wählen oder Lizenzschlüssel eingeben** auf **Datei auswählen**.

   Im Dialogfeld **Datei hochladen** navigieren Sie durch das Dateisystem und suchen die neue Lizenzdatei, die Sie verwenden möchten. Suchen Sie zum Beispiel `Software-YourCompany.lic`.

   b. Klicken Sie auf die Lizenzdatei und klicken Sie auf **Öffnen**.

   Das Dialogfeld **Datei hochladen** wird geschlossen. Die Lizenzdatei, die Sie ausgewählt haben, wird im Lizenz-Textfeld angezeigt.

   c. Klicken Sie im Dialogfeld **Lizenz ändern** auf **Weiter**.

   Die Lizenzdatei, die Sie ausgewählt haben, wird authentifiziert und diese Lizenz wird dem Core zugeordnet.

   d. Fahren Sie mit Schritt 7 fort.
6. Wenn Sie den Lizenzschlüssel manuell eingeben möchten, geben Sie im Textfeld **Lizenzdatei wählen oder Lizenzschlüssel eingeben** den Lizenzschlüssel sorgfältig ein und klicken Sie dann auf **Weiter**.

Das Dialogfeld wird geschlossen, die Lizenzdatei, die Sie ausgewählt haben, wird authentifiziert, und diese Lizenz wird dem Core zugeordnet.

7. Wenn die Willkommens-Seite des **Schnellstart-Handbuchs** angezeigt wird, können Sie das Handbuch starten oder dieses Tool schließen. Dies ist der letzte erforderliche Schritt für dieses Verfahren.

   NOTE: Weitere Informationen zum Schnellstarthandbuch finden Sie unter „Grundlegende Informationen zum Schnellstarthandbuch“ in *Rapid Recovery Benutzerhandbuch*.

8. Wenn Sie diese Schritte auf der Seite Core **Einstellungen** durchführen, führen Sie einen Bildlauf nach unten auf der rechten Seite der Seite **Einstellungen** durch, bis Sie die Lizenzserver-Überschrift sehen können.
9. Klicken Sie im Bereich „Lizenzserver“ auf **Jetzt Kontakt aufnehmen**.

   Nachdem die Lizenz im Lizenzserver registriert wurde, werden alle zugehörigen geschützten Maschinen automatisch mit der neuen Lizenz aktualisiert.

Wenn am oberen Rand des Rapid Recovery Core Console Fehlermeldungen angezeigt werden (z. B. bestimmte Dienste nicht gestartet), befolgen Sie die Anleitung zum Beheben dieser Fehler in der Fehlermeldung.

Hinzufügen einer Lizenz

Besitzer einer Sicherungs-Appliance der DL-Serie können eine oder mehrere Lizenzen in Rapid Recovery Core Console hinzufügen.

Nachdem Sie Ihre Rapid Recovery Lizenz aktualisiert oder gekauft haben, erhalten Sie eine Lizenzdatei oder einen Lizenzschlüssel.

Sie können auch eine vorhandene Lizenz auf der Core Console aktualisieren oder ändern. Weitere Informationen hierzu finden Sie unter Aktualisieren oder Ändern einer Lizenz.

NOTE: Nur Besitzer einer Sicherungs-Appliance der DL-Serie sehen die Schaltfläche **Appliance hinzufügen**.

NOTE: Weitere Informationen zum Erwerb eines Lizenzschlüssels finden Sie in *Rapid Recovery Lizenzportal - Benutzerhandbuch*.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen).
3. Führen Sie einen Bildlauf nach unten auf der rechten Seite der Seite **Einstellungen** durch, bis Sie die Lizenzierungs-Überschrift sehen können.

   Die Core-Einstellungen für die Lizenzierung werden angezeigt.
4. Um eine Lizenz hinzuzufügen und sie dem Core zuzuordnen, klicken Sie oben im Core-Einstellungsbereich „Lizenzdetails“ auf **Lizenz hinzufügen**. Führen Sie im daraufhin angezeigten Dialogfeld eine der folgenden Aktionen aus:
   a. Wenn Sie den Lizenzschlüssel manuell eingeben möchten, geben Sie den Schlüssel genau ein und klicken dann auf **Weiter**.

   Das Dialogfeld wird geschlossen, und die Lizenzdatei, die Sie ausgewählt haben, wird authentifiziert, und diese Lizenz wird dem Core zugeordnet.

   b. Wenn Sie eine Lizenzdatei hochladen möchten, klicken Sie auf **Datei auswählen**.

   Im Dialogfeld **Datei hochladen** navigieren Sie durch das Dateisystem und suchen die neue Lizenzdatei, die Sie verwenden möchten. Suchen Sie zum Beispiel `Software-YourCompany.lic`.

   c. Klicken Sie auf die Lizenzdatei und klicken Sie auf **Öffnen**.

   Das Dialogfeld „Datei hochladen“ wird geschlossen. Die ausgewählte Lizenzdatei wird im aktuellen Dialogfeld angezeigt.

   d. Klicken Sie im Dialogfeld auf **Weiter**.

Das Dialogfeld wird geschlossen, und die Lizenzdatei, die Sie ausgewählt haben, wird authentifiziert, und diese Lizenz wird dem Core zugeordnet.

5. Führen Sie einen Bildlauf nach unten auf der rechten Seite der Seite **Einstellungen** durch, bis Sie die Lizenzserver-Überschrift sehen können.

   Die Lizenzierungs-Core-Einstellungen werden angezeigt.

6. Klicken Sie im Bereich „Lizenzserver“ auf **Jetzt Kontakt aufnehmen**.

   Nachdem die Lizenz im Lizenzserver registriert wurde, werden alle zugehörigen geschützten Maschinen automatisch mit der neuen Lizenz aktualisiert.

Kontaktaufnahme mit dem Rapid Recovery Lizenzportal-Server

Der Rapid Recovery Core Console kontaktiert den Rapid Recovery Lizenzportal-Server regelmäßig, um sich mit Änderungen zu aktualisieren, die im Lizenz-Portal vorgenommen wurden.

Bei Lizenzen, die keine Testlizenzen sind, stellt der Rapid Recovery Core einmal pro Stunde eine Verbindung zum Lizenzportal her. Wenn der Core das Lizenzportal nach einem Toleranzzeitraum von 10 Tagen nicht erreichen kann, beendet der Core die Snapshot-Erstellung.

Die Kommunikation mit dem Portalserver erfolgt normalerweise automatisch in bestimmten Zeitabständen. Sie können die Kommunikation jedoch auch bei Bedarf starten.

Führen Sie die nachstehend beschriebenen Schritte aus, um eine Verbindung zum Lizenzportalserver herzustellen.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. In der Symbolleiste klicken Sie auf **Einstellungen** und führen dann einen Bildlauf nach unten auf der rechten Seite der Seite **Einstellungen** durch, bis Sie die Lizenzserver-Überschrift sehen können.
3. Klicken Sie im Lizenzserver-Bereich auf **Jetzt Kontakt aufnehmen**.

Grundlegende Informationen zu SNMP-Einstellungen

Das SNMP-Protokoll (Simple Network Management Protocol) ermöglicht die Verwaltung von Geräten in einem IP-Netzwerk. SNMP wird hauptsächlich für die Überwachung von Diensten in einem Netzwerk verwendet, um Zustände zu erkennen, die ein Eingreifen notwendig machen. Dieses Protokoll verwendet Softwarekomponenten (Agenten), um Informationen an Verwaltungscomputer (Manager) zu melden. Ein SNMP-Agent verarbeitet die Anforderungen des Managers, um bestimmte Parameters abzurufen oder festzulegen. Der SNMP-Agent kann auch Traps (Benachrichtigungen zu bestimmten Ergebnissen) an den Manager senden.

Die von den SNMP-Agenten verwalteten Datenobjekte werden in einer Management Information Base (MIB)-Datei verwaltet, die Objekt-IDs enthält. Jede Objekt-ID kennzeichnet eine Variable, die mit SNMP gelesen oder festgelegt werden kann.

Rapid Recovery bietet Unterstützung für die SNMP-Version 1.0.

Sie können den Rapid Recovery Core als einen SNMP-Agenten konfigurieren. Der Core kann Informationen wie Benachrichtigungen, Repositorystatus und geschützte Maschinen melden. Ein SNMP-Host kann diese Informationen über eine eigenständige Anwendung, SNMP-Browser genannt, lesen. Sie können den SNMP-Browser auf einer beliebigen Maschine installieren, auf die der Rapid Recovery Core über das Netzwerk zugreifen kann.

Um sicherzustellen, dass die Core SNMP-Ereignisbenachrichtigungen vom SNMP-Browser empfangen werden können, überprüfen Sie, ob die Benachrichtigungsoptionen für eine Benachrichtigungsgruppe für das Benachrichtigen über SNMP-Trap konfiguriert sind.

NOTE: Sie können die Standard-Gruppe verwenden oder eine benutzerdefinierte Benachrichtigungsgruppe erstellen. Der Vorgang ist identisch.

Öffnen Sie die Benachrichtigungsgruppe, wählen Sie die Registerkarte **Benachrichtigungsoptionen** aus und stellen Sie sicher, dass die Option **Über SNMP-Trap benachrichtigen** aktiviert ist. Die Benachrichtigungsgruppe bestimmt standardmäßig die Trap-Nummer 1. Falls erforderlich können Sie die Trap-Nummer ändern, um sicherzustellen, dass sie der Einstellung entspricht, die der SNMP-Browser erwartet.

Weitere Informationen und spezifische Details über die Konfiguration von Benachrichtigungsoptionen finden Sie unter Konfigurieren von Benachrichtigungsgruppen.

Alternativ können Sie eine MIB-Datei aus dem Rapid Recovery Core herunterladen. Diese Datei kann mithilfe eines SNMP-Browsers in einer benutzerfreundlicheren Form angezeigt werden als die direkt vom Core empfangenen Daten.

In diesem Abschnitt werden folgende Themen behandelt:

- Konfigurieren der SNMP-Einstellungen
- Herunterladen der SNMP MIB-Datei

Konfigurieren der SNMP-Einstellungen

Mithilfe der SNMP-Einstellungen können Sie die Kommunikation zwischen dem Rapid Recovery Core und dem SNMP-Browser steuern. Hierzu zählen die Einstellungen für SNMP-Port, Trap-Empfänger-Port und der Hostnamen für den Trap-Empfänger.

NOTE: Rapid Recovery Versionen vor Version 6.1 enthalten nicht die Möglichkeit, die **Community-Zeichenfolge** zu ändern.

Verwenden Sie dieses Verfahren zum Konfigurieren der SNMP-Einstellungen für den Core.

1. Navigieren Sie zur Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite „Einstellungen“ auf **SNMP-Konfiguration**.
   - Führen Sie einen Bildlauf nach unten auf der rechten Seite der Seite Einstellungen durch, bis Sie die SNMP-Konfigurations-Überschrift sehen können.

     Die SNMP-Konfigurationseinstellungen werden angezeigt.
3. Ändern Sie die in der folgenden Tabelle beschriebenen SNMP-Einstellungen.

Tabelle 21. Informationen zu SNMP Verbindungseinstellungen

Textfeld	Description
Eingehende Anfrage verarbeiten	Aktivieren Sie diese Option, damit der Core eingehende SNMP-Protokolle erkennen kann. Zum Blockieren eingehender SNMP-Protokolle deaktivieren Sie die Option. **NOTE:** Durch Aktivieren der Option zum Verarbeiten eingehender Anfragen können Sie die Community-Zeichenfolge bearbeiten.
Community-Zeichenfolge	Geben Sie einen Namen für die Community ein. **NOTE:** Sie können diese Einstellung nur ändern, wenn die Option **Eingehende Anfrage verarbeiten** auf **Ja** gesetzt ist.
Eingehender Port	Geben Sie eine Portnummer für die SNMP-Verbindung ein.

Textfeld	Description
	NOTE: Die Standardeinstellung ist 8161.
Traps senden	Damit Benachrichtigungen (Traps) über das SNMP-Protokoll gesendet werden, aktivieren Sie diese Option. Zum Blockieren von Warnmeldungen deaktivieren Sie die Option.
Trap-Empfänger-Port	Geben Sie eine Portnummer für die eingehende Warnung ein. Die Standardeinstellung ist 162.
Trap-Empfänger-Hostname	Geben Sie einen Hostnamen für die SNMP-Verbindung ein. **NOTE:** Der Standardhostname ist Localhost.

4. Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf ✓, um die Änderungen zu speichern und den Bearbeitungsmodus zu beenden, oder klicken Sie auf ✕, um den Bearbeitungsmodus ohne Speichern zu beenden.

Herunterladen der SNMP MIB-Datei

Das Simple Network Management-Protokoll wird zur Überwachung der Geräte in einem Netzwerk für Bedingungen, die Ihre Aufmerksamkeit erfordern, verwendet. Wenn der Rapid Recovery Core als ein SNMP-Agent eingestellt ist, meldet der Core Informationen wie z. B. Warnungen, Repository-Status und geschützte Maschinen. Diese Informationen können von einem SNMP-Host mithilfe einer eigenständigen Anwendung, einem so genannten SNMP-Browser, gelesen werden.

Die von den SNMP-Agenten verwalteten Datenobjekte werden in einer Management Information Base (MIB) verwaltet, die Objekt-IDs enthält. Jede Objekt-ID kennzeichnet eine Variable, die mit SNMP gelesen oder festgelegt werden kann.

Sie können auch eine MIB-Datei vom Rapid Recovery Core herunterladen. Die Datei mit dem Namen quest-rapid-recovery-core.mib kann von einem SNMP-Browser gelesen und in einer benutzerfreundlicheren Form angezeigt werden als die direkt vom Core empfangenen Daten.

Verwenden Sie dieses Verfahren zum Herunterladen der SNMP-MIB-Datei vom Rapid Recovery Core.

1. Navigieren Sie zur Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf ••• (Mehr) und klicken Sie dann auf **Downloads**.

   Die Seite **Downloads** wird angezeigt.
3. Scrollen Sie zum Fensterbereich „Andere Dateien“.
4. Um die MIB-Datei herunterzuladen, klicken Sie auf den Download-Link **SNMP-MIB-Datei**.

   Die SNMP-Konfigurationseinstellungen werden angezeigt.
5. Führen Sie im Dialogfeld **quest-rapid-recovery-core.mib öffnen** einen der folgenden Vorgänge aus:
   - Um die Protokolldatei zu öffnen, wählen Sie die Option **Öffnen mit** und wählen dann eine SNMP-Browser-Anwendung für die Anzeige der textbasierten MIB-Datei und klicken dann auf **OK**.

     Die MIB-Datei wird in der ausgewählten Anwendung geöffnet.
   - Zum Speichern der Datei lokal wählen Sie **Datei speichern** und klicken auf **OK**.

     Die Datei quest-rapid-recovery-core.mib wird im Ordner „Downloads“ gespeichert. Sie kann über einen SNMP Browser oder einen Texteditor geöffnet werden.

Konfigurieren von vSphere-Einstellungen

VMware vSphere ist eine Virtualisierungssoftware, über die Sie auf ESXi- oder vCenter-Servern laufende virtuelle Maschinen verwalten können. Bei Verwendung von vSphere müssen Sie die Rapid Recovery Agentensoftware nicht mehr auf einzelne VMs laden, um sie zu schützen. Diese Funktion wird als agentenloser Schutz bezeichnet. Diese Funktion gilt nur für virtuelle Maschinen.

Verwenden Sie dieses Verfahren zum Konfigurieren von vSphere-Einstellungen für den Core.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite "Einstellungen" auf **vSphere**.
   - Scrollen Sie auf der rechten Seite der Seite "Einstellungen" bis zur Überschrift "vSphere".
3. Ändern Sie die vSphere-Einstellungen wie in der folgenden Tabelle beschrieben.

Tabelle 22. Informationen zu den vSphere Core-Einstellungen

UI-Element	UI-Typ	Description
Verbindungslebensdauer	Datenfeld	Legt die Zeitdauer vor einer Zeitüberschreitung für die Verbindung mit dem ESXi-Server fest. Das Format ist HH:MM:SS (Stunden:Minuten:Sekunden). **NOTE:** Die Standardeinstellung ist 00:10:00 bzw. zehn Minuten.
Maximale Anzahl gleichzeitiger Konsolidierungen	Textfeld	Legt die maximale Anzahl gleichzeitiger Konsolidierungen für geschützte virtuellen Maschinen fest. **NOTE:** Die Standardeinstellung ist 0.
Maximale Anzahl der Wiederholungen	Textfeld	Legt die maximale Anzahl an Verbindungsversuchen mit einer virtuellen Festplatte oder der Lese- und Schreibversuche vor einer Zeitüberschreitung fest. **NOTE:** Die Standardeinstellung ist 10.
Parallel Wiederherstellung zulassen	Boolesch (Kontrollkästchen)	Wenn diese Option aktiviert ist, ist die parallele Wiederherstellung für eine agentenlose virtuelle Maschine aktiviert. Wenn diese Option deaktiviert ist, ist die Funktion deaktiviert. **NOTE:** Die Standardeinstellung ist "Nein" (deaktiviert).

4. Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf , um die Änderungen zu speichern und den Bearbeitungsmodus zu beenden, oder klicken Sie auf , um den Bearbeitungsmodus ohne Speichern zu beenden.

Verwalten der VMware Proxy-Einstellungen

Die VMware Proxy-Einstellungen sind für geschützte VMware ESXi-Maschinen vorgesehen, die Virtual Disk Development Kit (VDDK)-APIs für den Zugriff auf den VMware-Festplattenspeicher benötigen. Rapid Recovery geht auf diesen Zugriff und mögliche damit verbundene Zeitüberschreitungen ein, indem es einen Prozess namens VMware Proxy verwendet. Dieser Service wird automatisch mit dem Rapid Recovery Core installiert und läuft nur, wenn es notwendig ist. Auf der Seite „Core-Einstellungen“ können Sie die Einstellungen für den Service-Timeout nach eigenem Ermessen anpassen.

1. Klicken Sie auf der Symbolleiste der Rapid Recovery Core Console auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite „Einstellungen“ auf **VMware Proxy**.
   - Scrollen Sie auf der rechten Seite der Seite „Einstellungen“ nach unten, bis sie die Überschrift **VMware Proxy** sehen können.
2. Ändern Sie unter **VMware Proxy** die Einstellungen für die Zeitüberschreitung, wie in der folgenden Tabelle beschrieben.

Tabelle 23. Informationen zu VMware Proxyeinstellungen

UI-Element	Description
Zeitüberschreitungsverbindung	Die maximale Zeit, bevor der VMware Proxy aufhören sollte, eine Verbindung mit dem VMware Festplattenspeicher herzustellen, angegeben im Format hh:mm:ss. **NOTE:** Die Standardeinstellung beträgt 5 Minuten (00:05:00).
Zeitüberschreitung Lesen/Schreiben	Die maximale Zeit, bevor der VMware Proxy aufhören sollte, den VMware Festplattenspeicher zu lesen bzw. in diesen zu schreiben, angegeben im Format hh:mm:ss. **NOTE:** Die Standardeinstellung beträgt 5 Minuten (00:05:00).
Timeout für Starten des Dienstes	Die maximale Zeit, bevor Rapid Recovery aufhören sollte, den VMware Proxy-Dienst zu starten, angegeben im Format hh:mm:ss. **NOTE:** Die Standardeinstellung beträgt 5 Minuten (00:05:00).
Timeout für Stoppen des Dienstes	Die maximale Zeit, bevor Rapid Recovery aufhören sollte, den VMware Proxy-Dienst zu stoppen, angegeben im Format hh:mm:ss. **NOTE:** Die Standardeinstellung beträgt 1 Minute (00:01:00).

3. Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf die Kontrollhäkchen, um die Änderungen zu speichern und den Bearbeitungsmodus zu beenden, oder klicken Sie auf **X**, um den Bearbeitungsmodus ohne Speichern zu beenden.

Konfigurieren von vFoglight-Einstellungen

Wenn Sie Informationen zu vFoglight in den Core-Einstellungen bereitstellen, zeigt die Core Console eine vFoglight-URL für jede geschützte VM auf der Seite „Zusammenfassung“ an. Klicken Sie auf diese URL, um Informationen über die VM in vFoglight zu öffnen.

Führen Sie die folgenden Schritte aus, um Ihren vFoglight-Server mit Ihrem Rapid Recovery Core Server zu integrieren.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite „Einstellungen“ auf **vFoglight-Konfiguration**.
   - Scrollen Sie auf der rechten Seite der Seite „Einstellungen“, bis Sie die Überschrift „vFoglight“ sehen können.

     Die vFoglight-Konfigurationseinstellungen werden angezeigt.
3. Ändern Sie die in der folgenden Tabelle beschriebenen vFoglight-Einstellungen.

Tabelle 24. Informationen zu vFoglight-Verbindungseinstellungen

Textfeld	Description
Https verwenden	Aktiviert oder deaktiviert das sichere Hypertext Transfer Protocol. Sichere HTTPS ist die Standardeinstellung.
Host	Geben Sie einen Hostnamen oder eine IP-Adresse für Ihren vFoglight-Server ein. Wenden Sie sich an Ihren vFoglightServer-Administrator für weitere Details.
Port	Geben Sie den entsprechende Port an. Der Standardport ist 32896. Wenden Sie sich an Ihren vFoglightServer-Administrator für weitere Details.
Authentifizierungstoken	Geben Sie die korrekte Authentifizierung an, damit der Core mit Ihrem vFoglight-Server kommunizieren kann. Wenden Sie sich an Ihren vFoglightServer-Administrator für weitere Details.

4. Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf , um die Änderungen zu speichern und den Bearbeitungsmodus zu beenden, oder klicken Sie auf , um den Bearbeitungsmodus ohne Speichern zu beenden.

Tools auf Core-Ebene

Zusätzlich zum Konfigurieren von Kerneinstellungen können Sie auch die in der folgenden Tabelle beschriebenen Core-Ebene-Tools verwenden.

Tabelle 25. Andere Core-Ebene-Tools

UI-Element	Description
Systeminformationen	Rapid Recovery bietet die Möglichkeit, Informationen über den Rapid Recovery Core anzuzeigen, z. B. Systeminformationen, lokale und bereitgestellte Volumes sowie Replay Engine-Verbindungen. Weitere Informationen über die angezeigten Informationen auf der Seite mit den Systeminformationen finden Sie unter Grundlegende Informationen über Systeminformationen für den Core. Weitere Informationen zum Anzeigen von Systeminformationen finden Sie unter Anzeigen von Systeminformationen für den Core.
Herunterladen von Core-Protokolldateien	Informationen über verschiedene Aktivitäten für den Rapid Recovery Core sind in der Core-Protokolldatei gespeichert. Zur Diagnose möglicher Probleme können Sie Protokolle für Ihren Rapid Recovery Core herunterladen und anzeigen. Weitere Informationen zum Öffnen der Core-Protokolle finden Sie unter Zugriff auf Core-Protokolle. Jede geschützte Maschine speichert auch ein Protokoll der Aktivität. Dieses Protokoll kann auf den Core hochgeladen werden, wenn Sie den nächtlichen Job mit der Bezeichnung „Herunterladen der Protokolle von den geschützten Maschinen“ wählen. Weitere Informationen zu nächtlichen Jobs finden Sie unter Grundlegende Informationen zu nächtlichen Jobs. Weitere Informationen zum Konfigurieren dieser nächtlichen Job-Einstellungen für den Core finden Sie unter Konfigurieren nächtlicher Jobs für den Core. Weitere Informationen zum Konfigurieren nächtlicher Jobs für bestimmte geschützte Maschinen finden Sie unter Anpassen der nächtlichen Jobs für eine geschützte Maschine.

Grundlegende Informationen über Systeminformationen für den Core

In Rapid Recovery können Sie Informationen über den Rapid Recovery Core anzeigen. Sie können allgemeine Informationen, Informationen über lokale Volumes sowie Informationen zu bereitgestellten Volumes anzeigen.

Im Fensterbereich **Allgemein** können Sie die in der folgenden Tabelle beschriebenen Informationen anzeigen.

Tabelle 26. Systeminformationen

UI-Element	Description
Hostname	Den Maschinennamen des Rapid Recovery Core.
Betriebssystem-Version	Die Version des Betriebssystems, das auf dem Rapid Recovery Core installiert ist.
Betriebssystemarchitektur	Listet die zugrunde liegende Struktur und Bauart der Hostmachine für den Rapid Recovery Core auf. Dazu gehören ggf. Chipsatz und die Angabe, ob es sich um ein 64-Bit-System handelt. Rapid Recovery Core unterstützt nur 64-Bit-Systeme.
Speicher (Physisch)	Zeigt die Größe des in der Core-Maschine installierten Arbeitsspeichers (Random Access Memory, RAM) an.

UI-Element	Description
Anzeigename	Zeigt den konfigurierbaren Anzeigenamen des Core an (siehe Konfigurieren von allgemeinen Core-Einstellungen).
Vollqualifizierter Domänenname	Zeigt den vollständig qualifizierten Domänennamen für die Core-Maschine an.
Speicherort Metadaten-Cache	Zeigt den Pfad zum Speicherort des Metadaten-Cache an. Weitere Informationen hierzu finden Sie unter Grundlegende Informationen zu Deduplizierungscache und Speicherorten.
Speicherort primärer Cache	Zeigt den Pfad zum Speicherort des primären Deduplizierungscache an. Weitere Informationen hierzu finden Sie unter Grundlegende Informationen zu Deduplizierungscache und Speicherorten.
Speicherort sekundärer Cache	Zeigt den Pfad zum Speicherort des sekundären Deduplizierungscache an. Weitere Informationen hierzu finden Sie unter Grundlegende Informationen zu Deduplizierungscache und Speicherorten.

Der Fensterbereich **Volumes** enthält die folgenden Informationen über Speicher-Volumes für die Core-Maschine: Name, Geräte-ID, Dateisystem, RAW-Kapazität, formatierte Kapazität, genutzte Kapazität und Bereitstellungspunkte.

Im Fensterbereich **Replay Engine-Verbindungen** werden ausführliche Informationen zu den momentan bereitgestellten Wiederherstellungspunkten angezeigt. Angezeigt werden lokaler Endpunkt, Remote-Endpunkt, Agent-ID für bereitgestelltes Image, ID des bereitgestellten Image und Anzeigename des bereitgestellten Image. Sie können feststellen, ob die Bereitstellung Schreibzugriff erlaubt, sowie die authentifizierten Benutzer, die Anzahl der gelesenen Bytes und die Anzahl der geschriebenen Bytes anzeigen.

Sie können die Bereitstellung der Wiederherstellungspunkte, die lokal auf einem Core bereitgestellt wurden, über die Seite "Bereitstellung" aufheben. Weitere Informationen über das Aufheben der Bereitstellung von Wiederherstellungspunkten finden Sie unter Aufheben der Bereitstellung von Wiederherstellungspunkten.

Weitere Informationen hierzu finden Sie unter Anzeigen von Systeminformationen für den Core.

Anzeigen von Systeminformationen für den Core

Systeminformationen für den Core enthalten allgemeine Informationen, Informationen über lokale Volumes sowie Informationen zu bereitgestellten Volumes für den Core. Eine ausführliche Beschreibung der auf dieser Seite verfügbaren Informationen finden Sie unter Grundlegende Informationen über Systeminformationen für den Core.

Führen Sie die folgenden Schritte aus, um detaillierte Systeminformationen für den Core anzuzeigen.

NOTE: Sie können auch Systeminformationen für eine spezielle geschützte Maschine anzeigen. Weitere Informationen hierzu finden Sie unter Anzeigen von Systeminformationen für eine geschützte Maschine.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und dann auf **Systeminformationen**.

   Die Seite mit **Systeminformationen** wird angezeigt.

Zugriff auf Core-Protokolle

Informationen über verschiedene Aktivitäten für den Rapid Recovery Core sind in der Core-Protokolldatei gespeichert. Diese Datei, **AppRecovery.log**, ist standardmäßig unter dem Pfad `C: \ProgramData \AppRecovery\Logs` gespeichert.

NOTE: Abhängig von den jeweiligen Einstellungen ist das Verzeichnis "AppRecovery" auf dem Rapid Recovery Core möglicherweise nicht sichtbar. Damit das Verzeichnis sichtbar ist, müssen Sie u. U. die Ordneroptionen so ändern, dass versteckte Dateien, Ordner und Laufwerke angezeigt werden. Wenn diese Einstellungen die Option zum Ausblenden von Erweiterungen bei bekannten Dateitypen umfassen, kann die Core-Protokolldatei als AppRecovery ohne die Erweiterung `.log` angezeigt werden.

Das Core-Protokoll enthält Informationen über abgeschlossene Core-Jobs, Verbindungsfehler, Ergebnisse der Versuche das Core, sich mit dem Lizenzportal zu verbinden, und andere Informationen. Jeder in der Core-Protokolldatei gespeicherten Information geht eine von vier Kennzeichnungen voraus: INFO, DEBUG, ERROR und WARN. Diese Kennzeichnungen kategorisieren die Art der im Protokoll gespeicherten Informationen bei der Diagnose eines Problems.

NOTE: Gleichermaßen wird auch eine Protokolldatei auf jeder geschützten Maschine mit Angaben über Kommunikationsversuche mit dem Core gespeichert. Weitere Informationen zu Maschinenprotokollen finden Sie unter Herunterladen und Anzeigen der Protokolldatei für eine geschützte Maschine.

Die Zugriffsmöglichkeit auf Protokolle kann bei der Fehlerbehebung oder bei der Arbeit mit dem Quest Rapid Recovery-Support von Nutzen sein. Beachten Sie für den Zugriff auf Protokolle die nachfolgenden Verfahren:

See also: Herunterladen und Anzeigen der Core-Protokolldatei
See also: Herunterladen und Anzeigen der Protokolldatei für eine geschützte Maschine

Herunterladen und Anzeigen der Core-Protokolldatei

Falls bei einem Core Fehler oder Probleme auftreten, können Sie die Core-Protokolle herunterladen, um sie anzuzeigen oder an den Vertreter des Quest Support zu senden.

1. Klicken Sie von der Rapid Recovery Core Console auf der Symbolleiste auf (Mehr) und anschließend auf **Core-Protokol**.
2. Klicken Sie auf der Seite **Core-Protokoll herunterladen** auf **Klicken Sie hier, um den Download zu starten**.
3. Wenn Sie dazu aufgefordert werden, die Datei `Core AppRecovery.log` zu öffnen oder zu speichern, klicken Sie auf **Speichern**.
4. Wenn das Dialogfeld **Core AppRecovery.log öffnen** angezeigt wird, führen Sie eine der folgenden Möglichkeiten aus:
   - Um die Protokolldatei zu öffnen, wählen Sie die Option **Öffnen mit** und dann eine Anwendung (wie Notepad) für die Anzeige der textbasierten Protokolldatei und klicken dann auf **OK**.

     Die Datei **Core AppRecovery.log** wird in der ausgewählten Anwendung geöffnet.
   - Zum Speichern der Datei lokal wählen Sie **Datei speichern** und klicken auf **OK**.

     Die Datei **Core AppRecovery.log** wird im Ordner **Downloads** gespeichert. Sie kann über einen beliebigen Texteditor geöffnet werden.

See also: Herunterladen und Anzeigen der Core-Protokolldatei
See also: Herunterladen und Anzeigen der Protokolldatei für eine geschützte Maschine

Repositorys

In diesem Abschnitt wird die Arbeit mit von Rapid Recovery unterstützten Repositorys beschrieben. Er beschreibt die Funktionen und Attribute des primären Repositorytyps (Deduplication Volume Manager oder DVM) und des sekundären Typs (Tiering-Repository). Es werden die verschiedenen Deduplizierungsarten beschrieben, die in Rapid Recovery verwendet werden, und wie Deduplizierung in der gesamten Anwendung verwendet wird. Der Abschnitt beschreibt zudem das Verwalten von DVM und Tiering-Repositorys, einschließlich der Erstellung eines Repositorys, Anzeigen und Bearbeiten der Details und Löschen eines Repositorys. Sie erfahren zudem, wie Sie ein Repository von einem Core auf einem anderen Core öffnen.

Folgende Themen werden behandelt:

- Grundlegende Informationen zu Repositorys
- Deduplizierung in Rapid Recovery
- Verwalten eines DVM-Repositorys
- Verwalten eines Tiering-Repository
- Überprüfen eines Repositorys
- Ändern der Repository-Einstellungen
- Verbinden mit einem vorhandenen Repository
- Anzeigen oder Ändern von Details zu einem Repository
- Löschen eines Repositorys

Grundlegende Informationen zu Repositorys

Eine Repository ist eine Datenstruktur, die verwendet wird, um Rapid Recovery Daten zu speichern und zu verwalten. Sicherungsmomentaufnahmen werden in einem Repository in Form von Wiederherstellungspunkten gespeichert. Bevor Sie in Rapid Recovery Maschinen schützen, replizieren oder Daten wiederherstellen können, benötigen Sie mindestens ein Repository.

Ein Rapid Recovery Administrator erstellt explizit ein Repository an einem Speicherort (einem Datenträger-Volume), das einem bestimmten Core zugeordnet ist. Sie können ein Repository aus der Benutzeroberfläche oder über die Befehlszeile erstellen. Über Rapid Recovery Core Console können Sie eine neue primäre DVM-Repository oder ein sekundäres Tiering-Repository erstellen. Beim Schutz einer Maschine können Sie außerdem ein DVM-Repository als erweiterten Schritt im Assistenten-Workflow definieren.

Sie können auf der Seite **Repositorys** von Rapid Recovery Core Console ein neues Repository erstellen oder Ihren Core mit einem vorhandenen Repository verbinden, das derzeit von einem anderen Core verwendet wird. Generell können Sie Details für ein Repository und die Repository-Einstellungen anzeigen, ein Repository überprüfen oder ein Repository löschen. Bei DVM-Repositorys können Sie einen Speicherort hinzufügen oder ein Repository optimieren. Bei Tiering-Repositorys haben Sie die Möglichkeit, die Maschine mit den Repository-Dateien zu trennen. Weitere Informationen zum Verwalten eines bestimmten Repository-Typs finden Sie unter Verwalten eines DVM-Repositorys bzw. Verwalten eines Tiering-Repository.

Ein Repository kann sich auf verschiedenen Speichertechnologien befinden, wie beispielsweise Storage Area Network (SAN), direkt angeschlossener Speicher oder Network Attached Storage (NAS).

NOTE: Speichern Sie Rapid Recovery Repositorys auf primären Speichergeräten. Geschwindigkeit ist der wichtigste Faktor für das Speichervolume. Archivspeichergeräte, z. B. Data Domain-Geräte, werden aufgrund der beschränkten Leistung nicht unterstützt. Ebenso sollten 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.

DAS bietet die höchste Datenbandbreite und schnellste Zugriffsrate und ist einfach zu implementieren. Für optimale Ergebnisse verwenden Sie DAS mit RAID (Redundant Array of Independent Disks) 6-Speicher. Weitere Informationen finden Sie im Quest Knowledge Base-Artikel 118153, Repository Options: DAS, SAN oder NAS

Der Speicherort für ein primäres DVM-Repository sollte immer ein Unterverzeichnis sein, das Sie angeben (z. B. `E:\Repository`), nie das Stammverzeichnis eines Volumes (z. B. `E:\`). Beim Erstellen eines Tiering-Repository können Sie kein Verzeichnis angeben, aber Sie können einen Container vorgeben. Sie können den Standard-Container auswählen oder einen neuen erstellen.

DVM -Repositorys werden für primären Speicher verwendet, in dem Wiederherstellungspunkte vom Core direkt an das angegebene Speichersystem gespeichert werden.

Tiering-Repositorys werden für sekundären Speicher verwendet. In diesem Modell werden Wiederherstellungspunkte von einem primären DVM-Repository in ein sekundäres Speicher-Volume verlegt, das Sie angeben. Sobald die Wiederherstellungspunkte kopiert und verifiziert wurden, werden sie aus dem primären Repository entfernt, um Platz für mehr Sicherungsdaten zu schaffen.

NOTE: Für Version 6.2 werden Tiering-Repositorys nur auf Quest Sicherungs- und Deduplizierungs-Appliances der DR-Serie unterstützt.

Sie können eine beliebige Kombination von DVM- und Tiering-Repositorys erstellen, die für einen einzelnen Core definiert sind. Wenn alle Typen von Repositorys zu Ihrem Core hinzugefügt wurden, zeigt die Seite **Repositorys** einen separaten Fensterbereich an, in dem jeder Typ separat aufgelistet ist. Primäre Repositorys werden zuerst aufgelistet, gefolgt von (sekundären) Tiering-Repositorys.

Der folgende Abschnitt beschreibt die Funktionen jedes Repository-Typs, die von Rapid Recovery unterstützt werden.

DVM-Repository. Dieses Repository-Format verwendet Deduplication Volume Manager (DVM).

- DVM ist eine primäre Repository-Technologie zum Speichern von Wiederherstellungspunkten.
- DVM-Repositorys werden über Rapid Recovery Core Console erstellt und verwaltet.
- DVM-Repositorys unterstützen mehrere Volumes, bis zu 255 Repositorys auf einem Core.
- Sie können die Größe eines DVM-Repositorys bei der Erstellung festlegen und später Erweiterungen hinzufügen.
- Sie können DVM-Repositorys jedoch nur auf Maschinen mit nur Windows Betriebssysteme erstellen.
- Das DVM-Repository-Volume kann lokal (auf einem an den Core-Server angeschlossenen Speicher) oder auf einem freigegebenen Speicherort (CIFS, Common Internet File System) vorliegen.
- Sie können diesen Repository-Typ bei der Aktualisierung vorhandener AppAssure Installationen und bei neuen Rapid Recovery Installationen verwenden.
- DVM-Repositorys können die verschiedenen Speichertechnologien vereinigen.
- Unterstützte Speichertypen sind Storage Area Network (SAN), Direct Attached Storage (DAS) oder Network Attached Storage (NAS).
- Erfordert 8 GB RAM und vorzugsweise Error Checking and Correction (ECC).
- Erfordert Quad Core Prozessor auf der Core-Maschine
- Unterstützt mehrere DVM-Repositorys pro Host.
- Keine zusätzlichen Dienste erforderlich; das DVM-Repository verwendet systemeigene Core-Dienste für die Kommunikation mit Core und für die Nachverfolgung von Ereignissen
- Jedes DVM-Repository unterstützt bis zu 4096 Repository-Erweiterungen (als Speicherorte bezeichnet).
- Feste Größe; DVM-Repositorys erfordern die Angabe der Repository-Größe auf einem Volume. Die angegebene Größe darf die Größe des Volumes nicht überschreiten. Jedes Volume, das Sie als Speicherort definieren, muss über mindestens 1 GB freien Speicherplatz verfügen.
- Beim Repository-Speicherort kann es sich um einen einfachen oder dynamischen Datenträger handeln, wobei Geschwindigkeit der wichtigste Faktor ist.
- Kann standardmäßige Verschlüsselungsschlüssel verwenden, die in der Core Console (Core-basierte Verschlüsselung) erstellt und verwaltet werden.
- Dedupliziert Daten im gesamten Repository (oder über Verschlüsselungsdomains innerhalb jedes Repository, wenn Verschlüsselungsschlüssel verwendet werden).
- Verwendet einen dedizierten, voll veränderbaren DVM-Deduplizierungs-Cache mit einem in den Core-Einstellungen konfigurierbaren Speicherort.
- Ist optimiert für das Schreiben von Daten und Speichern von Snapshot-Daten in einem lokalen Repository auf dem Core, wobei alle Daten durch den Core verarbeitet werden.
- Kann nach der Erstellung nicht umbenannt werden.
- Neue Repositorys dieses Typs können über REST-APIs, das Rapid Recovery Command Line Management Utility (cmdutil.exe) oder das Windows PowerShell-Cmdlet erstellt werden.

Wenn Sie ein DVM-Repository erstellen, weist der Rapid Recovery Core vorab den Speicherplatz zu, der für die Daten und Metadaten am angegebenen Speicherort erforderlich ist. Die minimale DVM-Repository-Größe liegt bei 1 GB, was aus praktischen Gründen zu klein ist, außer für Testzwecke.

Da DVM-Deduplizierung einen primären und sekundären Cache erfordert, stellen Sie sicher, dass der reservierte Speicherplatz doppelt so groß wie die Größe Ihres Deduplizierungs-Cache ist. Beispiel: Wenn Sie in den DVM-Deduplizierungs-Cache-Einstellungen auf dem Core 1,5 GB reserviert haben, sollten sie 3 GB auf dem Cache-Volume reservieren. Der Standardinstallationspfad für den Cache ist auf Laufwerk C. Weitere Informationen hierzu finden Sie unter Grundlegende Informationen zu Deduplizierungscache und Speicherorten.

Tiering-Repository. Das Tiering-Repository wurde in Rapid Recovery Version 6.1 eingeführt.

- Tiering-Repository-Technologie wird nur für sekundären Speicher verwendet.
- Vorhandene Wiederherstellungspunkte (1 Woche alt oder älter), die noch nicht für die Archivierung geplant wurden, können so von Ihrem primären Rapid Recovery DVM-Repository verlegt werden. Diese Funktion wird durch die Aufbewahrungsfrist aktiviert.
- Tiering-Repositorys werden über Rapid Recovery Core Console erstellt und verwaltet.
- Derzeit werden Tiering-Repositorys nur auf Quest Sicherungs- und Deduplizierungs-Appliances der DR-Serie Version 4.0 unterstützt.
- Wiederherstellungspunkte in einem sekundären Speicher werden weiterhin mit Verschlüsselung gesichert und unterliegen Rollup. Die Aufbewahrungsrichtlinie und Rollup werden weiterhin vom Core an der neuen Speicherposition verwaltet.
- Während das Rollup weiterhin jede Nacht stattfindet, werden fortlaufend neue Wiederherstellungspunkte verlagert. Beim Anzeigen von Wiederherstellungspunkten nach geschützter Maschine sind die verlagerten Wiederherstellungspunkte durch das Symbol einer goldenen Datenbank gekennzeichnet.

Hinsichtlich Interoperabilität können Wiederherstellungspunkte, die in primären DVM-Repositorys gespeichert sind, auf ein sekundäres Repository verlagert werden. Da die DR-Appliances, die Tiering unterstützen, ein CentOS-Betriebssystem verwenden, werden DVM-Repositorys auf diesen Appliances nicht unterstützt.

Verwendung physischer oder virtueller Appliances für Repository-Speicher

Wenn Sie die Rapid Recovery auf einer Quest Sicherungs- und Wiederherstellungs-Appliance der Serie DL4300 verwenden, können Sie DVM- und Tiering-Repositorys erstellen. Bei Version 6.2 muss das Tiering-Repository auf einer Sicherungs- und Deduplizierungs-Appliance der DR-Serie mit Betriebssystem 4.0 gespeichert werden.

Tiering-Repositorys, die auf dem DL verwaltet werden, verwenden Kapazitäts-Lizenzen. Daher ist es zwar möglich, Wiederherstellungspunkte von Ihrem DVM-Repository, die mit einer DL-Appliance verknüpft sind, auf sekundären Speicher auf einer DR-Appliance zu verlagern doch der für die Wiederherstellungspunkte verbrauchte Speicherplatz wird Ihrer DL-Kapazität zugerechnet. Daher ist es kostengünstiger, Wiederherstellungspunkte von einer DL-Appliance zu archivieren und die Archive auf dem DR zu speichern.

Keine anderen Speicher-, Sicherungs-, Wiederherstellungs- oder Deduplizierungs-Appliances werden explizit für den Einsatz mit Rapid Recovery geprüft. Ihre Nutzung erfolgt auf eigene Gefahr.

Die virtuelle Appliance DR2000v kann für ein Tiering-Repository verwendet werden, vorausgesetzt, es sind darauf die richtigen RDS-Dienste installiert und das Betriebssystem 4.0 wird ausgeführt. Andere virtuelle Appliances werden noch nicht im Rapid Recovery Core Version 6.2 unterstützt.

See also: Verwalten eines DVM-Repositorys
See also: Verwalten eines Tiering-Repository

Deduplizierung in Rapid Recovery

Datendeduplizierung ist eine Datenkomprimierungstechnik, die sowohl Speicheranforderungen als auch Netzwerklast reduziert. Der Vorgang umfasst die physische Speicherung von eindeutigen Datenblöcken, und zwar nur einmal auf dem Laufwerk. Wenn in Rapid Recovery ein beliebiger eindeutiger Datenblock ein zweites Mal in einem Repository auftritt, wird anstatt einem erneuten Speichern der Daten ein virtueller Verweis auf die Daten gespeichert.

Deduplizierung findet in Sicherungs-Snapshots statt, die vom Rapid Recovery Core erfasst wurden..

- Sicherungsinformationen werden innerhalb eines einzelnen Repository dedupliziert. Sie können nicht über mehrere Repositorys dedupliziert werden .
- DVM-Repositorys verwenden eine zielbasierte Verschlüsselung. Zur Sicherheit wird die Verschlüsselung vor der Deduplizierung durchgeführt. Die Deduplizierung ist weiter auf die Daten beschränkt, die mit einem einzigen Verschlüsselungsschlüssel geschützt werden.

Wenn der Deduplizierungs-Cache voll ist, verschlechtert sich die Deduplizierung. In diesem Fall kann die Deduplizierung als Nachbearbeitungs-Prozess (auch als Blockrückforderung bekannt) ausgeführt werden. Führen Sie nach dem Erhöhen der Größe des Deduplizierungs-Cache den Repositoryoptimierungsjob aus. Anschließend wird der Core Blöcke rückfordern, wodurch mehr Platz in Ihrem Repository zur Verfügung steht.

Weitere Informationen zum Repository-Optimierungs-Job finden Sie unter Informationen über DVM Repository-Optimierung. Informationen zur Durchführung dieser Aufgabe finden Sie unter Optimierung eines DVM-Repositorys.

Somit nutzt Rapid Recovery alle Arten der Deduplizierung, die hier beschrieben sind: zielbasierte Deduplizierung, Inline-Deduplizierung und Nachbearbeitungs-Deduplizierung.

Weitere Informationen darüber, wo die Verweise auf einzigartige Blöcke für DVM-Repositorys gespeichert sind, finden Sie unter Grundlegende Informationen zu Deduplizierungscache und Speicherorten. Informationen zum Anpassen der DVM Deduplizierungs-Cache-Einstellungen finden Sie unter Konfigurieren von DVM-Deduplizierungscache-Einstellungen.

Verwalten eines DVM-Repositorys

Die Verwaltung eines DVM-Repositorys umfasst die folgenden Schritte:

1. **Erstellen eines DVM-Repository**s. Bevor Sie ein Repository erstellen, berücksichtigen Sie die vorgegebene Technologie.

   Informationen zu den verschiedenen Arten von Repositorys finden Sie unter Grundlegende Informationen zu Repositorys.
   Weitere Informationen zum Erstellen eines DVM-Repositorys finden Sie unter Erstellen eines DVM-Repository.
2. **Verbinden mit einem Repository**. Weitere Informationen zum Verbinden mit einem vorhandenen Repository, das derzeit von einem anderen Core verwaltet wird, finden Sie unter Verbinden mit einem vorhandenen Repository.
3. **Hinzufügen eines neuen Speicherorts.** Weitere Informationen zum Hinzufügen eines neuen Speicherorts zu einem DVM-Repository finden Sie unter Hinzufügen eines Speicherorts zu einem vorhandenen DVM-Repository.
4. **Prüfen eines Repositorys.** Weitere Informationen zum Überprüfen eines DVM-Repositorys finden Sie unter Überprüfen eines Repositorys.
5. **Ändern von Repository-Einstellungen**. Weitere Informationen zum Anzeigen der Repository-Details oder Ändern der Repository-Einstellungen finden Sie unter Anzeigen oder Ändern von Details zu einem Repository
6. **Durchführen einer DVM Repository-Optimierung**. Weitere Informationen zum Repository-Optimierungs-Job finden Sie unter Informationen über DVM Repository-Optimierung. Die erforderlichen Schritte für die Optimierung eines vorhandenen DVM-Repositorys finden Sie unter Optimierung eines DVM-Repositorys.
7. **Löschen eines Repository**. Weitere Informationen zum Löschen eines Repository finden Sie unter Löschen eines Repositorys.

Weitere Informationen zum Verwalten eines Tiering-Repository finden Sie unter Verwalten eines Tiering-Repository.

Erstellen eines DVM-Repository

Dieser Prozess beschreibt, wie Sie auf dem Core ein Repository mithilfe der Repository Technologie „Deduplizierungs-Volume-Manager“ (DVM) erstellen.

- Sie müssen Administratorrechte zum Zugriff auf die Maschine haben, auf der Sie ein DVM-Repository erstellen möchten.
- Dieser Repository-Typ erfordert mindestens 1 GB verfügbaren Speicherplatz auf dem Volume, das Sie als Speicherort definieren.
- Der Speicherort für ein DVM-Repository muss sich auf einem lokalen am Core-Server angeschlossenen Laufwerk oder auf einer CIFS-Freigabe befinden.
- Bei dem Core-Server kann es sich um ein beliebiges DL-Series-Gerät handeln (einschließlich des DL1000) oder es kann sich um einen beliebigen softwarebasierten Windows Server handeln, der den Systemanforderungen entspricht.

NOTE: DVM-Repositorys werden nicht auf DR-Serie von Festplattensicherungs- und Deduplizierungs-Appliances unterstützt. DR-Appliances verwenden ihre eigene Deduplizierung. Diese Deduplizierung ist nicht mit der Deduplizierung kompatibel, die der Rapid Recovery Core auf ein DVM-Repository anwendet.

Wenn Sie ein Tiering-Repository für die sekundäre Speicherung von Wiederherstellungspunkten erstellen möchten, die ursprünglich in Ihrem DVM-Repository gespeichert wurden, finden Sie im Thema Erstellen eines Tiering-Repositorys weitere Informationen.

Führen Sie die folgenden Schritte aus, um ein DVM-Repository zu erstellen.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Repositorys**.

   Die Seite **Repositorys** wird angezeigt.
3. Klicken Sie oben auf der Seite unter der Seitenüberschrift „Repositorys“ auf den Drop-Down-Pfeil neben **Erstellen** und wählen Sie dann **DVM-Repository**.

   Das Dialogfeld **Neues Repository hinzufügen** wird angezeigt.
4. Geben Sie die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 27. Einstellungen zum Hinzufügen eines neuen Repositorys

Textfeld	Description
Repositoryname	Geben Sie den Anzeigenamen des Repositorys ein. Dieses Textfeld enthält standardmäßig das Wort „Repository“ sowie eine Nummer, die der Nummer der Repositorys für diesen Core entspricht. Wenn es sich hierbei beispielsweise um das erste Repository handelt, lautet der Standardname „Repository 1“. Ändern Sie den Namen je nach Bedarf. Repository-Namen müssen zwischen 1 und 40 alphanumerischen Zeichen, einschließlich Leerzeichen enthalten. Verwenden Sie weder Unzulässige Zeichen noch Unzulässige Phrasen.
Gleichzeitige Vorgänge	Legen Sie die Anzahl gleichzeitiger Anforderungen fest, die das Repository unterstützen soll. Der Standardwert ist 64.

Textfeld	Description
Kommentare	Geben Sie eine beschreibende Anmerkung zu diesem Repository ein. Sie können bis zu 254 Zeichen eingeben. Geben Sie zum Beispiel **DVM-Repository 2** ein.

5. Klicken Sie auf **Speicherort hinzufügen**, um den spezifischen Speicherort oder das Volume für dieses Repository zu definieren. Verwenden Sie ein schnelles primäres Speicherlaufwerk mit ausreichend Speicherplatz. Der Speicherort für ein DVM-Repository kann entweder lokal (auf mit dem Core-Server verbundenem Speicher) oder auf eine Common Internet File System (CIFS)-Netzwerkfreigabe festgelegt werden. Sie können nicht beides für einen einzelnen Speicherort angeben.

   CAUTION: Definieren Sie einen dedizierten Ordner innerhalb des Stammverzeichnisses für den Speicherort für das Repository. Geben Sie nicht die Stammposition an. Verwenden Sie zum Beispiel `E:\Repository\`, nicht `E:\`. Wenn das -Repository, das Sie in diesem Schritt erstellen, später entfernt wird, werden auch alle Dateien am Speicherort des Repositorys gelöscht. Wenn Sie Ihren Speicherort unter dem Stammverzeichnis definieren, werden alle anderen Dateien im Volume (z. B. `E:\`) gelöscht, was zu verheerendem Datenverlust führen könnte.

   Das Dialogfeld **Speicherort hinzufügen** wird angezeigt.

6. Klicken Sie auf **Speicherort hinzufügen**, um den spezifischen Speicherort oder das Volume für das Repository zu definieren. Dieses Volume sollte ein primärer Speicherort sein.
7. Geben Sie im Bereich **Speicherort** an, wie die Datei für den Speicherort hinzugefügt werden soll. Sie können wählen, ein örtlich angeschlossenes Speicherplatz-Volume einzufügen (wie beispielsweise direkt angeschlossenen Speicherplatz, ein Storage Area Network oder einen Network Attached Storage). Sie sollten außerdem ein Speicher-Volume auf einem freigegebenen CIFS-Speicherort angeben.

   - Wählen Sie **Datei auf lokalem Datenträger hinzufügen** aus, um eine lokale Maschine anzugeben, und geben Sie dann die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 28. Einstellungen für lokale Datenträger

Textfeld	Description
Datenpfad	Geben Sie den Speicherort für die geschützten Daten ein. Geben Sie beispielsweise `X:\Repository\Data` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.
Metadatenpfad	Geben Sie den Speicherort für die geschützten Metadaten ein. Geben Sie beispielsweise `X:\Repository\Metadata` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.

   - Wählen Sie **Datei auf CIFS-Freigabe hinzufügen** aus, um eine Netzwerkfreigabe als Speicherort anzugeben, und geben Sie dann die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 29. Anmeldeinformationen für CIFS-Freigaben

Textfeld	Description
UNC-Pfad	Geben Sie den Pfad für den Speicherort der Netzwerkfreigabe ein. Definieren Sie einen dedizierten Ordnernamen (z. B. `Repository`), wenn sich der Speicherort im Stammverzeichnis befindet.

Textfeld	Description
	Der Pfad muss mit \\ beginnen. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.
Benutzername	Geben Sie einen Benutzernamen für den Zugriff auf den Speicherort der Netzwerkfreigabe an.
Kennwort	Geben Sie ein Kennwort für den Zugriff auf den Speicherort der Netzwerkfreigabe an.

8. Klicken Sie im Bereich **Speicherkonfiguration** auf **Weitere Details** und geben Sie dann die Details für den Speicherort ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 30. Details für Speicherkonfiguration

Textfeld	Description
Größe	Legen Sie die Größe oder Kapazität für den Speicherort fest. Die Mindestgröße beträgt 1 GB. Der Standardwert ist 250 GB. Sie können zwischen folgenden Optionen wählen: • GB • TB **NOTE:** Die angegebene Größe darf die Größe des Volumes nicht überschreiten. Wenn es sich beim Speicherort um ein NTFS-Volume (New Technology File System) unter Windows 8 oder höher oder Windows Server 2012 oder höher handelt, ist die Dateigröße auf 256 TB beschränkt. **NOTE:** Damit Rapid Recovery das Betriebssystem validieren kann, muss Windows Management Instrumentation (WMI) auf dem vorgesehenen Speicherort installiert sein.
Schreib-Caching-Richtlinie	Die Schreib-Caching-Richtlinie steuert, wie der Windows Cache-Manager im Repository verwendet wird. Sie ermöglicht die Optimierung der Repository-Leistung bei unterschiedlichen Konfigurationen. Legen Sie den Wert auf eine der folgenden Optionen fest: • Ein • Aus • Sync Bei Auswahl der Standardeinstellung Ein steuert Windows das Caching. Dies ist geeignet für Windows 10 und für Versionen von Windows Server 2012 und höher. **NOTE:** Wenn die Schreib-Caching-Richtlinie auf Ein festgelegt wird, kann die Leistung gesteigert werden. Wenn Sie Windows Server 2008 SP2 oder Windows Server 2008 R2 SP2 verwenden, ist die empfohlene Einstellung „Aus“. Wenn Sie „Aus“ festlegen, wird das Ablegen im Cache-Speicher von Rapid Recovery gesteuert. Bei Auswahl von Sync steuert Windows das Caching sowie die synchrone Eingabe/Ausgabe.
Bytes pro Sektor	Geben Sie die Anzahl an Bytes an, die jeder Sektor enthalten soll. Der Standardwert ist 512.

Textfeld	Description
Durchschnittliche Bytes pro Datensatz	Geben Sie die durchschnittliche Anzahl an Bytes pro Datensatz an. Der Standardwert ist 8192.

9. Klicken Sie auf **Speichern**.

   Das Dialogfeld **Speicherort hinzufügen** wird geschlossen und Ihre Einstellungen werden gespeichert. Das Dialogfeld **Neues Repository hinzufügen** zeigt Ihren neuen Speicherort an.
10. Wiederholen Sie ggf. Schritt 6 bis Schritt 9, um weitere Speicherorte für das Repository hinzuzufügen.
11. Wenn alle Speicherorte, die für das Repository erstellt werden sollen, zu diesem Zeitpunkt definiert wurden, klicken Sie im Dialogfeld **Neues Repository hinzufügen**, auf **Erstellen**.

    Das Dialogfeld **Neues Repository hinzufügen** wird geschlossen, und Ihre Änderungen werden angewendet. Die Seite **Repositorys** wird aufgerufen und das neu in der DVM-Repository-Zusammenfassungstabelle hinzugefügte Repository angezeigt.

Hinzufügen eines Speicherorts zu einem vorhandenen DVM-Repository

Um dieses Verfahren durchführen, muss ein DVM-Repository in Ihrem Repository vorhanden sein.

Durch das Hinzufügen eines Speicherorts zu einem DVM-Repository können Sie definieren, wo das Repository oder das Volume gespeichert werden soll.

Führen Sie die folgenden Schritte aus, um den Speicherort für das Repository oder Volume anzugeben.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Repositorys**.

   Die Seite **Repositorys** wird angezeigt.

   Der Bereich „DVM-Repositorys“ wird angezeigt.
3. Klicken Sie in der Repository-Übersichtstabelle in der Zeile für das DVM-Repository, für das Sie einen Speicherort hinzufügen möchten, auf das Drop-Down-Menü (Weitere Optionen) und wählen Sie **Speicherort hinzufügen**.

   Das Dialogfeld **Speicherort hinzufügen** wird angezeigt.
4. Geben Sie an, wie die Datei für den Speicherort hinzugefügt werden soll. Sie können die Datei auf einem lokalen Datenträger oder auf einer CIFS-Freigabe hinzufügen.
   - Wählen Sie **Datei auf lokalem Datenträger hinzufügen** aus, um eine lokale Maschine anzugeben, und geben Sie dann die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 31. Einstellungen für lokale Datenträger

Textfeld	Description
Datenpfad	Geben Sie den Speicherort für die geschützten Daten ein. Geben Sie beispielsweise `X:\Repository\Data` ein. Für den Pfad gelten ebenfalls die oben genannten Einschränkungen: Verwenden Sie nur alphanumerische Zeichen, Bindestrich oder Punkt und keine Leerzeichen oder Sonderzeichen.
Metadatenpfad	Geben Sie den Speicherort für die geschützten Metadaten ein. Geben Sie beispielsweise `X:\Repository\Metadata` ein.

Textfeld	Description
	Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.

- Wählen Sie **Datei auf CIFS-Freigabe hinzufügen** aus, um eine Netzwerkfreigabe als Speicherort anzugeben, und geben Sie dann die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 32. Anmeldeinformationen für CIFS-Freigaben

Textfeld	Description
UNC Path	Geben Sie den Pfad für den Speicherort der Netzwerkfreigabe ein. Definieren Sie einen dedizierten Ordnernamen (z. B. `Repository`), wenn sich der Speicherort im Stammverzeichnis befindet. Der Pfad muss mit \\ beginnen. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.
Benutzername	Geben Sie einen Benutzernamen für den Zugriff auf den Speicherort der Netzwerkfreigabe an.
Kennwort	Geben Sie ein Kennwort für den Zugriff auf den Speicherort der Netzwerkfreigabe an.

5. Klicken Sie im Bereich „Speicherkonfiguration“ auf **Weitere Details**, und geben Sie dann die Details für den Speicherort ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 33. Details für Speicherorte

Textfeld	Description
Größe	Legen Sie die Größe oder Kapazität für den Speicherort fest. Die Standardgröße beträgt 250 GB. Sie können zwischen folgenden Optionen wählen: • GB • TB **NOTE:** Die Mindestgröße beträgt 1 GB. Die angegebene Größe darf die Größe des Volumes nicht überschreiten. Wenn es sich beim Speicherort um ein NTFS-Volume (New Technology File System) unter Windows 8, 8.1 oder Windows Server 2012, 2012 R2 oder 2016 handelt, ist die Dateigröße auf 256 TB beschränkt. **NOTE:** Damit Rapid Recovery das Betriebssystem validieren kann, muss Windows Management Instrumentation (WMI) auf dem vorgesehenen Speicherort installiert sein.
Write Caching Policy	Die Schreib-Caching-Richtlinie steuert, wie der Windows Cache-Manager im Repository verwendet wird. Sie ermöglicht die Optimierung der Repository-Leistung bei unterschiedlichen Konfigurationen.

Textfeld	Description
	Legen Sie den Wert auf eine der folgenden Optionen fest: • Ein • Aus • Sync Bei Auswahl der Standardeinstellung Ein steuert Windows das Caching. Dies ist geeignet für Windows 10 und für Versionen von Windows Server 2012 und höher. **NOTE:** Wenn die Schreib-Caching-Richtlinie auf Ein festgelegt wird, kann die Leistung gesteigert werden. Wenn Sie Windows Server 2008 SP2 oder Windows Server 2008 R2 SP2 verwenden, ist die empfohlene Einstellung „Aus“. Wenn Sie „Aus“ festlegen, wird das Ablegen im Cache-Speicher von Rapid Recovery gesteuert. Bei Auswahl von Sync steuert Windows das Caching sowie die synchrone Eingabe/Ausgabe.
Bytes per Sector	Geben Sie die Anzahl an Bytes an, die jeder Sektor enthalten soll. Der Standardwert ist 512.
Average Bytes per Record	Geben Sie die durchschnittliche Anzahl an Bytes pro Datensatz an. Der Standardwert ist 8192.

6. Wenn Sie optional die Repository-Optimierungsaufgabe für das ausgewählte Repository durchführen möchten, wählen Sie **Run Repository Optimization Job for Repository [Repository name]** (Optimierungsaufgabe für Repository [Repository-Name] durchführen).

   Quest empfiehlt das Durchführen der Repository-Optimierungsaufgabe beim Hinzufügen von Speicherorten zu einem vorhandenen Repository. Diese Aufgabe optimiert den freien Speicherplatz durch Anwendung von Deduplizierung auf die im Repository gespeicherten Daten.

   Basierend auf Faktoren wie Größe Ihres Repositorys, Menge der Daten im Repository, verfügbare Netzwerkbandbreite und bestehende Belastung am Eingang und Ausgang Ihres Systems kann die Durchführung der Repository-Optimierungsaufgabe beträchtliche Zeit und Bandbreite in Ihrer Umgebung in Anspruch nehmen.

   Weitere Informationen zum Repository-Optimierungs-Job finden Sie unter Informationen über DVM Repository-Optimierung.

7. Klicken Sie auf **Speichern**.

   Das Dialogfeld wird geschlossen und der Speicherort wird aktualisiert. In der Repository-Übersichtstabelle wird der erstellte Speicherort angezeigt, wenn Sie die Details des Repositorys erweitern.

Informationen über das Überprüfen der Integrität der DVM Repositorys

In AppAssure Version 5.3.6 und früheren Versionen schloss die Replikation regelmäßig den Prozess des Kopierens von Wiederherstellungspunkten aus dem Quell- zum Ziel-Core ein. Ein Roll-up veralteter Wiederherstellungspunkte wurde aber nur auf dem Quell-Core durchgeführt. Zusammengehörige ältere Wiederherstellungspunkte wurden bei der Ausführung des nächtlichen Jobs synchronisiert.

Seit AppAssure Version 5.4.1 und in aktuellen Versionen von Rapid Recovery Core können Benutzer verschiedene Aufbewahrungsrichtlinien für Quell- und Ziel-Cores festlegen. Damit die Replikation mit unterschiedlichen Aufbewahrungsrichtlinien korrekt funktioniert, muss der Ziel-Core über die gleiche Softwareversion (oder höher) verfügen wie der Quell-Core.

Administratoren können jetzt das Roll-up auf den Ziel-Core in einer anderen Geschwindigkeit als auf dem Quell-Core konfigurieren. Ebenso können Sie jetzt eine benutzerdefinierte Aufbewahrungsrichtlinie für alle replizierten Maschinen definieren. Sie können beispielsweise das Roll-up der Wiederherstellungspunkte im Ziel-Core mit schnellerer Geschwindigkeit und weniger Granularität als auf dem Quell-Core durchführen, was Platz spart. Oder Sie können Wiederherstellungspunkte für eine bestimmte replizierte Maschine bei einer niedrigeren Geschwindigkeit im Ziel-Core aufrollen, wodurch mehr Granularität aufrechterhalten wird, was für Kompatibilitätszwecke nützlich sein kann. Weitere Informationen zur Verwendung einer Aufbewahrungsrichtlinie, die sich von der Standardeinstellung im Core unterscheidet, finden Sie unter Anpassen der Aufbewahrungsrichtlinieneinstellungen für eine geschützte Maschine.

Einige Kunden haben vor AppAssure Version 5.3.6 Inkonsistenzen in Wiederherstellungspunkten festgestellt, die auf einen Ziel-Core repliziert wurden. Um dieses Problem zu beheben, enthalten AppAssure Version 5.4.1 und höher einen Core-Job, der auf jedem DVM Repository läuft. Quest empfiehlt die einmalige Durchführung dieser Integritätsprüfung auf jedem DVM Repository auf einem replizierten Ziel-Core, falls das Repository vor Version 5.4.x erstellt wurde (wenn es in Version 5.3.x oder früher erstellt wurde).

Anweisungen zum Durchführen dieser Prüfung finden Sie unter Ausführen einer Integritätsprüfung auf einem DVM-Repository.

Die Integritätsprüfung ist **nicht** verfügbar:

- Auf einem neuen DVM Repository auf einem Ziel-Core, der in AppAssure Version 5.4.1 oder höher oder in Rapid Recovery erstellt wurde.
- Auf einem Quell-Core.
- Wenn Sie den Integritätsprüfjob (Repository-Prüfjob) für das betreffende Repository bereits durchgeführt haben.
- Die Replikationsfunktion wurde nicht verwendet.

Wenn Ihr Core irgendwann von AppAssure 5.3.x aktualisiert wurde und Sie Replikation verwendet haben, müssen Sie diesen Job ausführen, bevor Sie unterschiedliche Aufbewahrungsrichtlinien für Quell- und Ziel-Core oder eine benutzerdefinierte Aufbewahrungsrichtlinie auf einer replizierten Maschine konfigurieren können.

Sie sehen den Job nicht oder können ihn nicht ausführen, es sei denn, Sie haben eines oder mehrere Repositorys zur Wahl (erstellt vor 5.4.x und noch nicht ausgeführt).

Bei der Ausführung des Jobs überprüft das System die Integrität aller Daten, die im angegebenen Repository gespeichert sind, damit Daten aus allen Snapshot- oder Basisimages wiederhergestellt werden können. Falls bei der Integritätsprüfung ein Problem mit den Daten im Repository festgestellt wird, wird der Job sofort beendet. In den Ereignisdetails für den betreffenden Job auf dem Core werden Sie aufgefordert, Kontakt zum Quest Datenschutz-Support aufzunehmen, damit Sie zusammen mit einem Support-Mitarbeiter zu einem vereinbarten Zeitpunkt weitere Schritte durchführen können, um Dateninkonsistenzen zu ermitteln und zu beheben.

CAUTION: Die Ausführung des Jobs kann längere Zeit in Anspruch nehmen. Die Dauer unterscheidet sich je nach Menge und Art der Daten in Ihrem Repository und auf dem zugrundeliegenden Speichersystem. Während der Jobausführung können keine anderen Transaktionen im jeweiligen Repository durchgeführt werden, z. B. Übertragungen (Snapshot- und Basisimage-Sicherungen sowie Replikationen), nächtliche Jobs usw.

Sie können andere Vorgänge in anderen Repositorys durchführen, während der Job ausgeführt wird.

NOTE: Im Rahmen dieses Jobs wird die Integrität aller Inhalte in einem Repository überprüft. Mehr Information über den Job `Checking repository`, den Sie ausführen können, um sicherzustellen, dass ein Repository bereitgestellt werden kann und nutzbar ist, finden Sie unter Überprüfen eines Repositorys.

Ausführen einer Integritätsprüfung auf einem DVM-Repository

Eine Integritätsprüfung ist für DVM-Repositorys verfügbar. Mit diesem Verfahren wird die Integrität eines ganzen DVM-Repositorys überprüft. Sie sollten diese Schritte für replizierte Ziel-Cores ausführen, wenn Sie ein Upgrade

von AppAssure 5.3.x auf Version 5.4 durchführen. Während der Ausführung der Integritätsprüfung, die recht zeitaufwändig sein kann, können keinen anderen Aktionen im Repository durchgeführt werden.

Führen Sie diese Schritte einmal für jedes Repository durch, wenn mehrere DVM-Repositorys für einen Ziel-Core vorhanden sind.

NOTE: Wenn ein anderes DVM-Repository im Ziel-Core vorhanden ist, für das der Repository-Prüfjob bereits durchgeführt wurde, oder wenn Sie ein neues zusätzliches Repository für diesen Ziel-Core erstellen, können Sie im jeweiligen zweiten Repository Vorgänge durchführen, während der Repository-Prüfjob für das DVM-Repository ausgeführt wird, das Sie festgelegt haben.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Repositorys**.

   Die Seite **Repositorys** wird angezeigt.
3. Klicken Sie in der DVM-Repositorys-Übersichtstabelle in der Zeile für das DVM-Repository, das Sie überprüfen möchten, auf (Weitere Optionen) und wählen Sie aus dem Drop-Down-Menü **Integritätsprüfung**.

   Daraufhin wird eine Bestätigungsmeldung angezeigt.

   CAUTION: Bevor Sie bestätigen, dass der Job durchgeführt werden soll, sollten Sie unbedingt die dafür erforderliche Zeit beachten. Während der Jobausführung können keine anderen Transaktionen im jeweiligen Repository durchgeführt werden, z. B. Übertragungen (Snapshot- und Basisimage-Sicherungen sowie Replikationen), nächtliche Jobs usw.
4. Klicken Sie im Dialogfeld **Repositorys überprüfen** auf **Ja**, um die Integritätsprüfung durchzuführen.

   Das Dialogfeld wird geschlossen. Alle Jobs in der Warteschlange und alle laufenden Jobs werden abgebrochen, und der Integritätsprüfjob beginnt.
5. Um den Fortschritt des Jobs „Integritätsprüfung“ für ein Repository zu überwachen und festzustellen, ob ggf. weitere Schritte erforderlich sind, klicken Sie in der Symbolleiste auf (Ereignisse).
6. Klicken Sie auf der Seite **Aufgaben** auf **Job-Details** für den Job, um weitere Informationen zum Jobstatus anzuzeigen.
   - Falls in einer untergeordneten Aufgabe dieses Jobs ein Fehler angezeigt wird, notieren Sie sich den Fehler und übergeben Sie die Informationen an einen Mitarbeiter des technischen Supports von Quest.
   - Wenn alle untergeordneten Aufgaben des Jobs „Integritätsprüfung“ erfolgreich abgeschlossen wurden, können Sie eine benutzerdefinierte Aufbewahrungsrichtlinie für dieses Repository einrichten.

Informationen über DVM Repository-Optimierung

Bei Verwendung eines DVM-Repository werden die Daten, die Sie erfassen, in jedem Snapshot dedupliziert. Diese Deduplizierung findet stufenweise statt, da Snapshots in das Repository gespeichert werden. Ein Auftreten jeder Informationen-Zeichenkette wird in das Repository gespeichert. Wenn eine Informationen-Zeichenkette dupliziert wird, wird eine Referenz zu der ursprünglichen Zeichenkette im Deduplizierungs-Cache verwendet und spart so Speicherplatz im Repository.

Wenn der DVM Deduplizierungs-Cache gefüllt ist, werden nur Snapshot-Daten, die bereits referenziert sind, im Cache dedupliziert. Wenn Deduplizierung auftritt, wird der Cache weiterhin mit neuen eindeutigen Werten aktualisiert und der älteste Wert im Cache wird überschrieben. Dies führt zu einer suboptimalen Deduplizierung.

Weitere Informationen zur Replikation finden Sie unter Grundlegende Informationen zu Deduplizierungscache und Speicherorten.

Sie haben die Wahl, Ihren DVM Duplizierungs-Cache zu erhöhen, bevor er voll ist, was zu kontinuierlich optimaler Deduplizierung Ihrer Daten in diesem Repository führt. Weitere Informationen hierzu finden Sie unter Konfigurieren von DVM-Deduplizierungscache-Einstellungen.

Sie können auch Ihren Deduplizierungs-Cache erhöhen, wenn er voll ist. Wenn Sie Speicherplatz im Repository nach Erhöhung des Cache zurückfordern möchten, können Sie das Repository optimieren. Diese Maßnahme erzwingt ein Vergleich der Daten in Ihrer Snapshots zu den Informationen im Deduplizierungs-Cache. Wenn alle wiederholten Zeichenketten im Repository gefunden werden, werden diese Daten durch Verweise auf die Daten ersetzt und so Speicherplatz im Repository gespart. Dies wird in manchen Fällen auch als Offline-Deduplizierung bezeichnet, da dieser Deduplizierungsprozess auf Wunsch auftritt, anstatt inkrementell da Snapshot Daten übertragen werden.

Die Optimierung ist Prozessor-intensiv. Die erforderliche Zeit für eine Ausführung dieses Jobs ist von verschiedenen Faktoren abhängig. Zu diesen Faktoren gehören die Größe Ihres Repositorys; die Menge an Daten im Repository; verfügbare Netzwerkbandbreite; und die vorhandene Last am Eingang und Ausgang Ihres Systems. Je mehr Daten in Ihrem Repository sind, desto länger dauert die Ausführung dieses Jobs.

Es werden die folgenden Aktionen außer Kraft gesetzt oder abgebrochen, wenn der Repository-Optimierungs-Job gerade läuft.

- Löschen aller Wiederherstellungspunkte-Jobs
- Löschen von Wiederherstellungspunkte-Ketten-Job
- Wartung Repository-Job
- Löschen von Wiederherstellungspunkte-Job-Basis
- Repository-Optimierungs-Job

Informationen zu Schritten zur Optimierung eines vorhandenen DVM-Repository finden Sie unter Optimierung eines DVM-Repositorys.

Sie können den Repository-Optimierungs-Job für eine beschränkte Zeit unterbrechen, falls erforderlich. Weitere Informationen hierzu finden Sie unter Unterbrechen oder Wiederaufnehmen der DVM-Repository-Optimierung.

Optimierung eines DVM-Repositorys

Sie müssen über ein DVM-Repostiory in Ihrem Core verfügen, um dieses Verfahren auszuführen.

Sie können eine Offline-Deduplizierung von auf einem vorhandenen DVM-Repository gespeicherten Daten durchführen. Dies geschieht durch Starten des Repository-Optimierungsjobs.

NOTE: Quest empfiehlt die Durchführung des Jobs „Repository optimieren“ erst, nachdem Sie die Größe des Deduplizierungs-Cache erhöht haben. Über diese Maßnahme können Sie Repository-Speicherplatz zurückfordern und den DVM Deduplizierungs-Cache effektiver nutzen.

Führen Sie die folgenden Schritte aus, um ein DVM-Repository zu optimieren.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Repositorys**.

   Die Seite **Repositorys** wird angezeigt.
3. Klicken Sie im Fensterbereich „DVM-Repositorys“ auf der Zeile, die das Repository darstellt, das Sie optimieren möchten, auf (Weitere Optionen) und wählen Sie dann **Optimieren** aus.

   Es wird eine Warnmeldung angezeigt, sie Sie zur Bestätigung der Optimierung auffordert.
4. Bestätigen Sie die Optimierung durch Klicken.

   Der Optimierungsjob hat Vorrang vor den meisten anderen Jobs. Falls erforderlich, können Sie einen laufenden Optimierungsjob unterbrechen. Weitere Informationen zum Unterbrechen und Wiederaufnehmen dieses Jobs finden Sie unter Unterbrechen oder Wiederaufnehmen der DVM-Repository-Optimierung.

Unterbrechen oder Wiederaufnehmen der DVM-Repository-Optimierung

Diese Aufgabe erfordert, dass ein DVM-Repository in ihrem Core vorliegt, auf dem ein Repository-Optimierungsauftrag ausgeführt wird.

Wenn Sie den Repository-Optimierungsjob initiieren, wird das ausgewählte DVM-Repository dedupliziert. Bei dieser Deduplizierungsoptimierung handelt es sich um einen prozessorintensiven Job zur Einsparung von Speicherplatz im Repository. Weitere Informationen finden Sie unter Informationen über DVM Repository-Optimierung.

Sobald dieser Job initiiert wurde, können Sie den Job mithilfe des folgenden Verfahrens unterbrechen. Dadurch wird die Deduplizierung angehalten. Wenn Sie eine Optimierung bereits unterbrochen haben, können Sie den Vorgang unter Verwendung dieses Verfahrens wieder aufnehmen.

NOTE: Dieses Verfahren gilt nur für DVM-Repositorys und nur, wenn der Repository-Optimierungsjob initiiert wurde.

Führen Sie die hier beschriebenen Schritte aus, um einen Repository-Optimierungsjob zu unterbrechen oder wieder aufzunehmen.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Repositorys**.

   Die Seite **Repositorys** wird angezeigt.

   Der Bereich „DVM-Repositorys“ wird angezeigt.
3. Gehen Sie folgendermaßen vor, wenn Sie einen Optimierungsjob unterbrechen möchten:
   a. Klicken Sie in der Repositorys-Übersichtstabelle auf der Zeile, die das gewünschte Repository darstellt, auf (Weitere Optionen) und wählen Sie dann **Optimierungsjob unterbrechen** aus.

   Es wird eine Warnmeldung angezeigt, sie Sie zur Bestätigung der Unterbrechung auffordert.

   b. Bestätigen Sie die Unterbrechung durch Klicken.
4. Gehen Sie folgendermaßen vor, wenn Sie einen unterbrochenen Optimierungsjob wieder aufnehmen möchten:
   a. Klicken Sie in der Repositorys-Übersichtstabelle auf der Zeile, die das gewünschte Repository darstellt, auf und wählen Sie dann **Optimieren** aus.

   Es wird eine Warnmeldung angezeigt, sie Sie zur Bestätigung der Optimierung auffordert.

   b. Wählen Sie im Dialogfeld die Option **Job ab dem Unterbrechungspunkt fortsetzen** und klicken Sie dann auf **Ja**.

   Das Dialogfeld wird geschlossen und der Repository-Optimierungsjob wird dort wieder aufgenommen, wo er zuletzt unterbrochen wurde.

Verwalten eines Tiering-Repository

Ein Tiering-Repository ist ein sekundäres, auf Ihrem Core definiertes Repository, in das Wiederherstellungspunkte von einem primären DVM-Repository verlegt werden können.

Sobald die Wiederherstellungspunkte verschoben wurden, werden sie aus dem primären DVM-Repository gelöscht. Der Core verwaltet die verlegten Wiederherstellungspunkte weiterhin, bis ein Rollup erfolgt und sie gelöscht werden.

Um Sicherungsdaten den entsprechenden Speicherklassen zuzuordnen, müssen Sie das Alter festlegen, ab dem Sie Wiederherstellungspunkte in Ihrem DVM-Repository in andere Repositorys verlagern wollen. Diese Angabe erfolgt auf der Seite zur Aufbewahrungsfrist.

Bevor Sie Wiederherstellungspunkte in ein Tiering-Repository verlagern können, müssen Sie das sekundäre Repository auf dem Rapid Recovery Core erstellen.

Die Verwaltung eines Tiering-Repository umfasst die folgenden Schritte:

1. **Erstellen eines Tiering-Repository**. Um Ihre veralteten Wiederherstellungspunkte in einen sekundären Speicher zu verlagern, müssen Sie das Tiering-Repository zunächst im Rapid Recovery Core Console definieren. In Version 6.2 wird Tiering nur auf Deduplizierungs-Appliances der DR-Serie mit OS 4.0 unterstützt. Auf diesem Repository müssen RDS-Dienste nativ auf der DR-Appliance installiert sein. Weitere Informationen hierzu finden Sie unter Grundlegende Informationen zu Repositorys. Weitere Informationen zum Erstellen eines Tiering-Repository finden Sie unter Erstellen eines Tiering-Repositorys.
2. **Verbinden mit einem Repository**. Weitere Informationen zum Verbinden mit einem vorhandenen Tiering-Repository finden Sie unter Verbinden mit einem vorhandenen Repository.
3. **Definieren des Aufbewahrungszeitraums.** Nachdem Sie ein Tiering-Repository zu Ihrem Core hinzugefügt haben, definieren Sie im Aufbewahrungszeitraum das Alter der Wiederherstellungspunkte, die Sie von Ihrem DVM-Repository auf das Tiering-Repository verlagern möchten. Sie müssen Tiering mithilfe einer benutzerdefinierten Aufbewahrungsrichtlinie für bestimmte geschützte Maschinen einrichten. Informationen zum Festlegen der Aufbewahrungsrichtlinie zum Verlagern der Wiederherstellungspunktefür bestimmte geschützte Maschinen finden Sie unter Anpassen der Aufbewahrungsrichtlinieneinstellungen für eine geschützte Maschine.
4. **Ändern von Repository-Einstellungen**. Weitere Informationen zum Ändern der Repository-Einstellungen für ein Tiering-Repository finden Sie unter Anzeigen oder Ändern von Details zu einem Repository.
5. **Prüfen eines Repositorys.** Weitere Informationen zum Prüfen eines Repository finden Sie unter Überprüfen eines Repositorys.
6. **Löschen eines Repository**. Weitere Informationen zum Löschen eines Repository finden Sie unter Löschen eines Repositorys.

Weitere Informationen zum Verwalten eines DVM-Repository finden Sie unter Verwalten eines DVM-Repositorys.

Erstellen eines Tiering-Repositorys

Dieser Prozess beschreibt, wie Sie ein Tiering-Repository über die Rapid Recovery Core Console erstellen, der ausschließlich für Sicherungen von geschützten Maschinen in Ihrem Core als sekundärer Speicher verwendet werden kann.

NOTE: In Version 6.2 ist der einzige unterstützte physische Speicherort für Tiering-Repositorys eine DR Deduplizierungs-Appliance mit OS 4.0. Durch Festlegen der Aufbewahrungsrichtlinie auf Tier können Sie den Zeitpunkt festlegen, nach dem Wiederherstellungspunkte von Ihrem DVM-Repository auf das Tiering-Repository auf der DR-Appliance verlagert werden. Die DR-Appliance umfasst Rapid Data Storage (RDS)-Dienste.

Informationen zum Erstellen eines primären DVM-Repository finden Sie unter dem Thema Erstellen eines DVM-Repository.

- Für die Planung sind 128 GB des Speichervolumes standardmäßig reserviert für das Deduplizierungs-Wörterbuch.
- Beim Core-Server kann es sich um einen ordnungsgemäß dimensionierten Software-basierten Windows Server handeln, der die Rapid Recovery-Anforderungen an Betriebssystem und Dateisystem erfüllt. Es kann auch jede DL Sicherungs-Appliance außer die DL1000 oder DL4000 sein. Diese Appliance-Modelle unterstützen derzeit nur DVM-Repositorys.

NOTE: Weitere Informationen zu Systemanforderungen finden Sie unter *Rapid Recovery Systemanforderungen-Handbuch*.

- Sie müssen Administratorrechte zum Zugriff auf das DR-Gerät haben, auf der Sie das Tiering-Repository erstellen möchten.
- Sie müssen den Hostnamen des DR-Geräts angeben.

Auf einem für schlanke Speicherzuweisung geeigneten Volume zeigt das Repository-Volume die Größe des belegten Speicherplatzes aus dem Betriebssystem an. Ein Volume mit herkömmlicher Speicherzuweisung zeigt möglicherweise den gesamten Inhalt des Laufwerks an, der von Daten verbraucht wird. Sie können Ihr Repository regelmäßig mit dem Repository-Bericht überwachen, der Ihnen beim Vermeiden des Füllens eines Repository-Volumes hilft. Informationen zum manuellen Erstellen eines Repository-Berichts finden Sie unter Bedarfsweise Generierung eines Core-Berichts. Informationen zum Automatisieren der laufenden Erstellung von Berichten finden Sie unter Planen eines Berichts.

Führen Sie die folgenden Schritte aus, um ein Tiering-Repository zu erstellen.

1. Navigieren Sie zur Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Repositorys**.

   Die Seite **Repositorys** wird angezeigt.
3. Klicken Sie oben auf der Seite unter der Seitenüberschrift „Repositorys“ auf den Drop-Down-Pfeil neben **Erstellen** und klicken Sie dann auf **Tiering-Repository**.

   Der **Assistent zum Erstellen eines Repository** wird angezeigt.
4. Geben Sie auf der Seite **Verbindung** im Textfeld „Server“ die IP-Adresse oder den Netzwerkserver-Namen für die Maschine ein, die Sie verbinden und auf der Sie das Repository erstellen möchten. Klicken Sie anschließend auf **Weiter**.

   RDS-Dienste sind auf DR-Appliances vorinstalliert. Wenn die Maschine einen RDS-Server enthält und das Betriebssystem 4.0 ausführt, können Sie eine Verbindung damit herstellen. Andernfalls bitten Sie den DR-Appliance-Administrator um Unterstützung bei der Aktualisierung auf die richtige RDS-Server-Version und kehren dann zu diesem Schritt zurück.
5. Geben Sie auf der Seite **Konfiguration** die in der folgenden Tabelle beschriebenen Konfigurations-Informationen ein und klicken Sie dann auf **Weiter**.

Tabelle 34. Einstellungen der Seite „Konfiguration“

Beschreibungen zum Konfigurieren des Repositorys verfügbaren Einstellungen.

Textfeld	Description
Name	Geben Sie einen Anzeigenamen für Ihr Repository ein. Dieses Textfeld enthält standardmäßig das Wort „Repository“ sowie eine Zahl. Der vorgeschlagene Name entspricht der Anzahl der Repositorys, die aktuell für diesen Core bestehen. Für das erste Repository ist beispielsweise der vorgeschlagene Name „Repository 1“ oder für das zweite Repository ist der vorgeschlagene Name „Repository 2“ usw. Wenn Sie Repositorys mit mehreren Technologietypen verwenden, sollten Sie den Typ im Namen angeben, wie z. B. `TieringRepository1`. Repository-Namen müssen zwischen 1 und 40 alphanumerischen Zeichen, einschließlich Leerzeichen enthalten. Verwenden Sie weder Unzulässige Zeichen noch Unzulässige Phrasen.
Kommentare	Diese Information ist optional. Sie können sie zum Beschreiben der Art von Informationen verwenden, die in diesem Repository gespeichert werden. Zum Beispiel: „Dieses Repository hält veraltete

Textfeld	Description
	Wiederherstellungspunkte für alle SQL- und Exchange Server in der Buchhaltungs-Domain“. Diese Informationen können jederzeit geändert werden.
Speichergruppen- und Container-Optionen	Wählen Sie Optionen für Ihr Tiering-Repository wie folgt aus: • Wählen Sie **Standard-Speichergruppe und -Container verwenden**, um die Struktur für Ihr Repository in Standardverzeichnissen zu erstellen. Die meisten Benutzer wählen diese Standardoption. • Wählen Sie **Eine vorhandene Speichergruppe und Container verwenden**, wenn Sie die Struktur für Ihr Tiering-Repository angeben und die entsprechenden Objekte auswählen möchten. Diese Option ist für fortgeschrittene Benutzer, die über Kenntnisse der Speichergruppe und des Containers verfügen.

6. Führen Sie auf der Seite **Sicherheitsoptionen** eine der folgenden Aktionen aus:

   • Um den Zugriff auf den von Ihnen erstellten Core zu beschränken und zu verhindern, dass andere Benutzer auf Ihrem Netzwerk auf Informationen zu diesem Repository zugreifen können, wählen Sie **Dieses Repository mit Ihrer eindeutigen Lizenz sichern**. Klicken Sie anschließend auf **Fertigstellen**.

   Dieser Schritt ist eine optionale Vorsichtsmaßnahme. Das Repository ist bereits geschützt; allerdings ist für den Zugriff auf den Rapid Recovery Core eine Authentifizierung erforderlich. Diese Sicherheitsfunktionen gelten, wenn ein Benutzer versucht, dieses Repository aus einem anderen Rapid Recovery Core zu öffnen. Für zusätzliche Sicherheit können Sie auch Verschlüsselungsschlüssel auf Core-Ebene auf Backups für jede geschützte Maschine anwenden.

   • Um den Prozess für die Erstellung eines Tiering-Repositorys ohne Sicherung des Repositorys mit Ihrer Lizenz fertigzustellen, deaktivieren Sie die Option **Dieses Repository mit Ihrer eindeutigen Lizenz sichern**, klicken Sie auf **Fertig stellen** und klicken Sie im Dialogfeld **Warnung: Unsicheres Repository** auf **Ja**.

   Der **Assistent zum Erstellen des Repository** wird geschlossen. Die Repository-Informationen, die Sie angegeben haben, erzeugen einen Job „Repository erstellen“, der sofort gestartet wird. Dieser Job und die daraus resultierende Repository-Erstellung dauert einige Minuten. Wenn der Auftrag abgeschlossen ist, wird der Bereich **Tiering-Repositorys** am unteren Rand der Seite **Repository** mit dem neuen Tiering-Repository angezeigt, das Sie gerade hinzugefügt haben.
7. Optional können Sie den Fortschritt der Tiering-Repository-Erstellungsaufgabe verfolgen. Weitere Informationen hierzu finden Sie unter Anzeigen von Aufgaben.

Überprüfen eines Repositorys

Rapid Recovery gestattet Ihnen, beim Auftreten von Fehlern auf dem Core eine Diagnoseprüfung eines Repository-Volumes durchzuführen. Fehler können durch fehlerhaftes Herunterfahren des Core, fehlerhafte Bereitstellung bzw. fehlerhaftes Aufheben einer Bereitstellung, Hardwarefehler oder umgebungsbedingte Faktoren auf den unteren Ebenen des IP-Stacks, die in Rapid Recovery auftreten können, verursacht werden.

Für alle Repository-Technologietypen werden durch die Konsistenzprüfung folgende Tasks ausgeführt:

- Repository überprüfen
- Bereitstellen des Repository
- Laden der Wiederherstellungspunkte vom Repository

Nur für DVM-Repositorys wird durch die Konsistenzprüfung auch die Task „Neu berechnen des Deduplizierungs-Cache für Repository“ ausgeführt.

NOTE: Dieser Vorgang sollte nur zu diagnostischen Zwecken durchgeführt werden. Beispiel: Führen diese Überprüfung bei einem Hardwarefehler, bei unsachgemäßem Herunterfahren des Core oder bei einem Fehler beim Import eines Repositorys durch.

1. Navigieren Sie zur Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Repositorys**.

   Die Seite **Repositorys** wird angezeigt.
3. Um ein Repository zu überprüfen, klicken Sie in jeder Zeile der Übersichtstabelle für einen der Repository-Technologietypen auf (Weitere Optionen) und klicken Sie dann auf **Überprüfen**.

   Das Dialogfeld **Repository überprüfen** wird angezeigt.
4. Bestätigen Sie im Dialogfeld **Repository überprüfen**, dass Ihnen bewusst ist, dass alle aktiven Aufgaben im Zusammenhang mit diesem Repository abgebrochen werden und dass Sie fortfahren möchten.

   Aktive Aufträge werden abgebrochen und der Job „Repository überprüfen“ wird gestartet.
5. Optional können Sie den Status des Jobs durch Klicken auf das Drop-Down-Menü **Ausgeführte Aufgaben** in der unteren Schaltflächenleiste und Auswählen des Jobs „Wartung des Repositorys“ verfolgen.

Ändern der Repository-Einstellungen

Dieser Vorgang setzt voraus, dass Ihr Core ein funktionierendesTiering-Repository hat. Informationen zum Anzeigen oder Ändern der Repository-Einstellungen für ein DVM-Repository finden Sie in Anzeigen oder Ändern von Details zu einem Repository.

In den Repository-Einstellungen können Sie den angezeigten Namen, Kommentare und die Sicherheitsoption ändern.

1. Klicken Sie in Rapid Recovery Core Console auf der Symbolleiste auf (Mehr) und wählen Sie dann **Repositorys**.
2. Führen Sie auf der Seite **Repositorys** einen Bildlauf nach unten bis zum Fensterbereich **Tiering-Repositorys** durch.
3. Klicken Sie auf der Zeile, die das Repository darstellt, das Sie aktualisieren möchten, auf das Symbol für (Weitere Optionen) und wählen Sie **Einstellungen** aus.

   Der Assistent **Repository-Einstellungen bearbeiten** wird angezeigt.
4. Auf der Seite **Konfiguration** können Sie die Einstellungen ändern, wie in der folgenden Tabelle beschrieben.

Option	Description
Name	Der Anzeigename des Repositorys. Zum Beispiel Repository 1.
Kommentare	Anmerkungen oder eine Beschreibung, die Sie diesem Repository zuordnen möchten.

5. Klicken Sie auf **Weiter**.
6. Damit Sie auf der Seite **Sicherheitsoptionen** die Sicherheit so festlegen können, dass nur ein Core mit der gleichen Lizenznummer wie dieser Core zur Kommunikation mit dem Repository berechtigt ist, wählen Sie **Sichern dieses Repository mit Ihrer eindeutigen Lizenz**.

NOTE: Dieser Schritt ist eine optionale Vorsichtsmaßnahme. Das Repository ist bereits geschützt; allerdings ist für den Zugriff auf den Rapid Recovery Core eine Authentifizierung erforderlich. Diese Sicherheitsfunktionen gelten, wenn ein Benutzer versucht, dieses Repository aus einem anderen Rapid Recovery Core zu öffnen. Für zusätzliche Sicherheit können Sie auch Verschlüsselungsschlüssel auf Core-Ebene auf Backups für jede geschützte Maschine anwenden.

7. Klicken Sie auf **Fertig stellen**.

   Die Änderungen wurden in das Repository übernommen.

8. Wenn Sie im vorherigen Schritt gewählt haben, dass Sie keine weiteren Sicherheitsfunktionen zu Ihrem Repository hinzufügen möchten, wird das Dialogfeld **Warnung zu nicht sicherem Repository** angezeigt. Klicken Sie auf **Ja**, um zu bestätigen, dass Sie das Repository nicht mit einem Lizenzschlüssel sichern möchten.

   Der Assistent **Repository-Einstellungen bearbeiten** wird geschlossen. Die an den Repository-Einstellungen vorgenommenen Änderungen werden sofort angewendet.

Verbinden mit einem vorhandenen Repository

Zum Durchführen dieses Verfahrens müssen Sie über die entsprechenden Anmeldeinformationen für den ursprünglichen Core verfügen, und Sie müssen den lokalen oder Netzwerkpfad, die IP-Adresse oder den Servernamen haben.

CAUTION: Führen Sie dieses Verfahren nur für Repositorys und Daten aus, für die Sie eine rechtliche Zugriffsberechtigung haben.

Wenn Sie eine Verbindung zu einem Tiering-Repository herstellen, muss das Repository vom Core getrennt werden, der es zuvor verwendete. Weitere Informationen zum Trennen eines Repository finden Sie unter dem Thema Trennen eines Repository.

Wenn Sie eine Verbindung zu einem DVM-Repository herstellen, das derzeit nicht mit einem anderen Core verbunden ist, gelten keine anderen Voraussetzungen.

Wenn Sie eine Verbindung zu einem DVM-Repository herstellen, das derzeit im Besitz eines anderen funktionierenden Core ist, müssen Sie zuerst Vorbereitungen für die bevorstehende Übertragung der Besitzrechte treffen. Es gelten die folgenden Voraussetzungen:

- Wenn der ursprüngliche Core, der das Repository enthält, nicht funktioniert, wird der Schutz der Maschinen auf diesem Core vorübergehend angehalten.
- Stoppen Sie dann den Core-Dienst des ursprünglichen Core, während Sie die Besitzrechte übertragen.
- Nachdem Sie das Repository mit dem neuen Core verbunden haben, wie in diesem Abschnitt beschrieben, kehren Sie zum ursprünglichen Core zurück. Stellen Sie sicher, dass mit allen Maschinen, die Sie schützen, weiterhin ein Repository verknüpft ist.
- Starten Sie anschließend die Core-Dienste auf dem Core erneut.

Weitere Informationen zum Anhalten des Schutzes finden Sie unter Vorübergehendes Deaktivieren und erneutes Aktivieren der Schutzfunktion. Weitere Informationen zum Herunterfahren und Neustarten des Core-Dienstes finden Sie unter Neustarten oder Herunterfahren des Core-Dienstes.

Von Ihrem Rapid Recovery Core Console aus können Sie eine Verbindung zu einem vorhandenen Repository herstellen, das derzeit in einem anderen Core verwaltet wird. Durch Herstellen dieser Verbindung wechselt das Eigentum des Repository vom ursprünglichen Core zu Ihrem aktuellen Core. Wenn Sie die Verbindung zu diesem Repository herstellen, sind die Informationen dann nur auf dem zweiten Core und nicht auf dem ursprünglichen Core zugänglich. Das Repository, mit dem Sie eine Verbindung herstellen, muss auf einem freigegebenen Netzwerk-Speicherort oder auf einem Speichergerät verfügbar sein, auf das der zweite Core zugreifen kann.

Dieser Vorgang ist hilfreich, wenn Ihr ursprünglicher Core ausgeschaltet ist und Sie einen Ersatz-Core bereitstellen möchten. Wenn Sie später die Besitzrechte vom zweiten Core zu einem dritten (oder dem ursprünglichen) Core wechseln möchten, können Sie dies tun. Es gelten die gleichen Regeln.

Der ursprüngliche Core, der das Repository verliert, darf nicht in Verwendung sein. Zum Beispiel, wenn die Maschine ausgeschaltet werden muss, nicht zugänglich mit dem Netzwerk ist oder die Core-Dienste gestoppt werden müssen.

Tiering-Repositorys können mit einer eindeutigen Lizenz abgesichert werden. Durch Auswahl dieser zusätzliche Sicherheit wird verhindert, dass unbefugte Personen die Kontrolle über Ihr Repository an ein anderes Repository übergeben können. Wenn Sie Ihr Repository durch seine eindeutige Lizenz absichern, können nur Administratoren mit Zugriff auf Ihren Lizenzschlüssel eine Verbindung zu Ihrem Repository herstellen. Weitere Informationen zum Aktualisieren Ihrer Repository-Einstellungen finden Sie unter dem Verfahren Ändern der Repository-Einstellungen.

Führen Sie die folgenden Schritte aus, um eine Verbindung mit einem vorhandenen Repository herzustellen.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Repositorys**.

   Die Seite **Repositorys** wird angezeigt.
3. Um eine Verbindung mit einem vorhandenen DVM-Repository herzustellen, klicken Sie auf das Drop-Down-Menü neben **Mit bestehenden verbinden** und wählen Sie dann **DVM-Repository**.

   Das Dialogfeld **Vorhandenes DVM-Repository verbinden** wird angezeigt.
4. Fahren Sie mit Schritt 6 fort..
5. Um eine Verbindung mit einem vorhandenen Tiering-Repository herzustellen, klicken Sie auf das Drop-Down-Menü neben **Mit bestehenden verbinden** und wählen Sie dann **Tiering-Repository**. Fahren Sie mit Schritt 7 fort.
6. Geben Sie im Dialogfeld **Vorhandenes DVM-Repository verbinden** die folgenden Informationen für das Repository ein, das Sie öffnen möchten, und klicken Sie dann auf **Verbinden**.

Tabelle 35. Optionen für „Vorhandenes DVM-Repository öffnen“

Textfeld	Description
Pfad	Pfad für das Repository (z. B. `D:\work\machine` für einen lokalen Pfad oder `\\10.10.99.155\repositories` nach IP-Adresse oder \\servername\sharename für einen Netzwerk-Pfad).
Benutzername	Geben Sie den Benutzernamen für die Anmeldung bei der Netzwerkfreigabe ein, wenn sich das Repository in einem Netzwerkpfad befindet.
Kennwort	Geben Sie das Kennwort für die Anmeldung bei der Netzwerkfreigabe ein, wenn sich das Repository in einem Netzwerkpfad befindet.

   Das Dialogfeld wird geschlossen und das ausgewählte Repository wird auf Ihren derzeitigen Core hinzugefügt.
7. Geben Sie im **Assistenten zum Verbinden des Repository** auf der Seite **Verbindung** den Servernamen oder die IP-Adresse der Maschine ein, die das Repository hostet, das Sie mit diesem Core verbinden möchten, und klicken Sie dann auf **Weiter**.
8. Wählen Sie auf der Seite **Cores** des Assistenten den entsprechenden Core aus und klicken Sie dann auf **Weiter**.
9. Überprüfen Sie auf der Seite **Details** des Assistenten die Details, um sicherzustellen, dass der ausgewählte Core geeignet ist. Um die Verbindung mit dem ausgewählten Core herzustellen, klicken Sie auf **Fertig stellen**.

   Wenn Sie eine Fehlermeldung erhalten, die angibt, dass das ausgewählte Repository verwendet wird, melden Sie sich bei diesem Core an und bereiten Sie die Übertragung der Besitzrechte seines Repository

auf diesen Core vor. Halten Sie jeglichen vorhandenen Schutz an; halten Sie jegliche vorhandene Replikation an; warten Sie, bis Jobs in der Warteschlange abgeschlossen sind, oder brechen Sie sie ab. Fahren Sie die Core-Dienste herunter oder schalten Sie den Core-Server ordnungsgemäß aus und wiederholen Sie den Vorgang. Weitere Informationen zum Anhalten des Schutzes finden Sie unter Vorübergehendes Deaktivieren und erneutes Aktivieren der Schutzfunktion. Weitere Informationen zum Anhalten der Replikation finden Sie unter Anhalten und Fortsetzen der Replikation. Weitere Informationen zum Herunterfahren und Neustarten des Core-Dienstes finden Sie unter Neustarten oder Herunterfahren des Core-Dienstes.

Anzeigen oder Ändern von Details zu einem Repository

Zum Anzeigen von Details zu einem Repository, muss Ihr Core zunächst ein Repository enthalten. Weitere Informationen zum Erstellen eines DVM- oder Tiering-Repositorys finden Sie unter Erstellen eines DVM-Repository bzw. Erstellen eines Tiering-Repositorys.

Im Fensterbereich **DVM-Repositorys** jedes wird das zum Core hinzugefügte DVM-Repository angezeigt.

- Wenn Sie auf (Erweitern) klicken, zeigen untergeordnete Zeilen die Speicherorte der Daten und Metadaten für das DVM-Repository an.
- Sie können die Ansicht auch (Reduzieren).

Im Fensterbereich **Tiering-Repositorys** wird jedes bestehende Repository durch mindestens drei Zeilen mit Daten dargestellt:

- Die oberste Zeile ist der RDS-Server. Sie können maximal drei RDS-Server pro Core verbinden.
- Die zweite Zeile zeigt die Speichergruppe. Jeder RDS-Server kann maximal fünf Speichergruppen enthalten.
- Die dritte Zeile enthält Tiering-Repository hat.

Sie können die Ansicht (Erweitern) und (Verkleinern) in denFensterbereichen **Tiering-Repositorys**, um Platz zu sparen.

Details zu einem Repository unterscheiden sich je nach Repository-Technologie. Zum Anzeigen oder Ändern von Repository-Details verwenden Sie das folgende Verfahren:..

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Repositorys**.

   Die Seite **Repositorys** wird angezeigt.
3. Folgende allgemeine Aktionen sind verfügbar:

Option	Description
+ Erstellen	Wählen Sie aus dem Dropdown-Menü den entsprechenden Repository-Typ, um ein Repository zu erstellen. Sie haben folgende Auswahlmöglichkeiten: • DVM-Repository • Tiering-Repository

Option	Description
Mit bestehenden verbinden	Wählen Sie aus dem Dropdown-Menü den entsprechenden Repository-Typ, um ein Repository aus einem anderen Core zu öffnen. Durch diesen Vorgang geht das Eigentumsrecht des Repository auf Ihren Core über. Sie haben folgende Auswahlmöglichkeiten: • DVM-Repository • Tiering-Repository Weitere Informationen hierzu finden Sie unter Verbinden mit einem vorhandenen Repository.
Aktualisieren	Aktualisiert die Liste der Repositorys, die auf der Seite angezeigt werden.

4. Im Fensterbereich **DVM-Repositorys** können Sie über das Dropdown-Menü [Weitere Optionen] für jedes DVM-Repository die folgenden Aktionen durchführen:

Option	Description
Speicherort hinzufügen	Erweitern des vorhandenen Repository durch Hinzufügen eines Speicherorts **NOTE:** Beim Erweitern eines DVM-Repository-Volumes müssen Sie zunächst den Schutz vorübergehend ausschalten. Erweitern Sie dann das Volume und aktivieren Sie anschließend den Schutz wieder. Diese Maßnahme verhindert einen seltenen Fehler, der nur auftreten kann, wenn das Erweitern eines Volumes gleichzeitig mit einer bestimmten Übertragungsphase stattfindet.
Überprüfen	Durchführen einer Repository-Überprüfung.
Einstellungen	Anzeigen oder Ändern der Repository-Einstellungen. Diese Einstellungen umfassen: • Anzeigen des Repository-Namens • Anzeigen oder Ändern der maximalen Anzahl gleichzeitiger Vorgänge • Anzeigen oder Ändern einer Beschreibung für das Repository • Aktivieren und Deaktivieren von Deduplizierung • Aktivieren oder Deaktivieren von Komprimierung für im Repository gespeicherte Daten
Optimieren	Durchführen einer Optimierungsaufgabe für das Repository. Weitere Informationen hierzu finden

Option	Description
	Sie unter Informationen über DVM Repository-Optimierung.
Löschen	Löschen eines Repository. **CAUTION: Mit dieser Option werden das ausgewählte DVM-Repository und alle darin enthaltenen Daten vollständig gelöscht.**

5. Im Fensterbereich **Tiering-Repositorys** können Sie über das Dropdown-Menü ••• für jeden RDS-Dienst die folgenden zusätzlichen Aktionen durchführen:

Option	Description
Anmeldeinformationen ändern	Sie können Ihr Kennwort ändern, das mit dem derzeit ausgewählten Host verknüpft ist. Diese Aktion ist nützlich, wenn zur Aufrechterhaltung der Sicherheit das Eigentumsrecht eines Repository übertragen wird. **NOTE:** Bestätigen Sie das neue Kennwort und klicken Sie auf **Speichern**, um Ihre Anmeldeinformationen zu aktualisieren.

6. Es sind keine Aktionen für Speichergruppen verfügbar.
7. In demFensterbereich **Tiering-Repositorys** können Sie im Drop-Down-Menü ••• (Weitere Optionen) für alle Tiering-Repositorys die folgenden Aktionen durchführen:

Option	Description
Einstellungen	Öffnet den Assistenten zum Ändern der Repository-Einstellungen, in dem Sie die Repository-Einstellungen anzeigen oder ändern können. Diese Einstellungen umfassen: • Anzeigen des Servers oder Hosts • Anzeigen oder Ändern des Repository-Namens • Anzeigen oder Ändern der Kommentare für das Repository
Überprüfen	Bricht alle aktiven Aufgaben für das ausgewählte Repository ab und führt dann eine Repository-Überprüfung durch.
Verbindung trennen	Hebt die Bereitstellung des ausgewählten Repository auf. **NOTE:** Nachdem das Repository getrennt wurde, können Sie es über die Funktion **Mit bestehenden verbinden** am oberen Rand der Seite „Repositorys“ wieder verbinden.
Löschen	Löschen eines Repository.

Option	Description
	CAUTION: Mit dieser Option werden das ausgewählte Repository und alle darin enthaltenen Daten vollständig gelöscht.

Trennen eines Repository

Dieser Vorgang setzt voraus, dass Ihr Core ein funktionierendes Tiering-Repository hat.

Über die Seite **Repositorys** können Sie ein vorhandenes Repository trennen. Durch diesen Prozess werden die Daten in dem Repository nicht gelöscht. Es wird lediglich die aktuelle Verbindung zum Repository und seinem Inhalt getrennt. Dies ist zum Beispiel in einer Situation nützlich, bei der Sie von einem anderen Core aus eine Verbindung zum Repository herstellen möchten.

Führen Sie dieses Verfahren aus, um ein Tiering-Repository zu trennen.

1. Klicken Sie in der Rapid Recovery Core Console in der Symbolleiste auf das Menüsymbol (Mehr) und dann auf **Repositorys**.
2. Klicken Sie auf der Seite **Repositorys** in der Zeile, die das Repository darstellt, das Sie trennen möchten, auf das Symbol für (Weitere Optionen) und wählen Sie **Trennen** aus.

   Das Dialogfeld **Repositorys trennen** wird geöffnet.
3. Klicken Sie, um die Aktion zum Trennen des vorhandenen Repository zu bestätigen.

   Das Repository wird getrennt und die Seite **Repositorys** wird aktualisiert. Das Repository wird nicht mehr in der Liste der aktuell verfügbaren Repositorys aufgeführt.

Informationen zum erneuten Verbinden des Repository finden Sie im Verfahren Verbinden mit einem vorhandenen Repository.

Löschen eines Repositorys

Führen Sie die folgenden Schritte aus, um ein Repository zu löschen.

1. Navigieren Sie zur Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Repositorys**.

   Die Seite **Repositorys** wird angezeigt.
3. Klicken Sie in der entsprechenden Repository-Zusammenfassungstabelle auf der Zeile für das Repository, das Sie löschen möchten, auf (Weitere Optionen), um das Drop-Down-Menü zu erweitern, und wählen Sie dann **Löschen**.

   In einer Warnmeldung werden Sie aufgefordert, den Löschvorgang zu bestätigen.

   CAUTION: Wenn ein Repository gelöscht wird, werden die Daten im Repository verworfen und können nicht wiederhergestellt werden.
4. Klicken Sie auf **Ja**, um das Löschen des Repositorys zu bestätigen.

Datenschutzverwaltung

Dieser Abschnitt beschreibt die personenbezogenen Daten, die Rapid Recovery erheben kann, wofür die Daten verwendet werden und wie Sie den Schutz Ihrer Daten steuern können.

Folgende Themen werden behandelt:

- Einhaltung der Datenschutz-Grundverordnung
- Verwendung von personenbezogenen Daten durch Rapid Recovery
- Einschränkungen der Non-Phone-Home-Lizenz
- Erhalten und Verwenden von Non-Phone-Home-Lizenzen

Einhaltung der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung (DSGVO) ist eine Gesetzgebung zur Stärkung und Vereinheitlichung des Datenschutzes für alle Einzelpersonen innerhalb der Europäischen Union (EU). Sie umfasst auch den Export von personenbezogenen Daten aus der EU, weshalb sie für Softwarehersteller in den USA und anderen Ländern relevant ist. Sie aktualisiert die Regeln für den Umgang mit personenbezogenen Daten von Einzelpersonen. Die DSGVO wird in der Softwarebranche weitgehend akzeptiert.

Zur Einhaltung der DSGVO wurde die Erhebung von personenbezogenen Daten (Personally Identifiable Information, PII) durch Rapid Recovery Core sorgfältig geprüft. Die Datenerhebung wurde optimiert und die erhobenen Daten werden eindeutig dokumentiert.

Bei Installation von Rapid Recovery Core, Ausführen der Recovery and Update Utility (RUU) bzw. Ausführen des Informationserfassungs-Tools erhalten Sie eine Beschreibung der Daten, die Rapid Recovery erhebt, sowie des Zwecks der Datenerhebung.

Wenn Sie der genannten Nutzung der personenbezogenen Daten zustimmen, können Sie anschließend eine Lizenz (die im Standard-Phone-Home-Modus ausgeführt wird) Ihrem Core zuordnen. Wenn Sie der Verwendung von personenbezogenen Daten in den Datenschutzbestimmungen nicht zustimmen, müssen Sie eine spezielle Non-Phone-Home-Lizenz anfordern. Nachdem Sie diese Lizenz erhalten und Ihrem Core zugeordnet haben, werden Ihre personenbezogenen Daten nicht verwendet und bestimmte Funktionen (automatische Aktualisierung und die Aktivierung der Integration zwischen dem Core und Datenschutz-Portal) sind deaktiviert.

Unabhängig von der Datenschutzoption, die Sie während der Installation gewählt haben, können Sie diese Einstellung in den allgemeinen Einstellungen des Core mit der Option **Nutzung persönlicher Daten zustimmen** ändern. Um zwischen Phone-Home-Modus und Non-Phone-Home-Modus zu wechseln, müssen Sie Zugriff auf die entsprechende Lizenz haben.

Weitere Informationen über die DSGVO finden Sie auf der EU-Website zur Datenschutz-Grundverordnung unter http://www.eugdpr.org/eugdpr.org.html.

Weitere Informationen zur Verwaltung des Datenschutzes finden Sie in den folgenden Themen in *Rapid Recovery Benutzerhandbuch*:

- Bestimmte Geschäftsregeln gelten beim Wechsel zwischen Phone-Home-Modus und Non-Phone-Home-Modus mithilfe der allgemeinen Einstellung **Nutzung persönlicher Daten zustimmen**. Weitere Informationen finden Sie im Thema „Konfigurieren von allgemeinen Core-Einstellungen“.
- Informationen dazu, welche Daten Rapid Recovery erhebt und unter welchen Umständen sowie warum die Daten erhoben werden, finden Sie unter „Verwendung von personenbezogenen Daten durch Rapid Recovery“.
- Informationen dazu, welche Funktionen Sie nicht ausführen können, wenn Sie eine Non-Phone-Home-Lizenz verwenden, finden Sie im Thema „Einschränkungen der Non-Phone-Home-Lizenz“.
- Um eine Phone-Home-Lizenz herunterzuladen, melden Sie sich an bei Rapid Recovery Lizenzportal. Klicken Sie im Navigationsmenü auf **Lizenzierung** und wählen Sie aus dem Drop-Down-Menü oben rechts **Lizenzschlüssel** aus.
- Um zu erfahren, wie Sie eine Lizenz im Non-Phone-Home-Modus erhalten, finden Sie im Thema „Obtaining and using non-phone-home keys“ (Erhalten und Verwenden von Non-Phone-Home-Schlüsseln).

Verwendung von personenbezogenen Daten durch Rapid Recovery

Wie in Verwalten von Lizenzen beschrieben, verwendet Rapid Recovery drei Arten von Softwarelizenzen: Abonnement-, unbefristete und Testlizenzen.

Es gibt zwei Modi, in denen Lizenzen verwendet werden können:

- **Phone-Home-Modus.** Alle Lizenzen werden im Phone-Home-Modus ausgestellt, wenn nicht anders gewünscht. Wenn Sie eine Phone-Home-Lizenz für Rapid Recovery Lizenzportal registrieren, erhebt Rapid Recovery einige personenbezogene Daten. Welche Daten erhoben werden und wie diese verwendet werden, ist unten beschrieben.
- **Non-Phone-Home-Modus** Wenn Sie eine Non-Phone-Home-Lizenz erwerben und registrieren, gibt Rapid Recovery auch bei einer Verbindung über das Internet Ihre personenbezogenen Daten nicht weiter. Bei Verwendung dieses Modus können Sie bestimmte Funktionen nicht ausführen, wie im Thema Erhalten und Verwenden von Non-Phone-Home-Lizenzen beschrieben.

Abonnement-Lizenzen können nur im Phone-Home-Modus verwendet werden. Unbefristete und Testlizenzen können entweder im Phone-Home-Modus oder im Non-Phone-Home-Modus verwendet werden.

Wenn Sie eine Phone-Home-Lizenz registrieren, erteilen Sie Rapid Recovery die Erlaubnis, die folgenden personenbezogenen Daten zu erheben:

- Die IP-Adressen und Hostnamen der Hosts, die auf Rapid Recovery Core und Agent ausgeführt werden oder damit interagieren.
- Die E-Mail-Adressen in Zusammenhang mit Rapid Recovery Lizenzen; und
- Der Verbrauch von Lizenzen im Vergleich zu der Anzahl an Lizenzen im Lizenzpool.

Diese Informationen werden an Quest Software, Inc. zu folgenden Zwecken gesendet:

- Um die entsprechenden Lizenzbedingungen für das Produkt richtig anzuwenden;
- Um Kunden-Support zu bieten; zum Beispiel werden, wenn Sie das Informationserfassungs-Tool ausführen, Protokolle und diagnostische Daten, die Sie spezifiziert haben, in einen lokalen Ordner zum

Senden an Quest abgelegt oder ggf. auf Amazon hochgeladen, wo Sie nur für Quest Datenschutz-Support zugänglich sind.

- Zum Benachrichtigen der Benutzer über verfügbare Updates (falls die Update Einstellungen auf dem Core eine andere Option als **Nie nach Updates suchen** aufweisen); und
- Um die Kommunikation zwischen dem Core und Datenschutz-Portal zu ermöglichen. Diese Kommunikation kann über die Einstellungen des **Datenschutz-Portals** auf dem Core aktiviert und deaktiviert werden. Mit diesem Portal können Benutzer mit einer gültigen Lizenz und einem aktuellen Support-Vertrag den Zustand von Cores und geschützten Maschinen überwachen, mehrere Cores verwalten und bedarfsweise Berichte für die jeweiligen Cores und geschützten Maschinen erzeugen.

Sie haben das Recht zu entscheiden, ob Sie diese Informationen an Quest weitergeben möchten oder nicht. Sie können zuerst beim Installieren oder Aktualisieren von Rapid Recovery Core auf der **Datenschutz**-Seite des Installationsprogramms auswählen, ob diese Informationen weitergegeben werden sollen. Zudem können Sie, wenn Sie sich entscheiden, keine Informationen an Quest weiterzugeben, die allgemeine Einstellung **Nutzung persönlicher Daten zustimmen** des Cores ändern. Wenn Sie diese Einstellung ändern, werden Sie aufgefordert, eine Lizenz anzugeben. Wenn Sie eine Non-Phone-Home-Lizenz angeben, wird die automatische Aktualisierung deaktiviert, genau wie die Verbindung mit Datenschutz-Portal.

Weitere Ressourcen zu diesem Thema finden Sie unter den folgenden zugehörigen Links.

- Weitere Informationen zu den Funktionen, die Sie nicht ausführen können, wenn Sie den Non-Phone-Home-Modus verwenden, finden Sie im Thema Einschränkungen der Non-Phone-Home-Lizenz.
- Weitere Informationen zur Erlangung einer Lizenz, die den Non-Phone-Home-Modus nutzt, erhalten Sie über das Webformular des Quest Lizenzteams, wie im Thema Erhalten und Verwenden von Non-Phone-Home-Lizenzen beschrieben.
- Weitere Informationen zum Ändern der allgemeinen Einstellungen, einschließlich der Weitergabe von personenbezogenen Daten, finden Sie im Thema Konfigurieren von allgemeinen Core-Einstellungen.
- Weitere Informationen zum Anzeigen von Lizenzinformationen für eine einzelne geschützte Maschine finden Sie unter Anzeigen von Lizenzinformationen für eine Maschine.
- Weitere Informationen über die Eingabe von Lizenzschlüssel- oder Dateiinformationen (zum Beispiel zum Aktualisieren einer unbefristeten Phone-Home-Lizenz auf eine unbefristete Non-Phone-Home-Lizenz) finden Sie unter Aktualisieren oder Ändern einer Lizenz.
- Weitere Informationen zu sämtlichen verfügbaren Lizenzarten finden Sie unter Verwalten von Lizenzen.
- Weitere Informationen zur Kontaktaufnahme mit dem Lizenzportalserver finden Sie unter Kontaktaufnahme mit dem Rapid Recovery Lizenzportal-Server.
- Weitere Themen in Bezug auf die Verwaltung von Lizenzen finden Sie in *Rapid Recovery Lizenzportal - Benutzerhandbuch*.

Einschränkungen der Non-Phone-Home-Lizenz

Bei Registrieren einer Rapid Recovery Lizenz im Non-Phone-Home-Modus kann der Core Ihre personenbezogenen Daten nicht weiterleiten. Dies umfasst E-Mail-Adresse, IP-Adressen und Lizenzverbrauchsinformationen.

Nach Registrieren einer Non-Phone-Home-Lizenz werden Sie nicht in der Lage sein, Folgendes zu tun:

- Anzeigen von Lizenzserverinformationen auf der Seite **Einstellungen** auf der Core Console (da der Core nicht mit Rapid Recovery Lizenzportal kommunizieren darf).
- Verwalten des Lizenzverbrauchs über die Core Console.
- Einreichen von Informationen zu Quest Datenschutz-Support über das Rapid Recovery Informationserfassungs-Tool.
- Überwachen des Zustands von Cores und geschützten Maschinen, Verwalten mehrerer Cores und bedarfsgerechte Erstellung von Berichten für die entsprechenden Maschinen auf mehreren Cores aus Datenschutz-Portal.
- Verwenden der Funktion für automatische Updates zur Aktualisierung auf eine neue Version von Rapid Recovery Core (der Core wird nicht darüber benachrichtigt, dass neue Versionen zur Verfügung stehen).
- Verwenden der Funktion für automatische Updates zum direkten Aktualisieren geschützter Linux-Maschinen mit Paket-Managern wie Yum, Zypper oder Apt (Sie können trotzdem noch ein Installationspaket von einer über Internet zugänglichen Linux-Maschine herunterladen und Installationsdateien manuell auf den geschützten Computer verschieben).

Erhalten und Verwenden von Non-Phone-Home-Lizenzen

Wenn Sie die Non-Phone-Home-Lizenz erhalten, bevor Sie Rapid Recovery Core Version 6.2 installieren oder aktualisieren, übertragen Sie die Lizenz auf den Core-Server. Wählen Sie beim Ausführen des Installationsprogramms auf der Seite **Datenschutzrichtlinien** die Option zum Ablehnen der Weiterleitung von Daten aus und registrieren Sie die Non-Phone-Home-Lizenz, wenn Sie dazu aufgefordert werden.

Wenn Ihr Rapid Recovery Core Version 6.2 bereits mit einem Non-Phone-Home-Schlüssel registriert ist, rufen Sie die allgemeinen Einstellungen des Core auf, wählen Sie die Option zum Ablehnen der Weiterleitung von Daten aus und registrieren Sie den Non-Phone-Home-Schlüssel, wenn Sie dazu aufgefordert werden.

Weitere Informationen oder Schritt-für-Schritt-Anweisungen zum Ändern der allgemeinen Einstellungen für Ihren Core finden Sie im Thema Konfigurieren von allgemeinen Core-Einstellungen.

Weitere Informationen zur Verwaltung von Lizenzen aus Rapid Recovery Core finden Sie unter Verwalten von Lizenzen.

Führen Sie die Schritte in diesem Verfahren durch, um das Quest Lizenzierungsteam zu kontaktieren, um eine Non-Phone-Home-Lizenz anzufordern.

1. Navigieren Sie in einem Web Browser zu der Quest Lizenzierungs-Support-Website unter https://support.quest.com/contact-us/licensing.
2. Wählen Sie aus dem Drop-Down-Menü **Wie können wir Ihnen helfen Lizenz für mein Produkt erhalten** aus.
3. Wählen Sie aus dem Drop-Down-Menü **Produkt auswählen Rapid Recovery** aus.
4. Wählen Sie aus dem Drop-Down-Menü **Produktversion** die entsprechende Option aus.

   Wählen Sie beispielsweise **6.2** aus.
5. Geben Sie im Abschnitt des Formulars mit den Kontaktinformationen die Informationen an, die in der folgenden Tabelle beschrieben sind.

Feldname	Beschreibung	Erforderliches Feld
Geschäfts-E-Mail	Geben Sie die E-Mail-Adresse an, unter der Sie das Quest Lizenzierungsteam kontaktieren soll. Wenn Sie den Zugriff auf das Ihrer	Ja

Feldname	Beschreibung	Erforderliches Feld
	Rapid Recovery Lizenz zugeordnete E-Mail-Konto haben, verwenden Sie diese Adresse, um so schnell wie möglich eine Antwort zu erhalten.	
Vorname des Ansprechpartners	Geben Sie Ihren Vornamen an	Ja
Nachname des Ansprechpartners	Geben Sie Ihren Nachnamen an	Ja
Firmenname	Geben Sie den Namen der Firma in Zusammenhang mit der Rapid Recovery Lizenz an	
US Federal	Wählen Sie diese Option aus, wenn Ihre Lizenz mit einer Organisation der US-Regierung in Zusammenhang steht.	Nein
Land	Wählen Sie Ihr Land aus.	Ja
Telefonnummer	Geben Sie Ihre Telefonnummer einschließlich Vorwahl ein. Wenn Sie außerhalb der USA wohnen, geben Sie die Landesvorwahl an.	Ja
Lizenznummer (falls vorhanden)		Nein
Lizenzschlüssel (falls vorhanden)	Lizenzschlüssel wurden in AppAssure 5.4.1 und früheren Versionen verwendet. Dies ist in der Regel eine Zeichenkette mit 30 Zeichen (6 Gruppen mit 5 Ziffern und Großbuchstaben, die durch Bindestriche getrennt sind).	Nein
Maschinen-ID	Der Name der registrierten Core-Maschine.	Nein
Service-Tag-Nummer (falls vorhanden)	Geben Sie die Service-Tag-Nummer an, falls verfügbar.	Nein
Details zur Lizenzanforderung	Geben Sie in diesem Feld an, dass Sie gemäß DSGVO eine Non-Phone-Home-Lizenz anstatt einer Phone-Home-Lizenz zum Schutz Ihrer personenbezogenen Daten haben möchten. **NOTE:** Mit dieser Anfrage erklären Sie sich damit einverstanden, dass Sie den Phone-Home-Lizenzschlüssel löschen, sobald Sie den Non-Phone-Home-Schlüssel erhalten haben. Sie stimmen auch zu, dass Sie diesen Schlüssel nicht weitergeben.	Ja
Lizenzdatei	Wenn Sie über eine Phone-Home-Lizenz verfügen, können Sie die Lizenzdatei anhängen.	Nein

6. Um Ihre Anfrage zu bestätigen und das Formular zu senden, wählen Sie **Ich bin kein Roboter**, und klicken Sie dann auf **Weiter**.

   Das Formular wird übermittelt und Sie erhalten eine Nachricht mit einer Serviceanfragenummer (SR).

Wenn Sie die Non-Phone-Home-Lizenzdatei erhalten, laden Sie sie auf den Core-Server hoch, um die Lizenz zu registrieren. Weitere Informationen hierzu finden Sie unter Aktualisieren oder Ändern einer Lizenz.

Verschlüsselung

In diesem Kapitel wird beschrieben, wie Sie Daten in Ihrer Umgebung mithilfe von Verschlüsselungsschlüsseln und Snapshot-Verschlüsselungseinstellungen auf Maschinenebene schützen können.

Grundlegende Informationen zu Verschlüsselungsschlüsseln

Der Rapid Recovery Core kann Snapshot-Daten für alle Volumes in jedem beliebigen Repository mithilfe von Verschlüsselungsschlüsseln, die Sie von der Core Console aus definieren und verwalten, verschlüsseln.

Anstatt das ganze Repository zu verschlüsseln, bietet Rapid Recovery Ihnen die Möglichkeit, einen Verschlüsselungsschlüssel für einzelne oder mehrere Maschinen festzulegen, die von einem Rapid Recovery Core geschützt werden. Jeder aktive Verschlüsselungsschlüssel erstellt einen Verschlüsselungsbereich. Sie können unbegrenzt viele Verschlüsselungsschlüssel auf dem Core erstellen.

In einer Umgebung mit mehreren Nutzern (mit einem einzelnen Core als Host für mehrere Verschlüsselungsbereiche) werden Daten in einzelne Verschlüsselungsbereiche partitioniert und jeweils dort dedupliziert. Daher empfiehlt Quest, einen einzigen Verschlüsselungsschlüssel für mehrere geschützte Maschinen zu verwenden, um die Vorteile der Deduplizierung für mehrere geschützte Maschinen zu maximieren.

Darüber hinaus können Sie ein der drei folgenden Methoden verwenden, um Verschlüsselungsschlüssel auf Cores gemeinsam zu nutzen. Eine Methode besteht darin, einen Verschlüsselungsschlüssel als Datei von einem Rapid Recovery Core zu exportieren und in einen anderen Core zu importieren. Eine zweite Methode besteht darin, die mit einem Verschlüsselungsschlüssel geschützten Daten zu archivieren und die archivierten Daten anschließend in einen anderen Rapid Recovery Core zu importieren. Die dritte Methode besteht darin, Wiederherstellungspunkte einer geschützten Maschine mit einem Verschlüsselungsschlüssel zu replizieren. Nach der Replikation der geschützten Maschinen werden die im Quell-Core verwendeten Verschlüsselungsschlüssel im Ziel-Core als replizierte Verschlüsselungsschlüssel angezeigt.

In allen Fällen werden Verschlüsselungsschlüssel nach dem Import im Core als gesperrt angezeigt. Um auf die Daten eines gesperrten Verschlüsselungsschlüssels zugreifen zu können, muss der Verschlüsselungsschlüssel entsperrt werden. Informationen zum Importieren, Exportieren, Sperren oder Entsperren von Verschlüsselungsschlüsseln finden Sie unter Verwalten von Verschlüsselungsschlüsseln.

Wichtige Sicherheitskonzepte und -überlegungen sind u. a.:

- Die Verschlüsselung erfolgt mit 256-Bit-AES (Advanced Encryption Standard) im CBC-Modus (Cipher Block Chaining), der mit SHA-3 kompatibel ist.
- Die Deduplizierung erfolgt innerhalb eines Verschlüsselungsbereichs, um den Datenschutz zu gewährleisten.
- Die Verschlüsselung wirkt sich nicht auf die Leistung aus.
- Sie können einen Verschlüsselungsschlüssel für eine beliebige Anzahl von geschützten Maschinen verwenden, für eine geschützte Maschine kann aber jeweils nur ein Verschlüsselungsschlüssel verwendet werden.
- Sie können die auf dem Rapid Recovery Core konfigurierten Verschlüsselungsschlüssel hinzufügen, entfernen, importieren, exportieren, ändern und löschen.

CAUTION: Rapid Recovery **erstellt jedes Mal einen neuen Snapshot, wenn Sie einen Verschlüsselungsschlüssel auf einer geschützten Maschine anwenden. Ein neuer Snapshot wird auch erstellt, wenn Sie einen Verschlüsselungsschlüssel für eine geschützte Maschine entfernen.**

Vom Rapid Recovery Core erstellte Verschlüsselungsschlüssel sind Textdateien, die vier Parameter enthalten (siehe Beschreibung in der folgenden Tabelle):

Tabelle 36. Komponenten eines Verschlüsselungsschlüssels

Komponente	Description
Name	Dieser Wert entspricht dem Schlüsselnamen, der beim Hinzufügen eines Schlüssels in der Rapid Recovery Core Console angegeben wurde.
Schlüssel	Dieser Parameter umfasst 107 zufallsgenerierte Zeichen des englischen Alphabets, Zahlen und mathematischen Operatorzeichen.
ID	Sie Schlüssel-ID besteht aus 26 zufallsgenerierten Groß- und Kleinbuchstaben des englischen Alphabets.
Anmerkung	Die Anmerkung enthält den Text der Schlüsselbeschreibung, die beim Erstellen des Schlüssels eingegeben wurde.

Verschlüsseln von Daten, die über ein Netzwerk transportiert werden

Rapid Recovery CoreVersion 6.2 umfasst eine neue Verschlüsselungsfunktion: Sie können jetzt alle Daten, die über ein Netzwerk transportiert werden, verschlüsseln; Quest empfiehlt diese Verschlüsselungseinstellung, wenn Daten zwischen dem Core und geschützten Maschinen (oder zwischen zwei Cores z. B. für die Replikation) über das öffentliche oder nicht vertrauenswürdige Netzwerke, wie z. B. das Internet, geleitet werden müssen.

Zwar geht bei Aktivierung dieser Verschlüsselung nur ein kleiner Teil der Leistung verloren; wenn die Cores und geschützten Maschinen innerhalb der Grenzen eines privaten lokalen Netzwerks kommunizieren, können Sie diese Option jedoch ruhigen Gewissens deaktivieren.

Bitte lesen Sie die folgenden Informationen und passen Sie Ihre Umgebung entsprechend an.

Standardmäßig wird beim Schützen einer Maschine mithilfe des Assistenten zum Schützen einer Maschine oder des Assistenten zum Schützen mehrerer Maschinen die Verschlüsselung der Daten beim Transport über ein Netzwerk aktiviert. Wenn Sie erweiterte Optionen für den Assistenten auswählen, können Sie die Verschlüsselungsoptionen anzeigen. Auf der Verschlüsselungsseite des Assistenten können Sie, wenn gewünscht, die Option **Die Daten verschlüsseln, die über ein Netzwerk transportiert werden** deaktivieren.

NOTE: Wenn Sie die erweiterten Optionen im Assistenten nicht auswählen, ist die Verschlüsselung von Daten beim Transport auf jeden Fall aktiviert.

Nach Abschluss des entsprechenden Assistenten zum Schützen können Sie die Verschlüsselung von Snapshot-Daten jederzeit aktivieren oder deaktivieren durch Ändern der Übertragungseinstellungen auf Computerebene. Wählen Sie die geschützte Maschine aus, klicken Sie auf **Einstellungen** und wählen Sie unter den Übertragungseinstellungen für die Einstellung **Snapshot-Daten verschlüsseln Ja**, um die Verschlüsselung zu aktivieren, oder **Nein**, um die Verschlüsselung während des Transports zu deaktivieren. Weitere Informationen finden Sie unter Anzeigen und Ändern von geschützten Maschineneinstellungen in *Rapid Recovery Benutzerhandbuch*.

Anwenden oder Entfernen von Verschlüsselungsschlüsseln

Sie können die im Core geschützten Daten jederzeit verschlüsseln, indem Sie einen Verschlüsselungsschlüssel definieren und auf geschützte Maschinen im Repository anwenden. Sie können einen Verschlüsselungsschlüssel für eine beliebige Anzahl von geschützten Maschinen verwenden, für eine geschützte Maschine kann aber jeweils nur ein Verschlüsselungsschlüssel verwendet werden.

Die Deduplizierung in Rapid Recovery ist auf geschützte Maschinen beschränkt, die das gleiche Repository und den gleichen Verschlüsselungsschlüssel verwenden. Daher empfiehlt Quest, einen einzigen Verschlüsselungsschlüssel für so viele geschützte Maschinen zu verwenden wie möglich, um den Nutzen der Deduplizierung zu maximieren. Sie können jedoch unbegrenzt viele Verschlüsselungsschlüssel auf dem Core erstellen. Sie können daher beliebig viele Verschlüsselungsschlüssel hinzufügen und verwalten, falls Rechtsvorschriften, Sicherheitsregeln, Datenschutzrichtlinien oder andere Umstände dies erfordern. Sie können einen Schlüssel dann lediglich für eine geschützte Maschine oder für mehrere Maschinen im Repository verwenden.

Jedes Mal, wenn ein Verschlüsselungsschlüssel für eine geschützte Maschine angewendet wurde oder von einer geschützten Maschine entfernt wurde, erstellt Rapid Recovery beim nächsten geplanten oder erzwungenen Snapshot ein neues Basisimage für die entsprechende Maschine. Die im betreffenden Basisimage (und allen nachfolgend erstellten inkrementellen Snapshots mit diesem Verschlüsselungsschlüssel) gespeicherten Daten werden mit 256-Bit AES verschlüsselt. Es gibt keine bekannten Methoden, die eine derartige Verschlüsselung gefährden können.

Wenn Sie den Namen oder die Passphrase für einen vorhandenen Verschlüsselungsschlüssel, der derzeit auf einer geschützten Maschine verwendet wird, ändern, wird Rapid Recovery Core beim nächsten geplanten oder erzwungen Snapshot die aktualisierten Eigenschaften des Schlüssels erfassen und spiegeln. Die im betreffenden Basisimage (und allen nachfolgend erstellten inkrementellen Snapshots mit diesem Verschlüsselungsschlüssel) gespeicherten Daten werden standardmäßig mit 256-Bit AES verschlüsselt. Es gibt keine bekannten Methoden, die eine derartige Verschlüsselung gefährden können.

Nachdem ein Verschlüsselungsschlüssel erstellt und auf eine geschützte Maschine angewendet wurde, gibt es zwei Möglichkeiten, die Verschlüsselung zu deaktivieren. Die erste besteht darin, die Schlüsselzuordnung zur geschützten Maschine aufzuheben. Nachdem die Zuordnung der Verschlüsselungsschlüssel für alle geschützten Maschinen aufgehoben wurde, kann der Schlüssel ggf. von Rapid Recovery Core gelöscht werden.

In diesem Abschnitt werden folgende Themen behandelt:

- Zuordnen eines Verschlüsselungsschlüssels zu einer geschützten Maschine
- Anwenden eines Verschlüsselungsschlüssels auf der Seite „Geschützte Maschinen“
- Aufheben der Verschlüsselungsschlüsselzuordnung für eine geschützte Maschine

Zuordnen eines Verschlüsselungsschlüssels zu einer geschützten Maschine

Es gibt zwei Möglichkeiten, um einen Verschlüsselungsschlüssel auf eine geschützte Maschine anzuwenden.

- **Beim Schützen einer Maschine:** Bei dieser Möglichkeit können Sie die Verschlüsselung für eine oder mehrere Maschinen gleichzeitig aktivieren. Bei dieser Methode können Sie einen neuen Verschlüsselungsschlüssel hinzufügen oder einen vorhandenen Verschlüsselungsschlüssel auf ausgewählte Maschinen anwenden.

  Wenn Sie eine Maschine erstmals unter Schutz stellen und die Verschlüsselung aktivieren möchten, müssen Sie „Erweiterte Optionen“ im jeweiligen Assistenten zum Schützen von Maschinen auswählen.

Dadurch wird die Seite „Verschlüsselung“ in den Ablauf des Assistenten eingefügt. Wählen Sie auf dieser Seite **Verschlüsselung aktivieren** aus. Wählen Sie dann einen vorhandenen Verschlüsselungsschlüssel aus oder geben Sie die Parameter für einen neuen Schlüssel an. Weitere Informationen finden Sie unter Schützen einer Maschine bzw. So schützen Sie mehrere Maschinen.

- **Durch Ändern der Konfigurationseinstellungen für eine Maschine:** Bei dieser Möglichkeit wird ein Verschlüsselungsschlüssel jeweils auf eine geschützte Maschine angewendet. Es gibt zwei Verfahren zum Ändern der Konfigurationseinstellungen für eine Maschine in der Benutzeroberfläche von Rapid Recovery:
  - Ändern Sie die Konfigurationseinstellungen für eine speziell geschützte Maschine. Der Verschlüsselungsschlüssel, den Sie für diesen Ansatz verwenden wollen, muss bereits auf dem Rapid Recovery Core vorhanden, ein Universalgruppen-Schlüsseltyp und in einem nicht gesperrten Zustand sein. Verschlüsselung ist Teil der allgemeinen Einstellungen. Weitere Informationen finden Sie unter Anzeigen und Ändern von geschützten Maschineneinstellungen.
  - Klicken Sie auf das Symbol **Nicht verschlüsselt** auf der Seite „Geschützte Maschinen“. Bei diesem Verfahren können Sie einen neuen Verschlüsselungsschlüssel erstellen und anwenden oder der jeweiligen geschützten Maschine einen vorhandenen nicht gesperrten Schlüssel zuweisen. Weitere Informationen finden Sie unter Anwenden eines Verschlüsselungsschlüssels auf der Seite „Geschützte Maschinen“.

Anwenden eines Verschlüsselungsschlüssels auf der Seite „Geschützte Maschinen“

Nachdem ein Verschlüsselungsschlüssel zu einem Rapid Recovery Core hinzugefügt wurde, kann er für eine beliebige Anzahl geschützter Maschinen verwendet werden.

Wenn Sie einen Verschlüsselungsschlüssel auswählen, wenn Maschinen erstmals unter Schutz gestellt wird, wird dieser Schlüssel automatisch für alle Maschinen verwendet, die mit dem Assistenten geschützt werden. In diesem Fall müssen die folgenden Schritte nicht ausgeführt werden.

Gehen Sie wie folgt vor:

- Wenn Sie einen bestehenden, universellen, entsperrten Verschlüsselungsschlüssel auf einer geschützten Maschine in Ihrem Core anwenden möchten.
- Wenn Sie soeben mithilfe der unter dem Thema Hinzufügen eines Verschlüsselungsschlüssels beschriebenen Vorgehensweise einen neuen Verschlüsselungsschlüssel hinzugefügt haben und diesen auf einer geschützten Maschine anwenden möchten.
- Wenn die Verschlüsselung bereits auf einer geschützten Maschine in Ihrem Core angewendet wurde, Sie den Schlüssel aber in einen anderen in Ihrem Core verfügbaren universellen, entsperrten Schlüssel ändern möchten.

CAUTION: Nachdem ein Verschlüsselungsschlüssel auf eine geschützte Maschine angewendet wurde, erstellt Rapid Recovery **beim nächsten geplanten oder erzwungenen Snapshot ein neues Basisimage für diese Maschine.**

1. Navigieren Sie zum Rapid Recovery Core und klicken Sie auf **Geschützte Maschinen**.

   Daraufhin werden auf der Seite **Geschützte Maschinen** alle Maschinen angezeigt, die durch diesen Core geschützt werden. Für jede Maschine ohne Verschlüsselungsschlüssel wird ein geöffnetes Schloss angezeigt. Ein geschlossenes Schloss weist darauf hin, dass die Verschlüsselung für eine geschützte Maschine aktiviert ist.
2. Klicken Sie im Bereich „Geschützte Maschinen“ auf das Schlosssymbol der geschützten Maschine, die sie konfigurieren möchten.

Das Dialogfeld **Verschlüsselungskonfiguration** wird angezeigt.

3. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie einen vorhandenen Verschlüsselungsschlüssel auf dieser Maschine anwenden möchten, wählen Sie **Daten mit Core-basierter Verschlüsselung mit einem vorhandenen Schlüssel verschlüsseln** und anschließend im Dropdownmenü den entsprechenden Schlüssel aus. Klicken Sie zur Bestätigung auf **OK**.
   - Wenn Sie einen vorhandenen Verschlüsselungsschlüssel in einen anderen universellen entsperrten Schlüssel ändern möchten, wählen Sie **Daten mit Core-basierter Verschlüsselung mit einem neuen Schlüssel verschlüsseln** und anschließend im Dropdownmenü den entsprechenden Schlüssel aus. Klicken Sie zur Bestätigung auf **OK**.
   - Wenn Sie einen neuen Verschlüsselungsschlüssel erstellen und auf dieser geschützten Maschine anwenden möchten, wählen Sie **Daten mit Core-basierter Verschlüsselung mit einem neuen Schlüssel verschlüsseln** aus. Geben Sie die Details für den Schlüssel ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 37. Details für neue Verschlüsselungsschlüssel

Textfeld	Description
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein. Namen für Verschlüsselungsschlüssel müssen 1 bis 64 alphanumerische Zeichen umfassen. Verwenden Sie keine unzulässigen Zeichen oder unzulässigen Phrasen.
Description	Geben Sie einen beschreibenden Kommentar für den Verschlüsselungsschlüssel ein. Diese Informationen werden im Beschreibungsfeld angezeigt, wenn Verschlüsselungsschlüssel in der Rapid Recovery Core Console angezeigt werden. Die Beschreibung kann bis zu 254 Zeichen umfassen. Es hat sich bewährt, die Verwendung von unzulässigen Zeichen und unzulässigen Phrasen zu vermeiden.
Passphrase	Geben Sie eine Passphrase für die Zugriffssteuerung ein. Sie sollten keine unzulässigen Zeichen verwenden. Bewahren Sie die Passphrase an einem sicheren Ort auf. Der Quest Support kann eine Passphrase nicht wiederherstellen. Wenn Sie einen Verschlüsselungsschlüssel erstellt und für eine geschützte Maschine verwendet haben, können Sie keine Daten dieser geschützten Maschine mehr wiederherstellen, wenn die Passphrase verloren geht.
Passphrase wiederholen	Geben Sie die Passphrase erneut ein. Dies wird zur Bestätigung der Passphraseneingabe verwendet.

4. Klicken Sie auf **OK**.

   Das Dialogfeld wird geschlossen. Der angegebene Verschlüsselungsschlüssel wird für zukünftige Sicherungen für diese geschützte Maschine verwendet. Das Schloss ist jetzt geschlossen.

   Wenn der Verschlüsselungsschlüssel sofort verwendet werden soll, können Sie ggf. einen Snapshot erzwingen. Weitere Informationen hierzu finden Sie unter Erzwingen eines Snapshots.

> **CAUTION:** Rapid Recovery **verwendet 256-Bit-AES-Verschlüsselung im CBC-Modus (Cipher Block Chaining) mit 256-Bit-Schlüsseln. Obwohl die Verwendung der Verschlüsselung optional ist, wird von** Quest **dringend empfohlen, einen Verschlüsselungsschlüssel einzurichten und die festgelegte Passphrase zu schützen. Speichern Sie die Passphrase an einem sicheren Speicherort, da sie für die Datenwiederherstellung von entscheidender Bedeutung ist. Ohne Passphrase ist keine Datenwiederherstellung möglich.**

Aufheben der Verschlüsselungsschlüsselzuordnung für eine geschützte Maschine

Nachdem ein Verschlüsselungsschlüssel auf eine geschützte Maschine angewendet wurde, werden alle danach im Rapid Recovery Core gespeicherten Snapshot-Daten verschlüsselt.

Sie können die Verschlüsselungsschlüsselzuordnung für eine geschützte Maschine aufheben. Dabei werden die vorhandenen Sicherungsdaten nicht entschlüsselt, sondern beim nächsten geplanten oder erzwungenen Snapshot ein neues Basisimage für die betreffende Maschine erstellt.

NOTE: Wenn Sie einen Verschlüsselungsschlüssel vom Core entfernen können (siehe Beschreibung unter Entfernen eines Verschlüsselungsschlüssels), müssen Sie zuerst die Zuordnung des Verschlüsselungsschlüssels zu geschützten Maschinen aufheben.

Führen Sie die folgenden Schritte aus, um die Verschlüsselungsschlüsselzuordnung für eine bestimmte geschützte Maschine aufzuheben.

1. Navigieren Sie zum Rapid Recovery Core und klicken Sie auf **Geschützte Maschinen**.

   Daraufhin werden auf der Seite Geschützte Maschinen alle Maschinen angezeigt, die durch diesen Core geschützt werden. Für jede Maschine ohne Verschlüsselungsschlüssel wird ein geöffnetes Schloss angezeigt. Ein geschlossenes Schloss weist darauf hin, dass die Verschlüsselung für eine geschützte Maschine aktiviert ist.

2. Klicken Sie im Bereich „Geschützte Maschinen“ auf das Symbol **Verschlüsselt** der geschützten Maschine, die sie konfigurieren möchten.

   Das Dialogfeld **Verschlüsselungskonfiguration** wird angezeigt.

3. Wählen Sie **Daten mit einer Core-basierten Verschlüsselung mit vorhandenem Schlüssel verschlüsseln** und wählen Sie aus dem Dropdown-Menü **(Keine)**und klicken Sie dann auf **OK**.
4. Wenn Sie diesen Verschlüsselungsschlüssel vom Rapid Recovery Core entfernen möchten, müssen Sie die obigen Schritte für alle geschützten Maschinen wiederholen, die diesen Schlüssel verwenden. Führen Sie dann die unter dem Thema Entfernen eines Verschlüsselungsschlüssels beschriebenen Schritte durch.

Verwalten von Verschlüsselungsschlüsseln

Zum Verwalten von Verschlüsselungsschlüsseln für Rapid Recovery Core klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Verschlüsselungsschlüssel**. Die Seite **Verschlüsselungsschlüssel** wird angezeigt. Für jeden Verschlüsselungsschlüssel, der zu Rapid Recovery Core hinzugefügt wurde (sofern definiert), werden die in der folgenden Tabelle aufgeführten Informationen angezeigt.

Tabelle 38. Informationen für Verschlüsselungsschlüssel

UI-Element	Description
Ausgewähltes Element	Für jeden Verschlüsselungsschlüssel können Sie das Kontrollkästchen aktivieren, um Aktionen aus der Liste der Menüoptionen oberhalb der Tabelle auszuführen.
Name	Der Name für den Verschlüsselungsschlüssel.
Fingerabdruck	Dieser Parameter ist eine aus 26 Zeichen bestehende alphabetische Zeichenfolge aus zufallsgenerierten Groß- und Kleinbuchstaben des englischen Alphabets, die einen Verschlüsselungsschlüssel eindeutig kennzeichnet.
Typ	Der Status beschreibt den Ausgangspunkt eines Verschlüsselungsschlüssels und die Möglichkeit, den Schlüssel zu verwenden. Ein Verschlüsselungsschlüssel kann einen von zwei möglichen Typen aufweisen: **Universell**: Der Typ „Universell“ ist der Standardzustand, wenn ein Verschlüsselungsschlüssel erstellt wird. Ein Schlüssel vom Typ „Universell“ in Kombination mit dem Zustand „Entsperrt“ bedeutet, dass der Schlüssel auf eine geschützte Maschine angewendet werden kann. Sie können einen Schlüssel vom Typ „Universell“ nicht manuell sperren. Sie müssen vielmehr zuerst den Typ, wie unter Ändern von Verschlüsselungsschlüsseltypen beschrieben, ändern. **Replikation**. Wenn für eine geschützte Maschine in einem Quell-Core die Verschlüsselung aktiviert ist und Wiederherstellungspunkte der betreffenden Maschine auf einen Ziel-Core repliziert werden, weisen alle Verschlüsselungsschlüssel, die im Quell-Core verwendet werden, im Ziel-Core automatisch den Typ „Replikation“ auf. Der Standardzustand nach Erhalt eines replizierten Schlüssels ist gesperrt. Sie können einen Verschlüsselungsschlüssel des Typs „Replikation“ durch Angabe der Passphrase entsperren. Ein entsperrter Schlüssel kann manuell gesperrt werden. Weitere Informationen dazu finden Sie unter Entsperren eines Verschlüsselungsschlüssels.
Zustand	Der Zustand zeigt an, ob ein Verschlüsselungsschlüssel verwendet werden kann. Es gibt zwei mögliche Zustände: • **Entsperrt**. Der Zustand „Entsperrt“ zeigt an, dass der Schlüssel sofort verwendet werden kann. Sie können beispielsweise Snapshots für eine geschützte Maschine verschlüsseln oder Daten aus einem replizierten Wiederherstellungspunkt auf dem Ziel-Core wiederherstellen. • **Gesperrt**. Der Zustand „Gesperrt“ zeigt an, dass der Schlüssel erst verwendet werden kann, wenn er durch Angabe der Passphrase entsperrt wurde. Ein neu importierter oder replizierter Verschlüsselungsschlüssel ist standardmäßig gesperrt. Wenn ein Verschlüsselungsschlüssel gesperrt ist, muss er erst entsperrt werden, damit er verwendet werden kann. Wenn Sie einen zuvor gesperrten Verschlüsselungsschlüssel entsperrt haben und der Zeitraum abgelaufen ist, für den der Schlüssel entsperrt bleiben soll, ändert sich der Zustand von „Entsperrt“ in „Gesperrt“. Nachdem der Schlüssel automatisch gesperrt wurde, müssen Sie den Schlüssel wieder entsperren, damit er verwendet werden kann. Weitere Informationen dazu finden Sie unter Entsperren eines Verschlüsselungsschlüssels.
Description	Die Beschreibung ist ein optionales Feld, das ausgefüllt werden sollte, um nützliche Informationen zum Verschlüsselungsschlüssel anzugeben, z. B. beabsichtigte Verwendung oder Hinweis zur Passphrase.

Oben im Fensterbereich „Verschlüsselungsschlüssel“ können Sie einen Verschlüsselungsschlüssel hinzufügen oder einen Schlüssel über eine Datei importieren, die auf einem anderen Rapid Recovery Core exportiert wurde. Sie können auch in der Zusammenfassungstabelle ausgewählte Schlüssel löschen.

Sobald ein Verschlüsselungsschlüssel für einen Core vorhanden ist, können Sie die vorhandenen Schlüssel verwalten, indem Sie die Eigenschaften „Name“ oder „Beschreibung“ bearbeiten, die Passphrase ändern, einen gesperrten Verschlüsselungsschlüssel entsperren oder den Schlüssel aus dem Rapid Recovery Core entfernen. Sie können einen Schlüssel auch in eine Datei exportieren, die dann in einen anderen Rapid Recovery Core importiert werden kann.

Wenn Sie einen Verschlüsselungsschlüssel auf der Seite **Verschlüsselungsschlüssel** hinzufügen, wird er in der Liste der Verschlüsselungsschlüssel angezeigt, aber nicht für eine bestimmte geschützte Maschine verwendet. Informationen zum Anwenden eines Verschlüsselungsschlüssels, der im Fensterbereich **Verschlüsselungsschlüssel** erstellt wurde, oder zum vollständigen Löschen eines Schlüssels aus Rapid Recovery Core finden Sie unter Anwenden oder Entfernen von Verschlüsselungsschlüsseln.

Im Fensterbereich **Verschlüsselungsschlüssel** können Sie die Verschlüsselung für die im Core gespeicherten Sicherungsdaten aller geschützten Maschinen im Repository folgendermaßen verwalten:

- Hinzufügen eines Verschlüsselungsschlüssels
- Importieren eines Verschlüsselungsschlüssels
- Entsperren eines Verschlüsselungsschlüssels
- Bearbeiten eines Verschlüsselungsschlüssels
- Ändern der Passphrase für einen Verschlüsselungsschlüssel
- Exportieren eines Verschlüsselungsschlüssels
- Entfernen eines Verschlüsselungsschlüssels
- Ändern von Verschlüsselungsschlüsseltypen

Hinzufügen eines Verschlüsselungsschlüssels

Rapid Recovery verwendet 256-Bit-AES-Verschlüsselung im CBC-Modus (Cipher Block Chaining) mit 256-Bit-Schlüsseln. Obwohl die Verwendung der Verschlüsselung optional ist, wird von Quest dringend empfohlen, einen Verschlüsselungsschlüssel einzurichten und die festgelegte Passphrase zu schützen.

CAUTION: Bewahren Sie die Passphrase an einem sicheren Ort auf. Ohne eine Passphrase können Sie keine Daten aus verschlüsselten Wiederherstellungspunkten wiederherstellen.

Nachdem ein Verschlüsselungsschlüssel definiert wurde, können Sie damit Daten verschlüsseln. Verschlüsselungsschlüssel können für eine beliebige Anzahl geschützter Maschinen verwendet werden.

In diesem Abschnitt wird beschrieben, wie ein Verschlüsselungsschlüssel in der Rapid Recovery Core Console hinzugefügt wird. Der Schlüssel wird dabei nicht auf Maschinen angewendet, die derzeit im Core geschützt werden. Sie können einen Verschlüsselungsschlüssel auch hinzufügen, wenn Sie eine Maschine unter Schutz stellen. Weitere Informationen zum Hinzufügen eines Verschlüsselungsschlüssels, wenn eine Maschine unter Schutz gestellt wird, finden Sie unter Schützen einer Maschine. Weitere Informationen zum Hinzufügen eines Verschlüsselungsschlüssels, wenn zwei oder mehr Maschinen erstmals unter Schutz gestellt werden, finden Sie unter So schützen Sie mehrere Maschinen.

Führen Sie die folgenden Schritte aus, um einen Verschlüsselungsschlüssel hinzuzufügen.

1. Navigieren Sie zur Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Verschlüsselungsschlüssel**.

   Die Seite **Verschlüsselungsschlüssel** wird angezeigt.
3. Klicken Sie auf **Verschlüsselungsschlüssel hinzufügen**.

Das Dialogfeld **Verschlüsselungsschlüssel erstellen** wird angezeigt.

4. Geben Sie im Dialogfeld **Verschlüsselungsschlüssel erstellen** die in der folgenden Tabelle beschriebenen Details für den Schlüssel ein.

Tabelle 39. Details zum Erstellen eines Verschlüsselungsschlüssels

Textfeld	Description
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein. Namen für Verschlüsselungsschlüssel müssen 1 bis 64 alphanumerische Zeichen umfassen. Verwenden Sie keine unzulässigen Zeichen oder unzulässigen Phrasen.
Description	Geben Sie eine Anmerkung für den Verschlüsselungsschlüssel ein. Diese Informationen werden im Beschreibungsfeld angezeigt, wenn Verschlüsselungsschlüssel in der Core Console angezeigt werden. Sie können bis zu 254 Zeichen eingeben. Es hat sich bewährt, die Verwendung von unzulässigen Zeichen und unzulässigen Phrasen zu vermeiden.
Passphrase	Geben Sie eine Passphrase für die Zugriffssteuerung ein. Sie sollten keine unzulässigen Zeichen verwenden. **CAUTION: Bewahren Sie die Passphrase an einem sicheren Ort auf.Der Quest Support kann eine Passphrase nicht wiederherstellen. Wenn Sie einen Verschlüsselungsschlüssel erstellt und für eine geschützte Maschine verwendet haben, können Sie keine Daten dieser geschützten Maschine mehr wiederherstellen, wenn die Passphrase verloren geht.**
Passphrase bestätigen	Geben Sie die Passphrase erneut ein. Dies wird zur Bestätigung der Passphraseneingabe verwendet.

5. Klicken Sie auf **OK**.

   Das Dialogfeld wird geschlossen und der erstellte Verschlüsselungsschlüssel wird auf der Seite „Verschlüsselungsschlüssel“ angezeigt.

6. Informationen zum Anwenden des Verschlüsselungsschlüssels auf eine geschützte Maschine finden Sie unter Anwenden eines Verschlüsselungsschlüssels auf der Seite „Geschützte Maschinen“.

Importieren eines Verschlüsselungsschlüssels

Sie können einen Verschlüsselungsschlüssel von einem anderen Rapid Recovery Core importieren und damit Daten für eine geschützte Maschine in Ihrem Core verschlüsseln. Um den Schlüssel importieren zu können, müssen Sie auf der Core-Maschine lokal oder über das Netzwerk auf den Schlüssel zugreifen können. Sie müssen auch die Passphrase für den Verschlüsselungsschlüssel kennen.

Führen Sie die folgenden Schritte aus, um einen Verschlüsselungsschlüssel zu importieren.

NOTE: Der Schlüssel wird dabei nicht auf geschützte Maschinen angewendet. Weitere Informationen zum Anwenden von Verschlüsselungsschlüsseln finden Sie unter Anwenden eines Verschlüsselungsschlüssels auf der Seite „Geschützte Maschinen“.

1. Navigieren Sie zum Rapid Recovery Core.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Verschlüsselungsschlüssel**.

Die Seite **Verschlüsselungsschlüssel** wird angezeigt.

3. Klicken Sie auf **Importieren**.

   Das Dialogfeld **Datei hochladen** wird angezeigt.

4. Im Dialogfeld **Datei hochladen** navigieren Sie zu dem Netzwerk- oder lokalen Verzeichnis, mit dem Verschlüsselungsschlüssel, den Sie importieren möchten.

   Navigieren Sie zum Beispiel zu dem Ordner **Downloads** für den angemeldeten Benutzer.

   Der Schlüsseldateiname beginnt „EncryptionKey-“ mit der Schlüssel-ID dahinter und endet mit der Dateierweiterung „.key“. Ein Beispiel für den Namen eines Verschlüsselungsschlüssels ist beispielsweise EncryptionKey-RandomAlphabeticCharacters.key.

5. Wählen Sie den Schlüssel aus, den Sie importieren möchten, und klicken Sie dann auf **Öffnen**.
6. Klicken Sie im Dialogfeld **Schlüssel importieren** auf **OK**.

   Das Dialogfeld wird geschlossen und der importierte Verschlüsselungsschlüssel wird auf der Seite **Verschlüsselungsschlüssel** angezeigt. Wenn der Verschlüsselungsschlüssel vor dem Export zum Verschlüsseln eines Volumes verwendet wurde, ist der Schlüsselt gesperrt.

Entsperren eines Verschlüsselungsschlüssels

Verschlüsselungsschlüssel haben den Status entsperrt oder gesperrt. Ein entsperrter Verschlüsselungsschlüssel kann auf eine geschützte Maschine angewendet werden, um die Sicherungsdaten, die für diese Maschine im Repository gespeichert wurden, abzusichern. Auf einem Rapid Recovery Core können Sie mit einem entsperrten Verschlüsselungsschlüssel auch Daten aus einem Wiederherstellungspunkt wiederherstellen.

Wenn Sie einen Verschlüsselungsschlüssel in einen Rapid Recovery Core importieren, ist dieser standardmäßig gesperrt. Dies gilt unabhängig davon, ob der Schlüssel explizit importiert wurde oder ob der Verschlüsselungsschlüssel durch Replikation verschlüsselter geschützter Maschinen oder Import eines Archivs mit verschlüsselten Wiederherstellungspunkten zum Rapid Recovery Core hinzugefügt wurde.

Bei Verschlüsselungsschlüsseln, die lediglich durch Replikation zum Rapid Recovery Core hinzugefügt wurden, können Sie beim Entsperren eines Schlüssels einen Zeitraum (in Stunden, Tagen oder Monaten) angeben, für den der Verschlüsselungsschlüsse entsperrt bleiben soll. Jedem Tag liegt ein Zeitraum von 24 Stunden zugrunde, beginnend mit dem Zeitpunkt, an dem die Entsperranforderung im Rapid Recovery Core gespeichert wurde. Wenn der Schlüssel beispielsweise um 11:24 Uhr am Dienstag entsperrt wird und als Dauer 2 Tage ausgewählt wird, wird der Schlüssel am Donnerstag um 11:24 Uhr automatisch wieder gesperrt.

NOTE: Sie können einen gesperrten Verschlüsselungsschlüssel nicht für die Wiederherstellung von Daten auf einer geschützten Maschine verwenden. Sie müssen zuerst die Passphrase eingeben und dadurch den Schlüssel entsperren.

Sie können auch einen entsperrten Verschlüsselungsschlüssel sperren und so sicherstellen, dass er nicht auf eine geschützte Maschine angewendet werden kann, bis er wieder entsperrt wird. Um einen Verschlüsselungsschlüssel mit dem Status „Universell“ zu sperren, müssen Sie zuerst den Typ in „Repliziert“ ändern.

Wenn ein entsperrter Verschlüsselungsschlüssel derzeit zum Schutz einer Maschine im Core verwendet wird, müssen Sie zunächst diesen Verschlüsselungsschlüssel von der geschützten Maschine trennen, bevor Sie ihn sperren können.

Führen Sie die folgenden Schritte aus, um einen gesperrten Verschlüsselungsschlüssel zu entsperren.

1. Navigieren Sie zum Rapid Recovery Core.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Verschlüsselungsschlüssel**.

Die Seite **Verschlüsselungsschlüssel** wird angezeigt. Die Spalte „Status“ zeigt an, welche Schlüssel gesperrt sind.

3. Ermitteln Sie den Verschlüsselungsschlüssel, den Sie entsperren möchten, klicken Sie auf sein Drop-Down-Menü und wählen Sie **Entsperren**.

   Das Dialogfeld **Verschlüsselungsschlüssel entsperren** wird angezeigt.

4. Geben Sie im Dialogfeld im Feld „Passphrase“ die Passphrase zum Entsperren des Schlüssels ein.
5. Um die Länge der Zeit einzugeben, in der der Schlüssel entsperrt bleibt, führen Sie unter der Option „Dauer“ einen der folgenden Schritte aus:

   - Um anzugeben, dass der Schlüssel in Rapid Recovery entsperrt bleibt, bis Sie ihn explizit sperren, wählen Sie **Bis manuell gesperrt** aus.
   - Um festzulegen, dass der Schlüssel für eine Dauer, die Sie in Stunden, Tagen oder Monaten konfigurieren, gesperrt bleibt, gehen Sie wie folgt vor:
     - Wählen Sie das Zahlenfeld aus und geben Sie einen Wert zwischen 1 und 999 ein.
     - Geben Sie an, ob es sich bei der Zahl um Stunden, Tage oder Monate handelt.
     - Klicken Sie anschließend auf **OK**.

     Diese Option steht für Verschlüsselungsschlüssel zur Verfügung, die durch Replikation hinzugefügt wurden.
     Das Dialogfeld wird geschlossen und die Änderungen des ausgewählten Verschlüsselungsschlüssels werden auf der Seite „Verschlüsselungsschlüssel“ angezeigt.
   - Um festzulegen, dass der Schlüssel bis zu dem Datum und der Uhrzeit gesperrt bleibt, die Sie vorgeben, gehen Sie wie folgt vor:
     - Wählen Sie die Option **Bis** aus.
     - Geben Sie mithilfe des Textfelds oder unter Verwendung von Kalender- und Uhr-Widget explizit das Datum und die Uhrzeit an, bis zu dem/der der Verschlüsselungsschlüssel gesperrt bleiben soll.
     - Klicken Sie anschließend auf **OK**.

     Diese Option steht für Verschlüsselungsschlüssel zur Verfügung, die durch Replikation hinzugefügt wurden.
     Das Dialogfeld wird geschlossen und die Änderungen des ausgewählten Verschlüsselungsschlüssels werden auf der Seite „Verschlüsselungsschlüssel“ angezeigt.

Sperren eines Verschlüsselungscodes

Wenn ein Verschlüsselungsschlüssel-Zustand gesperrt ist, kann er nicht mehr auf eine beliebige Maschine angewendet werden, bis er entsperrt ist. Um einen Verschlüsselungsschlüssel mit dem Typ „Universell“ zu sperren, müssen Sie zuerst den Typ in „Repliziert“ ändern.

Führen Sie die folgenden Schritte aus, um einen Verschlüsselungsschlüssel zu sperren.

1. Navigieren Sie zum Rapid Recovery Core.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Verschlüsselungsschlüssel**.

   Die Seite **Verschlüsselungsschlüssel** wird angezeigt. In der Spalte „Zustand“ wird angezeigt, welche Verschlüsselungsschlüssel entsperrt sind. Darüber hinaus wird der Typ für jeden Schlüssel angezeigt.
3. Ermitteln Sie den Verschlüsselungsschlüssel, den Sie sperren wollen. Wenn der Typ „Universell“ ist, klicken Sie auf dessen Drop-Down-Menü und wählen Sie **Typ auf „Repliziert“ ändern**.

Das Dialogfeld **Verschlüsselungsschlüssel-Typ ändern** wird angezeigt.

4. Bestätigen Sie im Dialogfeld, dass Sie den Schlüsseltyp auf **Repliziert** ändern möchten.
5. Wenn Sie den Verschlüsselungsschlüssel-Status erfolgreich auf „Repliziert“ geändert haben, klicken Sie auf dessen Drop-Down-Menü ••• und wählen Sie **Sperren**.

   Das Dialogfeld **Verschlüsselungsschlüssel sperren** wird angezeigt.
6. Bestätigen Sie im Dialogfeld, dass der Schlüssel gesperrt werden soll.

   Das Dialogfeld wird geschlossen. Der Status des ausgewählten Verschlüsselungsschlüssels ist jetzt „gesperrt“.

NOTE: Diese Option steht für Verschlüsselungsschlüssel zur Verfügung, die durch Replikation hinzugefügt wurden.

Bearbeiten eines Verschlüsselungsschlüssels

Nachdem ein Verschlüsselungsschlüssel definiert wurde, können Sie den Namen des Verschlüsselungsschlüssels oder die Beschreibung des Schlüssels bearbeiten. Diese Eigenschaften werden in der Liste der Verschlüsselungsschlüssel im Fenster „Verschlüsselungsschlüssel“ angezeigt.

Führen Sie die folgenden Schritte aus, um Name oder Beschreibung eines vorhandenen Verschlüsselungsschlüssels zu bearbeiten.

CAUTION: Nachdem Sie den Namen oder die Beschreibung eines Verschlüsselungsschlüssels bearbeitet haben, der zum Schutz einer oder mehrerer Maschinen dient, erfasst Rapid Recovery ein neues Basisabbild. Dieser Basis-Image-Snapshot tritt für diese Maschine beim nächsten geplanten oder erzwungenen Snapshot auf.

1. Navigieren Sie zum Rapid Recovery Core.
2. Klicken Sie auf der Symbolleiste auf ••• (Mehr) und wählen Sie dann **Verschlüsselungsschlüssel**.

   Die Seite **Verschlüsselungsschlüssel** wird angezeigt.
3. Ermitteln Sie den Verschlüsselungsschlüssel, den Sie bearbeiten möchten und führen Sie die folgenden Schritte aus:
   - Wenn der Schlüssel gesperrt ist, müssen Sie diesen zuerst entsperren. Siehe Entsperren eines Verschlüsselungsschlüssels.
   - Wenn der Schlüssel nicht gesperrt ist, gehen Sie wie unten beschrieben vor.
4. Klicken Sie auf das Drop-Down-Menü ••• für den angegebenen Verschlüsselungsschlüssel und wählen Sie **Bearbeiten**.

   Das Dialogfeld **Verschlüsselungsschlüssel bearbeiten** wird angezeigt.
5. Bearbeiten Sie im Dialogfeld den Namen oder die Beschreibung des Verschlüsselungsschlüssels und klicken Sie dann auf **OK**.

   Das Dialogfeld wird geschlossen und die Änderungen des ausgewählten Verschlüsselungsschlüssels werden auf der Seite **Verschlüsselungsschlüssel** angezeigt.

Ändern der Passphrase für einen Verschlüsselungsschlüssel

Sie können die Passphrase für einen vorhandenen Verschlüsselungsschlüssel ändern, um eine möglichst hohe Sicherheit zu gewährleisten. Führen Sie die nachstehend beschriebenen Schritte aus, um die Passphrase für einen Verschlüsselungsschlüssel zu ändern.

CAUTION: Nachdem die Passphrase eines Verschlüsselungsschlüssels geändert wurde, mit dem geschützte Maschinen verschlüsselt werden, erfasst Rapid Recovery Core beim nächsten geplanten oder erzwungenen Snapshot einen inkrementellen Snapshot für diese Maschine.

1. Navigieren Sie zum Rapid Recovery Core.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Verschlüsselungsschlüssel**.

   Die Seite **Verschlüsselungsschlüssel** wird angezeigt.
3. Ermitteln Sie den Verschlüsselungsschlüssel, den Sie aktualisieren möchten, klicken Sie auf sein Drop-Down-Menü und wählen Sie **Passphrase ändern**.

   Das Dialogfeld **Passphrase ändern** wird angezeigt.
4. Geben Sie im Dialogfeld im Feld **Passphrase** , die neue Passphrase für die Verschlüsselung ein.
5. Geben Sie in dem Feld **Passphrase bestätigen** die identische Passphrase erneut ein.
6. Klicken Sie auf **OK**.

   Das Dialogfeld wird geschlossen und die Passphrase wird aktualisiert.
7. Wenn Sie optional einen Hinweis im Feld „Beschreibung“ verwenden, bearbeiten Sie den Verschlüsselungsschlüssel für die Aktualisierung des Hinweises. Weitere Informationen hierzu finden Sie unter Bearbeiten eines Verschlüsselungsschlüssels.

CAUTION: Rapid Recovery verwendet 256-Bit-AES-Verschlüsselung im CBC-Modus (Cipher Block Chaining) mit 256-Bit-Schlüsseln. Quest empfiehlt, dass Sie die Passphrase an einem sicheren Ort notieren und diese Informationen aktualisiert halten. Der Quest Support kann eine Passphrase nicht wiederherstellen. Ohne die Passphrase können Sie keine Informationen von verschlüsselten Wiederherstellungspunkten wiederherstellen.

Exportieren eines Verschlüsselungsschlüssels

Sie können einen Verschlüsselungsschlüssel von jedem Rapid Recovery Core exportieren, damit er auf einem anderen Core verwendet werden kann. Der Schlüssel wird dabei im Ordner **Downloads** des aktiven Windows-Benutzerkontos gespeichert.

Führen Sie die folgenden Schritte aus, um einen Verschlüsselungsschlüssel zu exportieren.

1. Navigieren Sie zum Rapid Recovery Core.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Verschlüsselungsschlüssel**.

   Die Seite **Verschlüsselungsschlüssel** wird angezeigt.
3. Ermitteln Sie den Verschlüsselungsschlüssel, den Sie exportieren möchten, klicken Sie auf sein Drop-Down-Menü und wählen Sie **Exportieren**.

   Das Dialogfeld **Verschlüsselungsschlüssel-[name.key] öffnen** wird angezeigt.
4. Klicken Sie im Dialogfeld auf **Datei speichern**, um die Verschlüsselungsschlüssel an einem sicheren Speicherort abzulegen und klicken Sie auf **OK**.

   Der Verschlüsselungsschlüssel wird als Textdatei in das Standardverzeichnis heruntergeladen, wie z. B. den Ordner **Downloads** des aktiven Windows-Benutzerkontos.
5. Wenn Sie ggf. diesen Schlüssel in einen anderen Core importieren möchten, kopieren Sie die Datei an einen Speicherort, der von diesem Core zugänglich ist.

Entfernen eines Verschlüsselungsschlüssels

Wenn Sie einen Verschlüsselungsschlüssel von der Seite „Verschlüsselungsschlüssel“ entfernen, wird der Schlüssel vom Rapid Recovery Core entfernt.

NOTE: Durch das Entfernen eines Verschlüsselungsschlüssels werden die bereits unter Verwendung des Schlüssels gespeicherten Wiederherstellungspunkte nicht entschlüsselt. Sie müssen die Passphrase für den Schlüssel trotzdem aufbewahren, um Daten für vorhandene verschlüsselte Wiederherstellungspunkte wiederherstellen zu können.

Sie können keinen Verschlüsselungsschlüssel entfernen, der bereits einer geschützten Maschine zugeordnet ist. Sie müssen zuerst die Verschlüsselungseinstellungen der geschützten Maschinen anzeigen, die den Schlüssel verwenden, und die Zuordnung des Verschlüsselungsschlüssels aufheben, der entfernt werden soll. Weitere Informationen dazu finden Sie unter Aufheben der Verschlüsselungsschlüsselzuordnung für eine geschützte Maschine.

Führen Sie die folgenden Schritte aus, um einen Verschlüsselungsschlüssel zu entfernen.

1. Navigieren Sie zum Rapid Recovery Core.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Verschlüsselungsschlüssel**.

   Die Seite **Verschlüsselungsschlüssel** wird angezeigt.
3. Machen Sie den Verschlüsselungscode ausfindig, den Sie entfernen möchten. Klicken Sie auf sein Drop-Down-Menü und wählen Sie **Entfernen**.

   Das Dialogfeld **Verschlüsselungsschlüssel entfernen** wird angezeigt. Daraufhin wird eine Meldung mit der Bestätigung angezeigt, dass der Verschlüsselungsschlüssel entfernt wird.
4. Bestätigen Sie im Dialogfeld, dass der Verschlüsselungsschlüssel entfernt werden soll.

   NOTE: Durch das Entfernen eines Verschlüsselungsschlüssels werden die bereits unter Verwendung des Schlüssels gespeicherten Wiederherstellungspunkte nicht entschlüsselt. Sie müssen den Schlüssel trotzdem aufbewahren, um Daten für vorhandene verschlüsselte Wiederherstellungspunkte wiederherstellen zu können.

   Das Dialogfeld wird geschlossen und der entfernte Verschlüsselungsschlüssel wird nicht mehr auf der Seite **Verschlüsselungsschlüssel** angezeigt.

Ändern von Verschlüsselungsschlüsseltypen

Verschlüsselungsschlüssel listen im Fensterbereich „Verschlüsselungsschlüssel“ einen von zwei möglichen Typen: Universell oder Replikation. Der Typ gibt die wahrscheinliche Herkunft des Verschlüsselungsschlüssels an und bestimmt, ob Details oder Passphrase geändert werden können. Sie können diese Attribute nur ändern, wenn der Typ „Universell“ ist. Wenn Sie diese Attribute für einen Schlüssel mit dem Status „Repliziert“ ändern müssen, müssen Sie die folgenden Schritte durchführen und den Typ in „Universell“ ändern. Wenn Sie den Typ eines Verschlüsselungsschlüssels in „Universell“ ändern, wird er manuell entsperrt und kann zum Verschlüsseln anderer geschützter Maschinen verwendet werden.

NOTE: Sie müssen die Passphrase kennen, um den Status von „Repliziert“ in „Universell“ ändern zu können.

Verschlüsselungsschlüssel weisen außerdem zwei mögliche Zustände auf: gesperrt oder entsperrt. Der Zustand beeinflusst die Möglichkeit, einen Verschlüsselungsschlüssel auf eine geschützte Maschine anzuwenden oder Daten aus einem Wiederherstellungspunkt mit Verschlüsselung wiederherzustellen. Sie können den Typ eines Verschlüsselungsschlüssels nur manuell ändern, wenn er entsperrt ist.

Wenn Sie einen Verschlüsselungsschlüssel erstellen, ist der Typ „Universell“ und der Status ist entsperrt. Sie können einen solchen Schlüssel sofort verwenden (z. B., um Sicherungen für eine geschützte Maschine zu verschlüsseln). Jedoch kann ein universeller Schlüsseltyp nicht manuell gesperrt werden. Wenn Sie einen Verschlüsselungsschlüssel mit dem Typ „Universell“ manuell sperren möchten, müssen Sie zuerst die folgenden Schritte durchführen und den Typ in „Repliziert“ ändern.

Sie können einen Verschlüsselungsschlüssel nicht ändern, wenn er bereits zum Verschlüsseln von Wiederherstellungspunkten für eine oder mehrere geschützte Maschine verwendet wird.

Verwenden Sie dieses Verfahren zum Ändern eines Schlüsseltyps.

1. Navigieren Sie zum Rapid Recovery Core.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Verschlüsselungsschlüssel**.

   Die Seite **Verschlüsselungsschlüssel** wird angezeigt. Alle auf dem Core verfügbaren Verschlüsselungsschlüssel werden in der Zusammenfassungstabelle angezeigt. Jede listet einen Typ „Universell“ oder „Repliziert“.
3. Ermitteln Sie den Verschlüsselungsschlüssel, den Sie aktualisieren wollen.
4. Wenn Sie einen universellen Verschlüsselungsschlüssel auf „Replikation“ ändern möchten, gehen Sie wie folgt vor:
   a. Klicken Sie auf sein Drop-Down-Menü und wählen Sie **Typ auf „Repliziert“ ändern**.

   Das Dialogfeld **Verschlüsselungsschlüssel-Typ ändern** wird angezeigt. Sie sehen eine Meldung, die bestätigt, dass Sie den Typ auf „Repliziert“ ändern möchten.

   - Bestätigen Sie im Dialogfeld, dass Sie den Schlüsseltyp auf „Repliziert“ ändern möchten.

   Das Dialogfeld wird geschlossen, und der Verschlüsselungsschlüsseltyp wird auf „Replikation“ aktualisiert.
5. Wenn Sie einen universellen Replikations-Verschlüsselungsschlüssel auf „Universell“ ändern möchten, gehen Sie wie folgt vor:
   a. Klicken Sie auf sein Drop-Down-Menü und wählen Sie **Typ auf „Universell“ ändern**.

   Das Dialogfeld **Verschlüsselungsschlüssel-Typ ändern** wird angezeigt. Sie sehen eine Meldung, die bestätigt, dass Sie den Typ auf „Universell“ ändern möchten.

   - Geben Sie im Dialogfeld im Feld **Passphrase** die Passphrase ein und klicken Sie auf **OK**, um zu bestätigen, dass Sie den Typ auf „Universell“ ändern möchten.

   Das Dialogfeld wird geschlossen, und der Verschlüsselungsschlüsseltyp wird auf „Universell“ aktualisiert.

Schützen von Maschinen

In diesem Kapitel wird beschrieben, wie geschützte Maschinen in der Rapid Recovery-Umgebung geschützt, konfiguriert und verwaltet werden.

Informationen über den Schutz von Maschinen mit Rapid Recovery

Zum Schutz Ihrer Daten bei Verwenden von Rapid Recovery müssen Sie die Arbeitsstationen, Server, Desktop- und Laptop-Computer, die Sie schützen möchten, Rapid Recovery Core hinzufügen.

In Rapid Recovery Core Console können Sie mithilfe eines der Assistenten zum Schutz von Maschinen die Maschinen identifizieren, die Sie schützen möchten. Sie können auf Folgendes zugreifen:

- eine einzelne Maschine über den Assistenten zum Schutz von Maschinen schützen, über den die Maschine über Netzwerk-Hostnamen oder IP-Adresse verbunden ist. Weitere Informationen zum Schützen einer einzelnen Maschine finden Sie unter Schützen einer Maschine.
- Sie können ein Netzwerk-Cluster über den Assistenten „Cluster schützen“ schützen, über den das Cluster und seine Knoten über Netzwerk-Hostnamen oder IP-Adresse verbunden sind. Weitere Informationen über das Schützen eines Clusters finden Sie unter Schützen eines Clusters.
- Sie können mit dem Assistenten zum Schützen mehrerer Maschinen mehrere Maschinen gleichzeitig schützen. Mit diesem Assistenten können Sie Maschinen, die mit einem Microsoft Active Directory-Server, Maschinen auf einem vCenter- oder ESXi-Host oder Maschinen auf einem Hyper-V-Host oder eine Hyper-V-Cluster verknüpft sind, miteinander verbinden. Sie können auch manuell Verbindungsinformationen (Hostnamen oder IP-Adresse des Netzwerks, Benutzername und Kennwort) für mehrere Maschinen eingeben. Weitere Informationen über das Schützen von mehreren Maschinen finden Sie unter So schützen Sie mehrere Maschinen.

NOTE: Quest empfiehlt, die Anzahl Maschinen, die Sie gleichzeitig schützen möchten, auf 50 oder weniger zu beschränken, um Ressourceneinschränkungen zu verhindern, die dazu führen können, dass der Schutzvorgang fehlschlägt.

Bei der Ermittlung Ihrer Anforderungen für den Schutz für eine einzelne Maschine im Assistenten können Sie festlegen, welche Volumes geschützt werden sollen. Wenn Sie Sie mehrere Maschinen schützen, werden standardmäßig alle Volumes geschützt. (Sie können dieses später auf einer individuellen Maschinenbasis ändern).

Beim Schutz einer virtuellen Maschine auf einem vCenter-/ESXi- oder Hyper-V-Host muss definiert werden, ob die Maschine mithilfe der Funktion Rapid Snap for Virtual oder durch die Installation von Rapid Recovery Agent geschützt werden soll. Weitere Informationen hierzu finden Sie unter Faktoren bei der Wahl zwischen agentenbasiertem und agentenlosem Schutz.

Mit dem Assistenten können Sie auch einen benutzerdefinierten Schutzzeitplan definieren (oder einen vorhandenen Zeitplan erneut verwenden).

Mit den erweiterten Optionen können Sie für die Maschinen, die Sie schützen möchten zusätzliche Sicherheitsmaßnahmen hinzufügen, und zwar durch Festlegen oder Anwenden eines Verschlüsselungsschlüssels für Sicherungen.

Schließlich können Sie, falls noch keines vorhanden ist, ein Repository mithilfe des Assistenten definieren.

Nach der Installation der Agentensoftware, muss jede Maschine nach der Installation neu gestartet werden.

Weitere Informationen zum Schützen von Arbeitsstationen und Servern finden Sie unter Schützen einer Maschine.

Faktoren bei der Wahl zwischen agentenbasiertem und agentenlosem Schutz

Die Rapid Snap for Virtual Funktion von Rapid Recovery wird auf vCenter/ESXi- oder auf Hyper-V-Hypervisors unterstützt. Mit dieser Funktion, die auch als agentenloser Schutz bekannt ist, können Sie virtuelle Maschinen (VMs) in Ihrem Core schützen, ohne die Rapid Recovery Agent Software auf jedem Gastcomputer installieren zu müssen.

Allgemeine Empfehlungen

Mit Version 6.2 ist die Rapid Snap for Virtual Funktion von Rapid Recovery fast gleichwertig zu einem Schutz durch Installation der Rapid Recovery Agent Software. Als allgemeine Regel empfiehlt Quest die Verwendung des agentenlosen Schutzes auf virtuellen ESXi- oder Hyper-V-Maschinen. Wenn die Agenten-Software auf ESXi- oder Hyper-V-VMs installiert ist und es keinen zwingenden Grund gibt, Ihre VM mithilfe von Rapid Recovery Agent zu schützen, empfiehlt Quest, den Agenten zu entfernen und die VMs agentenlos zu schützen.

Der agentenlose Schutz hat einige Vorteile und einige Einschränkungen. Diese werden im Thema Grundlegende Informationen zu Rapid Snap for Virtual ausführlich behandelt.

Ausnahmen von der Empfehlung zur Verwendung des agentenlosen Schutzes sind:

- Das Erheben von Metadaten ist bei agentenlosen Maschinen langsamer als bei Maschinen, die von der Rapid Recovery Agent Software geschützt werden. Wenn Probleme mit der Leistung in Zusammenhang mit Metadaten (insbesondere bei Exchange Server- oder SQL-Server-Maschinen mit agentenlosem Schutz) auftreten, empfiehlt Quest Datenschutz-Support eventuell eine Installation des softwarebasierten Agenten auf bestimmten Anwendungsservern zum Zweck der Fehlerbehebung.
- Beim Schutz von nur einer oder zwei VMs auf einem Hypervisor mit mehreren Steckplätzen werden ggf. weniger Lizenzen verbraucht, wenn der Agent direkt auf den VMs anstelle auf dem Host installiert wird.
- Wenn Sie Funktionen benötigen, die nur bei Rapid Recovery Agent verfügbar sind, installieren Sie die Agenten-Software auf den entsprechenden VMs.

Einige Funktionen sind nur beim Schutz durch Installation der Rapid Recovery Agent Software verfügbar. Nachfolgend einige Beispiele:

- Das Ausführen einer SQL-Anfügbarkeitsprüfung ist eine Funktion der Rapid Recovery Agent Software. Wenn der Schutz Ihrer SQL-Server-Maschine agentenlos ist, müssen Sie SQL-Anfügbarkeitsprüfungen mit einer Instanz des SQL-Servers ausführen, die auf dem Core-Server installiert ist. Um diese Prüfung durchzuführen, müssen Sie die Anfügbarkeitseinstellung des Core zu **SQL Server des Core verwenden** ändern.
- Dynamische Volumes, die agentenlos geschützt werden, werden auf Datenträgerebene und nicht auf Volume-Ebene geschützt.
- Live Recovery ist eine Funktion der Rapid Recovery Agent Software. Sie können diese Funktion nicht beim Wiederherstellen von Volumes verwenden, die mit Rapid Snap for Virtual geschützt sind.

Wenn Sie eine der Funktionen, die in der vorherigen Liste für eine bestimmte VM beschrieben sind, benötigen, empfiehlt Quest die Installation des Agenten anstatt des agentenlosen Schutzes der VM.

Weitere Informationen dazu finden Sie unter Grundlegende Informationen zu Rapid Snap for Virtual.

Lizenzverbrauchskonzepte Version 6.2

Rapid RecoveryVersion 6.2 verwendet nicht mehr spezifische Lizenzpools für Windows Server, Hyper-V-Hosts, VMware-Steckplätze, Exchange Server, SQL-Server, Linux-Server und so weiter. Das neue Modell ist stark vereinfacht.

Wie im Thema Verwalten von Lizenzen beschrieben, verwendet Rapid Recovery Version 6.2 nur zwei Lizenzpools: Kapazität und Enterprise. Wenn Sie für die Lizenzierung Ihres Core einen kapazitätsbasierten Pool verwenden, können Sie keinen anderen Pooltyp verwenden.

NOTE: In Zukunft plant Quest Lizenzpools hinzuzufügen, die auf anderen Maßeinheiten basieren. Kapazitäts- und Enterprise-Pools werden weiterhin unterstützt.

DL-Appliances nutzen eine kapazitätsbasierte Lizenzierung und sind nicht durch Lizenzpooleinschränkungen betroffen. In softwarebasierten Rapid Recovery Umgebungen mit Frontend-Kapazitäts-Lizenzierung ergeben sich ebenfalls keine Lizenzvorteile aus der Verwendung von agentenlosem Schutz. Weitere Vorteile bei Verwendung von agentenlosem Schutz sind auch bei Verwendung von Kapazitäts-Lizenzpools relevant.

Wenn Sie in Ihrer Rapid Recovery Version 6.2 Umgebung einen Enterprise-Lizenzpool verwenden, dann gelten die folgenden Regeln:

- Hyper-V- oder vCenter-/ESXi-Hypervisor-Hosts, die mit Rapid Recovery Agent geschützt sind, verbrauchen eine Lizenz aus dem Pool pro Prozessorsteckplatz. Wenn Ihr Hypervisor-Host sechs CPU-Steckplätze aufweist, verbraucht er 6 Lizenzen aus dem Enterprise-Pool.
- Jede andere Maschine (physisch oder virtuell), die in Ihrem Core mit Rapid Recovery Agent geschützt ist, verbraucht eine Lizenz aus diesem Pool. Dies gilt auch für Anwendungsserver (z. B. Exchange Server, SQL-Server oder Oracle Datenbank 12c) mit mehreren CPU-Steckplätzen.

Lizenzierungsvorteile bei Verwendung von agentenlosem Schutz

Sie können Gast-VMs auf einem vCenter-/ESXi-Hypervisor-Host schützen, indem Sie den Assistenten zum Schützen mehrerer Maschinen ausführen. Wenn Sie auf der Seite **Verbindung** dieses Assistenten **Ausgewählte VMs ohne Agenten schützen** auswählen, werden die Gast-VMs auf diesem Host ohne Agenten geschützt. Für diese VMs werden keine Lizenzen aus dem Lizenzpool verbraucht. Wenn Rapid Recovery Agent nicht auf dem Host installiert ist, wird durch Hinzufügen dieses Hosts zu Ihrem Core eine Lizenz für jeden CPU-Steckplatz verbraucht.

Wenn Sie einen Hyper-V-Server schützen, wird Rapid Recovery Agent auf dem Host installiert. Für jeden CPU-Steckplatz auf dem Hypervisor-Host wird eine Lizenz aus Ihrem Enterprise-Pool verbraucht. Wenn Sie angeben, dass der Schutz des Hyper-V-Servers agentenlos sein soll, werden Gast-VMs agentenlos geschützt, und für diese VMs werden keine Lizenzen aus dem verfügbaren Lizenzpool verbraucht.

Wenn Sie ein Hyper-V-Cluster schützen, wird Rapid Recovery Agent auf jedem Knoten im Cluster installiert. Nur eine einzelne Lizenz aus dem Lizenzpool wird verbraucht. Die Gesamtanzahl der CPU-Steckplätze im Cluster wird verbraucht. Wenn Sie angeben, dass der Schutz des Hyper-V-Clusters agentenlos sein soll, werden Gast-VMs agentenlos geschützt, und für diese VMs werden keine Lizenzen aus dem auf dem Cluster verfügbaren Lizenzpool verbraucht.

Der Hauptlizenzvorteil bei Verwendung von Rapid Snap for Virtual besteht in der Verringerung des Verbrauchs von Lizenzen aus Ihrem Enterprise-Lizenzpool für die VMs, die Sie schützen. Wenn Sie einen agentenlosen Schutz für einen ESXi-Hypervisor-Host oder einen Hyper-V-Server oder ein Hyper-V-Cluster angeben, werden alle neuen virtuellen Maschinen, die auf dem Host erstellt werden, automatisch agentenlos geschützt und verbrauchen keine Lizenzen aus Ihrem Enterprise-Lizenzpool.

Wenn auf einigen der VMs auf diesem Hypervisor-Host schon vorher Rapid Recovery Agent installiert war und der Core Rapid Recovery Version 6.2 ausführt, sollten Sie einen der folgenden Schritte ausführen:

- Entfernen Sie die Agenten-Software, um die VM ohne den Einsatz von Agenten zu schützen. Keine Lizenzen aus Ihrem Pool werden verbraucht.
- Fügen Sie manuell die Maschine zum agentenlosen Schutz hinzu.
- Wenn die Maschine durch einen Agenten geschützt werden soll und der Host zum Core hinzugefügt wird, ordnen Sie die VM dem übergeordneten Host zu. Sie erhalten die Vorteile eines agentenbasierten Schutzes, es wird aber keine Lizenz verbraucht.
- Nehmen Sie keine Änderungen vor. Die VM wird mit Hilfe der APIs in Rapid Recovery Agent geschützt und eine einzelne Lizenz wird verbraucht.

Jede virtuelle Maschine auf einem Hypervisor, der dem Core hinzugefügt wird, wird ohne den Einsatz von Agenten und ohne Verbrauchen einer Lizenz geschützt. Um diesen Vorteil zu erhalten, müssen Sie Folgendes tun:

Der Hauptlizenzvorteil bei Verwendung von Rapid Snap for Virtual besteht in der Verringerung des Verbrauchs von Lizenzen aus Ihrem Enterprise-Lizenzpool für die VMs, die Sie schützen. Jede virtuelle Maschine auf einem Hypervisor, der dem Core hinzugefügt wird, wird ohne den Einsatz von Agenten und ohne Verbrauchen einer Lizenz geschützt. Um diesen Vorteil zu erhalten, müssen Sie Folgendes tun:

- **Schützen von VMs ohne Agenten.** Sie können zum ausdrücklichen Schützen von VMs den Assistenten zum Schützen mehrerer Maschinen verwenden. Wenn ein Hypervisor-Host geschützt wird, können Sie auch die Option **Neue virtuelle Maschinen automatisch schützen** nutzen, die implizit neue VMs schützt, sobald sie erstellt werden.
- **Zuordnung der Gast-VM mit dem geschützten Hypervisor-Host.** Wenn Rapid Recovery Agent installiert ist, werden die entsprechenden APIs (nicht die für den Hypervisor nativen) verwendet, um die VM zu schützen. Sie können jedoch den Lizenzverbrauch reduzieren, indem Sie die virtuelle Maschine dem Host zuordnen, der dem Core hinzugefügt wurde. Diese Zuordnung erfolgt auf Computerebene für jede virtuelle Maschine. Der Vorgang des Verknüpfens der Gast-VM mit dem übergeordneten Hypervisor-Host ist in Schritt 3 des Verfahrens Anzeigen und Ändern von geschützten Maschineneinstellungen beschrieben.
- **Deinstallieren des Agenten.** Soweit nicht anders empfohlen, entfernen Sie alle Kopien der Agenten-Software von der virtuellen Maschine.

Informationen über die Vorteile und die Einschränkungen des agentenlosen Schutzes, zusätzliche empfohlene Software, die Mindestanforderungen für den Host usw. finden Sie im Thema Grundlegende Informationen zu Rapid Snap for Virtual.

Informationen über den Schutz von Linux-Computern mit Rapid Recovery

DieRapid Recovery Agenten-Software ist mit mehreren Linux-basierten Betriebssystemen kompatibel (Details finden Sie unter den Systemanforderungen, die jetzt in der *Rapid Recovery Systemanforderungen-Handbuch* definiert sind). Der Rapid Recovery Core kann nur auf Windows-Maschinen installiert werden. Obwohl Sie geschützte Linux-Maschinen in der Rapid Recovery Core Console verwalten können, weichen die Schritte einiger Verfahren für Linux-Maschinen von denen für Windows ab. Darüber hinaus können Sie einige Aktionen mit dem Befehlszeilenprogramm local_mount direkt auf einem geschützten Linux-Computer durchführen.

NOTE: Das Dienstprogramm local_mount hieß früher aamount.

Wenn Sie eine einzige Linux-Maschine schützen möchten, können Sie jetzt den Assistenten zum Schutz der Maschinen verwenden. Lesen Sie dazu das Thema Schützen einer Maschine. Informationen zum Schutz mehrerer Linux-Maschinen gleichzeitig mit dem Assistenten über die Core Console finden Sie im Thema Manuelles Schützen mehrerer Maschinen.

Um die Agenten-Software über die Core Console auf einer Linux-Maschine bereitstellen oder installieren zu können, benötigen Sie Folgendes:

- Das Benutzerkonto muss über SUDO-Berechtigungen verfügen.
- Die Linux-Maschine, die Sie schützen möchten, benötigt Zugriff auf einen SSH-Server.

Wenn eine Linux-Maschine, die Sie schützen möchten, diese Anforderungen nicht erfüllt, wenden Sie sich an einen Linux-Administrator. Nehmen Sie die relevanten Maßnahmen vor, damit Sie diese Anforderungen erfüllen, und führen Sie den entsprechenden Assistenten zum Bereitstellen und Installieren der Agenten-Software aus.

Informationen zum Schützen von Oracle Datenbankservern

Rapid RecoveryVersion 6.2 erweitert die Anwendungsunterstützung auf Agent-basierten Schutz von relationalen Oracle 12c Datenbankservern. Sie können einen Oracle Datenbankserver und alle seine Datenbanken schützen und zugehörige Aufgaben ausführen.

In dieser Version gelten die folgenden Einschränkungen:

- Oracle 12c ist die einzige getestete und unterstützte Version für Schutz auf dem Rapid Recovery Core. Die Verwendung anderer Oracle Versionen erfolgt auf eigene Gefahr.
- Auf den geschützten Oracle Datenbankserver müssen 64-Bit-Versionen von Windows Server 2012 R2 x64 oder Windows Server 2016 ausgeführt werden.
- Sie müssen die Rapid Recovery Agent-software (Version 6.2 oder höher) auf Ihrem Oracle Server installieren. Agentenloser Schutz ist für eine zukünftige Version geplant.
- Der Schutz von Oracle12c Datenbanken ist auf die Verwendung des Volume Snapshot Service (VSS) im ARCHIVELOG-Modus beschränkt.

> **NOTE:** Unterstützung für NOARCHIVELOG (standardmäßiger Protokollmodus für Oracle Datenbanken) ist für eine zukünftige Version geplant. Oracle Datenbanken mit aktiviertem ARCHIVELOG-Modus müssen weiterhin darauf eingestellt sein, dass alle Online-Redo-Protokolle mit dem ARCH (Archiv)-Prozess archiviert werden. Ein Datenbankadministrator (DBA) kann den Modus ändern und die Redo-Protokolle stattdessen mit Oracle SQL*Plus oder Oracle Enterprise Manage archivieren. Weitere Informationen zum Aktivieren des ARCHIVELOG-Modus und zur Archivierung finden Sie in der Oracle Dokumentation oder wenden Sie sich an einen qualifizierten Oracle 12c DBA.

Zum vollständige Schutz von Oracle Servern führen Sie die folgenden Aufgaben aus:

- Installieren Sie die Rapid Recovery Agenten-Software (Version 6.2 oder höher) auf Ihrem Oracle Server und starten Sie den Schutz. Verwenden Sie den Assistenten zum Schützen von Maschinen, um den Oracle Server in Ihrem Netzwerk zu ermitteln, die Agenten-Software bereitzustellen und einen Schutzplan aufzustellen. Weitere Informationen finden Sie unter Informationen über den Schutz von Maschinen mit Rapid Recovery.
- Geben Sie die Anmeldedaten für jede Datenbank in den Rapid Recovery Core Console ein. Der Core speichert Ihre Anmeldeinformationen auf sichere Weise zwischen und gestattet Ihnen den Zugriff auf die Metadaten aus der Benutzeroberfläche. Bevor Sie Anmeldeinformationen eingeben, können Sie die Details der Datenbanken auf Ihrem geschützten Oracle Server nicht sehen. Weitere Informationen finden Sie unter Eingeben oder Bearbeiten der Anmeldeinformationen für Oracle Datenbanken.
- Aktivieren Sie den ARCHIVELOG-Modus für den geschützten Oracle Server, und überprüfen Sie den Oracle-VSS-Writer über die Core Console. Weitere Informationen finden Sie unter Aktivieren des Archivprotokoll-Modus und Hinzufügen von VSS Writer für geschützte Oracle Datenbanken.
- Überprüfen Sie die Richtlinie zum Kürzen des Protokolls und konfigurieren Sie sie nach Bedarf. Wenn der ARCHIVELOG-Modus für eine Oracle Datenbank aktiviert ist, sammeln sich die Protokolle schnell an und verbrauchen erheblichen Speicherplatz. Aus diesem Grund ist ein nächtlicher Job zum Kürzen der Oracle Protokolle standardmäßig aktiviert. Sie können drei Löschoptionen für diesen nächtlichen Job festlegen

oder den nächtlichen Job ganz deaktivieren. Weitere Informationen finden Sie unter Informationen zum Kürzen von Oracle Protokollen.

Sie können Oracle Datenbankprotokolle nach Bedarf auch manuell kürzen. Weitere Informationen zu diesem Verfahren finden Sie unter Manuelles Kürzen der Oracle Datenbankprotokolle.

Nach dem Installieren des Agenten, dem Schutz der Maschine in ihrem Core und dem ordnungsgemäßem Konfigurieren der Einstellungen können Sie Folgendes tun:

- **Metadaten anzeigen.** Von der Seite **Zusammenfassung** der geschützten Maschine aus können Sie Metadaten über jede Datenbank auf Ihrem Oracle Server anzeigen, einschließlich der Verbindung und des Status jeder Protokoll-, Kontroll- und Datendatei.
- **Datenbankintegrität prüfen.** Sie können Integritätsprüfungen in der Core Console mithilfe des DBVERIFY Utility durchführen.
- **Archivprotokolle kürzen**, mithilfe einer der drei Optionen zum Löschen.
- **Datenbanken wiederherstellen.** Sie können gesamte Volumes oder Volumes mit ausgewählten Datenbanken wiederherstellen. Sobald Sie den ARCHIVELOG-Modus aktivieren, sind Snapshots der Oracle Datenbank aus Sicht des Oracle Service absturzkonsistent.
- **Virtuellen Export durchführen.** Sie können einen einmaligen Export durchführen oder eine virtuelle Standby-VM einrichten, die eine VM mit neuen Informationen kontinuierlich aktualisiert, sobald Sicherungen Ihrer geschützten Datenbank erfasst werden.

  Wenn Sie eine VM einer Oracle Datenbank starten, müssen Sie möglicherweise die Datenbank manuell starten und den Modus für die Datenbankdateien deaktivieren.

Eingeben oder Bearbeiten der Anmeldeinformationen für Oracle Datenbanken

Bevor Sie dieses Verfahren ausführen, müssen Sie zunächst einen Oracle Datenbankserver zum Schutz Ihres Core hinzufügen.

So geben Sie die Anmeldeinformationen für Oracle Datenbanken ein oder bearbeiten sie:

- Das Windows Benutzerkonto des Rapid Recovery Benutzers dieses Verfahrens muss über SYSDBA-Berechtigungen auf dem geschützten Datenbankserver verfügen.
- Die Datenbank muss für den Rapid Recovery Core Server verfügbar sein und es muss erfolgreich eine Verbindung hergestellt worden sein.

NOTE: SYSDBA ist ein Administratorrecht für Oracle Systems Datenbanken, das für High-Level-Verwaltungsvorgänge erforderlich ist. Diese Funktionen umfassen das Erstellen, Starten, Herunterfahren, Sichern oder Wiederherstellen einer Oracle Datenbank.

Nachdem Sie den Oracle Datenbankserver geschützt haben, können Sie erst dann wieder auf Metadaten zugreifen oder Datenbankdetails anzeigen, wenn Sie für jede Datenbank die Anmeldeinformationen eingeben. Bei diesem einmaligen Schritt werden Ihre Anmeldedaten sicher zwischengespeichert. Außerdem erhält die Core Console Zugriff auf Statusinformationen zu allen geschützten Transaktionsprotokolldateien, Kontrolldateien und Datendateien in Ihren Oracle Datenbanken.

Beispiel: Auf der Seite **Zusammenfassung** für die geschützte Oracle Maschine können Sie keine Details zu den geschützten Datenbanken im Fensterbereich „Oracle Serverinformationen“ erweitern, solange Sie nicht die Anmeldeinformationen eingeben.

NOTE: Dies ist ein einmaliger Schritt, der für jede neue geschützte Oracle Datenbank erforderlich ist.

Führen Sie die Schritte in diesem Verfahren aus, um den Rapid Recovery Core Console Zugriff auf die erforderlichen Metadaten für Ihre geschützten Oracle Datenbanken bereitzustellen.

1. Navigieren Sie zu der geschützten Oracle Maschine in der Rapid Recovery Core Console.

Die Seite **Zusammenfassung** für die geschützte Maschine wird angezeigt.

2. Führen Sie auf der Seite **Zusammenfassung** einen Bildlauf nach unten bis zum Fensterbereich **Oracle Serverinformationen** durch.
3. Für die erste Datenbank in der Tabelle klicken Sie auf die Drop-Down-Liste (Weitere Optionen) und wählen Sie **Anmeldeinformationen bearbeiten** aus.

   Das Dialogfeld **Anmeldeinformationen für Instanz bearbeiten** wird angezeigt.
4. Zwei Verbindungstypen werden unterstützt: Grundlegend und Transparent Network Substrate (TNS), eine proprietäre Oracle Netzwerktechnologie. Führen Sie eine der folgenden Aktionen aus:

   - Um die Verbindung über eine grundlegende Verbindung herzustellen, geben Sie die Informationen in die folgende Tabelle ein:

Option	Description
Verbindungstyp	Grundlegend
Hostname	Geben Sie den Hostnamen oder die IP-Adresse ein.
Port	Geben Sie den entsprechende Port ein. Der Standardport für diesen Zweck ist 1521.
SID- oder Dienstname	Wählen Sie die entsprechende Verbindungsmethode aus. Sie können eine der folgenden verwenden: • **SID.** Der Oracle System Identifier (SID) ist eine eindeutige ID, die Ihre Datenbankinstanz eindeutig identifiziert. • **Dienstname.** Der Dienstname ist das TNS-Alias, mit dem eine Remote-Verbindung zu Ihrer Datenbank hergestellt wird. **NOTE:** Den Namen des Dienstes finden Sie in der TNSNAMES.ORA-Datei.
Dienstname	Der Dienstname ist das TNS-Alias, das Sie angeben, wenn Sie eine Remote-Verbindung zu Ihrer Datenbank und diesem Dienst herstellen

   - Um die Verbindung über TNS herzustellen, geben Sie die Informationen in die folgende Tabelle ein:

Option	Description
Verbindungstyp	TNS
Netzwerk-Alias	Wählen Sie dieses Drop-Down-Menü aus, um Datenbank-Aliase anzuzeigen, die in dem Netzwerk verfügbar sind, und wählen Sie das entsprechende Alias aus.

5. Zwei Typen von Anmeldedaten werden unterstützt: Oracle und Betriebssystem. Führen Sie eine der folgenden Aktionen aus:

   - Für die Verbindung mit Oracle Anmeldedaten geben Sie den Benutzernamen und das Kennwort für die Oracle Datenbank in die entsprechenden Textfelder ein.

NOTE: Ihr Windows-Benutzerkonto muss über SYSDBA-Berechtigungen verfügen.

- Um die Verbindung mit zwischengespeicherten Anmeldeinformationen vom Betriebssystem aus herzustellen, wählen Sie **Betriebssystem** aus.

NOTE: Ihr Windows Benutzerkonto muss ein Mitglied der lokalen ORA_DBA-Gruppe sein, was gewährleistet, dass der Benutzer über SYSDBA-Berechtigungen verfügt.

6. Zum Überprüfen der Anmeldeinformationen klicken Sie auf **Überprüfen**.

   Ein Dialogfeld wird angezeigt, wenn die Testverbindung erfolgreich war.
7. Führen Sie eine der folgenden Aktionen aus:
   - Wenn die Überprüfung erfolgreich war, klicken Sie auf **OK**, um die Meldung zu schließen.
   - Wenn sie nicht erfolgreich war, schließen Sie das Dialogfeld, und überarbeiten Sie die Instanz-Anmeldeinformationen, bis die Verbindung verifiziert ist. Wenden Sie sich an Ihren Systemadministrator, wenn Sie Fragen zu Anmeldedaten haben.
8. Klicken Sie im Dialogfeld **Anmeldeinformationen für Instanz bearbeiten** nach erfolgreicher Überprüfung auf **OK**.

   Das Dialogfeld wird geschlossen und Rapid Recovery Core Console wendet die Anmeldeinformationen sofort an und speichert sie zwischen. Sehr bald danach sind Metadaten in der Core Console verfügbar und die Statusanzeige für die ausgewählte Datenbank zeigt einen grünen Status (online) an.
9. Wiederholen Sie Schritt 3 bis Schritt 8 für jede Datenbank, die im Fensterbereich „Oracle Serverinformationen“ aufgelistet ist.

Nach Eingabe und Zwischenspeichern der Anmeldeinformationen für alle Datenbanken auf dieser geschützten Oracle Maschine führen Sie die im Thema Aktivieren des Archivprotokoll-Modus und Hinzufügen von VSS Writer für geschützte Oracle Datenbanken beschriebenen Verfahren aus.

Aktivieren des Archivprotokoll-Modus und Hinzufügen von VSS Writer für geschützte Oracle Datenbanken

Bevor Sie dieses Verfahren ausführen, müssen Sie zunächst einen Oracle Datenbankserver auf Ihrem Core hinzufügen und die Anmeldedaten für jede Datenbank in die Core Console eingeben.

Datenbankanwendungen erfordern das Vorhandensein einer Kombination bestimmter Dateien (z. B. Konfigurations-, Protokoll- und Kontrolldateien), die jeweils auf einen bestimmten Status festgelegt sind, um anwendungskonsistent zu sein. In Version 6.2 erfordern Oracle Datenbanken, dass der Archivprotokoll-Modus aktiviert ist. Bis Sie dieses Verfahren durchführen, sind Ihre Snapshots des Datenbankservers absturzkonsistent, aber nicht anwendungskonsistent.

Oracle VSS-Writer wird verwendet, um Snapshots mit Volume Snapshot Service zu erfassen. Der Writer muss aktiviert sein.

NOTE: Dies sind einmalige Schritte, die für jede neue geschützte Oracle Datenbank erforderlich sind.

Führen Sie die Schritte in diesem Verfahren aus, um zu überprüfen, ob der Archivprotokoll-Modus aktiviert ist, um ihn gegebenenfalls zu aktivieren und um VSS Writer zu Ihrem Core hinzuzufügen.

1. Navigieren Sie zu der geschützten Oracle Maschine in der Rapid Recovery Core Console.

   Die Seite **Zusammenfassung** für die geschützte Maschine wird angezeigt.
2. Führen Sie auf der Seite **Zusammenfassung** einen Bildlauf nach unten bis zum Fensterbereich **Oracle Serverinformationen** durch.
3. Wenn Sie im Fensterbereich **Oracle Serverinformationen** eine Warnmeldung sehen, dass der Archivprotokoll-Modus deaktiviert ist, klicken Sie auf **Archivprotokoll-Modus für diese Datenbanken aktivieren** und klicken Sie dann, um den Neustart der Datenbankinstanzen zu bestätigen.

NOTE: Durch Aktivieren des Archivprotokoll-Modus werden die entsprechenden Datenbank-Instanzen neu gestartet. Dieser Vorgang kann einige Minuten dauern.

4. Wenn Sie im Fensterbereich **Oracle Serverinformationen** eine Warnmeldung sehen, dass der Oracle-VSS-Writer keine Snapshots aufnehmen kann, klicken Sie auf **Oracle VSS-Writer** und dann erneut zum Bestätigen.

   Die Warnmeldung wird geschlossen und der VSS-Writer wird zu ihrem Core hinzugefügt.
5. Optional können Sie den Fortschritt durch Aktivieren des Archivprotokoll-Modus oder Hinzufügen eines VSS-Writers verfolgen. Weitere Informationen hierzu finden Sie unter Anzeigen von Aufgaben.

Informationen zum Kürzen von Oracle Protokollen

Der ARCHIVELOG-Modus, der für Oracle Support inVersion 6.2 erforderlich ist, führt zu einer erheblichen Anzahl von Protokolldateien, die sich auf dem Datenbankserver ansammeln und wertvollen Speicherplatz belegen. Relevante Protokolldateien werden bei jeder Erfassung eines Wiederherstellungspunkt-Snapshots in die Sicherungen des Oracle Servers eingeschlossen, wodurch die lokalen Protokolle überflüssig werden. Aus diesem Grund enthält Rapid Recovery Core verschiedene Methoden für das Kürzen von Oracle Protokollen.

1. Rapid Recovery Core umfasst nächtliche Job-Einstellungen zum Kürzen von Oracle Protokollen. Die Kürzung der Oracle Protokolle ist mit der **automatischen** Löschrichtlinie als ein nächtlicher Job standardmäßig aktiviert. In diesem Modell werden die Protokolle einmal täglich bei Ausführung des nächtlichen Jobs gekürzt.

   Diese Einstellung ist darauf ausgelegt, die Anforderungen der meisten Benutzer zu erfüllen. Wenn Sie mit diesem Ansatz zufrieden sind, müssen Sie die Konfiguration nicht ändern. Sie ist standardmäßig aktiviert.
2. Sie können die Konfiguration des nächtlichen Jobs zur Kürzung der Oracle Protokolle für einen bestimmten Oracle Server anpassen. Sie können zwischen zwei anderen Löschrichtlinien wählen:

   - Mit der Löschrichtlinie **Neueste behalten** können Sie festlegen, wie lange (-n Tage, Wochen, Monate oder Jahre) die Oracle Protokolle aufbewahrt werden, bevor sie gekürzt werden. Wenn der Zeitraum abläuft, werden Protokolldateien, die älter als dieser Zeitpunkt sind, einmal täglich bei Ausführung des nächtlichen Jobs gekürzt.
   - Mit der Löschrichtlinie **Angegebene Anzahl behalten** können Sie eine bestimmte Anzahl von Protokolldateien angeben, die beibehalten werden sollen. Wenn dieser Schwellenwert erreicht ist, werden neuere Protokolle beibehalten und die älteren Protokolle einmal täglich bei Ausführung des nächtlichen Jobs gekürzt.

   Weitere Informationen zu Kürzungen als ein nächtlicher Job finden Sie unter dem Thema Grundlegende Informationen zu nächtlichen Jobs.
3. Sie können Protokolle auch jederzeit auf Abruf manuell kürzen. Weitere Informationen finden Sie unter Manuelles Kürzen der Oracle Datenbankprotokolle.

Die Kürzung von Oracle Protokollen durch einen nächtlichen Job oder manuell bei Bedarf, erfolgt, ohne dass ein Übertragungs-Job erforderlich ist.

Manuelles Kürzen der Oracle Datenbankprotokolle

Dieses Verfahren gilt nur für Oracle Datenbankserver, die auf Ihrem Core geschützt sind.

Um den Schutz von Oracle Datenbanken in Rapid Recovery Version 6.2 zu unterstützen, ist ein nächtlicher Job zum Kürzen der Oracle Archiv-Protokolle standardmäßig aktiviert. Sie können diesen nächtlichen Job deaktivieren, doch dies führt zum einem erheblichen Ansammeln von Protokolldateien auf dem lokalen Datenbankserver.

Sie können für alle geschützten Oracle Server die Oracle Datenbankprotokolle nach Bedarf jederzeit manuell kürzen. Durch das Kürzen werden die Archiv-Protokolle vom lokalen Server gelöscht. In jedem in Ihrem Repository gespeicherten Wiederherstellungspunkt bleiben die Datenbankprotokolle bestehen und stellen den Zustand der Datenbank zum Zeitpunkt des Sicherungs-Snapshots dar.

Führen Sie die Schritte in diesem Verfahren aus, um manuell Oracle Protokolldateien zu kürzen.

1. Navigieren Sie zu der geschützten Oracle Maschine in der Rapid Recovery Core Console.

   Die Seite **Zusammenfassung** für die geschützte Maschine wird angezeigt.
2. Führen Sie auf der Seite **Zusammenfassung** einen Bildlauf nach unten bis zum Fensterbereich **Oracle Serverinformationen** durch.
3. Klicken Sie in der Zeile, die die Oracle Datenbankinstanz darstellt, deren Protokolle Sie kürzen möchten, auf die Drop-Down-Liste (Weitere Optionen) und wählen Sie **Kürzen des Protokolls erzwingen**.

   Das Dialogfeld **Kürzen des Protokolls erzwingen** wird angezeigt.
4. Wenn Sie alle Oracle Protokolle vom lokalen Datenbankserver löschen möchten, wählen Sie **Automatisch** aus dem Drop-Down-Menü **Löschen** und klicken Sie dann auf **Erzwingen**.

   Eine Protokollkürzungsjob wird in die Warteschlange gestellt. Wenn das System nicht ausgelastet ist, wird der Job sofort ausgeführt, und die Protokolle werden gekürzt.
5. Wenn Sie alle lokal gespeicherten Protokolle vom Oracle Server löschen möchten (von denen Kopien im aktuellsten Wiederherstellungspunkt gespeichert sind), gehen Sie wie folgt vor:
   a. Wählen Sie **Neueste behalten** aus dem Drop-Down-Menü **Löschen**.
   b. Geben Sie im Textfeld **Protokolle aufbewahren für** eine Zahl ein und wählen Sie dann den relevanten Zeitraum (**Tage, Wochen, Monate** oder **Jahre**) aus dem Drop-down-Menü „Zeitraum“.
   c. Klicken Sie auf **Erzwingen**.

   Eine Protokollkürzungsjob wird in die Warteschlange gestellt. Wenn das System nicht ausgelastet ist, wird der Job sofort ausgeführt, und die Protokolle werden gekürzt.
6. Wenn Sie eine bestimmte Anzahl von Oracle Protokolldateien behalten und die verbleibenden Protokolle kürzen möchten, gehen Sie wie folgt vor:
   a. Wählen Sie **Angegebene Anzahl behalten** aus dem Drop-Down-Menü **Löschen**.
   b. Geben Sie im Textfeld **Anzahl der Archivdateien** eine Zahl für die Anzahl der neuesten Datenbankprotokolle, die Sie behalten möchten, ein.
   c. Klicken Sie auf **Erzwingen**.

   Eine Protokollkürzungsjob wird in die Warteschlange gestellt. Wenn das System nicht ausgelastet ist, wird der Job sofort ausgeführt, und die Protokolle werden gekürzt.
7. Wenn Sie Protokolle für andere Datenbankinstanzen auf diesem Server kürzen möchten, wiederholen Sie Schritt 3 bis Schritt 6 für jede relevante Datenbank, die im Bereich der Oracle Serverinformationen aufgelistet wird.

Informationen über das Verwalten von Anwendungsservern in Rapid Recovery Core

Rapid Recovery bietet Unterstützung für Anwendungsserver wie SQL-Server, Exchange Server und Oracle. Informationen zu den einzelnen Versionen, die Rapid Recovery unterstützt, finden Sie unter *Rapid Recovery Systemanforderungen-Handbuch*.

Spezielle Optionen für diese unterstützten Anwendungen werden in Rapid Recovery Core Console nur angezeigt, wenn eine Instanz der Software und zugehörige Dateien auf geschützten Servern erkannt werden. In diesen Fällen sind zusätzliche Optionen verfügbar, wenn Sie die geschützte Maschine in der Core Console auswählen.

Wenn Sie einen geschützten SQL-Server im linken Navigationsmenü auswählen, umfassen die Menüoptionen, die für diese geschützte Maschine angezeigt werden, die Drop-Down-Menüoption **SQL-Server**.

Wenn Sie zum Beispiel einen geschützten Exchange-Server im linken Navigationsmenü auswählen, umfassen die Menüoptionen, die für diese geschützte Maschine angezeigt werden, die Dropdown-Menüoption **Exchange**.

Wenn Sie einen geschützten Oracle Server auf der Seite **Zusammenfassung** für die geschützte Maschine auswählen, blättern Sie nach unten zum Bereich Oracle Serverinformationen, der nur für geschützte Oracle Datenbankserver verfügbar ist.

Obwohl diese Optionen möglicherweise unterschiedlich funktionieren, gibt es einige Gemeinsamkeiten. Zu den Funktionen, die Sie nur für geschützte SQL-Server, Exchange Server und Oracle Server ausführen können, gehören:

- **Kürzung des Serverprotokolls erzwingen.** SQL-Server, Exchange-E-Mail-Server und Oracle Datenbankserver enthalten Serverprotokolle. Beim Kürzen von SQL-Serverprotokollen wird der verfügbare Speicherplatz auf dem Server ermittelt. Beim Kürzen von Exchange-Serverprotokollen wird der verfügbare Speicherplatz ermittelt und mehr Speicherplatz auf dem Server freigegeben. Das gleiche gilt für Oracle: Durch Protokollkürzungen werden Archivdateien vom Oracle Server entfernt, wodurch Speicherplatz auf dem geschützten Server frei wird.
- **Anmeldeinformationen für den jeweiligen Server festlegen.** Bei SQL-Servern können Sie Anmeldeinformationen für eine einzelne geschützte SQL-Servermaschine oder Standardanmeldeinformationen für alle geschützten SQL-Server festlegen. Bei Exchange und Oracle Servern können Sie Anmeldeinformationen für die geschützte Maschine auf der Seite **Zusammenfassung** für den geschützten Server festlegen.
- **Anzeigen des Status von Wiederherstellungspunkt-Überprüfungen von SQL-Servern, Exchange Servern oder Oracle Servern**. Von einer Maschine eines geschützten SQL-Servers, Exchange Servers oder Oracle Servers erfasste Wiederherstellungspunkte verfügen über entsprechende Farb-Statusanzeigen. Diese Farben zeigen den Erfolg oder das Fehlschlagen der verschiedenen für diese Anwendungsserver relevanten Überprüfungen an.

Die folgenden Themen enthalten Informationen über das Verwalten von SQL-Servern, Exchange Servern oder geschützten Oracle Maschinen:

- Grundlegende Informationen zu Statusanzeigen für Wiederherstellungspunkte
- Einstellungen und Funktionen für geschützte SQL-Server
- Einstellungen und Funktionen für geschützte Exchange-Server
- Informationen zum Schützen von Oracle Datenbankservern

Schützen von Server-Clustern

In Rapid Recovery basiert der Schutz von Server-Clustern auf den geschützten Rapid Recovery-Maschinen, die auf den einzelnen Cluster-Knoten installiert sind (d. h. auf den einzelnen Maschinen im Cluster), und dem Rapid Recovery Core, der diese Maschinen so schützt, als ob es sich um eine einzige Maschine handeln würde.

Sie können einen Rapid Recovery Core problemlos zum Schützen und Verwalten eines Clusters konfigurieren. In der Core Console ist ein Cluster als separate Einheit organisiert, die einen „Container“ bildet, in dem die zugehörigen Knoten enthalten sind. Im linken Navigationsbereich werden beispielsweise unter dem Menü **Geschützte Maschinen** die geschützten Cluster aufgelistet. Direkt unter jedem Cluster werden die zugehörigen Knoten oder Agent-Maschinen angezeigt. Dabei handelt es sich jeweils um eine geschützte Maschine, auf der die Rapid Recovery Agentensoftware installiert ist. Wenn Sie auf das Cluster klicken, wird die Seite **Zusammenfassung** für das Cluster in der Core Console angezeigt.

Auf der Core- und der Cluster-Ebene können Sie Informationen zum Cluster anzeigen, z. B. die Liste der zugehörigen Knoten und die freigegebenen Volumes. Wenn Informationen über einen Cluster in der Core Console angezeigt werden, können Sie auf **Geschützte Knoten** in der oberen Navigationsmenü klicken, und so eine Übersichtstabelle mit einzelnen Knoten im Cluster anzeigen. Von dieser Übersichtstabelle können Sie für jeden Knoten bestimmte Funktionen durchführen, z. B. Erzwingen eines Snapshots; Ausführen eines einmaligen Exports oder Einrichten von Virtual Standby, Laden oder Anzeigen von Wiederherstellungspunkten; Wiederherstellung von einem Wiederherstellungspunkt; Konvertierung des Clusterknoten auf seine eigene geschützte Maschine; oder den Knoten aus dem Schutz entfernen. Wenn der Knoten ein Exchange- oder SQL-Server ist, sehen Sie außerdem die Option zum Abschneiden von Protokollen.

Auf der Cluster-Ebene können Sie auch die entsprechenden Exchange- und SQL-Cluster-Metadaten für die Knoten im Cluster anzeigen. Sie können die Einstellungen für das gesamte Cluster und für die freigegebenen Volumes in diesem Cluster festlegen.

Wenn Sie auf einen beliebigen Knoten im Cluster aus dem linken Navigationsmenü klicken, sind die Informationen, die in der Core Console angezeigt werden spezifisch für diesen Knoten des Clusters. Hier können Sie Informationen anzeigen, die spezifisch für diesen Knoten sind oder die Einstellungen nur für diesen Knoten konfigurieren.

Weitere Informationen über unterstützte Anwendungsversionen und Cluster-Konfigurationen und über Unterstützung für Cluster Shared Volumes finden Sie unter *Rapid Recovery Systemanforderungen-Handbuch*.

Grundlegende Informationen zu Rapid Snap for Virtual

Die Funktion Rapid Snap for Virtual von Rapid Recovery wird auch als agentenloser Schutz bezeichnet, da Sie virtuelle Maschinen (VMs) im Core ohne Installation des Rapid Recovery Agenten auf jeder VM schützen können.

CAUTION: Quest **empfiehlt, dass Sie den agentenlosen Schutz zuerst auf maximal 200 VMs gleichzeitig begrenzen. Wählen Sie bei der Verwendung des Assistenten zum Schützen mehrerer Maschinen nicht mehr als 200 virtuelle Maschinen aus. Der Versuch, mehr als 200 VMs zu schützen, kann zu einer langsamen Benutzeroberfläche führen. Es gibt keine Beschränkung, wie viele virtuelle Maschinen ein Core agentenlos über einen bestimmten Zeitraum schützen kann. Sie könnten zum Beispiel heute 200 und morgen weitere 200 virtuelle Maschinen schützen.**

Weitere Informationen finden Sie unter Schützen von VMware vCenter-/ESXi-VMs und Schützen von VMs auf Hyper-V-Servern und -Clustern.

Schützen von VMware vCenter-/ESXi-VMs

Mit Rapid Recovery können Sie vCenter/ESXi-VMs ohne vorherige Installation des Rapid Recovery Agenten auf der VM oder dem ESXi-Host schützen, wodurch Sie agentenlosen Schutz erzielen. Rapid Recovery verwendet den ESXi-Client und die native VMware-API (Application Program Interface), um ausgewählte VMs auf einem einzigen Host zu erkennen und zu schützen. Rapid Recovery Core kommuniziert dann mit der Laufwerksdatei für eine virtuelle Maschine (VMDK), um die erforderlichen Details der geschützten Volumes zu bestimmen. Da Rapid Recovery basierend auf Volumes, und nicht VMDKs, Wiederherstellungspunkte erstellt, kann jedes Volume separat bereitgestellt, wiederhergestellt und exportiert werden.

Rapid Recovery schützt keinen VMware vCenter-/ESXi-Hypervisor-Host. Wenn Sie einen vCenter-/ESXi-Host mit Hilfe des Assistenten zum Schützen mehrerer Maschinen auswählen, fügen Sie den Host als übergeordnetes Element auf dem Rapid Recovery Core hinzu. Datendateien oder Daten von dem tatsächlichen Host sind in Snapshots auf dem Core nicht enthalten. Allerdings können die VM-Gastgeräte auf dem Host geschützt werden. Die geschützten VMs werden auf der Core-GUI als untergeordnete Elemente unter dem übergeordneten Host angezeigt. Wenn Sie den agentenlosen Schutz für ESXi-VMs auswählen, wird das Symbol für die geschützte VM () anders angezeigt als das Symbol einer ESXi-VM, die über Rapid Recovery Agent geschützt wird (zum Beispiel ).

NOTE: Quest empfiehlt, dass VMware-Tools auf virtuellen Maschinen installiert werden (VMs), die Sie auf vSphere- oder ESXi-Hosts schützen möchten. Wenn VMware Tools auf einer VM mit einem Windows-Betriebssystem (OS) installiert sind, verwenden die Sicherungen, die der Rapid Recovery Core erfasst, Microsoft Volume Shadow Copy Services (VSS). Dies bietet die Kapazität für anwendungskonsistente Sicherungen. Weitere Informationen über das Verhalten agentenloser VMs mit oder ohne VMware-Tools finden Sie unter Vorteile der Installation von Hypervisor-Tools für agentenlosen Schutz und Grundlegende Informationen zu absturzsicheren und anwendungskonsistenten Sicherungen.

Wenn VMware-Tools installiert sind, verwendet der agentenlose Schutz VMware Changed Block Tracking (CBT), um die Zeit für inkrementelle Snapshots zu reduzieren. CBT bestimmt die geänderten Blöcke in der VMDK-Datei und ermöglicht Rapid Recovery, nur die Teile des Laufwerks zu sichern, die seit dem letzten Snapshot

geändert wurden. Diese Sicherungsmethode führt häufig zu kürzeren Sicherungsvorgängen und geringerem Ressourcenverbrauch bei Netzwerk- und Speicherelementen.

Es gibt mehrere Vorteile agentenlosen Schutz zu verwenden. Einige der sinnvollsten Attribute sind die folgenden Eigenschaften:

- Keine zusätzliche Software ist auf dem Hostcomputer erforderlich.
- Mit agentenlosem Schutz können Sie neue dem ESXi-Host oder Hyper-V-Host hinzugefügte VMs automatisch schützen.
- Kein Neustart erforderlich während des Schutz-Prozesses.
- Die Anmeldeinformationen sind für jede einzelne VM nicht erforderlich.
- Mit agentenlosem Schutz können Sie eine VM auch schützen, wenn sie ausgeschaltet ist.
- Mit agentenlosem Schutz können Sie Datenträger wiederherstellen.
- Agentenloser Schutz unterstützt alle Gastbetriebssysteme.
- Wenn Sie ein Gast-VM dem geschützten übergeordneten Hypervisor-Host zuordnen, wird keine Enterprise-Lizenz verbraucht, wenn die VM in Ihrem Core geschützt wird.
- Optional können Sie Metadaten schützen und erheben fürSQL-Server und Exchange.
- Der Core (nicht der Agent) kann Anfügbarkeitsprüfungen, Protokollkürzungen und Bereitstellbarkeitsprüfungen für Wiederherstellungspunkte durchführen, die erfasst wurden von geschütztenSQL- und Exchange Servern.
- Agentenloser Schutz ermöglicht Ihnen das Exportieren dynamischer Datenträger oder Volumes.

  NOTE: Wenn dynamische Volumes komplex sind (Stripeset-Volumes, gespiegelte Volumes, übergreifende Volumes oder RAID 1-Volumes), exportieren Sie als Image-Dateien und parsen in Volumes, nachdem der Exportvorgang auf die exportierte VM abgeschlossen ist.

Während es viele Gründe für die Verwendung von agentenlosem Schutz für ESXi VMs gibt, wählen Sie die Schutzmethode aus, die sich am besten für Ihre Umgebungen und geschäftlichen Anforderungen eignet. Zusammen mit den zuvor erwähnten Vorteilen, gilt es bei der Auswahl von agentenlosem Schutz auch die folgenden Überlegungen zu beachten:

- Beim agentenlosen Schutz von Oracle Datenbankservern werden keine Oracle Metadaten erfasst. Während die Dateien und das Betriebssystem in Snapshots gesichert werden, werden keine auf Oracle bezogenen Funktionen unterstützt. Um eine Unterstützung für Oracle Datenbankanwendungen zu erhalten, schützen Sie Ihre Server mit Rapid Recovery Agent.
- Agentenloser Schutz unterstützt nicht den Schutz von dynamischen Volumes (z. B. Stripeset-Volumes, gespiegelte Volumes, übergreifende Volumes oder RAID 1-Volumes) auf Volume-Ebene. Er schützt sie auf Datenträgerebene.
- Agentenloser Schutz unterstützt keine Live Recovery. Weitere Informationen zu dieser Funktion finden Sie unter Grundlegendes zu Live Recovery.
- Während des Wiederherstellungsprozesses für ein einzelnes Volume auf der geschützten VM, wird die VM automatisch neu gestartet.
- Agentenloser Schutz zeigt nicht die tatsächliche Größe des genutzten Speicherplatzes auf einer VM an, wenn der Typ des virtuellen Laufwerks „Thick Provision Eager Zeroed“ ist.

Wenn Sie den agentenlosen Schutz für Ihre ESXi VMs wählen, muss der Host folgende Mindestanforderungen erfüllen, dass der agentenlose Schutz erfolgreich ist.

- Die Host-Maschine muss ESXi Version 5.0.0 Build 623860 oder höher ausführen.
- Der Hostcomputer muss den Mindestsystemanforderungen entsprechen, die in *Rapid Recovery Systemanforderungen-Handbuch* angegeben sind.
- Für Schutz auf Volumestufe müssen VMDKs entweder MBR (Master Boot Record) Partitionstabellen oder GUID Partition Tabellen (GPTs) einschließen. VMDKs ohne diese Partitionstabellen werden als ganze Datenträger statt als einzelne Volumes geschützt.
- Jede virtuelle VMware Maschine muss die VMware Tools installiert haben, um Snapshot-Konsistenz sicherzustellen.

Schützen von VMs auf Hyper-V-Servern und -Clustern

Um Hyper-V-VMs agentenlos zu schützen, ist es nicht notwendig, Rapid Recovery auf jeder VM zu installieren. Sie müssen ihn nur auf dem Hostcomputer oder Clusterknoten installieren. Der Agent schützt die virtuelle Festplatte auf dem Host und konvertiert alle Änderungen an den Festplattendateien in ein Volume- oder das Datenträger-Abbild, je nach dem Dateisystem. Ein neuer Treiber bietet Unterstützung auf Dateiebene für VMs auf Hosts und auf freigegebenen Clustervolumes (CSVs).

Agentenlose Unterstützung für Hyper-V wird durch das Betriebssystem auf dem Host bestimmt. Eine vollständige Liste der Betriebssysteme und Rapid Recovery Komponenten, die jeweils unterstützt werden, finden Sie in *Rapid Recovery Systemanforderungen-Handbuch*. Weitere Informationen finden Sie im Thema „Rapid Recovery Version 6.2 Betriebssystem-Installations- und Kompatibilitätsmatrix“ in diesem Dokument.

Quest empfiehlt, dass Hyper-V -Integrationsdienste auf virtuellen Maschinen (VMs) installiert werden, die Sie auf Hyper-V-Hosts schützen möchten. Wenn Hyper-V-Integrationsdienste auf einer VM mit einem Windows-Betriebssystem installiert sind, verwenden die Sicherungen, die Rapid Recovery Core erfasst, Microsoft VSS. Dies bietet die Kapazität für anwendungskonsistente Sicherungen. Weitere Informationen über das Verhalten agentenloser VMs mit oder ohne Hyper-V-Integrationsdiensten finden Sie unter Vorteile der Installation von Hypervisor-Tools für agentenlosen Schutz und Grundlegende Informationen zu absturzsicheren und anwendungskonsistenten Sicherungen.

NOTE: Rapid Recovery unterstützt das VHDx-Festplatten-Dateiformat. Es unterstützt nicht das VHD-Format.

Für den Schutz von VMs auf einem CSV müssen der Rapid Recovery Agent und Treiber über die automatische Bereitstellungsfunktion im Assistenten zum Schützen mehrerer Maschinen auf jedem Clusterknoten installiert werden. Von den Knoten aus kann der Agent auch alle VMs schützen, die auf CSVs operieren, indem zwei Arten von Änderungen für jede Datei erstellt werden. Die erste Art von Änderung wird nur vor oder nach einem Snapshot oder einem sauberen Neustart des Systems gespeichert. Die zweite Art von Änderung befindet sich auf dem Datenträger, welcher selbst im Falle eines Stromausfalls oder eines „Dirty Shutdown“ einen inkrementellen Snapshot verfügbar macht. Der auf dem Knoten installierte Agent führt alle Änderungen vor der Übertragung der Daten zusammen.

Wenn ein Host oder Knoten ausgeführt wird, erstellt Rapid Recovery eine Sicherung. Wenn der Host nicht ausgeführt wird, kann keine Sicherung erstellt werden; wenn jedoch nur einer der Knoten nicht ausgeführt wird, kann Rapid Recovery weiterhin Snapshots auf den VMs auf dem Cluster erstellen.

NOTE: Um eine optimale Leistung zu erzielen, wird empfohlen, die maximale Anzahl gleichzeitiger Übertragungen für den Hyper-V-Host oder -Knoten auf 1 zu setzen. Dies ist die Standardeinstellung.

Agentenloser Hyper-V-Schutz bietet viele der gleichen Funktionen wie herkömmlicher Schutz, bei dem der Agent auf jeder VM installiert ist, einschließlich:

- Archivierung
- Integritätsprüfungen des Wiederherstellungspunkts
- Bereitstellen von Wiederherstellungspunkten
- Automatische Ermittlung von neuen VMs (spezifisch für agentenlosen Schutz)
- Schutz vonSQL- und Exchange-Servern und Erheben von Metadaten
- Durchführen von Exchange-Bereitstellbarkeitsprüfungen
- Durchführung vonSQL-Anfügbarkeitsprüfungen
- Replikation
- Wiederherstellung von VMs, einschließlich der Wiederherstellung in CSVs oder freigegebene CIF-Ordner
- Wiederherstellung von Dateien in einem Gast-VHDX-Format
- Rollup
- Virtueller Export auf Hyper-V-VMs und andere Hypervisoren, einschließlich ESXi, VMWare Workstation und VirtualBox

Es sind bei der Auswahl von agentenlosem Hyper-V-Schutz jedoch auch Beschränkungen zu berücksichtigen. Die nicht verfügbaren Funktionen umfassen:

- Live Recovery
- Wiederherstellung von VMs auf CIFS mit VHD-Format
- Wiederherstellung von Dateien in einem Gast-VHD (.vhd)-Format
- Wiederherstellung von Dateien in einem Gast-VHD-Satz (.vhd)-Format

NOTE: Für einen anwendungskonsistenten Snapshot muss der SCSI-Controller auf jeder VM installiert sein. Ohne diesen Controller ist das Ergebnis immer ein absturzkonsistenter Snapshot.

Anwendungssupport

Mit Rapid Snap for Virtual können Sie agentenlosen Schutz aktivieren fürSQL-Server und Exchange-Anwendungen, die auf Hyper-V- und ESXi-VMs ausgeführt werden. Diese optionale Funktion ist für VMs mit Windows-Betriebssystemen verfügbar.

NOTE: Anwendungssupport nicht für Anwendungen, die auf Linux-VMs installiert sind.

Nach der Aktivierung von Anwendungssupport werden die Metadaten der Anwendungen auf der Seite

Zusammenfassung der VM angezeigt, außerdem erscheint ein Symbol neben dem VM-Namen auf der Seite **Maschinen**. Wenn ein Fehler den ordnungsgemäßen Anwendungssupport verhindert, wechselt das Symbol von Grün zu Rot.

Bevor Sie entscheiden, agentenlosen Schutz für einenSQL-Server oder Exchange Server einzurichten, beachten Sie die folgenden Hinweise:

- Zum Schützen der Anwendung muss die VM eingeschaltet sein. Der Core ruft keine Metadaten von Maschinen ab, die ausgeschaltet sind.
- VMware-Tools oder Hyper-V-Integrationsdienst-Dienstprogramme müssen auf den VMs installiert werden, die Sie schützen möchten.
- Auf einer VM, auf der Exchange Server und SQL-Server installiert sind, besteht keine Möglichkeit, die Protokolle separat zu kürzen. Wenn beide Anwendungen installiert sind, werden die Protokolle zusammen gekürzt.
- SQL-Server-Anfügbarkeitsprüfungen sind nur auf dem Core verfügbar und können nicht auf der geschützten Maschine durchgeführt werden.
- Um die Protokollkürzung auf einem EsXi-Host VM auszuführen, muss der Host ESXi Version 6.5 oder höher verwenden.

Vorteile der Installation von Hypervisor-Tools für agentenlosen Schutz

Beim Schutz von virtuellen Maschinen (VMs) ohne Verwendung des Rapid Recovery Agenten empfiehlt Quest die Installation von VMware-Tools auf geschützten VMs auf vSphere- oder EsXi-Hosts. Gleichermaßen empfiehlt Quest die Installation von Hyper-V-Integrationsdiensten für VMs, die auf Hyper-V-Hosts geschützt werden sollen.

Durch Installation dieser nativen Hypervisor Dienstprogramme kann Rapid Recovery die Microsoft Volume Shadow Copy Services (VSS)-Funktionalität voll ausnutzen.

Wenn diese Dienstprogramme auf VMs mit Windows-Betriebssystemen installiert sind, können die von Rapid Recovery Core erstellten Sicherungen auch VSS verwenden. Wenn diese Tools nicht installiert sind, erfasst Rapid Recovery zwar noch Snapshots, jedoch nur in einem absturzsicheren Zustand. Weitere Informationen hierzu finden Sie unter Grundlegende Informationen zu absturzsicheren und anwendungskonsistenten Sicherungen.

Die folgenden Bedingungen gelten je nachdem, ob VMware-Tools oder Hyper-V-Integrationsdienste installiert sind und ob sich die VM im eingeschalteten Zustand befindet:

Tabelle 40. Sicherungstyp-Bedingungen für VM

Hypervisor-Tool	VM eingeschaltet	Art der Sicherung
Nicht installiert	Ja	Absturzkonsistent
Nicht installiert	Nein (fehlerhaftes Herunterfahren)	Absturzkonsistent
Nicht installiert	Nein (fehlerfreies Herunterfahren)	Anwendungskonsistent
Installiert	Ja	Anwendungskonsistent
Installiert	Nein (fehlerhaftes Herunterfahren)	Absturzkonsistent
Installiert	Nein (fehlerfreies Herunterfahren)	Anwendungskonsistent

Grundlegende Informationen zu absturzsicheren und anwendungskonsistenten Sicherungen

Beim Schutz von virtuellen Maschinen ohne den Einsatz von Agenten mit der Funktion Rapid Snap for Virtual können sich die in Sicherungsmomentaufnahmen erfassten Daten in einem von zwei Zuständen befinden:

- Absturzkonsistent. Mindestens alle agentenlosen Sicherungen, die durch Rapid Recovery Core erfasst wurden, sind absturzkonsistent. Die Sicherung ist ein Snapshot aller Daten und Betriebssystemdateien auf jedem geschützten Volume zu dem Zeitpunkt, zu dem diese Dateien erfasst wurden. Wenn Sie aus einem absturzkonsistenten Wiederherstellungspunkt wiederherstellen, wird das VM-Betriebssystem gestartet und kann das Dateisystem sowie alle Dateien darin lesen und nachvollziehen.

  Beim Wiederherstellen einer transaktionalen Anwendung aus einem absturzkonsistenten Zustand kehrt die Datenbank zum letzten gültigen Zustand zurück. Dieser letzte gültige Zustand kann vom Zeitpunkt des Absturzes von einem Zeitpunkt vor dem Absturz stammen. Wenn er von vor dem Absturz stammt, muss die Datenbank ein Rollforward einiger Tätigkeiten durchführen, damit die Datendateien mit den Informationen in den Protokollen übereinstimmen. Dieser Vorgang kann beim ersten Öffnen der Datenbank einige Zeit in Anspruch nehmen, was zu einer Verzögerung beim Hochfahren der Maschine führt.

- **Anwendungskonsistent**. Anwendungskonsistente Sicherungen verwenden den Microsoft Volume Shadow Copy Service (VSS) zur Gewährleistung der Kohärenz der Anwendungsdaten, wenn eine Schattenkopie erstellt wird. Mit VSS Writern werden ausstehende Eingabe-/Ausgabevorgänge abgeschlossen und Protokolldateien übernommen, bevor Snapshots erfasst werden. Daher wird das VM-Betriebssystem, wenn Sie aus einem anwendungskonsistenten Wiederherstellungspunkt wiederherstellen, gestartet und kann das Dateisystem lesen und nachvollziehen. Zusätzlich befinden sich Dateien für transaktionale Anwendungen wie SQL-Server oder Exchange in einem konsistenten Zustand. Z. B. stimmen SQL-Server-Protokolle mit Datendateien überein und die Datenbank öffnet sich schnell, ohne dass Reparaturen vorgenommen werden müssen.

Grundlegende Informationen zum Installationsprogramm der Rapid Recovery Agentensoftware

Mit Rapid Recovery können Sie Installationsprogramme vom Rapid Recovery Core herunterladen. Auf der Seite **Downloads** können Sie das Installationsprogramm für den Agenten, die Local Mount Utility (LMU) oder eine SNMP MIB-Datei herunterladen. Weitere Informationen zu LMU finden Sie unter Das Local Mount Utility. Weitere Informationen zu SNMP finden Sie unter Grundlegende Informationen zu SNMP-Einstellungen.

NOTE: Weitere Informationen zum Zugriff auf das Installationsprogramm für den Agenten finden Sie unter Herunterladen des Rapid Recovery Agent Installers. Weitere Informationen zum Bereitstellen des Installationsprogramms für den Agenten finden Sie im Rapid Recovery Installations- und Aktualisierungshandbuch.

Das Installationsprogramm für den Agenten wird verwendet, um die Rapid Recovery Agenten-Anwendung auf Maschinen zu installieren, die durch den Rapid Recovery Core geschützt werden sollen. Wenn Sie feststellen, dass das Installationsprogramm für den Agenten auf einer Maschine installiert werden muss, können Sie das Webinstallationsprogramm über die Registerkarte "Downloads" der Rapid Recovery Core Console herunterladen.

NOTE: Das Herunterladen des Core erfolgt über das Rapid Recovery Lizenzportal. Informationen zum Herunterladen des Installationsprogramms für den Rapid Recovery Core finden Sie unter https://licenseportal.com. Weitere Informationen finden Sie im Rapid Recovery Lizenzportal Benutzerhandbuch.

Herunterladen des Rapid Recovery Agent Installers

Laden Sie das Rapid Recovery Agenten-Installationsprogramm herunter und stellen Sie es auf einer beliebigen Maschine bereit, die Sie auf dem Rapid Recovery Core schützen möchten. Führen Sie die folgenden Schritte aus, um das Webinstallationsprogramm herunterzuladen.

1. Zum Herunterladen des Agenten-Installationsprogramms direkt von der Maschine, die Sie schützen möchten, gehen Sie wie folgt vor:
    a. Öffnen Sie in einem Web-Browser das Rapid Recovery Lizenzportal unter https://licenseportal.com.
    b. Klicken Sie im linken Navigationsmenü auf **Downloads**.
    c. Führen Sie vom Fensterbereich **Windows-basierte Anwendungen** einen Bildlauf nach unten durch zu der Zeile **Windows Agent** und klicken Sie auf **Download** für das entsprechende Installationsprogramm (32-Bit- oder 64-Bit-Systeme).

    Das Installationsprogramm, z. B. `Agent-X64-6.0.1.xxxx.exe`, wird in dem Downloads-Zielordner gespeichert.
2. Zum Herunterladen des Web-Installationsprogramms aus dem Core, klicken Sie auf der Core Console Symbolleiste auf das Symbol **Mehr** und wählen Sie **Downloads** aus.
3. Klicken Sie auf der Seite **Downloads** im Fensterbereich **Agent** auf **Download Internet-Installationsprogramm**.
4. Klicken Sie im Dialogfeld **Agent-Web.exe öffnen** auf **Datei speichern**.

    Das Installationsprogramm, z. B. `Agent-X64-6.0.1.xxxx.exe`, wird in dem Downloads-Zielordner gespeichert.
5. Verschieben Sie das Installationsprogramm auf die geeignete Maschine und installieren Sie die Rapid Recovery Agentensoftware neu.

    Weitere Informationen zum Installieren der Rapid Recovery Agentensoftware finden Sie im Installations- und Aktualisierungshandbuch für Rapid Recovery.

Bereitstellen des Agenten auf mehreren Maschinen gleichzeitig aus der Core Console

Sie können die Rapid Recovery Agenten-Software auf mehreren Windows-Maschinen gleichzeitig bereitstellen. Die Maschinen können Teil einer Active Directory-Domäne oder eines virtuellen vCenter- oder ESX(i)-Hosts oder eines virtuellen Hyper-V-Hosts sein. Sie können auch Maschinen sein, die bereits vom lokalen Rapid Recovery Core geschützt sind, wie im Falle eines Hochstufens der Rapid Recovery Agenten-Software. Sie haben auch die Option zum manuellen Bereitstellen der Software auf Maschinen, die nicht unbedingt einer bestimmten Domäne oder einem bestimmten Host zugeordnet sind.

Sie können die Rapid Recovery Agenten-Software auch manuell auf einer oder mehreren Linux-Maschinen in der Core Console implementieren.

CAUTION: Wenn AppAssure Agent zuvor auf einer Linux-Maschine installiert war, müssen Sie vor der Installation des Rapid Recovery Agent den AppAssure Agent über ein Shell-Skript von der Maschine entfernen. Weitere Informationen zum Entfernen des Agenten von einer Linux-Maschine finden Sie unter dem Thema „Deinstallation der AppAssure Agent Software von einer Linux-Maschine“ im *Rapid Recovery-Installations- und Aktualisierungshandbuch*. Zur erfolgreichen Bereitstellung der Agenten-Software auf Linux-Maschinen lesen Sie die Voraussetzungen unter dem Thema „Informationen zum Installieren der Agentensoftware auf Linux-Maschinen“ im gleichen Dokument.

Durch Bereitstellen der Rapid Recovery Agenten-Software werden die Maschinen nicht automatisch geschützt. Wählen Sie nach der Bereitstellung die Option **Mehrere Maschinen schützen** aus der Schaltflächenleiste der Core Console aus.

NOTE: Die Funktion eines Bereitstellens von mehreren Maschinen gleichzeitig wurde früher als Massenbereitstellung bezeichnet. Die Funktion eines Schützens von mehreren Maschinen gleichzeitig wurde früher als Massenschutz bezeichnet.

Führen Sie zum Bereitstellen und Schützen mehrerer Maschinen gleichzeitig die folgenden Aufgaben durchführen:

- Stellen Sie Rapid Recovery Agent auf mehreren Maschinen bereit. Informationen dazu finden Sie unter Bereitstellen des Agenten auf mehreren Maschinen gleichzeitig aus der Core Console.
- Überwachen Sie die Bereitstellung. Informationen dazu finden Sie unter Überprüfen der Bereitstellung auf mehreren Maschinen.
- Mehrere Maschinen schützen. Informationen dazu finden Sie unter So schützen Sie mehrere Maschinen.

  NOTE: Wenn Sie während der Bereitstellung die Option "Maschine nach Installation schützen" ausgewählt haben, überspringen Sie diese Aufgabe.
- Überwachen Sie die Aktivität des Massenschutzes. Informationen dazu finden Sie unter Überwachen des Schutzes von mehreren Maschinen.

Verwendung des Bereitstellungsassistenten für die Agentensoftware zum Bereitstellen einer oder mehrerer Maschinen

Sie können die Bereitstellung der Rapid Recovery Agenten-Software auf einer oder mehreren Maschinen durch Verwendung des Bereitstellungsassistenten für die Agenten-Software vereinfachen.

Wenn Sie die Bereitstellung auf Linux-Maschinen durchführen, ist diese Methode geeignet.

NOTE: In der Vergangenheit wurde diese Funktion auch als „Massenbereitstellung“ bezeichnet.

Bei der Verwendung des Bereitstellungsassistenten für die Agenten-Software ist der Rapid Recovery Core zu Folgendem in der Lage:

1. Windows Maschinen in einer Active Directory Domain erkennen und die Agentensoftware mithilfe von Push auf die ausgewählten Maschinen übertragen.
2. Eine Verbindung zu einem VMware vCenter- oder ESXi-Host herstellen, die Gäste erkennen und die Agentensoftware mithilfe von Push auf die ausgewählten Maschinen übertragen.

3. Eine Verbindung zu einem lokalen Rapid Recovery Core herstellen und die aktuelle (neuere) Agenten-Software auf Windows-Maschinen, die von diesem Core bereits geschützt werden, bereitstellen. (Für Linux Maschinen verwenden Sie die Option für die manuelle Bereitstellung.)
4. Eine Verbindung zu einem Hyper-V-Server oder -Cluster herstellen, die Gäste erkennen und die Agentensoftware mithilfe von Push auf die ausgewählten Maschinen übertragen.
5. Manuell die Linux oder Windows Maschinen mithilfe von, IP-Adressen und Anmeldeinformationen festlegen und die Agentensoftware mithilfe von Push auf die ausgewählten Maschinen übertragen.

Von innerhalb der Core Console können Sie die folgenden Aufgaben ausführen:

- Bereitstellung auf Maschinen in einer Active Directory-Domäne
- Bereitstellung auf Maschinen auf einem virtuellen VMware vCenter/ESXi-Host
- Bereitstellung einer Erweiterung der Rapid Recovery-Agentensoftware auf geschützten Maschinen
- Manuelles Bereitstellen auf Maschinen

NOTE: Quest empfiehlt, die Anzahl der Maschinen, auf die Sie gleichzeitig bereitstellen, auf 50 oder weniger zu beschränken, um Ressourceneinschränkungen zu verhindern, die dazu führen könnten, dass der Bereitstellungsvorgang fehlschlägt.

NOTE: Die Zielmaschinen müssen zum Herunterladen und Installieren von Bits Zugriff auf das Internet haben, da Rapid Recovery die Webversion des Rapid Recovery Agenteninstallationsprogramm zur Bereitstellung der Installationskomponenten verwendet. Wenn kein Internetzugang verfügbar ist, verwenden Sie die Core Console, um das Installationsprogramm auf ein Speichermedium wie z. B. ein USB-Laufwerk herunterzuladen. Installieren Sie dann physisch die Software auf die Maschinen, die Sie schützen möchten. Weitere Informationen hierzu finden Sie unter Herunterladen des Rapid Recovery Agent Installers.

Bereitstellung auf Maschinen in einer Active Directory-Domäne

Bevor Sie diesen Vorgang starten, müssen Sie über die Domänen-Informationen und die Anmeldeinformationen für den Active Directory-Server verfügen.

Verwenden Sie dieses Verfahren, um die Rapid Recovery Agentensoftware auf einer Maschine oder auf mehreren Maschinen auf einer Active Directory-Domäne gleichzeitig bereitzustellen.

1. Klicken Sie auf der Rapid Recovery Core Console auf das Drop-Down-Menü **Schützen** und dann auf **Bereitstellung der Agentensoftware**.

   Der Bereitstellungsassistent für die Agentensoftware wird geöffnet.
2. Wählen Sie auf der Seite **Verbindung** des Assistenten von der Drop-Down-Liste **QuelleActive Directory**.
3. Geben Sie die Domänen-Informationen und Anmeldeinformationen ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 41. Domäneninformationen und Anmeldeinformationen

Textfeld	Description
Host	Der Hostname oder die IP-Adresse der Active Directory-Domäne.
Benutzername	Der Benutzername für die Verbindung zur Domäne, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).

Textfeld	Description
Kennwort	Das sichere Kennwort, das für die Verbindung zur Domäne verwendet wird.

4. Klicken Sie auf **Weiter**.
5. Wählen Sie auf der Seite **Maschinen** die Maschinen aus, für die Sie die Rapid Recovery Agentensoftware neu bereitstellen möchten.
6. Wahlweise können Sie zum automatischen Neustart der geschützten Maschinen, nachdem der Agent installiert ist, **Nach der Agenteninstallation die Maschinen automatisch neu starten (Empfohlen)** wählen.
7. Klicken Sie auf **Fertig stellen**.

   Das System prüft automatisch jede Maschine, die Sie ausgewählt haben.

   Wenn Rapid Recovery erkennt, dass es Probleme während der automatischen Überprüfung der Assistent gibt, fährt der Assistent mit einer Seite Warnungen fort. Dort können Sie Maschinen aus der Auswahl löschen und manuell die ausgewählten Maschinen überprüfen. Wenn die Maschinen, die Sie hinzugefügt haben, die automatische Überprüfung bestehen, werden sie im Fensterbereich Bereitstellung von Agenten auf Maschinen angezeigt.
8. Wenn die Warnseite angezeigt wird und Sie trotzdem mit Ihrer Auswahl zufrieden sind, klicken Sie erneut auf **Finish** (Fertig stellen).

Die Rapid Recovery Agentensoftware wird auf den angegebenen Maschinen bereitstellt. Die Maschinen sind noch nicht geschützt. Schutz beginnt nach Abschluss von Schutz mehrerer Maschinen in einer Active Directory-Domäne.

Bereitstellung auf Maschinen auf einem virtuellen VMware vCenter/ESXi-Host

Verwenden Sie dieses Verfahren, um die Rapid Recovery Agentensoftware auf einer Maschine oder auf mehreren Maschinen auf einem virtuellen VMware vCenter/ESXi-Host gleichzeitig bereitzustellen.

Bevor Sie diesen Vorgang starten, müssen Sie die folgenden Informationen haben:

- Anmeldeinformationen für den virtuellen VMware vCenter/ESXi-Host.
- Host-Standort.
- Anmeldeinformationen für jede Maschine, die Sie schützen möchten.

NOTE: Auf allen virtuellen Maschinen müssen die VMware Tools installiert sein, da Rapid Recovery den Hostnamen der virtuellen Maschine sonst nicht ermitteln kann, auf der die Bereitstellung erfolgen soll. Anstelle des Hostnamens verwendet Rapid Recovery den Namen der virtuellen Maschine. Dies kann zu Problemen führen, wenn der Hostname mit dem Namen der virtuellen Maschine nicht übereinstimmt.

1. Klicken Sie auf der Rapid Recovery Core Console auf das Drop-Down-Menü **Schützen** und dann auf **Bereitstellung der Agentensoftware**.

   Der **Bereitstellungsassistent für die Agentensoftware** wird geöffnet.
2. Wählen Sie auf der Seite **Verbindung** des Assistenten von der Drop-Down-Liste **QuellevCenter / ESXi**.
3. Geben Sie die in der folgenden Tabelle beschriebenen Host- und Anmeldedaten ein.

Tabelle 42. vCenter/ESXi-Verbindungseinstellungen

Textfeld	Description
Host	Geben Sie den Hostnamen oder die IP-Adresse des virtuellen Hosts des VMware vCenter Server/ESXi ein.

Textfeld	Description
Port	Der Port für die Verbindung zum virtuellen Host. Die Standardeinstellung ist 443.
Benutzername	Der Benutzername für die Verbindung zum virtuellen Host, z. B. „Administrator“ (bzw. „[Domänenname]\Administrator“, wenn sich die Maschine in einer Domäne befindet).
Kennwort	Das sichere Kennwort, das für die Verbindung zum jeweiligen virtuellen Host verwendet wird.

4. Klicken Sie auf **Weiter**.
5. Wählen Sie auf der Seite **Maschinen** des Assistenten eine der folgenden Optionen aus dem Drop-Down-Menü aus:
   - Hosts und Cluster
   - VMs und Vorlagen
6. Erweitern Sie die Liste der Machines und wählen Sie dann die VMs, auf denen Sie die Software bereitstellen möchten.

   Eine Benachrichtigung wird angezeigt, wenn Rapid Recovery erkennt, dass eine Maschine offline ist oder dass VMware-Tools nicht installiert sind.
7. Wenn Sie die Maschinen automatisch nach der Bereitstellung neu starten möchten, wählen Sie **Nach der Agenteninstallation die Maschinen automatisch neu starten (Empfohlen)**.
8. Klicken Sie auf **Weiter**.

   Rapid Recovery prüft automatisch jede Maschine, die Sie ausgewählt haben.
9. Geben Sie auf der Seite **Anpassungen** des Assistenten die Anmeldeinformationen für jede Maschine im folgenden Format ein: `hostname::username::password`.

   NOTE: Geben Sie eine Maschine pro Zeile ein.
10. Klicken Sie auf **Fertig stellen**.

    Das System prüft automatisch jede Maschine, die Sie ausgewählt haben.

    Wenn Rapid Recovery erkennt, dass es Probleme während der automatischen Überprüfung der Assistent gibt, fährt der Assistent mit einer Seite Warnungen fort. Dort können Sie Maschinen aus der Auswahl löschen und manuell die ausgewählten Maschinen überprüfen. Wenn die Maschinen, die Sie hinzugefügt haben, die automatische Überprüfung bestehen, werden sie im Fensterbereich Bereitstellung von Agenten auf Maschinen angezeigt.
11. Wenn die Warnseite angezeigt wird und Sie trotzdem mit Ihrer Auswahl zufrieden sind, klicken Sie erneut auf **Finish** (Fertig stellen).

Die Rapid Recovery Agentensoftware wird auf den angegebenen Maschinen bereitstellt. Die Maschinen sind noch nicht geschützt. Schutz beginnt nach Abschluss von Schutz von mehreren Maschinen auf einem virtuellen VMware vCenter/ESXi-Host.

Bereitstellung einer Erweiterung der Rapid Recovery-Agentensoftware auf geschützten Maschinen

Sie können mit dem Bereitstellungsassistent für die Agentensoftware eine Erweiterung der Rapid Recovery Agentensoftware auf Windows-Maschinen, die bereits vom lokalen Rapid Recovery Core geschützt sind, anstoßen.

NOTE: Für Linux Benutzer gilt Folgendes: Wenn die frühere Version des Agent die Marke AppAssure (Version 5.4.3 oder früher) aufweist, müssen Sie zunächst die Agentensoftware mit dem entsprechenden Shell-Script für Ihre spezifische Version des AppAssure Agent entfernen. Durch Entfernen des AppAssure Agent nach der Installation des Rapid Recovery Agent kann die Verbindung zwischen der Linux-Maschine und dem Core unterbrochen werden. Weitere Informationen zum Deinstallieren von AppAssure Agent von einer Linux-Maschine finden Sie unter Deinstallation der AppAssure Agentensoftware von einer Linux-Maschine im *Rapid Recovery Installations- und -Aktualisierungshandbuch*.

1. Klicken Sie auf der Rapid Recovery Core Console auf das Drop-Down-Menü **Schützen** und dann auf **Bereitstellung der Agentensoftware**.

   Der **Bereitstellungsassistent für die Agentensoftware** wird geöffnet.
2. Wählen Sie auf der Seite **Verbindung** des Assistenten, von der Drop-Down-Liste **QuelleLokaler Core**.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Maschinen** des Assistenten die geschützten Maschinen aus, für die Sie die Rapid Recovery-Agentensoftware bereitstellen und aktualisieren möchten.

   NOTE: Zu diesem Zeitpunkt können Sie geschützte Linux-Maschinen mit diesem Verfahren nicht aktualisieren.
5. Es hat sich bewährt, jede Maschine nach Installation oder Aktualisierung von Agentensoftware neu zu starten. Wenn Sie die Maschinen nach der Bereitstellung neu starten möchten, wählen Sie **Nach der Agenteninstallation die Maschinen automatisch neu starten (Empfohlen)**. Falls Sie die aktualisierten Maschinen nicht neu starten möchten, deaktivieren Sie die Option.
6. Klicken Sie auf **Fertig stellen**.

   Das System prüft automatisch jede Maschine, die Sie ausgewählt haben.

   Wenn Rapid Recovery erkennt, dass es Probleme während der automatischen Überprüfung der Assistent gibt, fährt der Assistent mit einer Seite **Warnungen** fort. Dort können Sie Maschinen aus der Auswahl löschen und manuell die ausgewählten Maschinen überprüfen. Wenn die Maschinen, die Sie hinzugefügt haben, die automatische Überprüfung bestehen, werden sie im Fensterbereich **Bereitstellung von Agenten auf Maschinen** angezeigt.
7. Wenn die Seite **Warnung** angezeigt wird und Sie weiterhin mit Ihrer Auswahl zufrieden sind, klicken Sie erneut auf **Fertigstellen**.

Manuelles Bereitstellen auf Maschinen

Verwenden Sie das folgende Verfahren zur Bereitstellung des Rapid Recovery Agenten auf mehreren Maschinen auf jeder Art von Host, außer lokalem Core, Active Directory, vCenter/ESXi oder Hyper-V.

CAUTION: Wenn AppAssure Agent zuvor auf einer Linux-Maschine installiert war, müssen Sie vor der Installation des Rapid Recovery Agent den AppAssure Agent über ein Shell-Skript von der Maschine entfernen. Weitere Informationen zum Entfernen des Agenten von einer Linux-Maschine finden Sie unter dem Thema „Deinstallation der AppAssure Agent Software von einer Linux-Maschine“ im *Rapid Recovery-Installations- und Aktualisierungshandbuch.* Zur erfolgreichen Bereitstellung der Agenten-Software auf Linux-Maschinen lesen Sie die Voraussetzungen unter dem Thema „Informationen zum Installieren der Agentensoftware auf Linux-Maschinen“ im gleichen Dokument.

1. Klicken Sie auf der Rapid Recovery Core Console auf das Drop-Down-Menü **Schützen** und wählen Sie dann **Agentensoftware bereitstellen**.

   Der **Bereitstellungsassistent für die Agentensoftware** wird geöffnet.
2. Wählen Sie auf der Seite **Verbindung** des Assistenten aus der Drop-Down-Liste **QuelleManuell** aus.
3. Klicken Sie auf **Weiter**.
4. Geben Sie auf der Seite **Maschinen** des Agenten für jede Maschine, auf der Sie den Agenten bereitstellen möchten, die Maschinendetails im Dialogfeld ein. Drücken Sie die **Eingabetaste,**, um separate Information für jede Maschine einzugeben. Verwenden Sie das Format `Hostname::Benutzername::Kennwort::Port`. Für Windows-Maschinen ist die Porteinstellung optional. Für Linux-Maschinen schließen Sie immer den SSH-Port ein, der standardmäßig auf 22 gesetzt ist. Beispiele:

   ```
   10.255.255.255::administrator::&11@yYz90z
   abc-host-00-1::administrator::99!zU$o83r::8006
   Linux-host-00-2::administrator::p@$$w0rD::22
   ```
5. Wenn Sie die Maschinen automatisch nach der Bereitstellung neu starten möchten, wählen Sie **Nach der Agenteninstallation die Maschinen automatisch neu starten (Empfohlen)**.
6. Klicken Sie auf **Fertig stellen**.

   Das System prüft automatisch jede Maschine, die Sie ausgewählt haben.

   Wenn Rapid Recovery erkennt, dass es Probleme während der automatischen Überprüfung der Assistent gibt, fährt der Assistent mit einer Seite **Warnungen** fort. Dort können Sie Maschinen aus der Auswahl löschen und manuell die ausgewählten Maschinen überprüfen. Wenn die Maschinen, die Sie hinzugefügt haben, die automatische Überprüfung bestehen, werden sie im Fensterbereich **Bereitstellung von Agenten auf Maschinen** angezeigt.
7. Wenn die Seite **Warnung** angezeigt wird und Sie weiterhin mit Ihrer Auswahl zufrieden sind, klicken Sie erneut auf **Fertigstellen**.

Die Rapid Recovery Agentensoftware wird auf den angegebenen Maschinen bereitstellt. Die Maschinen sind noch nicht geschützt. Schutz beginnt nach Abschluss von Manuelles Schützen mehrerer Maschinen.

Überprüfen der Bereitstellung auf mehreren Maschinen

Nach der Bereitstellung der Rapid Recovery Agentensoftware auf mehreren Maschinen, können Sie überprüfen, ob die Bereitstellung erfolgreich war, indem Sie die einzelnen Maschinen in der Liste unter dem Menü „Geschützte Maschinen“ anzeigen.

Sie können die Informationen zur Massenbereitstellung auch auf der Seite „Ereignisse“ sehen. Führen Sie die folgenden Schritte aus, um die Bereitstellung zu überprüfen.

1. Navigieren Sie zur Rapid Recovery Core Console, klicken Sie auf (Ereignisse) und klicken Sie dann auf **Warnungen**.

In der Liste werden die Benachrichtigungsereignisse mit der Uhrzeit, zu der das Ereignis aufgetreten ist, und eine zugehörige Meldung angezeigt. Für jede erfolgreiche Bereitstellung der Agent-Software wird eine Benachrichtigung angezeigt, dass die geschützte Maschine hinzugefügt wurde.

2. Sie können auf jeden Link für eine geschützte Maschine klicken.

   Die Seite **Zusammenfassung** für die ausgewählte Maschine wird mit Informationen zur jeweiligen Maschine angezeigt, z. B.:

   - Hostname der geschützten Maschine
   - Letzter Snapshot (sofern zutreffend)
   - Planmäßiger Zeitpunkt der nächsten Snapshot-Erstellung gemäß Schutzzeitplan für die ausgewählte Maschine
   - Verschlüsselungsschlüssel (sofern vorhanden) für die jeweilige geschützte Maschine.
   - Version der Agent-Software

Ändern von Bereitstellungseinstellungen

Führen Sie die nachstehend beschriebenen Schritte durch, um die Bereitstellungseinstellungen zu ändern.

1. Klicken Sie in der Rapid Recovery Core Console auf (Einstellungen).
2. Klicken Sie auf der Seite **Einstellungen** in der linken Spalte auf **Bereitstellen**, um zum Bereitstellungsabschnitt zu navigieren.
3. Ändern Sie die folgenden Optionen durch Klicken auf die Einstellung, die Sie ändern möchten, damit sie als Textfeld oder Drop-Down-Liste bearbeitet werden kann, und klicken Sie dann auf , um die Einstellung zu speichern.

Tabelle 43. Bereitstellungsoptionen

Option	Description
Agenten-Installationsprogramm	Geben Sie den Namen der ausführbaren Datei für den Agenten ein. Der Standardname ist „Agent-web.exe“.
Kern-Adresse	Geben Sie die Adresse für den Core ein.
Zeitüberschreitung Empfang fehlgeschlagen	Geben Sie die Anzahl der Minuten ein, die ohne Aktivität vor einer Zeitüberschreitung gewartet werden sollen.
Maximale Anzahl paralleler Installationen	Geben Sie einen Wert für die Höchstanzahl von Installationen ein, die Sie gleichzeitig installieren möchten. Der Standard- und Grenzwert beträgt 100.
Automatischer Neustart nach Installation	Markieren Sie das Kontrollkästchen für „Ja“ oder löschen Sie es für „Nein“.

Option	Description
Nach Bereitstellung schützen	Markieren Sie das Kontrollkästchen für „Ja“ oder löschen Sie es für „Nein“.

Grundlegende Informationen zu Schutzzeitplänen

Ein Schutzzeitplan definiert, wann Sicherungskopien von geschützten Agentenmaschinen auf den Rapid Recovery Core übertragen werden.

Die erste Sicherungs-Übertragung für eine beliebige Maschine, die unter den Schutz durch den Core gestellt wird, wird als Basisimage-Snapshot bezeichnet. Alle Daten auf allen angegebenen Volumes (einschließlich Betriebssystem, Anwendungen und Einstellungen) werden im Repository gespeichert. Dies kann abhängig von der Menge der Daten, die übertragen werden, relativ viel Zeit in Anspruch nehmen. Danach werden regelmäßig inkrementelle Snapshots (kleinere Sicherungen, die nur die seit der letzten Sicherung geänderten Daten auf der geschützten Maschine umfassen) im festgelegten Zeitintervall (z. B. alle 60 Minuten) im Repository gespeichert. Diese Sicherungskopie enthält weniger Daten als ein Basisabbild, und daher dauert die Übertragung nicht so lang.

Die Schutzzeitpläne werden zunächst mit den Assistenten zum Schützen einer Maschine bzw. zum Schützen mehrerer Maschinen definiert. Mit einem Assistenten können Sie gemäß Ihrer Unternehmensanforderungen Schutzzeitpläne anpassen, (indem Sie die gewünschten Zeiträume auswählen oder eine tägliche Schutzzeit angeben). Sie können dann den vorhandenen Zeitplan ändern oder jederzeit im Dialogfeld „Schutzzeitplan“ auf der Seite „Zusammenfassung“ einer bestimmten geschützten Maschine einen neuen Zeitplan erstellen.

Rapid Recovery bietet einen Standardschutzzeitplan, der alle Wochentage beinhaltet, mit einem einzigen festgelegten Zeitraum (von 00:00 bis 23:59). Das Standardintervall (der Zeitabstand zwischen Snapshots) beträgt 60 Minuten. Wenn Sie das erste Mal Schutz aktivieren, aktivieren Sie auch den Zeitplan. So wird mit den Standardeinstellungen die erste Sicherung unabhängig von der Tageszeit zu jeder vollen Stunde durchgeführt (00:00, 01:00, 02:00 usw.).

Wenn Sie Zeiträume auswählen, wird der Standardschutzzeitplan angezeigt, den Sie je nach Bedarf anpassen können. Wenn Sie eine tägliche Schutzzeit auswählen, sichert Rapid Recovery Core die angegebenen geschützten Maschinen einmal täglich zur der von Ihnen angegebenen Uhrzeit.

Sie können den Zeitplan für die Definition von Spitzen- und Nebenzeiten mithilfe der verfügbaren Wochentag- und Wochenende-Punkte anpassen. Wenn beispielsweise Ihre geschützten Maschinen meistens an Werktagen in Verwendung sind, könnten Sie festlegen, das Intervall für die Wochentag-Periode auf bis zu 20 Minuten zu verringern, was alle 60 Minuten zu drei Snapshots führt. Sie können auch das Intervall an Wochenenden von 60 Minuten auf 180 Minuten vergrößern, sodass alle drei Stunden Snapshots erstellt werden, wenn das Datenverkehrsaufkommen gering ist.

Sie können den Standardzeitplan auch ändern, um täglich Haupt- und Nebenzeiten festzulegen. Ändern Sie dazu die Standardstart- und -endzeit in einen kleineren Bereich (z. B. 00:00 bis 16:59) und legen Sie ein geeignetes Intervall fest (z. B. 20 Minuten). In diesen Spitzennutzungszeiten werden häufig Sicherungen erstellt. Fügen Sie dann einen zusätzlichen Werktag-Zeitraum für den verbleibenden Zeitraum hinzu (17:00 bis 23:59) und geben Sie ein geeignetes (größeres) Intervall an (z. B. 180 Minuten). Diese Einstellungen legen einen Zeitraum mit geringer Auslastung jeden Tag von 17:00 bis Mitternacht fest. Diese Anpassung führt dazu, dass Snapshots von 17:00 bis 23:59 alle 3 Stunden und von 0:00 bis 16:59 alle 20 Minuten erstellt werden.

Wenn Sie über das Dialogfeld „Schutzzeitplan“ einen Schutzzeitplan ändern oder erstellen, gibt Ihnen Rapid Recovery die Möglichkeit, diesen Zeitplan als wiederverwendbare Vorlage zu speichern, die Sie dann auf anderen geschützten Maschinen anwenden können.

Zu weitere Optionen der Schutzassistenten gehören die Festlegung einer täglichen Schutzzeit. Zum festgelegten Zeitpunkt (Standardeinstellung: 12:00 Uhr) wird dann täglich eine einzelne Sicherung durchgeführt.

Wenn Sie Maschinen mit dem Assistenten schützen, können Sie den Schutz zunächst vorübergehend deaktivieren, der den Schutzzeitplan festlegt, ohne die Maschinen zu schützen. Wenn der Schutz der Maschinen gemäß dem eingerichteten Schutzzeitplan gestartet werden kann, müssen Sie den Schutz explizit wieder aktivieren. Weitere Informationen zum erneuten Aktivieren der Schutzfunktion finden Sie unter Anhalten und Fortsetzen der Replikation. Wenn eine Maschine sofort geschützt werden soll, können Sie ggf. einen Snapshot erzwingen. Weitere Informationen hierzu finden Sie unter Erzwingen eines Snapshots.

See also: Erstellen von benutzerdefinierten Schutzzeitplänen im einfachen Modus
See also: Erstellen mehrerer Schutzzeitplan-Zeiträume im erweiterten Modus

Schützen einer Maschine

Starten Sie die Maschine neu, wenn die Rapid Recovery Agent Software auf der zu schützenden Maschine bereits installiert ist, die Maschine aber noch nicht neu gestartet wurde.

In diesem Abschnitt wird beschrieben, wie der Schutz der Daten für eine einzelne Maschine gestartet wird, die Sie im Assistenten zum Schützen einer Maschine angeben. Informationen zum Schützen mehrerer Maschinen gleichzeitig finden Sie unter So schützen Sie mehrere Maschinen.

NOTE: Sofern Sie nicht agentenlosen Schutz auf einem VMware- oder ESXi-Host oder einem Hyper-V-Host verwenden, muss auf der Maschine, die Sie schützen möchten, die Rapid Recovery Agent Software installiert sein, um geschützt zu sein. Sie können die Agent-Software installieren, bevor Sie die nachstehend beschriebenen Schritte ausführen, oder die Software im Rahmen der Durchführung des Assistenten zum Schützen einer Maschine auf der Zielmaschine bereitstellen. Weitere Informationen zu agentenlosem Schutz und seinen Einschränkungen finden Sie unter Grundlegende Informationen zu Rapid Snap for Virtual.

NOTE: Weitere Informationen zum Installieren der Agenten-Software finden Sie im Abschnitt „Installieren der Rapid Recovery Agent Software“ im *Rapid Recovery Installations- und Aktualisierungshandbuch*. Wenn die Agent-Software nicht installiert wurde, bevor eine Maschine geschützt wird, können Sie im Assistenten nicht bestimmte Volumes auswählen, die geschützt werden sollen. In diesem Fall, werden standardmäßig alle Volumes auf der agentenlos geschützten Maschine geschützt. Rapid Recovery unterstützt Schutz und Wiederherstellung von Maschinen mit EISA-Partitionen. Die Unterstützung wurde auch auf Maschinen mit Windows 8 und 8.1 sowie Windows 2012 und 2012 R2 erweitert, die Windows RE (Windows Recovery Environment) verwenden.

Wenn Sie eine Maschine unter Schutz stellen, müssen Sie Verbindungsinformationen wie IP-Adresse und Port festlegen und Anmeldeinformationen für die zu schützende Maschine angeben. Optional können Sie einen Anzeigenamen eingeben, der in der Core Console anstelle der IP-Adresse angezeigt wird. Wenn Sie diese Änderung vornehmen, wird für die geschützte Maschine bei Anzeige der Details in der Core Console keine IP-Adresse angezeigt. Sie legen auch den Schutzzeitplan für die Maschine fest.

Diese Vorgehensweise zum Schutz umfasst optionale Schritte, die Sie durchführen können, wenn Sie eine erweiterte Konfiguration auswählen. Zu den erweiterten Optionen zählen Repositoryfunktionen und Verschlüsselung. Sie können beispielsweise ein vorhandenes Rapid Recovery Repository zum Speichern von Snapshots angeben oder ein neues Repository erstellen. Sie können auch einen vorhandenen Verschlüsselungsschlüssel angeben (oder einen neuen Verschlüsselungsschlüssel hinzufügen), um die Daten der jeweiligen Maschine, die im Core gespeichert werden, zu verschlüsseln. Weitere Informationen zum Konfigurieren von Verschlüsselungsschlüsseln finden Sie unter Verschlüsselung.

Der Workflow des Schutzassistenten kann abhängig von der jeweiligen Umgebung geringfügig abweichen. Wenn beispielsweise die Rapid Recovery Agentensoftware auf der zu schützenden Maschine installiert ist, werden Sie im Assistenten nicht aufgefordert, die Software zu installieren. Ebenso werden Sie nicht aufgefordert, ein Repository zu erstellen, wenn im Core bereits ein Repository vorhanden ist.

CAUTION: Rapid Recovery unterstützt keine BMR-Wiederherstellungen von Linux-Maschinen mit ext2-Startpartitionen. Bei einer BMR-Wiederherstellung auf eine Maschine mit einer derartigen Partition führt dazu, dass die Maschine nicht gestartet wird. Wenn Sie später in der Lage sein möchten, auf dieser Maschinen eine BMR-Wiederherstellung durchzuführen, müssen die ext2-Partitionen vor dem Schützen und Sichern der Maschine in ext3 oder ext4 konvertiert werden.

1. Führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie mit dem Assistent zum Schützen einer Maschine beginnen, fahren Sie mit Schritt 2 fort.
   - Wenn Sie mit der Rapid Recovery Core Console Core Console beginnen, klicken Sie in der Schaltflächenleiste auf **Schützen**.

   Der **Assistent zum Schutz von Maschine**n wird angezeigt.
2. Wählen Sie auf der Seite **Welcome** (Willkommen) die entsprechenden Installationsoptionen aus:
   - Wählen Sie **Standard** aus, wenn Sie kein Repository definieren und keine Verschlüsselung einrichten müssen.
   - Wählen Sie **Erweitert (optionale Schritte anzeigen)** aus, wenn Sie ein Repository erstellen, ein anderes Repository für Sicherungen der ausgewählten Maschine angeben oder die Verschlüsselung mit dem Assistenten einrichten müssen.
   - Wenn die Seite **Willkommen** für den Assistenten zum Schützen der Maschine künftig nicht angezeigt werden soll, wählen Sie die Option **Seite „Willkommen“ beim nächsten Öffnen des Assistenten ignorieren** aus.
3. Wenn Sie die gewünschten Optionen auf der Begrüßungsseite festgelegt haben, klicken Sie auf **Weiter**.

   Die Seite **Connection** (Verbindung) wird angezeigt.
4. Geben Sie auf der Seite **Verbindung** die in der folgenden Tabelle beschriebenen Verbindungsinformationen für die Maschine ein und klicken Sie dann auf **Weiter**.

Tabelle 44. Verbindungseinstellungen für Maschinen

Textfeld	Description
Betriebssystem	Wählen Sie Windows oder Linux, basierend auf dem Betriebssystem der Maschine, die Sie schützen möchten.
Host	Der Hostname oder die IP-Adresse der Maschine, die Sie schützen möchten.
Port	Die Portnummer, über die der Rapid Recovery Core mit dem Agenten auf der Maschine kommuniziert. Die Standardportnummer ist 8006.
Benutzername	Der Benutzername für die Verbindung zu dieser Maschine, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).
Kennwort	Das Kennwort, das für die Verbindung zu dieser Maschine verwendet wird.

Wenn die Seite **Agenten installieren** als nächstes im Assistenten zum Schützen einer Maschine angezeigt wird, bedeutet das, dass Rapid Recovery nicht den Rapid Recovery Agenten auf der Maschine erkennt und die aktuelle Version der Software installiert. Fahren Sie mit Schritt 6 fort.

Wenn im Assistenten als Nächstes die Seite **Agent aktualisieren** angezeigt wird, bedeutet dies, dass eine ältere Version der Agent-Software auf der zu schützenden Maschine vorhanden ist.

NOTE: Die Agent-Software muss auf der zu schützenden Maschine installiert sein und die Maschine muss neu gestartet worden sein, damit sie im Core gesichert werden kann. Wählen Sie die Option **Maschine nach der Installation automatisch neu starten (empfohlen)** aus, bevor Sie auf „Weiter“ klicken, damit das Installationsprogramm die geschützte Maschine neu startet.

5. Führen Sie auf der Seite **Agent aktualisieren** eine der folgenden Aktionen aus:
   - Um die neue Version der Agenten-Software (entsprechend der Version für Rapid Recovery Core) bereitzustellen, wählen Sie **Rapid Recovery-Agentensoftware auf die neueste Version aktualisieren** aus.
   - Wählen Sie die Option **Rapid Recovery-Agentensoftware auf die neueste Version aktualisieren** ab, wenn die Maschine weiterhin geschützt werden soll, ohne die Version der Agentensoftwareversion zu aktualisieren.
6. Klicken Sie auf **Weiter**.

   Die Seite **Schutz** wird angezeigt.
7. Sie können ggf. auf der Seite **Schutz**, wenn in der Rapid Recovery Core Console anstelle der IP-Adresse ein Name für die geschützte Maschine angezeigt werden soll, im Feld **Anzeigename** einen Namen in das Dialogfeld eingeben.

   Sie können bis zu 64 Zeichen eingeben. Verwenden Sie keine Sonderzeichen (siehe Beschreibung in Unzulässige Zeichen). Darüber hinaus darf der Anzeigename nicht mit den im Abschnitt Unzulässige Phrasen aufgeführten Zeichenkombinationen beginnen.
8. Wählen Sie die gewünschte Einstellung für den Schutzzeitplan aus (siehe nachstehende Beschreibung):
   - Wählen Sie unter **Zeitplaneinstellungen** die Option **Standardschutz (stündliche Snapshots aller Volumes)** aus, um den Standardschutzzeitplan zu verwenden.

     Im Standardschutzzeitplan erstellt der Core jede Stunde Snapshots aller Volumes der geschützten Maschine. Auf der Registerkarte **Zusammenfassung** für die jeweilige geschützte Maschine können Sie jederzeit die Schutzeinstellungen ändern, nachdem der Assistent beendet wurde, z. B. die zu schützenden Volumes auswählen.
   - Wählen Sie unter **Zeitplaneinstellungen** die Option **Benutzerdefinierter Schutz** aus, um einen anderen Schutzzeitplan zu definieren.

     Zeitplanoptionen werden dem Assistenten-Workflow hinzugefügt.
9. Klicken Sie unten auf der Seite **Schutz** auf die Option **Neues Repository für diese Maschine auswählen**, wenn Sie eine Maschine erneut schützen möchten, die zuvor auf diesem Core geschützt wurde, und ein anderes Repository als das ursprüngliche Repository festlegen möchten.

   Erweiterte Optionen (einschließlich Repository und Verschlüsselung) werden dem Assistenten-Workflow hinzugefügt.
10. Setzen Sie die Konfiguration wie folgt fort:
    - Wenn Sie im Assistenten zum Schützen einer Maschine in Schritt 2 eine Standardkonfiguration ausgewählt und Standardschutz festgelegt haben und ein Repository vorhanden ist, klicken Sie auf

Fertigstellen, um die ausgewählten Einstellungen zu bestätigen, den Assistenten zu schließen und die angegebene Maschine zu schützen.

- Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und Standardschutz festgelegt haben und kein Repository vorhanden ist, klicken Sie auf **Weiter** und fahren Sie mit Schritt 13 fort, um ein Repository zu erstellen.
- Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und benutzerdefinierten Schutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit Schritt 11 fort, um auszuwählen, welche Volumes geschützt werden sollen.
- Wenn Sie im Assistenten zum Schützen einer Maschine in Schritt 2 eine erweiterte Konfiguration ausgewählt und den Standardschutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit Schritt 13 fort, um die Repository- und Verschlüsselungsoptionen anzuzeigen.
- Wenn Sie im Assistenten zum Schützen einer Maschine eine erweiterte Konfiguration ausgewählt und benutzerdefinierten Schutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit Schritt 11 fort, um auszuwählen, welche Volumes geschützt werden sollen.

Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, wird anhand des von Ihnen definierten Zeitplans ein Basisabbild (d. h. ein Snapshot aller Daten im geschützten Volume) zum Repository auf dem Rapid Recovery Core übertragen, es sei denn, Sie haben angegeben, den Schutz anfänglich vorübergehend zu deaktivieren.

11. Wählen Sie auf der Seite **Schutz-Volumes** die Volumes aus, die Sie schützen möchten. Klicken Sie in der Spalte „Überprüfen“ auf die aufgelisteten Volumes, die nicht geschützt werden sollen, um die Auswahl aufzuheben. Klicken Sie anschließend auf **Weiter**.

   NOTE: In der Regel sollten zumindest das Volume „System-reserviert“ und das Volume mit dem Betriebssystem (normalerweise Laufwerk C:) geschützt werden.

12. Legen Sie auf der Seite **Schutzzeitplan** einen benutzerdefinierten Schutzzeitplan fest und klicken Sie auf **Weiter**. Ausführliche Informationen zum Festlegen eines benutzerdefinierten Schutzzeitplans finden Sie unter Erstellen von benutzerdefinierten Schutzzeitplänen im einfachen Modus.

    Wenn Sie die Repository-Informationen bereits konfiguriert haben, aber nicht angegeben haben, dass Sie das Repository ändern möchten, und Sie die erweiterte Option in Schritt 2 ausgewählt haben, dann wird die Seite **Verschlüsselung** angezeigt. Fahren Sie mit Schritt 16 fort.

    Wenn Sie die Repository-Informationen bereits konfiguriert haben und die erweiterte Option in Schritt 2 ausgewählt haben, oder wenn Sie angegeben haben, dass Sie das Repository ändern möchten, wird die Seite **Repository** angezeigt. Fahren Sie mit Schritt 13 fort.

13. Führen Sie auf der Seite **Repository** folgende Aktion aus:

    - Wenn Sie bereits über ein Repository verfügen und die Daten für diese Maschine zum Schutz im bestehenden Repository speichern möchten, führen Sie einen der folgenden Schritte aus:

      1. Wählen Sie **Vorhandenes Repository verwenden** aus.
      2. Wählen Sie aus der Liste ein bestehendes Repository aus.
      3. Klicken Sie auf **Weiter**.

      Die Seite **Encryption** (Verschlüsselung) wird angezeigt. Wechseln Sie zu Schritt 15, um ggf. Verschlüsselungseinstellungen zu definieren.

    - Wenn Sie ein Repository erstellen möchten, geben Sie auf der Seite **Repository** die in der folgenden Tabelle beschriebenen Informationen ein und klicken Sie dann auf **Weiter** bzw. **Fertig stellen**.

Tabelle 45. Repository-Einstellungen

Textfeld	Description
Name	Geben Sie den Anzeigenamen des Repositorys ein. Dieses Textfeld enthält standardmäßig das Wort „Repository“ sowie eine Nummer, die der Nummer der Repositorys für diesen Core entspricht. Wenn es sich hierbei

Textfeld	Description
	beispielsweise um das erste Repository handelt, lautet der Standardname „Repository 1“. Ändern Sie den Namen je nach Bedarf. Repository-Namen müssen zwischen 1 und 40 alphanumerischen Zeichen, einschließlich Leerzeichen enthalten. Verwenden Sie weder Unzulässige Zeichen noch Unzulässige Phrasen.
Speicherort	Geben Sie den Speicherort für die geschützten Daten ein. Dieses Volume sollte ein primärer Speicherort sein. Der Speicherort kann lokal (ein Laufwerk auf dem Core-Computer) oder ein freigegebenes CIFS-Netzwerklaufwerk sein. Für eine CIFS-Freigabe muss der Pfad mit \\ beginnen. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig. **CAUTION: Definieren Sie einen dedizierten Ordner innerhalb des Stammverzeichnisses für den Speicherort für das Repository. Geben Sie nicht die Stammposition an. Verwenden Sie zum Beispiel `E:\Repository\`, nicht `E:\`. Wenn das -Repository, das Sie in diesem Schritt erstellen, später entfernt wird, werden auch alle Dateien am Speicherort des Repositorys gelöscht. Wenn Sie Ihren Speicherort unter dem Stammverzeichnis definieren, werden alle anderen Dateien im Volume (z. B. `E:\`) gelöscht, was zu verheerendem Datenverlust führen könnte.** Geben Sie beispielsweise `X:\Repository\Data` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.
Benutzername	Geben Sie einen Benutzernamen für einen Benutzer mit Administratorrechten an. Diese Information ist nur erforderlich, wenn der Repository-Speicherort ein Netzwerkpfad ist.
Kennwort	Geben Sie das Kennwort für den Benutzer mit Administratorrechten ein. Diese Information ist nur erforderlich, wenn der Repository-Speicherort ein Netzwerkpfad ist.
Metadatenpfad	Geben Sie den Speicherort für die geschützten Metadaten ein. Geben Sie beispielsweise `X:\Repository\Metadata` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.

14. Konfigurieren Sie auf der Seite **Repository-Konfiguration** die Menge an Speicherplatz auf der Festplatte, die dem Repository zugewiesen werden soll. Quest empfiehlt die Reservierung von 20 Prozent des Volumens für Metadaten, was die Standard-Einstellung ist. Optional können Sie mit dem Schieberegler oder im Feld **Größe** mehr oder weniger Speicherplatz auf dem Volume dem Repository zuordnen.
15. Wählen Sie optional **Erweiterte Optionen anzeigen** aus und passen Sie die Einstellungen wie in der folgenden Tabelle beschrieben an, wenn Sie detaillierte Informationen über Speicherorteinstellungen anzeigen und eingeben möchten. Um diese Optionen auszublenden, deaktivieren Sie die Option **Erweiterte Optionen anzeigen**. Wenn Sie Ihre Repository-Konfiguration abgeschlossen haben, klicken Sie auf **Weiter** bzw. **Fertig stellen**.

Tabelle 46. Details für Speicherkonfiguration

Textfeld	Description
Bytes pro Sektor	Geben Sie die Anzahl an Bytes an, die jeder Sektor enthalten soll. Der Standardwert ist 512.
Bytes pro Datensatz	Geben Sie die durchschnittliche Anzahl an Bytes pro Datensatz an. Der Standardwert ist 8192.
Schreib-Caching-Richtlinie	Die Schreib-Caching-Richtlinie steuert, wie der Windows Cache-Manager im Repository verwendet wird. Sie ermöglicht die Optimierung der Repository-Leistung bei unterschiedlichen Konfigurationen. Legen Sie den Wert auf eine der folgenden Optionen fest: • Ein • Aus • Sync Bei Auswahl der Standardeinstellung Ein steuert Windows das Caching. Dies ist geeignet für Windows 10 und für Versionen von Windows Server 2012 und höher. **NOTE:** Wenn die Schreib-Caching-Richtlinie auf Ein festgelegt wird, kann die Leistung gesteigert werden. Wenn Sie Windows Server 2008 R2 SP2 verwenden, ist die empfohlene Einstellung „Aus“. Wenn Sie „Aus“ festlegen, wird das Ablegen im Cache-Speicher von Rapid Recovery gesteuert. Bei Auswahl von Sync steuert Windows das Caching sowie die synchrone Eingabe/Ausgabe.

Wenn Sie in Schritt 1 die Option **Erweitert** ausgewählt haben, wird die Seite **Verschlüsselung** angezeigt.

16. Wenn Sie Verschlüsselungsschlüssel für im Repository gespeicherte Daten verwenden möchten, wählen Sie optional auf der Seite **Verschlüsselung Die Daten im Ruhezustand in einem Repository verschlüsseln** aus und führen Sie dann einen der folgenden Schritte aus:

    - Um einen vorhandenen Verschlüsselungsschlüssel auf alle neuen Daten, die im Repository gespeichert werden, anzuwenden, wählen Sie **Daten mit einer Core-basierten Verschlüsselung mit vorhandenem Schlüssel verschlüsseln** und wählen Sie im Drop-Down-Menü **Verschlüsselungsschlüssel auswählen** den Verschlüsselungsschlüssel aus.
    - Um nun einen neuen Verschlüsselungsschlüssel festzulegen, der für alle zukünftigen Daten in Ihrem Repository angewendet werden soll, wählen Sie **Daten mit Core-basierter Verschlüsselung mit einem neuen Schlüssel verschlüsseln** und geben Sie anschließend die Informationen zu dem Schlüssel wie in der folgenden Tabelle beschrieben ein:

Tabelle 47. Neuen Verschlüsselungsschlüssel definieren

Textfeld	Description
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein. Namen für Verschlüsselungsschlüssel müssen 1 bis 64 alphanumerische Zeichen umfassen. Verwenden Sie keine unzulässigen Zeichen oder unzulässigen Phrasen.
Description	Geben Sie einen beschreibenden Kommentar für den Verschlüsselungsschlüssel ein. Diese Informationen werden im Beschreibungsfeld angezeigt, wenn Verschlüsselungsschlüssel in Rapid Recovery Core Console angezeigt werden. Die Beschreibung kann bis zu 254 Zeichen umfassen.

Textfeld	Description
	Es hat sich bewährt, die Verwendung von unzulässigen Zeichen und unzulässigen Phrasen zu vermeiden.
Passphrase	Geben Sie eine Passphrase für die Zugriffssteuerung ein. Sie sollten keine unzulässigen Zeichen verwenden. Bewahren Sie die Passphrase an einem sicheren Ort auf. Quest Datenschutz-Support kann eine Passphrase nicht wiederherstellen. Wenn Sie einen Verschlüsselungsschlüssel erstellt und für eine geschützte Maschine verwendet haben, können Sie keine Daten dieser geschützten Maschine mehr wiederherstellen, wenn die Passphrase verloren geht.
Passphrase bestätigen	Geben Sie die Passphrase erneut ein. Dies wird zur Bestätigung der Passphraseneingabe verwendet.

17. Optional können Sie auf der Seite **Verschlüsselung Die Daten verschlüsseln, die über ein Netzwerk transportiert werden** auswählen, um alle Daten zu verschlüsseln, die über ein Netzwerk transportiert werden. Diese Option ist standardmäßig aktiviert; wenn Sie Daten nicht auf diese Art und Weise verschlüsseln möchten, müssen Sie diese Option also deaktivieren.
18. Klicken Sie auf **Fertigstellen**, um die Einstellungen zu speichern und zu übernehmen.

    Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, wird anhand des von Ihnen definierten Zeitplans ein Basisabbild (d. h. ein Snapshot aller Daten im geschützten Volume) zum Repository auf dem Rapid Recovery Core übertragen, es sei denn, Sie haben angegeben, den Schutz anfänglich vorübergehend deaktivieren.

Schützen eines Clusters

In diesem Thema wird beschrieben, wie Sie einen Cluster in Rapid Recovery unter Schutz stellen. Wenn Sie einen Cluster unter Schutz stellen, müssen Sie den Hostnamen oder die IP-Adresse des Clusters, die Cluster-Anwendung oder einen Cluster-Knoten (Cluster-Maschine) angeben, auf dem die Rapid Recovery Agent-Software installiert ist.

NOTE: Die Snapshots der Daten, die von den geschützten Knoten erfasst werden, werden In einem Repository gespeichert. Damit Sie Daten im Cluster schützen können, müssen Sie mindestens ein Repository erstellen, das dem Rapid Recovery Core zugewiesen ist.

Weitere Informationen zum Einrichten von Repositorys finden Sie unter Grundlegende Informationen zu Repositorys.

1. Klicken Sie in der Rapid Recovery Core Console auf die das Dropdownmenü der Schaltfläche **Protect** (Schützen) und klicken Sie dann auf **Protect Cluster** (Cluster schützen).
2. Wählen Sie auf der Seite **Willkommen** eine der folgenden Optionen aus:
   - Standard
   - Erweitert (optionale Schritte anzeigen)
3. Klicken Sie auf **Weiter**.
4. Geben Sie auf der Seite **Verbindung** des Assistenten die folgenden Informationen an:

Tabelle 48. Einstellungen für Cluster-Verbindungen

Textfeld	Description
Host	Der Hostname oder die IP-Adresse des Clusters, die Cluster-Anwendung oder ein Cluster-Knoten.

Textfeld	Description
Port	Die Portnummer der Maschine, auf der der Rapid Recovery Core mit dem Agenten kommuniziert. Der Standardport ist 8006.
Benutzername	Der Benutzername des Domänenadministrators für die Verbindung zu dieser Maschine, z. B. domain_name\administrator. **NOTE:** Der Domänenname muss angegeben werden. Mit dem Benutzernamen eines lokalen Administrators können Sie keine Verbindung zum Cluster herstellen.
Kennwort	Das Kennwort, das für die Verbindung zu dieser Maschine verwendet wird.

5. Klicken Sie auf **Weiter**.

   NOTE: Wenn auf den Clusterknoten bereits eine ältere Version von Rapid Recovery Agent installiert ist, wird eine Upgrade-Seite im Assistenten angezeigt, die die Möglichkeit bietet, den Agenten zu aktualisieren.

6. Wählen Sie auf der Seite **Knoten** des Assistenten die Knoten aus, die Sie schützen möchten.

   Das System prüft automatisch jede Maschine, die Sie ausgewählt haben.

7. Klicken Sie auf **Weiter**.

   Wenn als Nächstes die Seite **Schutz** im Assistenten „Cluster-Assistenten schützen“ angezeigt wird, fahren Sie mit Schritt 11 fort.

   Wenn die Agent-Software noch nicht auf den zu schützenden Maschinen bereitgestellt wurde oder eine der von Ihnen angegebenen Maschinen aus einem anderen Grund nicht geschützt werden kann, werden die ausgewählten Maschinen auf der Warnseite angezeigt.

8. Optional können Sie eine Maschine auf der Seite **Warnungen** des Assistenten auch selbst überprüfen, indem Sie die Maschine auswählen und in der Symbolleiste auf **Überprüfen** klicken.
9. Wählen Sie auf der **Warnseite** für Maschinen ggf. **Maschinen nach der Agent-Installation automatisch neu starten** aus.

   NOTE: Quest empfiehlt diese Option. Sie müssen die Agent-Maschinen neu starten, damit sie geschützt werden können.

10. Klicken Sie auf **Weiter**, wenn der Status anzeigt, dass die Maschine erreichbar ist, um die Rapid Recovery Agent-Software zu installieren.

    Die Seite **Schutz** wird angezeigt.

11. Sie können ggf. auf der Seite **Schutz**, wenn in der Rapid Recovery Core Console anstelle der IP-Adresse ein Name für die geschützte Maschine angezeigt werden soll, im Feld **Anzeigename** einen Namen in das Dialogfeld eingeben.

    Sie können bis zu 64 Zeichen eingeben. Verwenden Sie keine Sonderzeichen (siehe Beschreibung in). Darüber hinaus darf der Anzeigename nicht mit den im Abschnitt aufgeführten Zeichenkombinationen beginnen.

12. Wählen Sie die gewünschte Einstellung für den Schutzzeitplan aus (siehe nachstehende Beschreibung):

    - Wählen Sie unter „Zeitplaneinstellungen“ die Option **Standardschutz (stündliche Snapshots aller Volumes)** aus, um den Standardschutzzeitplan zu verwenden.

    Im Standardschutzzeitplan erstellt der Core jede Stunde Snapshots aller Volumes der geschützten Maschine. Auf der Registerkarte **Zusammenfassung** für die jeweilige geschützte Maschine können Sie

jederzeit die Schutzeinstellungen ändern, nachdem der Assistent beendet wurde, z. B. die zu schützenden Volumes auswählen.

- Wählen Sie unter „Zeitplaneinstellungen“ die Option **Benutzerdefinierter Schutz** aus, um einen anderen Schutzzeitplan zu definieren.

13. Setzen Sie die Konfiguration wie folgt fort:

    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und Standardschutz festgelegt haben und ein Repository vorhanden ist, klicken Sie auf **Fertigstellen**, um die ausgewählten Einstellungen zu bestätigen, den Assistenten zu schließen und die angegebene Maschine zu schützen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und Standardschutz festgelegt haben und kein Repository vorhanden ist, klicken Sie auf **Weiter** und fahren Sie mit Schritt 16 fort, um ein Repository zu erstellen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und benutzerdefinierten Schutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit dem nächsten Schritt fort, um auszuwählen, welche Volumes geschützt werden sollen.
    - Wenn Sie „Advanced Configuration“ (Erweiterte Konfiguration) für den Protect Machine Wizard (Assistenten zum Schützen der Maschine) und den Standardschutz ausgewählt haben, klicken Sie auf **Weiter** und fahren Sie mit Schritt 16 fort, um die Repository- und Verschlüsselungsoptionen anzuzeigen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine erweiterte Konfiguration ausgewählt und benutzerdefinierten Schutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit dem nächsten Schritt fort, um auszuwählen, welche Volumes geschützt werden sollen.

    Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, wird anhand des von Ihnen definierten Zeitplans ein Basisabbild (d. h. ein Snapshot aller Daten im geschützten Volume) zum Repository auf dem Rapid Recovery Core übertragen, es sei denn, Sie haben angegeben, den Schutz anfänglich vorübergehend zu deaktivieren.

14. Wählen Sie auf der Seite **Schutz-Volumes** die Volumes aus, die Sie schützen möchten. Klicken Sie in der Spalte „Überprüfen“ auf die aufgelisteten Volumes, die nicht geschützt werden sollen, um die Auswahl aufzuheben. Klicken Sie anschließend auf **Weiter**.

    NOTE: In der Regel sollten zumindest das Volume „System-reserviert“ und das Volume mit dem Betriebssystem (normalerweise Laufwerk C:) geschützt werden.

15. Legen Sie auf der Seite **Schutzzeitplan** einen benutzerdefinierten Schutzzeitplan fest und klicken Sie auf **Weiter**. Ausführliche Informationen zum Festlegen eines benutzerdefinierten Schutzzeitplans finden Sie unter Erstellen von benutzerdefinierten Schutzzeitplänen im einfachen Modus.

    Wenn Sie bereits Repository-Informationen konfiguriert und die Option „Erweitert“ in Schritt 1 gewählt haben, wird die Seite „Verschlüsselung“ angezeigt. Fahren Sie mit Schritt 19 fort.

16. Führen Sie auf der Seite **Repository** folgende Aktion aus:

    - Wenn Sie bereits über ein Repository verfügen und die Daten für diese Maschine zum Schutz im bestehenden Repository speichern möchten, führen Sie einen der folgenden Schritte aus:

        1. Wählen Sie **Vorhandenes Repository verwenden** aus.
        2. Wählen Sie aus der Liste ein bestehendes Repository aus.
        3. Klicken Sie auf **Weiter**.

        Die Seite **Encryption** (Verschlüsselung) wird angezeigt. Wechseln Sie zu Schritt 19, um ggf. Verschlüsselungseinstellungen zu definieren.

    - Wenn Sie ein Repository erstellen möchten, geben Sie auf der Seite **Repository** die in der folgenden Tabelle beschriebenen Informationen ein und klicken Sie dann auf **Weiter** bzw. **Fertig stellen**.

Tabelle 49. Repository-Einstellungen

Textfeld	Description
Name	Geben Sie den Anzeigenamen des Repositorys ein. Dieses Textfeld enthält standardmäßig das Wort „Repository“ sowie eine Nummer, die der Nummer der Repositorys für diesen Core entspricht. Wenn es sich hierbei beispielsweise um das erste Repository handelt, lautet der Standardname „Repository 1“. Ändern Sie den Namen je nach Bedarf. Repository-Namen müssen zwischen 1 und 40 alphanumerischen Zeichen, einschließlich Leerzeichen enthalten. Verwenden Sie weder Unzulässige Zeichen noch Unzulässige Phrasen.
Speicherort	Geben Sie den Speicherort für die geschützten Daten ein. Dieses Volume sollte ein primärer Speicherort sein. Der Speicherort kann lokal (ein Laufwerk auf dem Core-Computer) oder ein freigegebenes CIFS-Netzwerklaufwerk sein. Für eine CIFS-Freigabe muss der Pfad mit \\ beginnen. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig. **CAUTION: Definieren Sie einen dedizierten Ordner innerhalb des Stammverzeichnisses für den Speicherort für das Repository. Geben Sie nicht die Stammposition an. Verwenden Sie zum Beispiel `E:\Repository\`, nicht `E:\`. Wenn das -Repository, das Sie in diesem Schritt erstellen, später entfernt wird, werden auch alle Dateien am Speicherort des Repositorys gelöscht. Wenn Sie Ihren Speicherort unter dem Stammverzeichnis definieren, werden alle anderen Dateien im Volume (z. B. `E:\`) gelöscht, was zu verheerendem Datenverlust führen könnte.** Geben Sie beispielsweise `X:\Repository\Data` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.
Benutzername	Geben Sie einen Benutzernamen für einen Benutzer mit Administratorrechten an. Diese Information ist nur erforderlich, wenn der Repository-Speicherort ein Netzwerkpfad ist.
Kennwort	Geben Sie das Kennwort für den Benutzer mit Administratorrechten ein. Diese Information ist nur erforderlich, wenn der Repository-Speicherort ein Netzwerkpfad ist.
Metadatenpfad	Geben Sie den Speicherort für die geschützten Metadaten ein. Geben Sie beispielsweise `X:\Repository\Metadata` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.

17. Konfigurieren Sie auf der Seite **Repository-Konfiguration** die Menge an Speicherplatz auf der Festplatte, die dem Repository zugewiesen werden soll. Quest empfiehlt die Reservierung von 20 Prozent des Volumens für Metadaten, was die Standard-Einstellung ist. Optional können Sie mit dem Schieberegler oder im Feld **Größe** mehr oder weniger Speicherplatz auf dem Volume dem Repository zuordnen.
18. Wählen Sie optional **Erweiterte Optionen anzeigen** aus und passen Sie die Einstellungen wie in der folgenden Tabelle beschrieben an, wenn Sie detaillierte Informationen über Speicherorteinstellungen anzeigen und eingeben möchten. Um diese Optionen auszublenden, deaktivieren Sie die Option

Erweiterte Optionen anzeigen. Wenn Sie Ihre Repository-Konfiguration abgeschlossen haben, klicken Sie auf **Weiter** bzw. **Fertig stellen**.

Tabelle 50. Details für Speicherkonfiguration

Textfeld	Description
Bytes pro Sektor	Geben Sie die Anzahl an Bytes an, die jeder Sektor enthalten soll. Der Standardwert ist 512.
Bytes pro Datensatz	Geben Sie die durchschnittliche Anzahl an Bytes pro Datensatz an. Der Standardwert ist 8192.
Schreib-Caching-Richtlinie	Die Schreib-Caching-Richtlinie steuert, wie der Windows Cache-Manager im Repository verwendet wird. Sie ermöglicht die Optimierung der Repository-Leistung bei unterschiedlichen Konfigurationen. Legen Sie den Wert auf eine der folgenden Optionen fest: • Ein • Aus • Sync Bei Auswahl der Standardeinstellung Ein steuert Windows das Caching. Dies ist geeignet für Windows 10 und für Versionen von Windows Server 2012 und höher. **NOTE:** Wenn die Schreib-Caching-Richtlinie auf Ein festgelegt wird, kann die Leistung gesteigert werden. Wenn Sie Windows Server 2008 R2 SP2 verwenden, ist die empfohlene Einstellung „Aus“. Wenn Sie „Aus“ festlegen, wird das Ablegen im Cache-Speicher von Rapid Recovery gesteuert. Bei Auswahl von Sync steuert Windows das Caching sowie die synchrone Eingabe/Ausgabe.

Wenn Sie in Schritt 1 die Option **Erweitert** ausgewählt haben, wird die Seite **Verschlüsselung** angezeigt.

19. Wenn Sie Verschlüsselungsschlüssel für im Repository gespeicherte Daten verwenden möchten, wählen Sie optional auf der Seite **Verschlüsselung Die Daten im Ruhezustand in einem Repository verschlüsseln** aus und führen Sie dann einen der folgenden Schritte aus:
    - Um einen vorhandenen Verschlüsselungsschlüssel auf alle neuen Daten, die im Repository gespeichert werden, anzuwenden, wählen Sie **Daten mit einer Core-basierten Verschlüsselung mit vorhandenem Schlüssel verschlüsseln** und wählen Sie im Drop-Down-Menü **Verschlüsselungsschlüssel auswählen** den Verschlüsselungsschlüssel aus.
    - Um nun einen neuen Verschlüsselungsschlüssel festzulegen, der für alle zukünftigen Daten in Ihrem Repository angewendet werden soll, wählen Sie **Daten mit Core-basierter Verschlüsselung mit einem neuen Schlüssel verschlüsseln** und geben Sie anschließend die Informationen zu dem Schlüssel wie in der folgenden Tabelle beschrieben ein:

Tabelle 51. Neuen Verschlüsselungsschlüssel definieren

Textfeld	Description
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein. Namen für Verschlüsselungsschlüssel müssen 1 bis 64 alphanumerische Zeichen umfassen. Verwenden Sie keine unzulässigen Zeichen oder unzulässigen Phrasen.
Description	Geben Sie einen beschreibenden Kommentar für den Verschlüsselungsschlüssel ein. Diese Informationen werden im Beschreibungsfeld angezeigt, wenn

Textfeld	Description
	Verschlüsselungsschlüssel in Rapid Recovery Core Console angezeigt werden. Die Beschreibung kann bis zu 254 Zeichen umfassen. Es hat sich bewährt, die Verwendung von unzulässigen Zeichen und unzulässigen Phrasen zu vermeiden.
Passphrase	Geben Sie eine Passphrase für die Zugriffssteuerung ein. Sie sollten keine unzulässigen Zeichen verwenden. Bewahren Sie die Passphrase an einem sicheren Ort auf. Quest Datenschutz-Support kann eine Passphrase nicht wiederherstellen. Wenn Sie einen Verschlüsselungsschlüssel erstellt und für eine geschützte Maschine verwendet haben, können Sie keine Daten dieser geschützten Maschine mehr wiederherstellen, wenn die Passphrase verloren geht.
Passphrase bestätigen	Geben Sie die Passphrase erneut ein. Dies wird zur Bestätigung der Passphraseneingabe verwendet.

20. Optional können Sie auf der Seite **Verschlüsselung Die Daten verschlüsseln, die über ein Netzwerk transportiert werden** auswählen, um alle Daten zu verschlüsseln, die über ein Netzwerk transportiert werden. Diese Option ist standardmäßig aktiviert; wenn Sie Daten nicht auf diese Art und Weise verschlüsseln möchten, müssen Sie diese Option also deaktivieren.
21. Klicken Sie auf **Fertigstellen**, um die Einstellungen zu speichern und zu übernehmen.

    Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, wird anhand des von Ihnen definierten Zeitplans ein Basisabbild (d. h. ein Snapshot aller Daten im geschützten Volume) zum Repository auf dem Rapid Recovery Core übertragen, es sei denn, Sie haben angegeben, den Schutz anfänglich vorübergehend deaktivieren.

Schützen von Knoten in einem Cluster

Diese Aufgabe erfordert, dass Sie zuerst einen Cluster schützen. Weitere Informationen hierzu finden Sie unter Schützen eines Clusters.

In diesem Thema wird beschrieben, wie Sie die Daten auf einem Cluster-Knoten oder einer Cluster-Maschine schützen, auf der ein Rapid Recovery Agent installiert ist. Mit dieser Prozedur können Sie einzelne Knoten zum Schutz hinzufügen, die Sie möglicherweise beim Schützen eines Clusters übersehen haben..

1. Klicken Sie in der Rapid Recovery Core Console unter „Geschützte Maschine“ auf den Cluster mit den Knoten, die Sie schützen möchten.
2. Klicken Sie auf der Übersichtsseite für den Cluster auf**geschützte Knoten**.
3. Klicken Sie auf der Seite „geschützte Knoten“ auf **Cluster-Knoten schützen**.
4. Wählen Sie im Dialogfeld „Cluster-Knoten schützen“ die folgenden Informationen aus, oder geben Sie sie ein.

Tabelle 52. Einstellungen für den Schutz von Cluster-Knoten

Textfeld	Description
Host	Eine Dropdown-Liste mit den Knoten, die im Cluster geschützt werden können.
Port	Die Portnummer, über die der Rapid Recovery Core mit dem Agenten auf dem Knoten kommuniziert.
Benutzername	Der Benutzername des Domänenadministrators für die Verbindung zu diesem Knoten , z. B. example_domain\administrator oder administrator@example_domain.com.

Textfeld	Description
Kennwort	Das Kennwort, das für die Verbindung zu dieser Maschine verwendet wird.

5. Um den Knoten hinzuzufügen, klicken Sie auf **Verbinden**.
6. Zum Starten des Schutzes dieses Knotens mit den standardmäßigen Schutzeinstellungen fahren Sie mit Schritt 13 fort.

   NOTE: Die Standardeinstellungen stellen sicher, dass alle Volumes der Maschine über einen Zeitplan alle 60 Minuten geschützt werden.
7. Wenn Sie ein anderes Repository als die Standardeinstellungen verwenden möchten, wählen Sie in der Dropdownliste des Dialogfelds „Protect [Node Name]“ ([Knotenname] schützen) ein Repository aus.
8. Wenn Sie die Wiederherstellungspunkte für diesen Cluster mithilfe von von Core-basierter Verschlüsselung sichern möchten, wählen Sie in der Dropdownliste einen Verschlüsselungsschlüssel aus.
9. Wählen Sie **Schutz zunächst vorübergehend deaktivieren** aus, wenn der Schutz nicht sofort nach Abschluss dieses Verfahrens beginnen soll.
10. Um benutzerdefinierte Einstellungen einzugeben (z. B. um den zeitlichen Verlauf des Schutzes für die freigegebenen Volumes anzupassen), gehen Sie wie folgt vor:
    a. Zum Anpassen von Einstellungen für ein einzelnes Volume, klicken Sie neben dem Volume, das Sie anpassen möchten, auf **Funktion**.
    b. Siehe Erstellen von benutzerdefinierten Schutzzeitplänen im einfachen Modus.
11. Klicken Sie auf **Protect** (Schützen).

Erstellen von benutzerdefinierten Schutzzeitplänen im einfachen Modus

Das Verfahren zum Erstellen eines benutzerdefinierten Schutzzeitplans von innerhalb eines Assistenten ist identisch mit dem Verfahren zum Erstellen eines Schutzzeitplan für eine bestehende Maschine in einfachen Modus. Schutzzeitpläne, die in einem Assistenten oder im einfachen Modus erstellt werden, werden nicht als Vorlage gespeichert. Zum Erstellen von Vorlagen oder mehreren Schutzzeitplänen, siehe Erstellen mehrerer Schutzzeitplan-Zeiträume im erweiterten Modus. Führen Sie die hier beschriebenen Schritte aus, um benutzerdefinierte Zeitpläne zu erstellen, anhand derer Rapid Recovery eine Sicherungskopie Ihrer Daten von geschützten Maschinen erstellen kann.

1. Führen Sie eine der folgenden Optionen aus:
   - Bei Verwendung eines Schutzassistenten (Maschine schützen, Mehrere Maschinen schützen, Cluster schützen) wählen Sie auf der Seite **Schutz** des Assistenten die Option **Benutzerdefinierter Schutz** und klicken Sie dann auf **Weiter**.
   - Wenn Sie einen Schutzzeitplan für eine Maschine erstellen, die bereits geschützt ist, erweitern Sie auf der Seite „Zusammenfassung“ der geschützten Maschine die Volumes der geschützten Maschine, wählen die gewünschten Volumes aus und klicken dann auf **Einen Zeitplan festlegen**.

   Die Seite bzw. das Dialogfeld **Schutzzeitplan** wird angezeigt.
2. Schließen Sie auf der Seite bzw. dem Dialogfeld **Schutzzeitplan** eine der folgenden Optionen ab:
   - Um einen Schutzzeitplan festzulegen, der an bestimmten Tagen und zu bestimmten Uhrzeiten aktiv wird, wählen Sie **Zeiträume** und fahren Sie mit Schritt 3 fort.
   - Zum Festlegen einer bestimmten Zeit zur täglichen Sicherung der Maschine wählen Sie **Uhrzeit für den täglichen Schutz** und fahren Sie mit Schritt 7 fort.
3. Zum Ändern des Intervallzeitplans für einen Zeitraum führen Sie die folgenden Schritte aus:
   a. Erstellen Sie einen Zeitraum durch Auswahl einer **Von**- und einer **Bis**-Zeit.
   b. Klicken Sie für jeden Zeitraum in das Textfeld „Intervall“ und geben Sie ein entsprechendes Intervall in Minuten ein.

Markieren Sie beispielsweise das Standard-Intervall 60 und ersetzten Sie den Wert durch den Wert 20, sodass in diesem Zeitraum alle 20 Minuten Snapshots erstellt werden.

4. Wenn Sie Snapshots für Spitzen- und Nebenzeiten anpassen möchten, führen Sie die folgenden Schritte aus: legen Sie ein optimales Intervall für den Spitzenzeitbereich fest, wählen Sie die Option **Snapshots für die verbleibenden Zeit erstellen** aus und legen Sie ein Intervall für Nebenzeiten fest, indem Sie die folgenden Schritte ausführen:
    a. Wählen Sie **Wochentage**.
    b. Geben Sie die **Von**- und **Bis**-Zeiten an, um einen Zeitraums während der Hauptgeschäftszeiten festzulegen.
    c. Geben Sie im Feld **Alle X Minuten** ein Intervall in Minuten ein, um festzulegen, wie oft Rapid Recovery Wiederherstellungspunkte während dieser Spitzenzeiten erstellen soll.

    Markieren Sie beispielsweise das Standard-Intervall 60 und ersetzten Sie den Wert durch den Wert 20, sodass in diesem Zeitraum alle 20 Minuten währen des Zeitbereichs, den Sie für diesen Zeitraum gewählt haben, Snapshots erstellt werden.
    d. Um einen Zeitplan für Snapshots außerhalb der Spitzenzeiten festzulegen, wählen Sie **Snapshots für den Rest der Zeit erfassen**.
    e. Geben Sie im Feld **Alle X Minuten** ein Intervall in Minuten ein, um festzulegen, wie oft Rapid Recovery Wiederherstellungspunkte außerhalb dieser Spitzenzeiten erstellen soll.

    Da während dieser Stunden weniger Geschäftsaktivitäten anstehen und weniger Änderungen zu sichern sind, können Sie sich beispielsweise dafür entscheiden, weniger Snapshots aufzunehmen und das Standardintervall von 60 Minuten zu behalten.
5. Fahren Sie mit Schritt 7 fort.
6. Wählen Sie **Tägliche Schutzzeit** aus, wenn täglich zu einer bestimmten Uhrzeit eine Sicherung durchgeführt werden soll, und geben Sie eine Uhrzeit im Format HH:MM AM ein. Geben Sie beispielsweise 9:00 PM ein, wenn täglich um 21:00 Uhr eine Sicherung durchgeführt werden soll.
7. Wählen Sie **Schutz zunächst vorübergehend deaktivieren** aus, um den Zeitplan zu definieren, ohne dass Sicherungen gestartet werden.

    Nachdem Sie den Schutz im Assistenten vorübergehend deaktiviert haben, bleibt dieser so lange deaktiviert, bis Sie ihn explizit wieder aktivieren. Sobald der Schutz wieder aktiviert wird, werden Sicherungen gemäß dem eingerichteten Zeitplan durchgeführt. Weitere Informationen zum Wiederaufnehmen des Schutzes finden Sie unter Anhalten und Wiederaufnehmen des Schutzes.
8. Klicken Sie auf **Fertigstellen** bzw. **Weiter**, wenn der Schutzzeitplan wie gewünscht geändert wurde.

    Wenn Sie einen Assistenten verwenden, fahren Sie mit dem nächsten Schritt im Assistenten fort. Kehren Sie zur Vorgehensweise des jeweiligen Assistenten zurück, um weitere erforderliche Einstellungen zu konfigurieren.

See also: Grundlegende Informationen zu Schutzzeitplänen
See also: Erstellen von benutzerdefinierten Schutzzeitplänen im einfachen Modus
See also: Erstellen mehrerer Schutzzeitplan-Zeiträume im erweiterten Modus

Erstellen mehrerer Schutzzeitplan-Zeiträume im erweiterten Modus

Ein Schutzzeitplan definiert, wann Sicherungskopien von geschützten Maschinen auf den Rapid Recovery Core übertragen werden. Die Schutzzeitpläne werden zunächst mit den Assistenten zum Schützen einer Maschine bzw. zum Schützen mehrerer Maschinen definiert.

Sie können bestehende Schutzzeitpläne jederzeit auf der Seite „Zusammenfassung“ für eine bestimmte Agent-Maschine ändern.

NOTE: Konzeptionelle Informationen zu Schutzzeitplänen finden Sie unter Grundlegende Informationen zu Schutzzeitplänen. Informationen zum Schützen einer einzelnen Maschine finden Sie unter Schützen einer Maschine. Informationen zum Massenschutz (Schützen mehrerer Maschinen) finden Sie unter So schützen Sie mehrere Maschinen. Informationen zum Anpassen von Schutzzeiträumen beim Schützen eines Agenten mit einem der beiden Assistenten finden Sie unter Erstellen von benutzerdefinierten Schutzzeitplänen im einfachen Modus. Informationen zum Ändern eines bestehenden Schutzzeitplans finden Sie unter Erstellen mehrerer Schutzzeitplan-Zeiträume im erweiterten Modus.

Führen Sie die folgenden Schritte aus, um einen bestehenden Schutzzeitplan für die Volumes einer geschützten Maschine zu ändern.

1. Wählen Sie in der Core Console aus der Liste der geschützten Maschinen den Namen der Maschine aus, die über den Schutzzeitplan verfügt, den Sie ändern möchten.
2. Erweitern Sie auf der Seite „Zusammenfassung“ für die ausgewählte Maschine im Fensterbereich „Volumes“ die Volumes der geschützten Maschine, wählen Sie die entsprechenden Volumes aus und klicken Sie dann auf **Einen Zeitplan festlegen**.

   Zunächst wird derselbe Schutzzeitplan für alle Volumes verwendet.

   Klicken Sie auf das Kontrollkästchen in der Kopfzeile, um alle Volumes gleichzeitig auszuwählen. Klicken Sie auf (Schutzgruppe) zum Erweitern der geschützten Volumes, damit Sie alle Volumes sehen und eines oder mehrere auswählen können.

   NOTE: In der Regel sollten zumindest das Volume „System-reserviert“ und das Volume mit dem Betriebssystem (normalerweise Laufwerk C:) geschützt werden.

   Das Dialogfeld **Schutzzeitplan** wird angezeigt.
3. Führen Sie eine der folgenden Möglichkeiten im Dialogfeld **Schutzzeitplan** aus:
   - Das Verfahren zum Ändern des vorhandenen Schutzzeitplan-Zeitraums, der auf der ersten Seite des Dialogfelds angezeigt wird und als „Einfacher Modus bezeichnet wird, finden Sie unter Erstellen mehrerer Schutzzeitplan-Zeiträume im erweiterten Modus.
   - Wenn Sie zuvor eine Schutzzeitplanvorlage erstellt haben und diese auf diese geschützte Maschine anwenden möchten, klicken Sie auf **Erweiterter Modus**, wählen Sie die Vorlage aus der Drop-Down-Liste **Vorlagen** aus, klicken Sie auf **OK** zum Bestätigen und wechseln Sie dann zu Schritt 7
   - Deaktivieren Sie die Kontrollkästchen neben den einzelnen Zeitraumoptionen, um einen bestehenden Zeitraum aus dem Zeitplan zu entfernen, und gehen Sie dann zu Schritt 7. Folgende Optionen sind verfügbar:
     - Wochentage (Mo-Fr): Dieser Zeitraum steht für eine typische 5-Tage-Woche.
     - Wochenenden (Sa, So): Dieser Zeitraum steht für ein typisches Wochenende.
   - Wenn Sie einen neuen Schutzzeitplan als Vorlage speichern möchten, klicken Sie auf **Erweiterter Modus** und wechseln Sie dann zu Schritt 4.
4. Ein Zeitraum ist ein festgelegter Zeitraum, in dem Sie bestimmen, wie viele Minuten zwischen jedem Snapshot verstreichen sollten. Wenn Start- und Endzeit für Wochentage auf 00:00 bis 23:59 eingestellt sind, ist nur ein Zeitraum vorhanden. Gehen Sie folgendermaßen vor, um Start- oder Endzeit eines festgelegten Zeitraums zu ändern:
   a. Wählen Sie den entsprechenden Zeitraum aus.
   b. Um die Startzeit für diese Periode zu ändern, verwenden Sie das Uhr-Symbol unter **Startzeit**.

   Verwenden Sie beispielsweise die Pfeile, um eine Uhrzeit von 08:00 Uhr anzuzeigen.

   c. Um die Endzeit für diese Periode zu ändern, verwenden Sie das Uhr-Symbol unter **Endzeit**.

   Verwenden Sie beispielsweise die Pfeile, um eine Uhrzeit von 18:00 Uhr anzuzeigen.

   d. Ändern Sie das Intervall den jeweiligen Anforderungen entsprechend. Ändern Sie beispielsweise das Intervall für Spitzenzeiten von 60 Minuten in 20 Minuten, damit jede Stunde drei Snapshots erstellt werden.

Eine blaue Leiste bietet eine visuelle Darstellung dieses Intervalls.

5. Wenn Sie einen anderen Zeitraum als 00:00 bis 23:59 Uhr in Schritt 7 definiert haben und Datensicherungen in den verbleibenden Zeiträumen ausgeführt werden sollen, müssen Sie anhand der folgenden Schritte weitere Zeiträume hinzufügen, um den Schutz zu definieren:
    a. Klicken Sie unter der entsprechenden Kategorie auf **Zeitraum hinzufügen.**
    b. Klicken Sie auf das Uhr-Symbol und wählen Sie entsprechend die gewünschten Start- und Endzeiten.

    Legen Sie beispielsweise eine Startzeit von 00:00 und eine Endzeit von 07:59 fest.

    c. Ändern Sie das Intervall den jeweiligen Anforderungen entsprechend. Ändern Sie beispielsweise das Intervall für Zeiten geringer Auslastung von 60 Minuten in 120 Minuten, damit alle zwei Stunden in Snapshot erstellt wird.
6. Erstellen Sie bei Bedarf weitere Zeiträume. Legen Sie dazu die gewünschten Start- und Endzeiten sowie Intervalle fest.

    NOTE: Wenn Sie einen Punkt entfernen möchten, den Sie hinzugefügt haben, klicken Sie auf das Papierkorb-Symbol rechts in dieser Periode und dann auf **Ja**, um den Vorgang zu bestätigen.
7. Um eine Vorlage aus dem Zeitplan, den Sie festgelegt haben zu erstellen, klicken Sie auf **Als Vorlage speichern**.
8. Geben Sie einen Namen für die Vorlage in das Fenster „Vorlage speichern“ ein und klicken Sie auf **Speichern**.
9. Wenn Ihr Schutzzeitplan Ihren Anforderungen entspricht, klicken Sie auf **Anwenden**.

    Das Dialogfeld „Schutzzeitplan“ wird geschlossen.

See also: Grundlegende Informationen zu Schutzzeitplänen
See also: Erstellen von benutzerdefinierten Schutzzeitplänen im einfachen Modus
See also: Erstellen mehrerer Schutzzeitplan-Zeiträume im erweiterten Modus

Vorübergehendes Deaktivieren und erneutes Aktivieren der Schutzfunktion

Wenn Sie den Schutz vorübergehend deaktivieren, werden vorübergehend alle Übertragungen der Daten von der ausgewählten Maschine zum Rapid Recovery Core angehalten. Wenn Sie den Schutz wieder aktivieren, folgt der Rapid Recovery Core dem festgelegten Schutzzeitplan, der die Daten dem jeweiligen Zeitplan entsprechend sichert.

Sie können den Schutz für eine Rapid Recovery geschützte Maschine vorübergehend deaktivieren:

- Beim Einrichten der Schutzfunktion mit den Assistenten zum Schützen einer Maschine bzw. zum Schützen mehrerer Maschinen
- Im Drop-Down-Menü „Geschützte Maschinen“ im linken Navigationsbereich dieses Rapid Recovery Core (Schutz für alle Agenten vorübergehend deaktivieren).
- Auf der Seite „Geschützte Maschinen“ (wird geöffnet, wenn Sie auf das Menü „Geschützte Maschinen“ klicken)
- Im Drop-Down-Menü „Geschützte Maschinen“ einer bestimmten geschützten Maschine.
- Von oben auf jeder Seite für eine bestimmte geschützte Maschine.

Wenn Sie den Schutz mit den Assistenten zum Schützen einer Maschine bzw. zum Schützen mehrerer Maschinen vorübergehend deaktivieren, ist der Schutz solange deaktiviert, bis es wieder explizit aktiviert wird.

Wenn Sie den Schutz außerhalb eines Assistenten vorübergehend deaktivieren, können Sie auswählen, ob der Schutz solange deaktiviert werden soll, bis er wieder aktiviert wird, oder die Schutzfunktion für einen bestimmten Zeitraum deaktivieren (Angabe als Kombination von Tagen, Stunden und Minuten). Wenn Sie den Schutz für einen bestimmten Zeitraum deaktivieren, wird die Schutzfunktion nach Ablauf dieses Zeitraums automatisch dem jeweiligen Schutzzeitplan entsprechend wieder aktiviert.

Sie können den Schutz für alle vorübergehend deaktivierte Rapid Recovery geschützten Maschinen wieder aktivieren:

- Im Drop-Down-Menü „Geschützte Maschinen“ im linken Navigationsbereich dieses Rapid Recovery Core (Schutz für alle Agenten wieder aufnehmen).
- Im Drop-Down-Menü „Geschützte Maschinen“ einer bestimmten geschützten Maschine.
- Auf der Seite „Geschützte Maschinen“ (wird geöffnet, wenn Sie auf das Menü „Geschützte Maschinen“ klicken)
- Von oben auf jeder Seite für eine bestimmte geschützte Maschine.

Gehen Sie folgendermaßen vor, um den Schutz vorübergehend zu deaktivieren bzw. wieder zu aktivieren.

1. Klicken Sie in der Rapid Recovery Core Console auf das Drop-Down-Menü „Geschützte Maschinen“ im linken Navigationsbereich, um den Schutz für alle Maschinen vorübergehend zu deaktivieren und gehen Sie dann wie folgt vor:
    a. Wählen Sie **Schutz vorübergehend deaktivieren** aus.

    Das Dialogfeld „Schutz vorübergehend deaktivieren“ wird angezeigt.

    b. Wählen Sie über die nachstehend beschriebenen Optionen die gewünschte Einstellung aus und klicken Sie auf **OK**.

    - Wählen Sie **Deaktivieren bis Wiederaktivierung**, wenn der Schutz deaktiviert werden soll, bis er wieder aktiviert wird.
    - Wählen Sie **Vorübergehend deaktivieren für (Dauer)** aus, wenn der Schutz für einen bestimmten Zeitraum deaktiviert werden soll, und geben Sie dann über die Steuerelemente Tage, Stunden und Minuten den gewünschten Deaktivierungszeitraum an.
2. Um den Schutz für alle Maschinen wieder zu aktivieren, gehen Sie wie folgt vor:
    a. Wählen Sie **Schutz wieder aktivieren** aus.

    Das Dialogfeld „Schutz wieder aktivieren“ wird angezeigt.

    b. Klicken Sie im Dialogfeld „Schutz wieder aktivieren“ auf **Ja**.

    Das Dialogfeld „Schutz wieder aktivieren“ wird geschlossen und der Schutz wird für alle Maschinen wieder aktiviert.
3. Um den Schutz für eine einzelne Maschine vorübergehend zu deaktivieren, klicken Sie dann im linken Navigationsbereich, auf das Drop-Down -Menü rechts neben der Maschine, die verändert werden soll und führen Sie dann die folgenden Schritte aus:
    a. Wählen Sie **Schutz vorübergehend deaktivieren** aus.

    Das Dialogfeld „Schutz vorübergehend deaktivieren“ wird angezeigt.

    b. Wählen Sie über die nachstehend beschriebenen Optionen die gewünschte Einstellung aus und klicken Sie auf **OK**.

    - Wählen Sie **Deaktivieren bis Wiederaktivierung**, wenn der Schutz deaktiviert werden soll, bis er wieder aktiviert wird.
    - Wählen Sie **Vorübergehend deaktivieren für (Dauer)** aus, wenn der Schutz für einen bestimmten Zeitraum deaktiviert werden soll, und geben Sie dann über die Steuerelemente Tage, Stunden und Minuten den gewünschten Deaktivierungszeitraum an.
4. Um den Schutz für eine Maschine wieder zu aktivieren, gehen Sie wie folgt vor:
    a. Wählen Sie **Schutz wieder aktivieren** aus.

    Das Dialogfeld „Schutz wieder aktivieren“ wird angezeigt.

    b. Klicken Sie im Dialogfeld „Schutz wieder aktivieren“ auf **Ja**.

    Das Dialogfeld „Schutz wieder aktivieren“ wird geschlossen und der Schutz wird für die ausgewählte Maschine wieder aktiviert.
5. Um den Schutz für eine einzelne Maschine über die Maschinenseiten vorübergehend zu deaktivieren, navigieren Sie zu der betreffenden Maschine.

Die Seite „Zusammenfassung“ für die ausgewählte Maschine wird angezeigt.

a. Klicken Sie oben auf der Seite auf **Vorübergehend deaktivieren**.

Das Dialogfeld „Schutz vorübergehend deaktivieren“ wird angezeigt.

b. Wählen Sie über die nachstehend beschriebenen Optionen die gewünschte Einstellung aus und klicken Sie auf **OK**.

- Wählen Sie **Deaktivieren bis Wiederaktivierung**, wenn der Schutz deaktiviert werden soll, bis er wieder aktiviert wird.
- Wählen Sie **Vorübergehend deaktivieren für (Dauer)** aus, wenn der Schutz für einen bestimmten Zeitraum deaktiviert werden soll, und geben Sie dann über die Steuerelemente Tage, Stunden und Minuten den gewünschten Deaktivierungszeitraum an.

6. Wenn Sie den Schutz wieder aktivieren möchten, gehen Sie wie folgt vor:
   a. Klicken Sie oben auf der Seite auf **Wieder aktivieren**.
   b. Klicken Sie im Dialogfeld „Schutz wieder aktivieren“ auf **Ja**.

   Das Dialogfeld „Schutz wieder aktivieren“ wird geschlossen und der Schutz wird für die ausgewählte Maschine wieder aktiviert.

So schützen Sie mehrere Maschinen

Mit dem Assistenten zum Schützen mehrerer Maschinen können Sie zwei oder mehr Windows-Maschinen gleichzeitig dem Schutz durch den Rapid Recovery Core unterstellen. Um Ihre Daten mit Rapid Recovery zu schützen, müssen Sie die zu schützenden Arbeitsstationen und Server, z. B. Exchange-Server, SQL Server, Linux-Server usw., zur Rapid Recovery Core Console hinzufügen.

Wie beim Schutz einzelner Maschinen, erfordert das gleichzeitige Schützen von mehreren Maschinen die Installation der Rapid Recovery-Agentensoftware auf jeder Maschine, die Sie schützen möchten.

NOTE: Als eine Ausnahme von dieser Regel, zum Schutz virtueller Maschinen auf einem VMware ESXi- oder einem Hyper-V-Host, können Sie agentenlosen Schutz verwenden. Weitere Informationen, einschließlich der Einschränkungen für agentenlosen Schutz, finden Sie unter Grundlegende Informationen zu Rapid Snap for Virtual.

Die geschützten Maschinen müssen mit einer Sicherheitsrichtlinie konfiguriert sein, die eine Remote-Installation zulässt.

Um eine Verbindung mit den Maschinen herzustellen, müssen sie eingeschaltet und zugreifbar sein.

Es gibt mehrere Möglichkeiten, die Agent-Software gleichzeitig auf mehreren Maschinen bereitzustellen. Beispiel:

- Sie können die Rapid Recovery-Agentensoftware auf mehreren Maschinen unter Verwendung des Bereitstellungsassistenten für die Agentensoftware installieren. Weitere Informationen hierzu finden Sie unter Verwendung des Bereitstellungsassistenten für die Agentensoftware zum Bereitstellen einer oder mehrerer Maschinen.
- Sie können die Rapid Recovery-Agentensoftware mit dem Assistenten zum Schützen mehrerer Maschinen einsetzen.

Diese Vorgehensweise zum Schutz mehrerer Maschinen umfasst optionale Schritte, die Sie durchführen können, wenn Sie eine erweiterte Konfiguration auswählen. Zu den erweiterten Optionen zählen Repositoryfunktionen und Verschlüsselung. Sie können beispielsweise ein vorhandenes Rapid Recovery-Repository zum Speichern von Snapshots angeben oder ein neues Repository erstellen. Sie können auch einen vorhandenen Verschlüsselungsschlüssel angeben (oder einen neuen Verschlüsselungsschlüssel hinzufügen), um die Daten der jeweiligen von Ihnen geschützten Maschine, die im Core gespeichert werden, zu verschlüsseln.

Der Workflow des Assistenten zum Schützen mehrerer Maschinen kann abhängig von der jeweiligen Umgebung geringfügig abweichen. Wenn beispielsweise die Rapid Recovery-Agentensoftware auf den zu schützenden

Maschinen installiert ist, werden Sie im Assistenten nicht aufgefordert, die Software zu installieren. Ebenso werden Sie nicht aufgefordert, ein Repository zu erstellen, wenn im Core bereits ein Repository vorhanden ist.

Beim Schutz mehrerer Maschinen befolgen Sie die entsprechenden Verfahren, basierend auf Ihrer Konfiguration. Informationen für den Schutz mehrerer Maschinen finden Sie in den folgenden Optionen:

- Schutz mehrerer Maschinen in einer Active Directory-Domäne
- Schutz von mehreren Maschinen auf einem virtuellen VMware vCenter/ESXi-Host
- Schutz von mehreren Maschinen auf einem virtuellen Hyper-V-Host
- Manuelles Schützen mehrerer Maschinen

Schutz mehrerer Maschinen in einer Active Directory-Domäne

Verwenden Sie dieses Verfahren, um gleichzeitig eine oder mehrere Maschinen auf einer Active Directory-Domäne zu schützen.

1. Klicken Sie auf der Rapid Recovery Core Console Core Console auf das Drop-Down-Menü **Schützen** und dann auf **Mehrere Maschinen schützen**.

   Daraufhin wird der Protect Multiple Machines Wizard (Assistent zum Schützen mehrerer Maschinen) angezeigt.
2. Wählen Sie auf der Seite **Willkommen** eine der folgenden Optionen aus:
   - Standard
   - Erweitert (optionale Schritte anzeigen)
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Verbindung** des Assistenten von der Drop-Down-Liste **QuelleActive Directory**.
5. Geben Sie die Domänen-Informationen und Anmeldeinformationen ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 53. Domäneninformationen und Anmeldeinformationen

Textfeld	Description
Host	Der Hostname oder die IP-Adresse der Active Directory-Domäne.
Benutzername	Der Benutzername für die Verbindung zur Domäne, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).
Kennwort	Das sichere Kennwort, das für die Verbindung zur Domäne verwendet wird.

6. Klicken Sie auf **Weiter**.
7. Wählen Sie auf der Seite **Maschinen auswählen** des Assistenten die Maschinen, die Sie schützen möchten.

   Das System prüft automatisch jede Maschine, die Sie ausgewählt haben.
8. Klicken Sie auf **Weiter**.

   Wechseln Sie zu **Schritt 12**, wenn als Nächstes die Seite Schutz im Assistent zum Schützen mehrerer Maschinen angezeigt wird.

Wenn die Agent-Software noch nicht auf den zu schützenden Maschinen bereitgestellt wurde oder eine der von Ihnen angegebenen Maschinen aus einem anderen Grund nicht geschützt werden kann, werden die ausgewählten Maschinen auf der Warnseite angezeigt.

9. Optional können Sie eine Maschine auf der Seite **Warnungen** des Assistenten auch selbst überprüfen, indem Sie die Maschine auswählen und in der Symbolleiste auf **Überprüfen** klicken.
10. Wählen Sie auf der **Warnseite** für Maschinen ggf. **Maschinen nach der Agent-Installation automatisch neu starten** aus.

    NOTE: Quest empfiehlt diese Option. Sie müssen die Agent-Maschinen neu starten, damit sie geschützt werden können.

11. Klicken Sie auf **Weiter**, wenn der Status anzeigt, dass die Maschine erreichbar ist, um die Rapid Recovery Agent-Software zu installieren.

    Die Seite **Schutz** wird angezeigt.
12. Sie können ggf. auf der Seite **Schutz**, wenn in der Rapid Recovery Core Console anstelle der IP-Adresse ein Name für die geschützte Maschine angezeigt werden soll, im Feld **Anzeigename** einen Namen in das Dialogfeld eingeben.

    Sie können bis zu 64 Zeichen eingeben. Verwenden Sie keine Sonderzeichen (siehe Beschreibung in). Darüber hinaus darf der Anzeigename nicht mit den im Abschnitt aufgeführten Zeichenkombinationen beginnen.
13. Wählen Sie die gewünschte Einstellung für den Schutzzeitplan aus (siehe nachstehende Beschreibung):

    - Wählen Sie unter „Zeitplaneinstellungen“ die Option **Standardschutz (stündliche Snapshots aller Volumes)** aus, um den Standardschutzzeitplan zu verwenden.

    Im Standardschutzzeitplan erstellt der Core jede Stunde Snapshots aller Volumes der geschützten Maschine. Auf der Registerkarte **Zusammenfassung** für die jeweilige geschützte Maschine können Sie jederzeit die Schutzeinstellungen ändern, nachdem der Assistent beendet wurde, z. B. die zu schützenden Volumes auswählen.

    - Wählen Sie unter „Zeitplaneinstellungen“ die Option **Benutzerdefinierter Schutz** aus, um einen anderen Schutzzeitplan zu definieren.
14. Setzen Sie die Konfiguration wie folgt fort:

    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und Standardschutz festgelegt haben und ein Repository vorhanden ist, klicken Sie auf **Fertigstellen**, um die ausgewählten Einstellungen zu bestätigen, den Assistenten zu schließen und die angegebene Maschine zu schützen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und Standardschutz festgelegt haben und kein Repository vorhanden ist, klicken Sie auf **Weiter** und fahren Sie mit Schritt 17 fort, um ein Repository zu erstellen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und benutzerdefinierten Schutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit dem nächsten Schritt fort, um auszuwählen, welche Volumes geschützt werden sollen.
    - Wenn Sie „Advanced Configuration“ (Erweiterte Konfiguration) für den Protect Machine Wizard (Assistenten zum Schützen der Maschine) und den Standardschutz ausgewählt haben, klicken Sie auf **Weiter** und fahren Sie mit Schritt 17 fort, um die Repository- und Verschlüsselungsoptionen anzuzeigen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine erweiterte Konfiguration ausgewählt und benutzerdefinierten Schutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit dem nächsten Schritt fort, um auszuwählen, welche Volumes geschützt werden sollen.

    Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, wird anhand des von Ihnen definierten Zeitplans ein Basisabbild (d. h. ein Snapshot aller Daten im geschützten Volume) zum Repository auf

dem Rapid Recovery Core übertragen, es sei denn, Sie haben angegeben, den Schutz anfänglich vorübergehend zu deaktivieren.

15. Wählen Sie auf der Seite **Schutz-Volumes** die Volumes aus, die Sie schützen möchten. Klicken Sie in der Spalte „Überprüfen“ auf die aufgelisteten Volumes, die nicht geschützt werden sollen, um die Auswahl aufzuheben. Klicken Sie anschließend auf **Weiter**.

    NOTE: In der Regel sollten zumindest das Volume „System-reserviert“ und das Volume mit dem Betriebssystem (normalerweise Laufwerk C:) geschützt werden.

16. Legen Sie auf der Seite **Schutzzeitplan** einen benutzerdefinierten Schutzzeitplan fest und klicken Sie auf **Weiter**. Ausführliche Informationen zum Festlegen eines benutzerdefinierten Schutzzeitplans finden Sie unter Erstellen von benutzerdefinierten Schutzzeitplänen im einfachen Modus.

    Wenn Sie bereits Repository-Informationen konfiguriert und die Option „Erweitert“ in Schritt 1 gewählt haben, wird die Seite „Verschlüsselung“ angezeigt. Fahren Sie mit Schritt 20 fort.

17. Führen Sie auf der Seite **Repository** folgende Aktion aus:

    - Wenn Sie bereits über ein Repository verfügen und die Daten für diese Maschine zum Schutz im bestehenden Repository speichern möchten, führen Sie einen der folgenden Schritte aus:

      1. Wählen Sie **Vorhandenes Repository verwenden** aus.
      2. Wählen Sie aus der Liste ein bestehendes Repository aus.
      3. Klicken Sie auf **Weiter**.

      Die Seite **Encryption** (Verschlüsselung) wird angezeigt. Wechseln Sie zu Schritt 20, um ggf. Verschlüsselungseinstellungen zu definieren.

    - Wenn Sie ein Repository erstellen möchten, geben Sie auf der Seite **Repository** die in der folgenden Tabelle beschriebenen Informationen ein und klicken Sie dann auf **Weiter** bzw. **Fertig stellen**.

Tabelle 54. Repository-Einstellungen

Textfeld	Description
Name	Geben Sie den Anzeigenamen des Repositorys ein. Dieses Textfeld enthält standardmäßig das Wort „Repository“ sowie eine Nummer, die der Nummer der Repositorys für diesen Core entspricht. Wenn es sich hierbei beispielsweise um das erste Repository handelt, lautet der Standardname „Repository 1“. Ändern Sie den Namen je nach Bedarf. Repository-Namen müssen zwischen 1 und 40 alphanumerischen Zeichen, einschließlich Leerzeichen enthalten. Verwenden Sie weder Unzulässige Zeichen noch Unzulässige Phrasen.
Speicherort	Geben Sie den Speicherort für die geschützten Daten ein. Dieses Volume sollte ein primärer Speicherort sein. Der Speicherort kann lokal (ein Laufwerk auf dem Core-Computer) oder ein freigegebenes CIFS-Netzwerklaufwerk sein. Für eine CIFS-Freigabe muss der Pfad mit \\ beginnen. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig. **CAUTION: Definieren Sie einen dedizierten Ordner innerhalb des Stammverzeichnisses für den Speicherort für das Repository. Geben Sie nicht die Stammposition an. Verwenden Sie zum Beispiel `E:\Repository\`, nicht `E:\`. Wenn das -Repository, das Sie in diesem Schritt erstellen, später entfernt wird, werden auch alle Dateien am Speicherort des Repositorys gelöscht. Wenn Sie Ihren Speicherort unter dem Stammverzeichnis definieren, werden alle anderen Dateien im Volume (z. B. `E:\`) gelöscht, was zu verheerendem Datenverlust führen könnte.** Geben Sie beispielsweise `X:\Repository\Data` ein.

Textfeld	Description
	Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.
Benutzername	Geben Sie einen Benutzernamen für einen Benutzer mit Administratorrechten an. Diese Information ist nur erforderlich, wenn der Repository-Speicherort ein Netzwerkpfad ist.
Kennwort	Geben Sie das Kennwort für den Benutzer mit Administratorrechten ein. Diese Information ist nur erforderlich, wenn der Repository-Speicherort ein Netzwerkpfad ist.
Metadatenpfad	Geben Sie den Speicherort für die geschützten Metadaten ein. Geben Sie beispielsweise `X:\Repository\Metadata` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.

18. Konfigurieren Sie auf der Seite **Repository-Konfiguration** die Menge an Speicherplatz auf der Festplatte, die dem Repository zugewiesen werden soll. Quest empfiehlt die Reservierung von 20 Prozent des Volumens für Metadaten, was die Standard-Einstellung ist. Optional können Sie mit dem Schieberegler oder im Feld **Größe** mehr oder weniger Speicherplatz auf dem Volume dem Repository zuordnen.
19. Wählen Sie optional **Erweiterte Optionen anzeigen** aus und passen Sie die Einstellungen wie in der folgenden Tabelle beschrieben an, wenn Sie detaillierte Informationen über Speicherorteinstellungen anzeigen und eingeben möchten. Um diese Optionen auszublenden, deaktivieren Sie die Option **Erweiterte Optionen anzeigen**. Wenn Sie Ihre Repository-Konfiguration abgeschlossen haben, klicken Sie auf **Weiter** bzw. **Fertig stellen**.

Tabelle 55. Details für Speicherkonfiguration

Textfeld	Description
Bytes pro Sektor	Geben Sie die Anzahl an Bytes an, die jeder Sektor enthalten soll. Der Standardwert ist 512.
Bytes pro Datensatz	Geben Sie die durchschnittliche Anzahl an Bytes pro Datensatz an. Der Standardwert ist 8192.
Schreib-Caching-Richtlinie	Die Schreib-Caching-Richtlinie steuert, wie der Windows Cache-Manager im Repository verwendet wird. Sie ermöglicht die Optimierung der Repository-Leistung bei unterschiedlichen Konfigurationen. Legen Sie den Wert auf eine der folgenden Optionen fest: • Ein • Aus • Sync Bei Auswahl der Standardeinstellung Ein steuert Windows das Caching. Dies ist geeignet für Windows 10 und für Versionen von Windows Server 2012 und höher. **NOTE:** Wenn die Schreib-Caching-Richtlinie auf Ein festgelegt wird, kann die Leistung gesteigert werden. Wenn Sie Windows Server 2008 R2 SP2 verwenden, ist die empfohlene Einstellung „Aus“. Wenn Sie „Aus“ festlegen, wird das Ablegen im Cache-Speicher von Rapid Recovery gesteuert.

Textfeld	Description
	Bei Auswahl von Sync steuert Windows das Caching sowie die synchrone Eingabe/Ausgabe.

Wenn Sie in Schritt 1 die Option **Erweitert** ausgewählt haben, wird die Seite **Verschlüsselung** angezeigt.

20. Wenn Sie Verschlüsselungsschlüssel für im Repository gespeicherte Daten verwenden möchten, wählen Sie optional auf der Seite **Verschlüsselung Die Daten im Ruhezustand in einem Repository verschlüsseln** aus und führen Sie dann einen der folgenden Schritte aus:

    - Um einen vorhandenen Verschlüsselungsschlüssel auf alle neuen Daten, die im Repository gespeichert werden, anzuwenden, wählen Sie **Daten mit einer Core-basierten Verschlüsselung mit vorhandenem Schlüssel verschlüsseln** und wählen Sie im Drop-Down-Menü **Verschlüsselungsschlüssel auswählen** den Verschlüsselungsschlüssel aus.
    - Um nun einen neuen Verschlüsselungsschlüssel festzulegen, der für alle zukünftigen Daten in Ihrem Repository angewendet werden soll, wählen Sie **Daten mit Core-basierter Verschlüsselung mit einem neuen Schlüssel verschlüsseln** und geben Sie anschließend die Informationen zu dem Schlüssel wie in der folgenden Tabelle beschrieben ein:

Tabelle 56. Neuen Verschlüsselungsschlüssel definieren

Textfeld	Description
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein. Namen für Verschlüsselungsschlüssel müssen 1 bis 64 alphanumerische Zeichen umfassen. Verwenden Sie keine unzulässigen Zeichen oder unzulässigen Phrasen.
Description	Geben Sie einen beschreibenden Kommentar für den Verschlüsselungsschlüssel ein. Diese Informationen werden im Beschreibungsfeld angezeigt, wenn Verschlüsselungsschlüssel in Rapid Recovery Core Console angezeigt werden. Die Beschreibung kann bis zu 254 Zeichen umfassen. Es hat sich bewährt, die Verwendung von unzulässigen Zeichen und unzulässigen Phrasen zu vermeiden.
Passphrase	Geben Sie eine Passphrase für die Zugriffssteuerung ein. Sie sollten keine unzulässigen Zeichen verwenden. Bewahren Sie die Passphrase an einem sicheren Ort auf. Quest Datenschutz-Support kann eine Passphrase nicht wiederherstellen. Wenn Sie einen Verschlüsselungsschlüssel erstellt und für eine geschützte Maschine verwendet haben, können Sie keine Daten dieser geschützten Maschine mehr wiederherstellen, wenn die Passphrase verloren geht.
Passphrase bestätigen	Geben Sie die Passphrase erneut ein. Dies wird zur Bestätigung der Passphraseneingabe verwendet.

21. Optional können Sie auf der Seite **Verschlüsselung Die Daten verschlüsseln, die über ein Netzwerk transportiert werden** auswählen, um alle Daten zu verschlüsseln, die über ein Netzwerk transportiert werden. Diese Option ist standardmäßig aktiviert; wenn Sie Daten nicht auf diese Art und Weise verschlüsseln möchten, müssen Sie diese Option also deaktivieren.
22. Klicken Sie auf **Fertigstellen**, um die Einstellungen zu speichern und zu übernehmen.

    Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, wird anhand des von Ihnen definierten Zeitplans ein Basisabbild (d. h. ein Snapshot aller Daten im geschützten Volume) zum Repository auf dem Rapid Recovery Core übertragen, es sei denn, Sie haben angegeben, den Schutz anfänglich vorübergehend deaktivieren.

Die Rapid Recovery Agenten-Software wird, sofern erforderlich, auf den angegebenen Maschinen bereitgestellt, und die Maschinen werden im Core zum Schutz hinzugefügt.

Schutz von mehreren Maschinen auf einem virtuellen VMware vCenter/ESXi-Host

Verwenden Sie dieses Verfahren zum Schützen einer oder mehrerer Maschinen gleichzeitig auf einem virtuellen VMware vCenter/ESXi-Host.

CAUTION: Wenn Sie agentenlosen Schutz verwenden, empfiehlt Quest**, dass Sie den Schutz auf nicht mehr als 200 virtuelle Maschinen gleichzeitig beschränken. Beispiel: Wählen Sie bei der Verwendung des Protect Multiple Machines Wizard (Assistent zum Schützen mehrerer Maschinen) nicht mehr als 200 virtuelle Maschinen aus. Das Schützen von mehr als 200 virtuellen Maschinen wirkt sich negativ auf die Leistung aus. Es gibt keine Beschränkung, wie viele virtuelle Maschinen ein Core agentenlos über einen bestimmten Zeitraum schützen kann. Sie könnten zum Beispiel heute 200 und morgen weitere 200 virtuelle Maschinen schützen.**

1. Klicken Sie auf der Rapid Recovery Core Console Core Console auf das Drop-Down-Menü **Schützen** und dann auf **Mehrere Maschinen schützen**.

   Daraufhin wird der Protect Multiple Machines Wizard (Assistent zum Schützen mehrerer Maschinen) angezeigt.
2. Wählen Sie auf der Seite **Willkommen** eine der folgenden Optionen aus:
   - Standard
   - Erweitert (optionale Schritte anzeigen)
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Verbindung** des Assistenten von der Drop-Down-Liste **QuellevCenter / ESXi**.
5. Geben Sie die in der folgenden Tabelle beschriebenen Host- und Anmeldedaten ein.

Tabelle 57. vCenter/ESXi-Verbindungseinstellungen

Textfeld	Description
Host	Geben Sie den Hostnamen oder die IP-Adresse des virtuellen Hosts des VMware vCenter Server/ESXi ein.
Port	Der Port für die Verbindung zum virtuellen Host. Die Standardeinstellung ist 443.
Benutzername	Der Benutzername für die Verbindung zum virtuellen Host, z. B. „Administrator“ (bzw. „[Domänenname]\Administrator“, wenn sich die Maschine in einer Domäne befindet).
Kennwort	Das sichere Kennwort, das für die Verbindung zum jeweiligen virtuellen Host verwendet wird.

   - Für die Verwendung von agentenlosem Schutz wählen Sie **Protect selected VMs Agentlessly** (Ausgewählte virtuelle Maschinen agentenlos schützen) aus und befolgen Sie anschließend die Anweisungen unter Schutz von virtuellen vCenter/ESXi-Maschinen mit agentenlosem Schutz.
6. Klicken Sie auf **Weiter**.
7. Führen Sie auf der Seite **Maschinen auswählen** eine der folgenden Aktionen aus:
   - Wählen Sie aus der angezeigten Liste die VMs aus, die Sie schützen möchten.
   - Um durch die VMware-Baumstruktur zu navigieren und mehrere VMs auszuwählen, klicken Sie auf **Baumstruktur anzeigen** und wählen Sie dann entweder **Hosts und Cluster** oder **VMs und Vorlagen** aus. Wählen Sie die VMs aus, die geschützt werden sollen.

Eine Benachrichtigung wird angezeigt, wenn Rapid Recovery erkennt, dass eine Maschine offline ist oder auf ihr keine VMware-Tools installiert sind.

8. Klicken Sie auf **Weiter**.
9. Geben Sie auf der Seite **Anpassungen** die Anmeldeinformationen für jede Maschine im folgenden Format ein: `hostname::username::password`.

   NOTE: Geben Sie eine Maschine pro Zeile ein.

10. Klicken Sie auf **Weiter**.

    Wechseln Sie zu **Schritt 14**, wenn als Nächstes die Seite Schutz im Assistent zum Schützen mehrerer Maschinen angezeigt wird.

    Wenn die Agent-Software noch nicht auf den zu schützenden Maschinen bereitgestellt wurde oder eine der von Ihnen angegebenen Maschinen aus einem anderen Grund nicht geschützt werden kann, werden die ausgewählten Maschinen auf der **Warnseite** angezeigt.

11. Sie können eine Maschine auf der **Warn**seite für Maschinen auch selbst überprüfen, indem Sie die Maschine auswählen und in der Symbolleiste auf **Überprüfen** klicken.
12. Wählen Sie auf der **Warnseite** für Maschinen ggf. **Maschinen nach der Agent-Installation automatisch neu starten** aus.

    NOTE: Quest empfiehlt diese Option. Sie müssen die Agent-Maschinen neu starten, damit sie geschützt werden können.

13. Klicken Sie auf **Weiter**, wenn der Status anzeigt, dass die Maschine erreichbar ist, um die Agent-Software zu installieren.

    Die Seite **Schutz** wird angezeigt.

14. Sie können ggf. auf der Seite **Schutz**, wenn in der Rapid Recovery Core Console anstelle der IP-Adresse ein Name für die geschützte Maschine angezeigt werden soll, im Feld **Anzeigename** einen Namen in das Dialogfeld eingeben.

    Sie können bis zu 64 Zeichen eingeben. Verwenden Sie keine Sonderzeichen (siehe Beschreibung in). Darüber hinaus darf der Anzeigename nicht mit den im Abschnitt aufgeführten Zeichenkombinationen beginnen.

15. Wählen Sie die gewünschte Einstellung für den Schutzzeitplan aus (siehe nachstehende Beschreibung):

    - Wählen Sie unter „Zeitplaneinstellungen“ die Option **Standardschutz (stündliche Snapshots aller Volumes)** aus, um den Standardschutzzeitplan zu verwenden.

    Im Standardschutzzeitplan erstellt der Core jede Stunde Snapshots aller Volumes der geschützten Maschine. Auf der Registerkarte **Zusammenfassung** für die jeweilige geschützte Maschine können Sie jederzeit die Schutzeinstellungen ändern, nachdem der Assistent beendet wurde, z. B. die zu schützenden Volumes auswählen.

    - Wählen Sie unter „Zeitplaneinstellungen“ die Option **Benutzerdefinierter Schutz** aus, um einen anderen Schutzzeitplan zu definieren.

16. Setzen Sie die Konfiguration wie folgt fort:

    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und Standardschutz festgelegt haben und ein Repository vorhanden ist, klicken Sie auf **Fertigstellen**, um

die ausgewählten Einstellungen zu bestätigen, den Assistenten zu schließen und die angegebene Maschine zu schützen.

- Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und Standardschutz festgelegt haben und kein Repository vorhanden ist, klicken Sie auf **Weiter** und fahren Sie mit Schritt 19 fort, um ein Repository zu erstellen.
- Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und benutzerdefinierten Schutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit dem nächsten Schritt fort, um auszuwählen, welche Volumes geschützt werden sollen.
- Wenn Sie „Advanced Configuration“ (Erweiterte Konfiguration) für den Protect Machine Wizard (Assistenten zum Schützen der Maschine) und den Standardschutz ausgewählt haben, klicken Sie auf **Weiter** und fahren Sie mit Schritt 19 fort, um die Repository- und Verschlüsselungsoptionen anzuzeigen.
- Wenn Sie im Assistenten zum Schützen einer Maschine eine erweiterte Konfiguration ausgewählt und benutzerdefinierten Schutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit dem nächsten Schritt fort, um auszuwählen, welche Volumes geschützt werden sollen.

Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, wird anhand des von Ihnen definierten Zeitplans ein Basisabbild (d. h. ein Snapshot aller Daten im geschützten Volume) zum Repository auf dem Rapid Recovery Core übertragen, es sei denn, Sie haben angegeben, den Schutz anfänglich vorübergehend zu deaktivieren.

17. Wählen Sie auf der Seite **Schutz-Volumes** die Volumes aus, die Sie schützen möchten. Klicken Sie in der Spalte „Überprüfen“ auf die aufgelisteten Volumes, die nicht geschützt werden sollen, um die Auswahl aufzuheben. Klicken Sie anschließend auf **Weiter**.

   NOTE: In der Regel sollten zumindest das Volume „System-reserviert“ und das Volume mit dem Betriebssystem (normalerweise Laufwerk C:) geschützt werden.

18. Legen Sie auf der Seite **Schutzzeitplan** einen benutzerdefinierten Schutzzeitplan fest und klicken Sie auf **Weiter**. Ausführliche Informationen zum Festlegen eines benutzerdefinierten Schutzzeitplans finden Sie unter Erstellen von benutzerdefinierten Schutzzeitplänen im einfachen Modus.

    Wenn Sie bereits Repository-Informationen konfiguriert und die Option „Erweitert“ in Schritt 1 gewählt haben, wird die Seite „Verschlüsselung“ angezeigt. Fahren Sie mit Schritt 22 fort.

19. Führen Sie auf der Seite **Repository** folgende Aktion aus:

    - Wenn Sie bereits über ein Repository verfügen und die Daten für diese Maschine zum Schutz im bestehenden Repository speichern möchten, führen Sie einen der folgenden Schritte aus:

      1. Wählen Sie **Vorhandenes Repository verwenden** aus.
      2. Wählen Sie aus der Liste ein bestehendes Repository aus.
      3. Klicken Sie auf **Weiter**.

      Die Seite **Encryption** (Verschlüsselung) wird angezeigt. Wechseln Sie zu Schritt 22, um ggf. Verschlüsselungseinstellungen zu definieren.

    - Wenn Sie ein Repository erstellen möchten, geben Sie auf der Seite **Repository** die in der folgenden Tabelle beschriebenen Informationen ein und klicken Sie dann auf **Weiter** bzw. **Fertig stellen**.

Tabelle 58. Repository-Einstellungen

Textfeld	Description
Name	Geben Sie den Anzeigenamen des Repositorys ein. Dieses Textfeld enthält standardmäßig das Wort „Repository“ sowie eine Nummer, die der Nummer der Repositorys für diesen Core entspricht. Wenn es sich hierbei beispielsweise um das erste Repository handelt, lautet der Standardname „Repository 1“. Ändern Sie den Namen je nach Bedarf.

Textfeld	Description
	Repository-Namen müssen zwischen 1 und 40 alphanumerischen Zeichen, einschließlich Leerzeichen enthalten. Verwenden Sie weder Unzulässige Zeichen noch Unzulässige Phrasen.
Speicherort	Geben Sie den Speicherort für die geschützten Daten ein. Dieses Volume sollte ein primärer Speicherort sein. Der Speicherort kann lokal (ein Laufwerk auf dem Core-Computer) oder ein freigegebenes CIFS-Netzwerklaufwerk sein. Für eine CIFS-Freigabe muss der Pfad mit \\ beginnen. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig. **CAUTION: Definieren Sie einen dedizierten Ordner innerhalb des Stammverzeichnisses für den Speicherort für das Repository. Geben Sie nicht die Stammposition an. Verwenden Sie zum Beispiel `E:\Repository\`, nicht `E:\`. Wenn das -Repository, das Sie in diesem Schritt erstellen, später entfernt wird, werden auch alle Dateien am Speicherort des Repositorys gelöscht. Wenn Sie Ihren Speicherort unter dem Stammverzeichnis definieren, werden alle anderen Dateien im Volume (z. B. `E:\`) gelöscht, was zu verheerendem Datenverlust führen könnte.** Geben Sie beispielsweise `X:\Repository\Data` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.
Benutzername	Geben Sie einen Benutzernamen für einen Benutzer mit Administratorrechten an. Diese Information ist nur erforderlich, wenn der Repository-Speicherort ein Netzwerkpfad ist.
Kennwort	Geben Sie das Kennwort für den Benutzer mit Administratorrechten ein. Diese Information ist nur erforderlich, wenn der Repository-Speicherort ein Netzwerkpfad ist.
Metadatenpfad	Geben Sie den Speicherort für die geschützten Metadaten ein. Geben Sie beispielsweise `X:\Repository\Metadata` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.

20. Konfigurieren Sie auf der Seite **Repository-Konfiguration** die Menge an Speicherplatz auf der Festplatte, die dem Repository zugewiesen werden soll. Quest empfiehlt die Reservierung von 20 Prozent des Volumens für Metadaten, was die Standard-Einstellung ist. Optional können Sie mit dem Schieberegler oder im Feld **Größe** mehr oder weniger Speicherplatz auf dem Volume dem Repository zuordnen.
21. Wählen Sie optional **Erweiterte Optionen anzeigen** aus und passen Sie die Einstellungen wie in der folgenden Tabelle beschrieben an, wenn Sie detaillierte Informationen über Speicherorteinstellungen anzeigen und eingeben möchten. Um diese Optionen auszublenden, deaktivieren Sie die Option **Erweiterte Optionen anzeigen**. Wenn Sie Ihre Repository-Konfiguration abgeschlossen haben, klicken Sie auf **Weiter** bzw. **Fertig stellen**.

Tabelle 59. Details für Speicherkonfiguration

Textfeld	Description
Bytes pro Sektor	Geben Sie die Anzahl an Bytes an, die jeder Sektor enthalten soll. Der Standardwert ist 512.
Bytes pro Datensatz	Geben Sie die durchschnittliche Anzahl an Bytes pro Datensatz an. Der Standardwert ist 8192.
Schreib-Caching-Richtlinie	Die Schreib-Caching-Richtlinie steuert, wie der Windows Cache-Manager im Repository verwendet wird. Sie ermöglicht die Optimierung der Repository-Leistung bei unterschiedlichen Konfigurationen. Legen Sie den Wert auf eine der folgenden Optionen fest: • Ein • Aus • Sync Bei Auswahl der Standardeinstellung Ein steuert Windows das Caching. Dies ist geeignet für Windows 10 und für Versionen von Windows Server 2012 und höher. **NOTE:** Wenn die Schreib-Caching-Richtlinie auf Ein festgelegt wird, kann die Leistung gesteigert werden. Wenn Sie Windows Server 2008 R2 SP2 verwenden, ist die empfohlene Einstellung „Aus“. Wenn Sie „Aus“ festlegen, wird das Ablegen im Cache-Speicher von Rapid Recovery gesteuert. Bei Auswahl von Sync steuert Windows das Caching sowie die synchrone Eingabe/Ausgabe.

Wenn Sie in Schritt 1 die Option **Erweitert** ausgewählt haben, wird die Seite **Verschlüsselung** angezeigt.

22. Wenn Sie Verschlüsselungsschlüssel für im Repository gespeicherte Daten verwenden möchten, wählen Sie optional auf der Seite **Verschlüsselung Die Daten im Ruhezustand in einem Repository verschlüsseln** aus und führen Sie dann einen der folgenden Schritte aus:
    - Um einen vorhandenen Verschlüsselungsschlüssel auf alle neuen Daten, die im Repository gespeichert werden, anzuwenden, wählen Sie **Daten mit einer Core-basierten Verschlüsselung mit vorhandenem Schlüssel verschlüsseln** und wählen Sie im Drop-Down-Menü **Verschlüsselungsschlüssel auswählen** den Verschlüsselungsschlüssel aus.
    - Um nun einen neuen Verschlüsselungsschlüssel festzulegen, der für alle zukünftigen Daten in Ihrem Repository angewendet werden soll, wählen Sie **Daten mit Core-basierter Verschlüsselung mit einem neuen Schlüssel verschlüsseln** und geben Sie anschließend die Informationen zu dem Schlüssel wie in der folgenden Tabelle beschrieben ein:

Tabelle 60. Neuen Verschlüsselungsschlüssel definieren

Textfeld	Description
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein. Namen für Verschlüsselungsschlüssel müssen 1 bis 64 alphanumerische Zeichen umfassen. Verwenden Sie keine unzulässigen Zeichen oder unzulässigen Phrasen.
Description	Geben Sie einen beschreibenden Kommentar für den Verschlüsselungsschlüssel ein. Diese Informationen werden im Beschreibungsfeld angezeigt, wenn Verschlüsselungsschlüssel in Rapid Recovery Core Console angezeigt werden. Die Beschreibung kann bis zu 254 Zeichen umfassen.

Textfeld	Description
	Es hat sich bewährt, die Verwendung von unzulässigen Zeichen und unzulässigen Phrasen zu vermeiden.
Passphrase	Geben Sie eine Passphrase für die Zugriffssteuerung ein. Sie sollten keine unzulässigen Zeichen verwenden. Bewahren Sie die Passphrase an einem sicheren Ort auf. Quest Datenschutz-Support kann eine Passphrase nicht wiederherstellen. Wenn Sie einen Verschlüsselungsschlüssel erstellt und für eine geschützte Maschine verwendet haben, können Sie keine Daten dieser geschützten Maschine mehr wiederherstellen, wenn die Passphrase verloren geht.
Passphrase bestätigen	Geben Sie die Passphrase erneut ein. Dies wird zur Bestätigung der Passphraseneingabe verwendet.

23. Optional können Sie auf der Seite **Verschlüsselung Die Daten verschlüsseln, die über ein Netzwerk transportiert werden** auswählen, um alle Daten zu verschlüsseln, die über ein Netzwerk transportiert werden. Diese Option ist standardmäßig aktiviert; wenn Sie Daten nicht auf diese Art und Weise verschlüsseln möchten, müssen Sie diese Option also deaktivieren.
24. Klicken Sie auf **Fertigstellen**, um die Einstellungen zu speichern und zu übernehmen.

    Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, wird anhand des von Ihnen definierten Zeitplans ein Basisabbild (d. h. ein Snapshot aller Daten im geschützten Volume) zum Repository auf dem Rapid Recovery Core übertragen, es sei denn, Sie haben angegeben, den Schutz anfänglich vorübergehend deaktivieren.

Die Rapid Recovery Agenten-Software wird, sofern erforderlich, auf den angegebenen Maschinen bereitgestellt, und die Maschinen werden im Core zum Schutz hinzugefügt.

Schutz von virtuellen vCenter/ESXi-Maschinen mit agentenlosem Schutz

Führen Sie die folgenden Verfahren zum agentenlosen Schutz virtueller ESXi Maschinen durch.

NOTE: Rapid Recovery empfiehlt, dass VMware-Tools auf virtuellen Maschinen installiert werden (VMs), die Sie auf vSphere- oder ESXi-Hosts schützen möchten. Wenn VMware Tools auf einer VM mit einem Windows Betriebssystem (OS) installiert sind, verwenden die Sicherungen, die der Rapid Recovery Core erfasst, Microsoft Volume Shadow Services (VSS). Weitere Informationen über das Verhalten agentenloser VMs mit oder ohne die VMware Tools finden Sie unter Vorteile der Installation von Hypervisor-Tools für agentenlosen Schutz.

CAUTION: Quest **empfiehlt, dass Sie den agentenlosen Schutz auf maximal 200 VMs gleichzeitig begrenzen. Beispiel: Wählen Sie bei der Verwendung des Protect Multiple Machines Wizard (Assistent zum Schützen mehrerer Maschinen) nicht mehr als 200 virtuelle Maschinen aus. Das Schützen von mehr als 200 virtuellen Maschinen wirkt sich negativ auf die Leistung aus. Es gibt keine Beschränkung, wie viele virtuelle Maschinen ein Core agentenlos über einen bestimmten Zeitraum schützen kann. Sie könnten zum Beispiel heute 200 und morgen weitere 200 virtuelle Maschinen schützen.**

1. Klicken Sie auf der Rapid Recovery Core Console, auf das Drop-Down-Menü **Schützen** und dann auf **Schutz mehrerer Maschinen**.

Daraufhin wird der Protect Multiple Machines Wizard (Assistent zum Schützen mehrerer Maschinen) angezeigt.

2. Wählen Sie auf der Seite **Willkommen** eine der folgenden Optionen aus:
   - Standard
   - Erweitert (optionale Schritte anzeigen)
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der **Verbindungsseite** des Assistenten aus dem Dropdownmenü **Quelle** die Option **vCenter / ESX(i)** aus.
5. Geben Sie die in der folgenden Tabelle beschriebenen Host- und Anmeldedaten ein.

Tabelle 61. vCenter/ESX(i)-Verbindungseinstellungen

Textfeld	Description
Host	Der Host-Name oder die IP-Adresse des virtuellen Hosts
Port	Der Port für die Verbindung zum virtuellen Host. Die Standardeinstellung ist 443.
Benutzername	Der Benutzername für die Verbindung zum virtuellen Host, z. B. „Administrator“ (bzw. „[Domänenname]\Administrator“, wenn sich die Maschine in einer Domäne befindet).
Kennwort	Das sichere Kennwort, das für die Verbindung zum jeweiligen virtuellen Host verwendet wird.

6. Stellen Sie sicher, dass **Ausgewählte VMs agentenlos schützen** ausgewählt ist. (Diese Option ist standardmäßig ausgewählt).
7. Führen Sie auf der Seite **Maschinen auswählen** eine der folgenden Aktionen aus:
   - Wählen Sie aus der angezeigten Liste die VMs aus, die Sie schützen möchten.
   - Um durch die VMware-Baumstruktur zu navigieren und mehrere VMs auszuwählen, klicken Sie auf **Baumstruktur anzeigen** und wählen Sie dann entweder **Hosts und Cluster** oder **VMs und Vorlagen** aus. Wählen Sie die VMs aus, die geschützt werden sollen.
8. Wenn Sie neue VMs automatisch schützen wollen, wenn Sie dem Host hinzugefügt werden, wählen Sie **Neue Maschinen automatisch schützen** und klicken Sie dann auf **Weiter**.

   NOTE: VMware Changed Block Tracking (CBT) muss auf jeder der VMs, die Sie schützen möchten, aktiviert sein. Falls dies nicht aktiviert ist, aktiviert Rapid Recovery automatisch CBT zum Schutz.

   a. Wählen Sie auf der Seite **Automatischer Schutz** einen beliebigen Container aus, in den Sie wahrscheinlich neue Geräte hinzufügen.
9. Klicken Sie auf **Weiter**.

   Wechseln Sie zu **Schritt 12**, wenn als Nächstes die Seite Schutz im Assistent zum Schützen mehrerer Maschinen angezeigt wird.

   Wenn die Agent-Software noch nicht auf den zu schützenden Maschinen bereitgestellt wurde oder eine der von Ihnen angegebenen Maschinen aus einem anderen Grund nicht geschützt werden kann, werden die ausgewählten Maschinen auf der **Warnseite** angezeigt.
10. Sie können eine Maschine auf der **Warn**seite für Maschinen auch selbst überprüfen, indem Sie die Maschine auswählen und in der Symbolleiste auf **Überprüfen** klicken.
11. Klicken Sie auf **Weiter**.

Schutz wird angezeigt.

12. Wählen Sie die gewünschte Einstellung für den Schutzzeitplan aus (siehe nachstehende Beschreibung):

    - Wählen Sie unter „Zeitplaneinstellungen“ die Option **Standardschutz (stündliche Snapshots aller Volumes)** aus, um den Standardschutzzeitplan zu verwenden.

    Im Standardschutzzeitplan erstellt der Core jede Stunde Snapshots aller Volumes der geschützten Maschine. Auf der Registerkarte **Zusammenfassung** für die jeweilige geschützte Maschine können Sie jederzeit die Schutzeinstellungen ändern, nachdem der Assistent beendet wurde, z. B. die zu schützenden Volumes auswählen.

    - Wählen Sie unter „Zeitplaneinstellungen“ die Option **Benutzerdefinierter Schutz** aus, um einen anderen Schutzzeitplan zu definieren.

13. Setzen Sie die Konfiguration wie folgt fort:

    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und Standardschutz festgelegt haben und ein Repository vorhanden ist, klicken Sie auf **Fertigstellen**, um die ausgewählten Einstellungen zu bestätigen, den Assistenten zu schließen und die angegebene Maschine zu schützen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und Standardschutz festgelegt haben und kein Repository vorhanden ist, klicken Sie auf **Weiter** und fahren Sie mit Schritt 15 fort, um ein Repository zu erstellen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und benutzerdefinierten Schutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit dem nächsten Schritt fort, um auszuwählen, welche Volumes geschützt werden sollen.
    - Wenn Sie „Advanced Configuration“ (Erweiterte Konfiguration) für den Protect Machine Wizard (Assistenten zum Schützen der Maschine) und den Standardschutz ausgewählt haben, klicken Sie auf **Weiter** und fahren Sie mit Schritt 15 fort, um die Repository- und Verschlüsselungsoptionen anzuzeigen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine erweiterte Konfiguration ausgewählt und benutzerdefinierten Schutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit dem nächsten Schritt fort, um auszuwählen, welche Volumes geschützt werden sollen.

    Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, wird anhand des von Ihnen definierten Zeitplans ein Basisabbild (d. h. ein Snapshot aller Daten im geschützten Volume) zum Repository auf dem Rapid Recovery Core übertragen, es sei denn, Sie haben angegeben, den Schutz anfänglich vorübergehend zu deaktivieren.

14. Legen Sie auf der Seite **Schutzzeitplan** einen benutzerdefinierten Schutzzeitplan fest und klicken Sie auf **Weiter**. Ausführliche Informationen zum Festlegen eines benutzerdefinierten Schutzzeitplans finden Sie unter Erstellen von benutzerdefinierten Schutzzeitplänen im einfachen Modus.

    Wenn Sie bereits Repository-Informationen konfiguriert und die Option „Erweitert“ in Schritt 1 gewählt haben, wird die Seite „Verschlüsselung“ angezeigt. Fahren Sie mit Schritt 18 fort.

15. Führen Sie auf der Seite **Repository** folgende Aktion aus:

    - Wenn Sie bereits über ein Repository verfügen und die Daten für diese Maschine zum Schutz im bestehenden Repository speichern möchten, führen Sie einen der folgenden Schritte aus:

      1. Wählen Sie **Vorhandenes Repository verwenden** aus.
      2. Wählen Sie aus der Liste ein bestehendes Repository aus.
      3. Klicken Sie auf **Weiter**.

      Die Seite **Encryption** (Verschlüsselung) wird angezeigt. Wechseln Sie zu Schritt 18, um ggf. Verschlüsselungseinstellungen zu definieren.

    - Wenn Sie ein Repository erstellen möchten, geben Sie auf der Seite **Repository** die in der folgenden Tabelle beschriebenen Informationen ein und klicken Sie dann auf **Weiter** bzw. **Fertig stellen**.

Tabelle 62. Repository-Einstellungen

Textfeld	Description
Name	Geben Sie den Anzeigenamen des Repositorys ein. Dieses Textfeld enthält standardmäßig das Wort „Repository“ sowie eine Nummer, die der Nummer der Repositorys für diesen Core entspricht. Wenn es sich hierbei beispielsweise um das erste Repository handelt, lautet der Standardname „Repository 1“. Ändern Sie den Namen je nach Bedarf. Repository-Namen müssen zwischen 1 und 40 alphanumerischen Zeichen, einschließlich Leerzeichen enthalten. Verwenden Sie weder Unzulässige Zeichen noch Unzulässige Phrasen.
Speicherort	Geben Sie den Speicherort für die geschützten Daten ein. Dieses Volume sollte ein primärer Speicherort sein. Der Speicherort kann lokal (ein Laufwerk auf dem Core-Computer) oder ein freigegebenes CIFS-Netzwerklaufwerk sein. Für eine CIFS-Freigabe muss der Pfad mit \\ beginnen. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig. **CAUTION: Definieren Sie einen dedizierten Ordner innerhalb des Stammverzeichnisses für den Speicherort für das Repository. Geben Sie nicht die Stammposition an. Verwenden Sie zum Beispiel `E:\Repository\`, nicht `E:\`. Wenn das -Repository, das Sie in diesem Schritt erstellen, später entfernt wird, werden auch alle Dateien am Speicherort des Repositorys gelöscht. Wenn Sie Ihren Speicherort unter dem Stammverzeichnis definieren, werden alle anderen Dateien im Volume (z. B. `E:\`) gelöscht, was zu verheerendem Datenverlust führen könnte.** Geben Sie beispielsweise `X:\Repository\Data` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.
Benutzername	Geben Sie einen Benutzernamen für einen Benutzer mit Administratorrechten an. Diese Information ist nur erforderlich, wenn der Repository-Speicherort ein Netzwerkpfad ist.
Kennwort	Geben Sie das Kennwort für den Benutzer mit Administratorrechten ein. Diese Information ist nur erforderlich, wenn der Repository-Speicherort ein Netzwerkpfad ist.
Metadatenpfad	Geben Sie den Speicherort für die geschützten Metadaten ein. Geben Sie beispielsweise `X:\Repository\Metadata` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.

16. Konfigurieren Sie auf der Seite **Repository-Konfiguration** die Menge an Speicherplatz auf der Festplatte, die dem Repository zugewiesen werden soll. Quest empfiehlt die Reservierung von 20 Prozent des Volumens für Metadaten, was die Standard-Einstellung ist. Optional können Sie mit dem Schieberegler oder im Feld **Größe** mehr oder weniger Speicherplatz auf dem Volume dem Repository zuordnen.
17. Wählen Sie optional **Erweiterte Optionen anzeigen** aus und passen Sie die Einstellungen wie in der folgenden Tabelle beschrieben an, wenn Sie detaillierte Informationen über Speicherorteinstellungen anzeigen und eingeben möchten. Um diese Optionen auszublenden, deaktivieren Sie die Option

Erweiterte Optionen anzeigen. Wenn Sie Ihre Repository-Konfiguration abgeschlossen haben, klicken Sie auf **Weiter** bzw. **Fertig stellen**.

Tabelle 63. Details für Speicherkonfiguration

Textfeld	Description
Bytes pro Sektor	Geben Sie die Anzahl an Bytes an, die jeder Sektor enthalten soll. Der Standardwert ist 512.
Bytes pro Datensatz	Geben Sie die durchschnittliche Anzahl an Bytes pro Datensatz an. Der Standardwert ist 8192.
Schreib-Caching-Richtlinie	Die Schreib-Caching-Richtlinie steuert, wie der Windows Cache-Manager im Repository verwendet wird. Sie ermöglicht die Optimierung der Repository-Leistung bei unterschiedlichen Konfigurationen. Legen Sie den Wert auf eine der folgenden Optionen fest: • Ein • Aus • Sync Bei Auswahl der Standardeinstellung Ein steuert Windows das Caching. Dies ist geeignet für Windows 10 und für Versionen von Windows Server 2012 und höher. **NOTE:** Wenn die Schreib-Caching-Richtlinie auf Ein festgelegt wird, kann die Leistung gesteigert werden. Wenn Sie Windows Server 2008 R2 SP2 verwenden, ist die empfohlene Einstellung „Aus“. Wenn Sie „Aus“ festlegen, wird das Ablegen im Cache-Speicher von Rapid Recovery gesteuert. Bei Auswahl von Sync steuert Windows das Caching sowie die synchrone Eingabe/Ausgabe.

Wenn Sie in Schritt 1 die Option **Erweitert** ausgewählt haben, wird die Seite **Verschlüsselung** angezeigt.

18. Wenn Sie Verschlüsselungsschlüssel für im Repository gespeicherte Daten verwenden möchten, wählen Sie optional auf der Seite **Verschlüsselung Die Daten im Ruhezustand in einem Repository verschlüsseln** aus und führen Sie dann einen der folgenden Schritte aus:
    - Um einen vorhandenen Verschlüsselungsschlüssel auf alle neuen Daten, die im Repository gespeichert werden, anzuwenden, wählen Sie **Daten mit einer Core-basierten Verschlüsselung mit vorhandenem Schlüssel verschlüsseln** und wählen Sie im Drop-Down-Menü **Verschlüsselungsschlüssel auswählen** den Verschlüsselungsschlüssel aus.
    - Um nun einen neuen Verschlüsselungsschlüssel festzulegen, der für alle zukünftigen Daten in Ihrem Repository angewendet werden soll, wählen Sie **Daten mit Core-basierter Verschlüsselung mit einem neuen Schlüssel verschlüsseln** und geben Sie anschließend die Informationen zu dem Schlüssel wie in der folgenden Tabelle beschrieben ein:

Tabelle 64. Neuen Verschlüsselungsschlüssel definieren

Textfeld	Description
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein. Namen für Verschlüsselungsschlüssel müssen 1 bis 64 alphanumerische Zeichen umfassen. Verwenden Sie keine unzulässigen Zeichen oder unzulässigen Phrasen.
Description	Geben Sie einen beschreibenden Kommentar für den Verschlüsselungsschlüssel ein. Diese Informationen werden im Beschreibungsfeld angezeigt, wenn

Textfeld	Description
	Verschlüsselungsschlüssel in Rapid Recovery Core Console angezeigt werden. Die Beschreibung kann bis zu 254 Zeichen umfassen. Es hat sich bewährt, die Verwendung von unzulässigen Zeichen und unzulässigen Phrasen zu vermeiden.
Passphrase	Geben Sie eine Passphrase für die Zugriffssteuerung ein. Sie sollten keine unzulässigen Zeichen verwenden. Bewahren Sie die Passphrase an einem sicheren Ort auf. Quest Datenschutz-Support kann eine Passphrase nicht wiederherstellen. Wenn Sie einen Verschlüsselungsschlüssel erstellt und für eine geschützte Maschine verwendet haben, können Sie keine Daten dieser geschützten Maschine mehr wiederherstellen, wenn die Passphrase verloren geht.
Passphrase bestätigen	Geben Sie die Passphrase erneut ein. Dies wird zur Bestätigung der Passphraseneingabe verwendet.

19. Optional können Sie auf der Seite **Verschlüsselung Die Daten verschlüsseln, die über ein Netzwerk transportiert werden** auswählen, um alle Daten zu verschlüsseln, die über ein Netzwerk transportiert werden. Diese Option ist standardmäßig aktiviert; wenn Sie Daten nicht auf diese Art und Weise verschlüsseln möchten, müssen Sie diese Option also deaktivieren.
20. Klicken Sie auf **Fertigstellen**, um die Einstellungen zu speichern und zu übernehmen.

    Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, wird anhand des von Ihnen definierten Zeitplans ein Basisabbild (d. h. ein Snapshot aller Daten im geschützten Volume) zum Repository auf dem Rapid Recovery Core übertragen, es sei denn, Sie haben angegeben, den Schutz anfänglich vorübergehend deaktivieren.

Schutz von mehreren Maschinen auf einem virtuellen Hyper-V-Host

Verwenden Sie dieses Verfahren zum Schützen einer oder mehrerer Maschinen gleichzeitig auf einem virtuellen Hyper-V-Host.

CAUTION: Wenn Sie agentenlosen Schutz verwenden, empfiehlt Quest, dass Sie den Schutz auf nicht mehr als 200 virtuelle Maschinen gleichzeitig beschränken. Beispiel: Wählen Sie bei der Verwendung des Protect Multiple Machines Wizard (Assistent zum Schützen mehrerer Maschinen) nicht mehr als 200 virtuelle Maschinen aus. Das Schützen von mehr als 200 virtuellen Maschinen wirkt sich negativ auf die Leistung aus. Es gibt keine Beschränkung, wie viele virtuelle Maschinen ein Core agentenlos über einen bestimmten Zeitraum schützen kann. Sie könnten zum Beispiel heute 200 und morgen weitere 200 virtuelle Maschinen schützen.

1. Klicken Sie auf der Rapid Recovery Core Console, auf das Drop-Down-Menü **Schützen** und dann auf **Schutz mehrerer Maschinen**.

Daraufhin wird der Protect Multiple Machines Wizard (Assistent zum Schützen mehrerer Maschinen) angezeigt.

2. Wählen Sie auf der Seite „Willkommen“ eine der folgenden Optionen aus:
   - Standard
   - Erweitert (optionale Schritte anzeigen)
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Verbindung** des Assistenten von der Drop-Down-Liste **Quelle** eine der folgenden Optionen.
   - Hyper-V-Server
   - Hyper-V-Cluster
5. Geben Sie die in der folgenden Tabelle beschriebenen Host- und Anmeldedaten ein.

Tabelle 65. Hyper-V-Verbindungseinstellungen

Textfeld	Description
Host	Der Host-Name oder die IP-Adresse des virtuellen Hosts
Port	Der Port für die Verbindung zum virtuellen Host. Die Standardeinstellung ist 8006.
Benutzername	Der Benutzername für die Verbindung zum virtuellen Host, z. B. „Administrator“ (bzw. „[Domänenname]\Administrator“, wenn sich die Maschine in einer Domäne befindet).
Kennwort	Das sichere Kennwort, das für die Verbindung zum jeweiligen virtuellen Host verwendet wird.

6. Für die Verwendung von agentenlosem Schutz wählen Sie optional **Hyper-V-Server ohne einen Agenten im Gast-VMs schützen** und lesen Sie anschließend die Anweisungen unter Schutz von virtuellen Hyper-V-Maschinen mit agentenlosem Schutz.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Maschinen** die VMs aus, die Sie schützen möchten.
9. Wenn Sie neue VMs automatisch schützen wollen, wenn Sie dem Host hinzugefügt werden, wählen Sie **Neue virtuelle Maschinen automatisch schützen**.
10. Klicken Sie auf **Weiter**.
11. Geben Sie auf der Seite **Anpassungen** die Anmeldeinformationen für jede Maschine im folgenden Format ein: `hostname::username::password`.

    NOTE: Geben Sie eine Maschine pro Zeile ein.
12. Klicken Sie auf **Weiter**.

    Wechseln Sie zu **Schritt 15**, wenn als Nächstes die Seite Schutz im Assistent zum Schützen mehrerer Maschinen angezeigt wird.

    Wenn die Agentensoftware auf den zu schützenden Maschinen nicht vorliegt oder Maschinen aus einem anderen Grund nicht geschützt werden können, werden die ausgewählten Maschinen auf einer entsprechenden **Warn**seite angezeigt.
13. Sie können eine Maschine auf der **Warn**seite für Maschinen auch selbst überprüfen, indem Sie die Maschine auswählen und in der Symbolleiste auf **Überprüfen** klicken.
14. Wählen Sie auf der **Warnseite** für Maschinen ggf. **Maschinen nach der Agent-Installation automatisch neu starten** aus.

NOTE: Quest empfiehlt diese Option. Sie müssen die Agent-Maschinen neu starten, damit sie geschützt werden können.

15. Klicken Sie auf **Weiter**, wenn der Status anzeigt, dass die Maschine erreichbar ist, um die Agent-Software zu installieren.

    Die Seite **Schutz** wird angezeigt.

16. Sie können ggf. auf der Seite **Schutz**, wenn in der Rapid Recovery Core Console anstelle der IP-Adresse ein Name für die geschützte Maschine angezeigt werden soll, im Feld **Anzeigename** einen Namen in das Dialogfeld eingeben.

    Sie können bis zu 64 Zeichen eingeben. Verwenden Sie keine Sonderzeichen (siehe Beschreibung in). Darüber hinaus darf der Anzeigename nicht mit den im Abschnitt aufgeführten Zeichenkombinationen beginnen.

17. Wählen Sie die gewünschte Einstellung für den Schutzzeitplan aus (siehe nachstehende Beschreibung):

    - Wählen Sie unter „Zeitplaneinstellungen“ die Option **Standardschutz (stündliche Snapshots aller Volumes)** aus, um den Standardschutzzeitplan zu verwenden.

    Im Standardschutzzeitplan erstellt der Core jede Stunde Snapshots aller Volumes der geschützten Maschine. Auf der Registerkarte **Zusammenfassung** für die jeweilige geschützte Maschine können Sie jederzeit die Schutzeinstellungen ändern, nachdem der Assistent beendet wurde, z. B. die zu schützenden Volumes auswählen.

    - Wählen Sie unter „Zeitplaneinstellungen“ die Option **Benutzerdefinierter Schutz** aus, um einen anderen Schutzzeitplan zu definieren.

18. Setzen Sie die Konfiguration wie folgt fort:

    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und Standardschutz festgelegt haben und ein Repository vorhanden ist, klicken Sie auf **Fertigstellen**, um die ausgewählten Einstellungen zu bestätigen, den Assistenten zu schließen und die angegebene Maschine zu schützen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und Standardschutz festgelegt haben und kein Repository vorhanden ist, klicken Sie auf **Weiter** und fahren Sie mit Schritt 20 fort, um ein Repository zu erstellen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und benutzerdefinierten Schutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit dem nächsten Schritt fort, um auszuwählen, welche Volumes geschützt werden sollen.
    - Wenn Sie „Advanced Configuration“ (Erweiterte Konfiguration) für den Protect Machine Wizard (Assistenten zum Schützen der Maschine) und den Standardschutz ausgewählt haben, klicken Sie auf **Weiter** und fahren Sie mit Schritt 20 fort, um die Repository- und Verschlüsselungsoptionen anzuzeigen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine erweiterte Konfiguration ausgewählt und benutzerdefinierten Schutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit dem nächsten Schritt fort, um auszuwählen, welche Volumes geschützt werden sollen.

    Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, wird anhand des von Ihnen definierten Zeitplans ein Basisabbild (d. h. ein Snapshot aller Daten im geschützten Volume) zum Repository auf dem Rapid Recovery Core übertragen, es sei denn, Sie haben angegeben, den Schutz anfänglich vorübergehend zu deaktivieren.

19. Wählen Sie auf der Seite **Schutz-Volumes** die Volumes aus, die Sie schützen möchten. Klicken Sie in der Spalte „Überprüfen“ auf die aufgelisteten Volumes, die nicht geschützt werden sollen, um die Auswahl aufzuheben. Klicken Sie anschließend auf **Weiter**.

NOTE: In der Regel sollten zumindest das Volume „System-reserviert“ und das Volume mit dem Betriebssystem (normalerweise Laufwerk C:) geschützt werden.

20. Legen Sie auf der Seite **Schutzzeitplan** einen benutzerdefinierten Schutzzeitplan fest und klicken Sie auf **Weiter**. Ausführliche Informationen zum Festlegen eines benutzerdefinierten Schutzzeitplans finden Sie unter Erstellen von benutzerdefinierten Schutzzeitplänen im einfachen Modus.

    Wenn Sie bereits Repository-Informationen konfiguriert und die Option „Erweitert“ in Schritt 1 gewählt haben, wird die Seite „Verschlüsselung“ angezeigt. Fahren Sie mit Schritt 23 fort.

21. Führen Sie auf der Seite **Repository** folgende Aktion aus:

    - Wenn Sie bereits über ein Repository verfügen und die Daten für diese Maschine zum Schutz im bestehenden Repository speichern möchten, führen Sie einen der folgenden Schritte aus:

        1. Wählen Sie **Vorhandenes Repository verwenden** aus.
        2. Wählen Sie aus der Liste ein bestehendes Repository aus.
        3. Klicken Sie auf **Weiter**.

        Die Seite **Encryption** (Verschlüsselung) wird angezeigt. Wechseln Sie zu Schritt 23, um ggf. Verschlüsselungseinstellungen zu definieren.

    - Wenn Sie ein Repository erstellen möchten, geben Sie auf der Seite **Repository** die in der folgenden Tabelle beschriebenen Informationen ein und klicken Sie dann auf **Weiter** bzw. **Fertig stellen**.

Tabelle 66. Repository-Einstellungen

Textfeld	Description
Name	Geben Sie den Anzeigenamen des Repositorys ein. Dieses Textfeld enthält standardmäßig das Wort „Repository“ sowie eine Nummer, die der Nummer der Repositorys für diesen Core entspricht. Wenn es sich hierbei beispielsweise um das erste Repository handelt, lautet der Standardname „Repository 1“. Ändern Sie den Namen je nach Bedarf. Repository-Namen müssen zwischen 1 und 40 alphanumerischen Zeichen, einschließlich Leerzeichen enthalten. Verwenden Sie weder Unzulässige Zeichen noch Unzulässige Phrasen.
Speicherort	Geben Sie den Speicherort für die geschützten Daten ein. Dieses Volume sollte ein primärer Speicherort sein. Der Speicherort kann lokal (ein Laufwerk auf dem Core-Computer) oder ein freigegebenes CIFS-Netzwerklaufwerk sein. Für eine CIFS-Freigabe muss der Pfad mit \\ beginnen. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig. **CAUTION: Definieren Sie einen dedizierten Ordner innerhalb des Stammverzeichnisses für den Speicherort für das Repository. Geben Sie nicht die Stammposition an. Verwenden Sie zum Beispiel `E:\Repository\`, nicht `E:\`. Wenn das -Repository, das Sie in diesem Schritt erstellen, später entfernt wird, werden auch alle Dateien am Speicherort des Repositorys gelöscht. Wenn Sie Ihren Speicherort unter dem Stammverzeichnis definieren, werden alle anderen Dateien im Volume (z. B. `E:\`) gelöscht, was zu verheerendem Datenverlust führen könnte.** Geben Sie beispielsweise `X:\Repository\Data` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.

Textfeld	Description
Benutzername	Geben Sie einen Benutzernamen für einen Benutzer mit Administratorrechten an. Diese Information ist nur erforderlich, wenn der Repository-Speicherort ein Netzwerkpfad ist.
Kennwort	Geben Sie das Kennwort für den Benutzer mit Administratorrechten ein. Diese Information ist nur erforderlich, wenn der Repository-Speicherort ein Netzwerkpfad ist.
Metadatenpfad	Geben Sie den Speicherort für die geschützten Metadaten ein. Geben Sie beispielsweise `X:\Repository\Metadata` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.

22. Konfigurieren Sie auf der Seite **Repository-Konfiguration** die Menge an Speicherplatz auf der Festplatte, die dem Repository zugewiesen werden soll. Quest empfiehlt die Reservierung von 20 Prozent des Volumens für Metadaten, was die Standard-Einstellung ist. Optional können Sie mit dem Schieberegler oder im Feld **Größe** mehr oder weniger Speicherplatz auf dem Volume dem Repository zuordnen.
23. Wählen Sie optional **Erweiterte Optionen anzeigen** aus und passen Sie die Einstellungen wie in der folgenden Tabelle beschrieben an, wenn Sie detaillierte Informationen über Speicherorteinstellungen anzeigen und eingeben möchten. Um diese Optionen auszublenden, deaktivieren Sie die Option **Erweiterte Optionen anzeigen**. Wenn Sie Ihre Repository-Konfiguration abgeschlossen haben, klicken Sie auf **Weiter** bzw. **Fertig stellen**.

Tabelle 67. Details für Speicherkonfiguration

Textfeld	Description
Bytes pro Sektor	Geben Sie die Anzahl an Bytes an, die jeder Sektor enthalten soll. Der Standardwert ist 512.
Bytes pro Datensatz	Geben Sie die durchschnittliche Anzahl an Bytes pro Datensatz an. Der Standardwert ist 8192.
Schreib-Caching-Richtlinie	Die Schreib-Caching-Richtlinie steuert, wie der Windows Cache-Manager im Repository verwendet wird. Sie ermöglicht die Optimierung der Repository-Leistung bei unterschiedlichen Konfigurationen. Legen Sie den Wert auf eine der folgenden Optionen fest: • Ein • Aus • Sync Bei Auswahl der Standardeinstellung Ein steuert Windows das Caching. Dies ist geeignet für Windows 10 und für Versionen von Windows Server 2012 und höher. **NOTE:** Wenn die Schreib-Caching-Richtlinie auf Ein festgelegt wird, kann die Leistung gesteigert werden. Wenn Sie Windows Server 2008 R2 SP2 verwenden, ist die empfohlene Einstellung „Aus“. Wenn Sie „Aus“ festlegen, wird das Ablegen im Cache-Speicher von Rapid Recovery gesteuert. Bei Auswahl von Sync steuert Windows das Caching sowie die synchrone Eingabe/Ausgabe.

Wenn Sie in Schritt 1 die Option **Erweitert** ausgewählt haben, wird die Seite **Verschlüsselung** angezeigt.

24. Wenn Sie Verschlüsselungsschlüssel für im Repository gespeicherte Daten verwenden möchten, wählen Sie optional auf der Seite **Verschlüsselung Die Daten im Ruhezustand in einem Repository verschlüsseln** aus und führen Sie dann einen der folgenden Schritte aus:

    - Um einen vorhandenen Verschlüsselungsschlüssel auf alle neuen Daten, die im Repository gespeichert werden, anzuwenden, wählen Sie **Daten mit einer Core-basierten Verschlüsselung mit vorhandenem Schlüssel verschlüsseln** und wählen Sie im Drop-Down-Menü **Verschlüsselungsschlüssel auswählen** den Verschlüsselungsschlüssel aus.
    - Um nun einen neuen Verschlüsselungsschlüssel festzulegen, der für alle zukünftigen Daten in Ihrem Repository angewendet werden soll, wählen Sie **Daten mit Core-basierter Verschlüsselung mit einem neuen Schlüssel verschlüsseln** und geben Sie anschließend die Informationen zu dem Schlüssel wie in der folgenden Tabelle beschrieben ein:

Tabelle 68. Neuen Verschlüsselungsschlüssel definieren

Textfeld	Description
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein. Namen für Verschlüsselungsschlüssel müssen 1 bis 64 alphanumerische Zeichen umfassen. Verwenden Sie keine unzulässigen Zeichen oder unzulässigen Phrasen.
Description	Geben Sie einen beschreibenden Kommentar für den Verschlüsselungsschlüssel ein. Diese Informationen werden im Beschreibungsfeld angezeigt, wenn Verschlüsselungsschlüssel in Rapid Recovery Core Console angezeigt werden. Die Beschreibung kann bis zu 254 Zeichen umfassen. Es hat sich bewährt, die Verwendung von unzulässigen Zeichen und unzulässigen Phrasen zu vermeiden.
Passphrase	Geben Sie eine Passphrase für die Zugriffssteuerung ein. Sie sollten keine unzulässigen Zeichen verwenden. Bewahren Sie die Passphrase an einem sicheren Ort auf. Quest Datenschutz-Support kann eine Passphrase nicht wiederherstellen. Wenn Sie einen Verschlüsselungsschlüssel erstellt und für eine geschützte Maschine verwendet haben, können Sie keine Daten dieser geschützten Maschine mehr wiederherstellen, wenn die Passphrase verloren geht.
Passphrase bestätigen	Geben Sie die Passphrase erneut ein. Dies wird zur Bestätigung der Passphraseneingabe verwendet.

25. Optional können Sie auf der Seite **Verschlüsselung Die Daten verschlüsseln, die über ein Netzwerk transportiert werden** auswählen, um alle Daten zu verschlüsseln, die über ein Netzwerk transportiert werden. Diese Option ist standardmäßig aktiviert; wenn Sie Daten nicht auf diese Art und Weise verschlüsseln möchten, müssen Sie diese Option also deaktivieren.
26. Klicken Sie auf **Fertigstellen**, um die Einstellungen zu speichern und zu übernehmen.

    Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, wird anhand des von Ihnen definierten Zeitplans ein Basisabbild (d. h. ein Snapshot aller Daten im geschützten Volume) zum Repository auf dem Rapid Recovery Core übertragen, es sei denn, Sie haben angegeben, den Schutz anfänglich vorübergehend deaktivieren.

Die Rapid Recovery Agent-Software wird, sofern erforderlich, auf den angegebenen Maschinen bereitgestellt, und die Maschinen werden im Core zum Schutz hinzugefügt.

Schutz von virtuellen Hyper-V-Maschinen mit agentenlosem Schutz

Mithilfe der Funktion „Rapid Snap for Virtual“ können Sie virtuelle Hyper-V-Maschinen oder -Cluster durch Installation des Rapid Recovery Agent auf dem Hyper-V-Host statt auf allen virtuellen Maschinen (VMs) agentenlos schützen.

CAUTION: Quest empfiehlt, dass Sie den agentenlosen Schutz auf maximal 200 VMs gleichzeitig begrenzen. Beispiel: Wählen Sie bei der Verwendung des Protect Multiple Machines Wizard (Assistent zum Schützen mehrerer Maschinen) nicht mehr als 200 virtuelle Maschinen aus. Das Schützen von mehr als 200 virtuellen Maschinen wirkt sich negativ auf die Leistung aus. Es gibt keine Beschränkung, wie viele virtuelle Maschinen ein Core agentenlos über einen bestimmten Zeitraum schützen kann. Sie könnten zum Beispiel heute 200 und morgen weitere 200 virtuelle Maschinen schützen.

1. Klicken Sie auf der Rapid Recovery Core Console, auf das Drop-Down-Menü **Schützen** und dann auf **Schutz mehrerer Maschinen**.

   Daraufhin wird der Protect Multiple Machines Wizard (Assistent zum Schützen mehrerer Maschinen) angezeigt.
2. Wählen Sie auf der Seite **Willkommen** eine der folgenden Optionen aus:
   - Standard
   - Erweitert (optionale Schritte anzeigen)
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Verbindung** des Assistenten von der Drop-Down-Liste **Quelle** eine der folgenden Optionen.
   - Hyper-V-Server
   - Hyper-V-Cluster
5. Geben Sie die in der folgenden Tabelle beschriebenen Host- und Anmeldedaten ein.

Tabelle 69. Hyper-V-Verbindungseinstellungen

Textfeld	Description
Host	Der Host-Name oder die IP-Adresse des virtuellen Hosts
Port	Der Port für die Verbindung zum virtuellen Host. Die Standardeinstellung ist 8006.
Benutzername	Der Benutzername für die Verbindung zum virtuellen Host, z. B. „Administrator“ (bzw. „[Domänenname]\Administrator“, wenn sich die Maschine in einer Domäne befindet).

Textfeld	Description
Kennwort	Das sichere Kennwort, das für die Verbindung zum jeweiligen virtuellen Host verwendet wird.

6. Stellen Sie sicher, dass **Hyper-V-Server ohne einen Agenten im Gast-VMs schützen** oder **Hyper-V-Cluster ohne einen Agenten im Gast-VMs schützen**, je nach Ihrer Wahl in Schritt 4, ausgewählt ist. (Diese Option ist standardmäßig ausgewählt).
7. Klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Ausgewählte Maschinen** die VMs aus, die Sie schützen möchten.
9. Wenn Sie neue VMs automatisch schützen wollen, wenn Sie dem Host hinzugefügt werden, wählen Sie **Neue virtuelle Maschinen automatisch schützen**.
10. Klicken Sie auf **Weiter**.
11. Sie können ggf. auf der Seite **Schutz**, wenn in der Rapid Recovery Core Console anstelle der IP-Adresse ein Name für die geschützte Maschine angezeigt werden soll, im Feld **Anzeigename** einen Namen in das Dialogfeld eingeben.

    Sie können bis zu 64 Zeichen eingeben. Verwenden Sie keine Sonderzeichen (siehe Beschreibung in Unzulässige Zeichen). Darüber hinaus darf der Anzeigename nicht mit den im Abschnitt Unzulässige Phrasen aufgeführten Zeichenkombinationen beginnen.
12. Wählen Sie die gewünschte Einstellung für den Schutzzeitplan aus (siehe nachstehende Beschreibung):
    - Wählen Sie unter „Zeitplaneinstellungen“ die Option **Standardschutz (stündliche Snapshots aller Volumes)** aus, um den Standardschutzzeitplan zu verwenden.

    Im Standardschutzzeitplan erstellt der Core jede Stunde Snapshots aller Volumes der geschützten Maschine. Auf der Registerkarte **Zusammenfassung** für die jeweilige geschützte Maschine können Sie jederzeit die Schutzeinstellungen ändern, nachdem der Assistent beendet wurde, z. B. die zu schützenden Volumes auswählen.
    - Wählen Sie unter „Zeitplaneinstellungen“ die Option **Benutzerdefinierter Schutz** aus, um einen anderen Schutzzeitplan zu definieren.
13. Setzen Sie die Konfiguration wie folgt fort:
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und Standardschutz festgelegt haben und ein Repository vorhanden ist, klicken Sie auf **Fertigstellen**, um die ausgewählten Einstellungen zu bestätigen, den Assistenten zu schließen und die angegebene Maschine zu schützen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und Standardschutz festgelegt haben und kein Repository vorhanden ist, klicken Sie auf **Weiter** und fahren Sie mit Schritt 16 fort, um ein Repository zu erstellen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und benutzerdefinierten Schutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit dem nächsten Schritt fort, um auszuwählen, welche Volumes geschützt werden sollen.
    - Wenn Sie „Advanced Configuration“ (Erweiterte Konfiguration) für den Protect Machine Wizard (Assistenten zum Schützen der Maschine) und den Standardschutz ausgewählt haben, klicken Sie auf **Weiter** und fahren Sie mit Schritt 16 fort, um die Repository- und Verschlüsselungsoptionen anzuzeigen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine erweiterte Konfiguration ausgewählt und benutzerdefinierten Schutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit dem nächsten Schritt fort, um auszuwählen, welche Volumes geschützt werden sollen.

    Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, wird anhand des von Ihnen definierten Zeitplans ein Basisabbild (d. h. ein Snapshot aller Daten im geschützten Volume) zum Repository auf

dem Rapid Recovery Core übertragen, es sei denn, Sie haben angegeben, den Schutz anfänglich vorübergehend zu deaktivieren.

14. Wählen Sie auf der Seite **Schutz-Volumes** die Volumes aus, die Sie schützen möchten. Klicken Sie in der Spalte „Überprüfen“ auf die aufgelisteten Volumes, die nicht geschützt werden sollen, um die Auswahl aufzuheben. Klicken Sie anschließend auf **Weiter**.

    NOTE: In der Regel sollten zumindest das Volume „System-reserviert“ und das Volume mit dem Betriebssystem (normalerweise Laufwerk C:) geschützt werden.

15. Legen Sie auf der Seite **Schutzzeitplan** einen benutzerdefinierten Schutzzeitplan fest und klicken Sie auf **Weiter**. Ausführliche Informationen zum Festlegen eines benutzerdefinierten Schutzzeitplans finden Sie unter Erstellen von benutzerdefinierten Schutzzeitplänen im einfachen Modus.

    Wenn Sie bereits Repository-Informationen konfiguriert und die Option „Erweitert“ in Schritt 1 gewählt haben, wird die Seite „Verschlüsselung“ angezeigt. Fahren Sie mit Schritt 19 fort.

16. Führen Sie auf der Seite **Repository** folgende Aktion aus:

    - Wenn Sie bereits über ein Repository verfügen und die Daten für diese Maschine zum Schutz im bestehenden Repository speichern möchten, führen Sie einen der folgenden Schritte aus:

        1. Wählen Sie **Vorhandenes Repository verwenden** aus.
        2. Wählen Sie aus der Liste ein bestehendes Repository aus.
        3. Klicken Sie auf **Weiter**.

        Die Seite **Encryption** (Verschlüsselung) wird angezeigt. Wechseln Sie zu Schritt 19, um ggf. Verschlüsselungseinstellungen zu definieren.

    - Wenn Sie ein Repository erstellen möchten, geben Sie auf der Seite **Repository** die in der folgenden Tabelle beschriebenen Informationen ein und klicken Sie dann auf **Weiter** bzw. **Fertig stellen**.

Tabelle 70. Repository-Einstellungen

Textfeld	Description
Name	Geben Sie den Anzeigenamen des Repositorys ein. Dieses Textfeld enthält standardmäßig das Wort „Repository“ sowie eine Nummer, die der Nummer der Repositorys für diesen Core entspricht. Wenn es sich hierbei beispielsweise um das erste Repository handelt, lautet der Standardname „Repository 1“. Ändern Sie den Namen je nach Bedarf. Repository-Namen müssen zwischen 1 und 40 alphanumerischen Zeichen, einschließlich Leerzeichen enthalten. Verwenden Sie weder Unzulässige Zeichen noch Unzulässige Phrasen.
Speicherort	Geben Sie den Speicherort für die geschützten Daten ein. Dieses Volume sollte ein primärer Speicherort sein. Der Speicherort kann lokal (ein Laufwerk auf dem Core-Computer) oder ein freigegebenes CIFS-Netzwerklaufwerk sein. Für eine CIFS-Freigabe muss der Pfad mit \\ beginnen. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig. **CAUTION: Definieren Sie einen dedizierten Ordner innerhalb des Stammverzeichnisses für den Speicherort für das Repository. Geben Sie nicht die Stammposition an. Verwenden Sie zum Beispiel `E:\Repository\`, nicht `E:\`. Wenn das -Repository, das Sie in diesem Schritt erstellen, später entfernt wird, werden auch alle Dateien am Speicherort des Repositorys gelöscht. Wenn Sie Ihren Speicherort unter dem Stammverzeichnis definieren, werden alle anderen Dateien im Volume (z. B. `E:\`) gelöscht, was zu verheerendem Datenverlust führen könnte.** Geben Sie beispielsweise `X:\Repository\Data` ein.

Textfeld	Description
	Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.
Benutzername	Geben Sie einen Benutzernamen für einen Benutzer mit Administratorrechten an. Diese Information ist nur erforderlich, wenn der Repository-Speicherort ein Netzwerkpfad ist.
Kennwort	Geben Sie das Kennwort für den Benutzer mit Administratorrechten ein. Diese Information ist nur erforderlich, wenn der Repository-Speicherort ein Netzwerkpfad ist.
Metadatenpfad	Geben Sie den Speicherort für die geschützten Metadaten ein. Geben Sie beispielsweise `X:\Repository\Metadata` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.

17. Konfigurieren Sie auf der Seite **Repository-Konfiguration** die Menge an Speicherplatz auf der Festplatte, die dem Repository zugewiesen werden soll. Quest empfiehlt die Reservierung von 20 Prozent des Volumens für Metadaten, was die Standard-Einstellung ist. Optional können Sie mit dem Schieberegler oder im Feld **Größe** mehr oder weniger Speicherplatz auf dem Volume dem Repository zuordnen.
18. Wählen Sie optional **Erweiterte Optionen anzeigen** aus und passen Sie die Einstellungen wie in der folgenden Tabelle beschrieben an, wenn Sie detaillierte Informationen über Speicherorteinstellungen anzeigen und eingeben möchten. Um diese Optionen auszublenden, deaktivieren Sie die Option **Erweiterte Optionen anzeigen**. Wenn Sie Ihre Repository-Konfiguration abgeschlossen haben, klicken Sie auf **Weiter** bzw. **Fertig stellen**.

Tabelle 71. Details für Speicherkonfiguration

Textfeld	Description
Bytes pro Sektor	Geben Sie die Anzahl an Bytes an, die jeder Sektor enthalten soll. Der Standardwert ist 512.
Bytes pro Datensatz	Geben Sie die durchschnittliche Anzahl an Bytes pro Datensatz an. Der Standardwert ist 8192.
Schreib-Caching-Richtlinie	Die Schreib-Caching-Richtlinie steuert, wie der Windows Cache-Manager im Repository verwendet wird. Sie ermöglicht die Optimierung der Repository-Leistung bei unterschiedlichen Konfigurationen. Legen Sie den Wert auf eine der folgenden Optionen fest: • Ein • Aus • Sync Bei Auswahl der Standardeinstellung Ein steuert Windows das Caching. Dies ist geeignet für Windows 10 und für Versionen von Windows Server 2012 und höher. **NOTE:** Wenn die Schreib-Caching-Richtlinie auf Ein festgelegt wird, kann die Leistung gesteigert werden. Wenn Sie Windows Server 2008 R2 SP2 verwenden, ist die empfohlene Einstellung „Aus“. Wenn Sie „Aus“ festlegen, wird das Ablegen im Cache-Speicher von Rapid Recovery gesteuert.

Textfeld	Description
	Bei Auswahl von Sync steuert Windows das Caching sowie die synchrone Eingabe/Ausgabe.

Wenn Sie in Schritt 1 die Option **Erweitert** ausgewählt haben, wird die Seite **Verschlüsselung** angezeigt.

19. Wenn Sie Verschlüsselungsschlüssel für im Repository gespeicherte Daten verwenden möchten, wählen Sie optional auf der Seite **Verschlüsselung Die Daten im Ruhezustand in einem Repository verschlüsseln** aus und führen Sie dann einen der folgenden Schritte aus:

    - Um einen vorhandenen Verschlüsselungsschlüssel auf alle neuen Daten, die im Repository gespeichert werden, anzuwenden, wählen Sie **Daten mit einer Core-basierten Verschlüsselung mit vorhandenem Schlüssel verschlüsseln** und wählen Sie im Drop-Down-Menü **Verschlüsselungsschlüssel auswählen** den Verschlüsselungsschlüssel aus.
    - Um nun einen neuen Verschlüsselungsschlüssel festzulegen, der für alle zukünftigen Daten in Ihrem Repository angewendet werden soll, wählen Sie **Daten mit Core-basierter Verschlüsselung mit einem neuen Schlüssel verschlüsseln** und geben Sie anschließend die Informationen zu dem Schlüssel wie in der folgenden Tabelle beschrieben ein:

Tabelle 72. Neuen Verschlüsselungsschlüssel definieren

Textfeld	Description
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein. Namen für Verschlüsselungsschlüssel müssen 1 bis 64 alphanumerische Zeichen umfassen. Verwenden Sie keine unzulässigen Zeichen oder unzulässigen Phrasen.
Description	Geben Sie einen beschreibenden Kommentar für den Verschlüsselungsschlüssel ein. Diese Informationen werden im Beschreibungsfeld angezeigt, wenn Verschlüsselungsschlüssel in Rapid Recovery Core Console angezeigt werden. Die Beschreibung kann bis zu 254 Zeichen umfassen. Es hat sich bewährt, die Verwendung von unzulässigen Zeichen und unzulässigen Phrasen zu vermeiden.
Passphrase	Geben Sie eine Passphrase für die Zugriffssteuerung ein. Sie sollten keine unzulässigen Zeichen verwenden. Bewahren Sie die Passphrase an einem sicheren Ort auf. Quest Datenschutz-Support kann eine Passphrase nicht wiederherstellen. Wenn Sie einen Verschlüsselungsschlüssel erstellt und für eine geschützte Maschine verwendet haben, können Sie keine Daten dieser geschützten Maschine mehr wiederherstellen, wenn die Passphrase verloren geht.
Passphrase bestätigen	Geben Sie die Passphrase erneut ein. Dies wird zur Bestätigung der Passphraseneingabe verwendet.

20. Optional können Sie auf der Seite **Verschlüsselung Die Daten verschlüsseln, die über ein Netzwerk transportiert werden** auswählen, um alle Daten zu verschlüsseln, die über ein Netzwerk transportiert werden. Diese Option ist standardmäßig aktiviert; wenn Sie Daten nicht auf diese Art und Weise verschlüsseln möchten, müssen Sie diese Option also deaktivieren.
21. Klicken Sie auf **Fertigstellen**, um die Einstellungen zu speichern und zu übernehmen.

    Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, wird anhand des von Ihnen definierten Zeitplans ein Basisabbild (d. h. ein Snapshot aller Daten im geschützten Volume) zum Repository auf dem Rapid Recovery Core übertragen, es sei denn, Sie haben angegeben, den Schutz anfänglich vorübergehend deaktivieren.

Manuelles Schützen mehrerer Maschinen

Verwenden Sie dieses Verfahren, um manuell Details für mehrere Maschinen anzugeben, die Sie gleichzeitig mit der Agent Software schützen möchten. Die Details bestimmen jede Maschine im Netzwerk eindeutig und beinhalten die Verbindungsinformationen und Anmeldedaten. Dieser Ansatz wird häufig beim Schutz von Linux-Maschinen verwendet. Sie können mit diesem jedoch nur Windows-Maschinen, nur Linux-Maschinen, oder eine Kombination aus beiden schützen.

1. Klicken Sie auf der Rapid Recovery Core Console, auf das Drop-Down-Menü **Schützen** und dann auf **Schutz mehrerer Maschinen**.

   Daraufhin wird der Protect Multiple Machines Wizard (Assistent zum Schützen mehrerer Maschinen) angezeigt.
2. Wählen Sie auf der Seite **Willkommen** eine der folgenden Optionen aus:

   - Standard
   - Erweitert (optionale Schritte anzeigen)
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Verbindung** des Assistenten aus der Drop-Down-Liste **QuelleManuell** aus.
5. Klicken Sie auf **Weiter**.
6. Geben Sie auf der Seite **Maschinen auswählen** für jede Maschine, die Sie schützen möchten, die Maschinendetails im Dialogfeld ein. Drücken Sie die **Eingabetaste**, um separate Information für jede Maschine einzugeben, die Sie hinzufügen möchten. Verwenden Sie das Format `hostname::username::password::port`. Die Porteinstellung ist optional. Der Standardport für die Installation von Agenten auf Windows- oder Linux-Maschinen ist 8006. Beispiele:

   ```
   10.255.255.255::administrator::&11@yYz90z
   Linux-host-00-2::administrator::p@$$w0rD::8006
   ```
7. Klicken Sie auf **Weiter**.

   Wechseln Sie zu **Schritt 11**, wenn als Nächstes die Seite Schutz im Assistent zum Schützen mehrerer Maschinen angezeigt wird.

   Wenn die Agent-Software noch nicht auf den zu schützenden Maschinen bereitgestellt wurde oder eine der von Ihnen angegebenen Maschinen aus einem anderen Grund nicht geschützt werden kann, werden die ausgewählten Maschinen auf der **Warnseite** angezeigt.
8. Sie können eine Maschine auf der **Warnseite für Maschinen** auch selbst überprüfen, indem Sie die Maschine auswählen und in der Symbolleiste auf **Überprüfen** klicken.
9. Wählen Sie auf der **Warnseite für Maschinen** ggf. **Maschinen nach der Agent-Installation automatisch neu starten** aus.

   NOTE: Quest empfiehlt diese Option. Sie müssen die Agent-Maschinen neu starten, damit sie geschützt werden können. Durch Neustarten wird sichergestellt, dass der Agent-Dienst ausgeführt wird, und dass das korrekte Kernel-Modul zum Schutze der Maschine verwendet wird, falls relevant.
10. Klicken Sie auf **Weiter**, wenn der Status anzeigt, dass die Maschine erreichbar ist, um die Agent-Software zu installieren.

    Die Seite **Schutz** wird angezeigt.
11. Sie können ggf. auf der Seite **Schutz**, wenn in der Rapid Recovery Core Console anstelle der IP-Adresse ein Name für die geschützte Maschine angezeigt werden soll, im Feld **Anzeigename** einen Namen in das Dialogfeld eingeben.

Sie können bis zu 64 Zeichen eingeben. Verwenden Sie keine Sonderzeichen (siehe Beschreibung in). Darüber hinaus darf der Anzeigename nicht mit den im Abschnitt aufgeführten Zeichenkombinationen beginnen.

12. Wählen Sie die gewünschte Einstellung für den Schutzzeitplan aus (siehe nachstehende Beschreibung):

    - Wählen Sie unter „Zeitplaneinstellungen“ die Option **Standardschutz (stündliche Snapshots aller Volumes)** aus, um den Standardschutzzeitplan zu verwenden.

    Im Standardschutzzeitplan erstellt der Core jede Stunde Snapshots aller Volumes der geschützten Maschine. Auf der Registerkarte **Zusammenfassung** für die jeweilige geschützte Maschine können Sie jederzeit die Schutzeinstellungen ändern, nachdem der Assistent beendet wurde, z. B. die zu schützenden Volumes auswählen.

    - Wählen Sie unter „Zeitplaneinstellungen“ die Option **Benutzerdefinierter Schutz** aus, um einen anderen Schutzzeitplan zu definieren.

13. Setzen Sie die Konfiguration wie folgt fort:

    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und Standardschutz festgelegt haben und ein Repository vorhanden ist, klicken Sie auf **Fertigstellen**, um die ausgewählten Einstellungen zu bestätigen, den Assistenten zu schließen und die angegebene Maschine zu schützen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und Standardschutz festgelegt haben und kein Repository vorhanden ist, klicken Sie auf **Weiter** und fahren Sie mit Schritt 16 fort, um ein Repository zu erstellen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine Standardkonfiguration ausgewählt und benutzerdefinierten Schutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit dem nächsten Schritt fort, um auszuwählen, welche Volumes geschützt werden sollen.
    - Wenn Sie „Advanced Configuration“ (Erweiterte Konfiguration) für den Protect Machine Wizard (Assistenten zum Schützen der Maschine) und den Standardschutz ausgewählt haben, klicken Sie auf **Weiter** und fahren Sie mit Schritt 16 fort, um die Repository- und Verschlüsselungsoptionen anzuzeigen.
    - Wenn Sie im Assistenten zum Schützen einer Maschine eine erweiterte Konfiguration ausgewählt und benutzerdefinierten Schutz festgelegt haben, klicken Sie auf **Weiter** und fahren Sie mit dem nächsten Schritt fort, um auszuwählen, welche Volumes geschützt werden sollen.

    Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, wird anhand des von Ihnen definierten Zeitplans ein Basisabbild (d. h. ein Snapshot aller Daten im geschützten Volume) zum Repository auf dem Rapid Recovery Core übertragen, es sei denn, Sie haben angegeben, den Schutz anfänglich vorübergehend zu deaktivieren.

14. Wählen Sie auf der Seite **Schutz-Volumes** die Volumes aus, die Sie schützen möchten. Klicken Sie in der Spalte „Überprüfen“ auf die aufgelisteten Volumes, die nicht geschützt werden sollen, um die Auswahl aufzuheben. Klicken Sie anschließend auf **Weiter**.

    NOTE: In der Regel sollten zumindest das Volume „System-reserviert“ und das Volume mit dem Betriebssystem (normalerweise Laufwerk C:) geschützt werden.

15. Legen Sie auf der Seite **Schutzzeitplan** einen benutzerdefinierten Schutzzeitplan fest und klicken Sie auf **Weiter**. Ausführliche Informationen zum Festlegen eines benutzerdefinierten Schutzzeitplans finden Sie unter Erstellen von benutzerdefinierten Schutzzeitplänen im einfachen Modus.

    Wenn Sie bereits Repository-Informationen konfiguriert und die Option „Erweitert“ in Schritt 1 gewählt haben, wird die Seite „Verschlüsselung“ angezeigt. Fahren Sie mit Schritt 19 fort.

16. Führen Sie auf der Seite **Repository** folgende Aktion aus:

    - Wenn Sie bereits über ein Repository verfügen und die Daten für diese Maschine zum Schutz im bestehenden Repository speichern möchten, führen Sie einen der folgenden Schritte aus:

      1. Wählen Sie **Vorhandenes Repository verwenden** aus.
      2. Wählen Sie aus der Liste ein bestehendes Repository aus.

3. Klicken Sie auf **Weiter**.

   Die Seite **Encryption** (Verschlüsselung) wird angezeigt. Wechseln Sie zu Schritt 19, um ggf. Verschlüsselungseinstellungen zu definieren.

- Wenn Sie ein Repository erstellen möchten, geben Sie auf der Seite **Repository** die in der folgenden Tabelle beschriebenen Informationen ein und klicken Sie dann auf **Weiter** bzw. **Fertig stellen**.

Tabelle 73. Repository-Einstellungen

Textfeld	Description
Name	Geben Sie den Anzeigenamen des Repositorys ein. Dieses Textfeld enthält standardmäßig das Wort „Repository“ sowie eine Nummer, die der Nummer der Repositorys für diesen Core entspricht. Wenn es sich hierbei beispielsweise um das erste Repository handelt, lautet der Standardname „Repository 1“. Ändern Sie den Namen je nach Bedarf. Repository-Namen müssen zwischen 1 und 40 alphanumerischen Zeichen, einschließlich Leerzeichen enthalten. Verwenden Sie weder Unzulässige Zeichen noch Unzulässige Phrasen.
Speicherort	Geben Sie den Speicherort für die geschützten Daten ein. Dieses Volume sollte ein primärer Speicherort sein. Der Speicherort kann lokal (ein Laufwerk auf dem Core-Computer) oder ein freigegebenes CIFS-Netzwerklaufwerk sein. Für eine CIFS-Freigabe muss der Pfad mit \\ beginnen. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig. **CAUTION: Definieren Sie einen dedizierten Ordner innerhalb des Stammverzeichnisses für den Speicherort für das Repository. Geben Sie nicht die Stammposition an. Verwenden Sie zum Beispiel `E:\Repository\`, nicht `E:\`. Wenn das -Repository, das Sie in diesem Schritt erstellen, später entfernt wird, werden auch alle Dateien am Speicherort des Repositorys gelöscht. Wenn Sie Ihren Speicherort unter dem Stammverzeichnis definieren, werden alle anderen Dateien im Volume (z. B. `E:\`) gelöscht, was zu verheerendem Datenverlust führen könnte.** Geben Sie beispielsweise `X:\Repository\Data` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.
Benutzername	Geben Sie einen Benutzernamen für einen Benutzer mit Administratorrechten an. Diese Information ist nur erforderlich, wenn der Repository-Speicherort ein Netzwerkpfad ist.
Kennwort	Geben Sie das Kennwort für den Benutzer mit Administratorrechten ein. Diese Information ist nur erforderlich, wenn der Repository-Speicherort ein Netzwerkpfad ist.
Metadatenpfad	Geben Sie den Speicherort für die geschützten Metadaten ein. Geben Sie beispielsweise `X:\Repository\Metadata` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Sie können mit dem

Textfeld	Description
	umgekehrten Schrägstrich nur Ebenen im Pfad festlegen. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.

17. Konfigurieren Sie auf der Seite **Repository-Konfiguration** die Menge an Speicherplatz auf der Festplatte, die dem Repository zugewiesen werden soll. Quest empfiehlt die Reservierung von 20 Prozent des Volumens für Metadaten, was die Standard-Einstellung ist. Optional können Sie mit dem Schieberegler oder im Feld **Größe** mehr oder weniger Speicherplatz auf dem Volume dem Repository zuordnen.
18. Wählen Sie optional **Erweiterte Optionen anzeigen** aus und passen Sie die Einstellungen wie in der folgenden Tabelle beschrieben an, wenn Sie detaillierte Informationen über Speicherorteinstellungen anzeigen und eingeben möchten. Um diese Optionen auszublenden, deaktivieren Sie die Option **Erweiterte Optionen anzeigen**. Wenn Sie Ihre Repository-Konfiguration abgeschlossen haben, klicken Sie auf **Weiter** bzw. **Fertig stellen**.

Tabelle 74. Details für Speicherkonfiguration

Textfeld	Description
Bytes pro Sektor	Geben Sie die Anzahl an Bytes an, die jeder Sektor enthalten soll. Der Standardwert ist 512.
Bytes pro Datensatz	Geben Sie die durchschnittliche Anzahl an Bytes pro Datensatz an. Der Standardwert ist 8192.
Schreib-Caching-Richtlinie	Die Schreib-Caching-Richtlinie steuert, wie der Windows Cache-Manager im Repository verwendet wird. Sie ermöglicht die Optimierung der Repository-Leistung bei unterschiedlichen Konfigurationen. Legen Sie den Wert auf eine der folgenden Optionen fest: • Ein • Aus • Sync Bei Auswahl der Standardeinstellung Ein steuert Windows das Caching. Dies ist geeignet für Windows 10 und für Versionen von Windows Server 2012 und höher. **NOTE:** Wenn die Schreib-Caching-Richtlinie auf Ein festgelegt wird, kann die Leistung gesteigert werden. Wenn Sie Windows Server 2008 R2 SP2 verwenden, ist die empfohlene Einstellung „Aus“. Wenn Sie „Aus“ festlegen, wird das Ablegen im Cache-Speicher von Rapid Recovery gesteuert. Bei Auswahl von Sync steuert Windows das Caching sowie die synchrone Eingabe/Ausgabe.

Wenn Sie in Schritt 1 die Option **Erweitert** ausgewählt haben, wird die Seite **Verschlüsselung** angezeigt.

19. Wenn Sie Verschlüsselungsschlüssel für im Repository gespeicherte Daten verwenden möchten, wählen Sie optional auf der Seite **Verschlüsselung Die Daten im Ruhezustand in einem Repository verschlüsseln** aus und führen Sie dann einen der folgenden Schritte aus:

    - Um einen vorhandenen Verschlüsselungsschlüssel auf alle neuen Daten, die im Repository gespeichert werden, anzuwenden, wählen Sie **Daten mit einer Core-basierten Verschlüsselung mit vorhandenem Schlüssel verschlüsseln** und wählen Sie im Drop-Down-Menü **Verschlüsselungsschlüssel auswählen** den Verschlüsselungsschlüssel aus.
    - Um nun einen neuen Verschlüsselungsschlüssel festzulegen, der für alle zukünftigen Daten in Ihrem Repository angewendet werden soll, wählen Sie **Daten mit Core-basierter Verschlüsselung mit einem neuen Schlüssel verschlüsseln** und geben Sie anschließend die Informationen zu dem Schlüssel wie in der folgenden Tabelle beschrieben ein:

Tabelle 75. Neuen Verschlüsselungsschlüssel definieren

Textfeld	Description
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein. Namen für Verschlüsselungsschlüssel müssen 1 bis 64 alphanumerische Zeichen umfassen. Verwenden Sie keine unzulässigen Zeichen oder unzulässigen Phrasen.
Description	Geben Sie einen beschreibenden Kommentar für den Verschlüsselungsschlüssel ein. Diese Informationen werden im Beschreibungsfeld angezeigt, wenn Verschlüsselungsschlüssel in Rapid Recovery Core Console angezeigt werden. Die Beschreibung kann bis zu 254 Zeichen umfassen. Es hat sich bewährt, die Verwendung von unzulässigen Zeichen und unzulässigen Phrasen zu vermeiden.
Passphrase	Geben Sie eine Passphrase für die Zugriffssteuerung ein. Sie sollten keine unzulässigen Zeichen verwenden. Bewahren Sie die Passphrase an einem sicheren Ort auf. Quest Datenschutz-Support kann eine Passphrase nicht wiederherstellen. Wenn Sie einen Verschlüsselungsschlüssel erstellt und für eine geschützte Maschine verwendet haben, können Sie keine Daten dieser geschützten Maschine mehr wiederherstellen, wenn die Passphrase verloren geht.
Passphrase bestätigen	Geben Sie die Passphrase erneut ein. Dies wird zur Bestätigung der Passphraseneingabe verwendet.

20. Optional können Sie auf der Seite **Verschlüsselung Die Daten verschlüsseln, die über ein Netzwerk transportiert werden** auswählen, um alle Daten zu verschlüsseln, die über ein Netzwerk transportiert werden. Diese Option ist standardmäßig aktiviert; wenn Sie Daten nicht auf diese Art und Weise verschlüsseln möchten, müssen Sie diese Option also deaktivieren.
21. Klicken Sie auf **Fertigstellen**, um die Einstellungen zu speichern und zu übernehmen.

    Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, wird anhand des von Ihnen definierten Zeitplans ein Basisabbild (d. h. ein Snapshot aller Daten im geschützten Volume) zum Repository auf dem Rapid Recovery Core übertragen, es sei denn, Sie haben angegeben, den Schutz anfänglich vorübergehend deaktivieren.

Die Rapid Recovery Agent-Software wird, sofern erforderlich, auf den angegebenen Maschinen bereitgestellt, und die Maschinen werden im Core zum Schutz hinzugefügt.

Überwachen des Schutzes von mehreren Maschinen

Sie können den Fortschritt überwachen, während Rapid Recovery die Schutzrichtlinien und Zeitpläne auf den Maschinen anwendet.

1. Navigieren Sie in der Rapid Recovery Core Console zur Rapid Recovery Startseite und klicken Sie dann auf  (Ereignisse).

   Auf der Seite **Ereignisse** werden Aufgaben, Benachrichtigungen und Ereignisse angezeigt. Wenn Volumes übertragen werden, werden im Fensterbereich „Aufgaben“ der jeweilige Status sowie Start- und Endzeiten angezeigt.

Sie können Aufgaben auch nach Status filtern (Aktiv, System wartet, Abgeschlossen und Fehlgeschlagen). Weitere Informationen hierzu finden Sie unter Anzeigen von Aufgaben.

NOTE: Damit nur Aufgaben angezeigt werden, die auf ihre Ausführung warten, müssen Sie das Symbol für wartende Aufgaben auswählen.

Beim Hinzufügen der einzelnen geschützten Maschinen wird eine Benachrichtigung protokolliert, die angibt, ob der Vorgang erfolgreich war oder ob Fehler gemeldet wurden. Weitere Informationen hierzu finden Sie unter Anzeigen von Benachrichtigungen.

Informationen zum Anzeigen aller Ereignisse finden Sie unter Anzeigen eines Journals aller protokollierten Ereignisse.

Aktivieren des Anwendungssupports

Nachdem eine VM unter agentenlosen Schutz gestellt wurde, können Sie die auf dieser Maschine installierte Exchange- oder SQL-Anwendung unterstützen.

Bevor Sie beginnen, müssen folgende Voraussetzungen erfüllt sein.

- **VM mit dem Rapid Recovery Core schützen.** Die Option zum Aktivieren der Anwendungsunterstützung ist während des Schutz-Prozesses nicht verfügbar. Die Schaltfläche zum Aktivieren dieser Funktion wird auf mehrere Seiten in der Benutzeroberfläche angezeigt, nachdem die SQL- oder Exchange-Maschine unter Schutz gestellt wurde. Weitere Informationen finden Sie unter Schutz von virtuellen vCenter/ESXi-Maschinen mit agentenlosem Schutz bzw. Schutz von virtuellen Hyper-V-Maschinen mit agentenlosem Schutz.
- **Remote-WMI-Zugriff aktivieren.** Um WMI-Zugriff zu gewähren, müssen Sie Windows Remote Management auf der virtuellen Maschine (VM) installieren und konfigurieren. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel unter https://msdn.microsoft.com/en-us/library/aa384372(v=vs.85).aspx.
- **Administratorrechte remote lokalen Benutzern gewähren.** Konfigurieren Sie LocalAccountTokenFilterPolicy, indem Sie die folgende administrative Eingabeaufforderung ausführen:

  ```
  winrm quickconfig
  ```

- **Zugangsberechtigung für den WMI-Root-Namespace erhalten.** Damit der Core Anwendungen ohne den Agenten verbindet, muss die VM eingehenden Netzwerkverkehr auf den TCP-Ports 135 und 445 und den dynamisch zugewiesenen Ports 1024 und 1034 zulassen.
- **Remote-Zugriff auf SQL Server und Exchange zulassen.** Diese Voraussetzung ist abhängig von der Anwendung, die Sie unterstützen möchten.
  - **SQL:** Konfigurieren Sie die Windows-Firewall durch Öffnen der Ports 1433 und 1434.
  - **Exchange:** Öffnen Sie die TCP- und UDP 389-Ports.
- **Integrieren Sie die Gäste mit dem Host.** Die Integration erfolgt durch die Installation des jeweiligen Optimierungspakets für den Hypervisor:
  - Für ESXi VMs verwenden Sie **VMware Tools**, die für agentenlosen ESXi VM-Schutz erforderlich sind.
  - Für Hyper-V verwenden Sie das **Integration Services**-Paket, das auf den meisten Windows Server-Betriebssystemen vorinstalliert ist.

Führen Sie die folgenden Schritte aus, um Anwendungssupport für agentenlos geschützte VMs zu aktivieren.

1. Rufen Sie in der Core Console die Seite **Maschinen** auf.
2. Führen Sie eine der folgenden Aktionen aus:
   - Zum Aktivieren der Unterstützung für einzelne VM klicken Sie auf das Menü **Aktionen** für diese VM und klicken Sie dann auf **Anwendungssupport aktivieren**.
   - Zum Aktivieren der Unterstützung für mehrere VMs gleichzeitig, wählen Sie die VMs aus, klicken auf das Drop-Down-Menü **Anwendungssupport** und klicken dann auf **Anwendungssupport aktivieren**.
3. Geben Sie im Dialogfeld **Anwendungssupport bearbeiten** die Anmeldeinformationen für die VM ein.

Ein grünes Symbol wird neben dem Namen der geschützten Maschine angezeigt, für die Anwendungssupport aktiviert ist.

Wenn Sie Anmeldeinformationen für die Anwendung hinzufügen möchten, können Sie dies tun, indem Sie auf **SQL** oder **Exchange** am oberen Rand der Seite mit der **Zusammenfassung** für die Maschine eingeben.

Einstellungen und Funktionen für geschützte Exchange-Server

Wenn Sie einen Microsoft Exchange-Server in Ihrem Core schützen, stehen Ihnen zusätzliche Einstellungen zur Konfiguration in der Rapid Recovery Core Console und zusätzliche ausführbare Funktionen zur Verfügung.

In Bezug auf Exchange Server steht in der Core Console eine einzige Einstellung, **Automatische Überprüfung der Bereitstellungsfähigkeit aktivieren**, zur Verfügung. Wenn diese Option aktiviert ist, werden Bereitstellungsfähigkeitsprüfungen von Exchange-Servern automatisch durchgeführt. Diese Einstellung ist verfügbar, wenn der Status für die geschützte Maschine grün (aktiv) oder gelb (angehalten) ist.

Weitere Informationen finden Sie unter Informationen über Überprüfungen der Bereitstellungsfähigkeit.

Sie können eine Überprüfung der Bereitstellungsfähigkeit auch auf Anforderung im Bereich „Wiederherstellungspunkte“ auf einer geschützten Exchange Server-Maschine durchführen. Weitere Informationen finden Sie unter Erzwingen einer Bereitstellbarkeitsprüfung für eine Exchange-Datenbank.

Im Folgenden sind Funktionen aufgeführt, die Sie für einen durch den Core geschützten Exchange-Server ausführen können.

- **Exchange Server-Anmeldeinformationen festlegen**. Rapid Recovery Core ermöglicht Ihnen das Festlegen von Anmeldeinformationen, damit der Core den Exchange-Server für den Erhalt von Informationen authentifizieren kann.

  Weitere Informationen zum Festlegen der Anmeldeinformationen für Exchange-Server finden Sie unter Festlegen der Anmeldeinformationen für eine Exchange Server-Maschine.

- **Exchange-Protokolle kürzen.** Wenn Sie die Kürzung von Exchange Server-Protokollen erzwingen, wird durch diesen Prozess der verfügbare Speicherplatz identifiziert und Speicherplatz auf dem geschützten Exchange-Server freigegeben.

  Weitere Informationen zum Kürzen von Exchange Server-Protokollen auf Anforderung finden Sie unter Erzwingen einer Protokollkürzung für eine Exchange-Maschine. Dieser Prozess kann auch als Teil der nächtlichen Jobs durchgeführt werden.

- **Erzwingen einer Bereitstellbarkeitsprüfung für eine Exchange-Datenbank.** Diese Funktion führt eine Bereitstellbarkeitsprüfung von Exchange-Datenbanken durch, um Beschädigungen zu erkennen und Administratoren zu warnen, sodass alle Daten auf dem Exchange-Server erfolgreich wiederhergestellt werden können.

  Weitere Informationen über das Erzwingen einer Überprüfung der Bereitstellungsfähigkeit auf Anforderung finden Sie unter Erzwingen einer Bereitstellbarkeitsprüfung für eine Exchange-Datenbank.

Sie können auch eine automatische Überprüfung der Bereitstellungsfähigkeit nach jedem Snapshot erzwingen. Weitere Informationen zum Bereitstellbarkeitsprüfungen finden Sie unter Informationen über Überprüfungen der Bereitstellungsfähigkeit.

- **Erzwingen von Prüfsummenprüfungen für Exchange Server-Wiederherstellungspunkte.** Diese Funktion prüft die Integrität von Wiederherstellungspunkten, die Exchange Datenbankdateien enthalten.

  Weitere Informationen über das Erzwingen einer Prüfsummenprüfung auf Anforderung finden Sie unter Erzwingen einer Prüfsummen-Überprüfung von Exchange-Datenbank-Dateien.

Sie können Exchange-Protokolle kürzen und eine Prüfsummenprüfung als Teil der nächtlichen Jobs durchführen. Weitere Informationen zu den Aufgaben, die Sie als nächtliche Jobs planen können, finden Sie unter Grundlegende Informationen zu nächtlichen Jobs. Weitere Informationen zum Konfigurieren von nächtlichen Jobs finden Sie unter Konfigurieren nächtlicher Jobs für den Core.

Festlegen der Anmeldeinformationen für eine Exchange Server-Maschine

Um die korrekten Anmeldeinformationen einzustellen, muss ein Exchange Server auf einem geschützten Volume vorhanden sein. Falls Rapid Recovery nicht feststellen kann, ob eine Datenbank vorhanden ist, wird die Prüfsummenprüffunktion nicht in der Core Console angezeigt.

Wenn die Daten eines Microsoft Exchange-Servers geschützt werden, können Sie die Anmeldeinformationen in der Rapid Recovery Core Console konfigurieren.

Führen Sie die hier beschriebenen Schritte aus, um die Anmeldeinformationen für jeden Exchange-Server festzulegen.

1. Wählen Sie im linken Navigationsbereich der Rapid Recovery Core Console die geschützte Exchange-Server-Maschine aus, für die Sie Anmeldeinformationen einstellen möchten.

   Die Seite **Zusammenfassung** wird für den geschützten Exchange-Server angezeigt.

2. Klicken Sie auf der Seite **Zusammenfassung** über die Links am oberen Rand der Seite auf den nach unten zeigenden Pfeil rechts neben dem Exchange-Menü und wählen Sie dann im resultierende Dropdown-Menü **Anmeldeinformationen festlegen** aus.

   Das Dialogfeld **Exchange-Anmeldeinformationen bearbeiten** für den geschützten Exchange-Server wird angezeigt.

3. Geben Sie im Dialogfeld**Exchange-Anmeldeinformationen bearbeiten** Ihre Anmeldeinformationen wie folgt ein:
   a. Geben Sie im Textfeld **Benutzername** den Benutzernamen eines Benutzers mit Berechtigungen für den Exchange-Server ein, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).
   b. Geben Sie im Textfeld **Kennwort** das Kennwort für den Benutzernamen ein, der für die Verbindung zum Exchange-Server angegeben wurde.
   c. Klicken Sie auf **OK** um die Einstellungen zu bestätigen und das Dialogfeld zu schließen.

Erzwingen einer Protokollkürzung für eine Exchange-Maschine

Damit ein Abschneiden des Protokolls erzwungen werden kann, muss auf einem geschützten Volume eine Exchange-Datenbank vorhanden sein. Falls Rapid Recovery nicht feststellen kann, dass eine Datenbank vorhanden ist, wird die Prüfsummenprüffunktion nicht in der Core Console angezeigt.

Wenn Sie das Abschneiden des Protokolls für einen geschützten Exchange Server erzwingen, wird die Größe der Protokolle auf diese Weise reduziert. Führen Sie die folgenden Schritte aus, um ein Abschneiden des Protokolls zu erzwingen.

1. Wählen Sie im linken Navigationsbereich der Rapid Recovery Core Console den geschützten Exchange Server, für den Sie Sie das Abschneiden des Protokolls erzwingen möchten

   Die Seite **Zusammenfassung** für die geschützte Maschine wird angezeigt.
2. Klicken Sie oben auf der Seite auf das Drop-Down-Menü **Exchange** und wählen Sie **Abschneiden des Protokolls erzwingen**.
3. Klicken Sie in das sich öffnende Dialogfeld, um zu bestätigen, dass Sie das Abschneiden des Protokolls erzwingen möchten.

   Das Dialogfeld wird geschlossen. Das System startet mit dem Abschneiden der Exchange Server-Protokolle. Wenn Popup-Warnungen für diesen Typ des Ereignisses aktiviert sind, wird eine Meldung angezeigt, dass der Prozess des Abschneidens des Protokolls gestartet wird.

Informationen über Überprüfungen der Bereitstellungsfähigkeit

Wenn Sie Rapid Recovery für die Sicherung von Microsoft Exchange-Servern verwenden, können nach jedem Snapshot für alle Exchange-Datenbanken Bereitstellbarkeitsprüfungen durchgeführt werden. Diese Funktion ermöglicht die Ermittlung von Beschädigungen. Sie weist Administratoren auf mögliche Fehler hin und stellt sicher, dass alle Daten auf den Exchange-Servern bei einem Ausfall erfolgreich wiederhergestellt werden.

Um diese Funktion zu aktivieren bzw. deaktivieren, gehen Sie für eine geschützte Maschine zum Menü **Einstellungen** und setzen die Option **Automatische Überprüfung der Bereitstellungsfähigkeit aktivieren** entsprechend auf **Ja** oder **Nein**. Weitere Informationen über die Veränderung der Einstellungen für eine geschützte Maschine finden Sie unter Anzeigen und Ändern von geschützten Maschineneinstellungen.

Bereitstellbarkeitsprüfungen sind nicht Teil der nächtlichen Einstellungen. Wenn die automatische Überprüfung der Bereitstellungsfähigkeit aktiviert ist, und wenn das Abschneiden der Exchange-Protokolle für eine nächtliche Aufgabe aktiviert ist, dann wird die Bereitstellbarkeitsprüfung nach dem Abschneiden des Protokolls ausgelöst.

Sie können eine Überprüfung der Bereitstellungsfähigkeit auch auf Anforderung im Bereich **Wiederherstellungspunkte** auf einer geschützten Exchange Server-Maschine durchführen. Weitere Informationen finden Sie unter Erzwingen einer Bereitstellbarkeitsprüfung für eine Exchange-Datenbank.

NOTE: Bereitstellbarkeitsprüfungen sind nur für Microsoft Exchange Server 2007, 2010, 2013 und 2016 relevant. Außerdem muss das Rapid Recovery Agenten-Dienstkonto über die Rolle als Organisationsadministrator in Exchange verfügen.

Erzwingen einer Bereitstellbarkeitsprüfung für eine Exchange-Datenbank

Damit eine Bereitstellbarkeitsprüfung erzwungen werden kann, muss auf einem geschützten Volume eine Exchange-Datenbank vorhanden sein. Falls Rapid Recovery nicht feststellen kann, ob eine Datenbank vorhanden ist, wird die Bereitstellbarkeitsprüffunktion nicht in der Core Console angezeigt.

Führen Sie die folgenden Schritte aus, damit das System eine Bereitstellbarkeitsprüfung für einen bestimmten Exchange Server-Wiederherstellungspunkt durchführt.

1. Wählen Sie im linken Navigationsbereich der Rapid Recovery Core Console die geschützte Exchange-Server-Maschine aus, für die Sie die Überprüfung der Bereitstellungsfähigkeit erzwingen möchten, und klicken Sie dann auf das Menü **Wiederherstellungspunkte**.
2. Scrollen Sie zum Fensterbereich **Wiederherstellungspunkte**.
3. Navigieren Sie durch die Wiederherstellungspunkte, um den gewünschten Wiederherstellungspunkt zu suchen. Optional können Sie auf den Pfeil ▸ rechts neben einem Wiederherstellungspunkt in der Liste klicken, um die Ansicht zu erweitern.

   In den erweiterten Wiederherstellungspunktinformationen werden im Wiederherstellungspunkt eingeschlossene Volumes angezeigt.
4. Klicken Sie im Fensterbereich **Wiederherstellungspunkte** auf der Zeile für den entsprechenden Wiederherstellungspunkt auf  und wählen Sie aus dem Drop-Down-Menü die Option **Überprüfung der Bereitstellungsfähigkeit erzwingen**.
5. Klicken Sie im sich öffnenden Dialogfeld, um zu bestätigen, dass Sie eine Überprüfung der Bereitstellungsfähigkeit erzwingen möchten.

   Das Dialogfeld wird geschlossen. Das System führt die Bereitstellbarkeitsprüfung durch. Wenn Toast-Warnungen für diese Art von Ereignissen aktiviert sind, wird eine Meldung angezeigt, dass die Überprüfung der Bereitstellungsfähigkeit gestartet wird.

Informationen zum Anzeigen des Status der Bereitstellbarkeitsprüfung finden Sie unter Anzeigen von Ereignissen mithilfe von Aufgaben, Warnungen und Journalseiten.

Erzwingen einer Prüfsummen-Überprüfung von Exchange-Datenbank-Dateien

Damit eine Prüfsummenprüfung erzwungen werden kann, muss auf einem geschützten Volume eine Exchange-Datenbank vorhanden sein. Falls Rapid Recovery nicht feststellen kann, ob eine Datenbank vorhanden ist, wird die Prüfsummenprüffunktion nicht in der Core Console angezeigt.

Führen Sie die folgenden Schritte aus, damit das System eine Prüfsummenprüfung für einen bestimmten Exchange Server-Wiederherstellungspunkt durchführt.

1. Wählen Sie im linken Navigationsbereich der Rapid Recovery Core Console den geschützten Exchange-Server aus, für den Sie die Prüfsummenprüfung erzwingen möchten, und klicken Sie dann auf das Menü **Wiederherstellungspunkte**.

   Die Seite **Wiederherstellungspunkte** wird für den geschützten Exchange-Server angezeigt.
2. Scrollen Sie zum Fensterbereich **Wiederherstellungspunkte**.
3. Navigieren Sie durch die Wiederherstellungspunkte, um den gewünschten Wiederherstellungspunkt zu suchen. Optional können Sie auf den Pfeil ▸ rechts neben einem Wiederherstellungspunkt in der Liste klicken, um die Ansicht zu erweitern.

   In den erweiterten Wiederherstellungspunktinformationen werden im Wiederherstellungspunkt eingeschlossene Volumes angezeigt.
4. Klicken sie im Fensterbereich **Wiederherstellungspunkte** auf der Zeile, die den richtigen Wiederherstellungspunkt darstellt, auf  und wählen Sie aus dem Drop-Down-Menü die Option **Prüfsummenprüfung erzwingen** aus.
5. Klicken Sie im sich öffnenden Dialogfeld, um zu bestätigen, dass Sie eine Prüfsummenprüfung erzwingen möchten.

Das Dialogfeld wird geschlossen. Das System führt die Prüfsummenprüfung durch. Wenn Toast-Warnungen für diese Art von Ereignissen aktiviert sind, wird eine Meldung angezeigt, dass die Prüfsummenprüfung gestartet wird.

Informationen zum Anzeigen des Status der Prüfsummenprüfung finden Sie unter Anzeigen von Ereignissen mithilfe von Aufgaben, Warnungen und Journalseiten.

Einstellungen und Funktionen für geschützte SQL-Server

Wenn Sie einen Microsoft SQL-Server in Ihrem Core schützen, stehen Ihnen zusätzliche Einstellungen zur Konfiguration in der Rapid Recovery Core Console und zusätzliche ausführbare Funktionen zur Verfügung.

In Bezug auf SQL-Server steht in der Core Console eine einzige Einstellung, **Anfügbarkeit**, zur Verfügung.

Mit Rapid Recovery Core können Sie eine SQL-Anfügbarkeitsprüfung durchführen, um die Integrität der Wiederherstellungspunkte, die SQL-Datenbanken enthalten, zu überprüfen. Mit dieser Maßnahme wird die Konsistenz von SQL-Datenbanken überprüft und sichergestellt, dass alle unterstützende MDF- (Daten) und LDF-Dateien (Protokoll) im Sicherungs-Snapshot verfügbar sind.

In früheren Versionen war für SQL-Anfügbarkeitsprüfungen in der Vergangenheit eine lizenzierte Version von SQL Server auf der Core-Maschine erforderlich. Rapid Recovery Core bietet jetzt die Möglichkeit, SQL-Anfügbarkeitsprüfungen von einer SQL Server-Instanz auf dem Core, oder von einer lizenzierten SQL Server-Version auf einer geschützten SQL-Maschine durchzuführen.

In den Anfügbarkeitseinstellungen können Sie angeben, welche lizenzierte Version von SQL Server verwendet wird, um diese Prüfung durchführen. Weitere Informationen zum Konfigurieren der Anfügbarkeitseinstellungen finden Sie unter Verwalten von Core-SQL-Anfügbarkeitseinstellungen.

Weitere Informationen zur SQL-Anfügbarkeit finden Sie unter Über die SQL-Anfügbarkeit.

Im Folgenden sind Funktionen aufgeführt, die Sie für einen durch den Core geschützten SQL-Server ausführen können.

- **SQL Server-Anmeldeinformationen festlegen.** Rapid Recovery Core ermöglicht Ihnen das Festlegen von Anmeldeinformationen, damit der Core den SQL-Server für den Erhalt von Informationen authentifizieren kann. Sie können Anmeldeinformationen für eine einzelne geschützte SQL-Servermaschine oder Standardanmeldeinformationen für alle geschützten SQL-Server festlegen.

  Weitere Informationen zum Festlegen der Anmeldeinformationen für SQL-Server finden Sie unter Festlegen der Anmeldeinformationen für eine SQL Server-Maschine.

- **SQL-Protokolle kürzen.** Wenn Sie die Kürzung von SQL Server-Protokollen erzwingen, wird durch diesen Prozess der verfügbare Speicherplatz auf dem geschützten Server identifiziert. Dieser Prozess gibt keinen Speicherplatz frei.

  Weitere Informationen zum Kürzen von SQL Server-Protokollen auf Anforderung finden Sie unter Erzwingen einer Protokollkürzung für eine SQL-Maschine.

- **Anfügbarkeitsprüfung eines SQL-Servers erzwingen**. Mit dieser Funktion wird die Konsistenz von SQL-Datenbanken überprüft und sichergestellt, dass alle unterstützende MDF- (Daten) und LDF-Dateien (Protokoll) im Sicherungs-Snapshot verfügbar sind.

  Weitere Informationen über das Erzwingen einer Anfügbarkeitsprüfung für SQL-Server auf Anforderung finden Sie unter Erzwingen einer SQL Server-Anfügbarkeitsprüfung.

Außer der Angabe von Anmeldeinformationen kann jeder der nachfolgend beschriebenen Funktionen auf Anforderung erfolgen und kann auch so konfiguriert werden, dass sie als Teil der nächtlichen Jobs für den Core stattfindet. Weitere Informationen zu den Aufgaben, die Sie als nächtliche Jobs planen können, finden Sie unter Grundlegende Informationen zu nächtlichen Jobs. Weitere Informationen zum Konfigurieren von nächtlichen Jobs finden Sie unter Konfigurieren nächtlicher Jobs für den Core.

Festlegen der Anmeldeinformationen für eine SQL Server-Maschine

Sie müssen die zu schützende SQL-Server-Maschine auf dem Rapid Recovery Core vor Durchführung dieses Verfahrens hinzufügen. Weitere Informationen zum Schützen von Maschinen finden Sie unter Schützen einer Maschine.

Wenn die Daten eines Microsoft Exchange-Servers geschützt werden, können Sie die Anmeldeinformationen für eine einzelne Instanz oder für alle SQL Server in der Rapid Recovery Core Console konfigurieren.

Führen Sie die hier beschriebenen Schritte aus, um die Anmeldeinformationen für jeden SQL-Server festzulegen.

1. Wählen Sie im linken Navigationsbereich der Rapid Recovery Core Console die geschützte SQL-Server-Maschine aus, für die Sie Anmeldeinformationen festlegen möchten.

   Die Seite **Zusammenfassung** wird für den geschützten SQL-Server angezeigt.
2. Klicken Sie auf der Seite **Zusammenfassung** über die Links am oberen Rand der Seite auf den nach unten zeigenden Pfeil ▾ rechts neben dem SQL-Menü und wählen Sie dann im resultierenden Dropdown-Menü eine der folgenden Vorgehensweisen:

   - Klicken Sie auf **Standardanmeldeinformationen für alle Instanzen festlegen**, wenn Sie die Standardanmeldeinformationen für alle SQL Server-Datenbankinstanzen festlegen möchten, und führen Sie im Dialogfeld **Standardanmeldeinformationen bearbeiten** die folgenden Schritte aus:

     1. Geben Sie im Textfeld **Benutzername** den Benutzernamen eines Benutzers mit Berechtigungen für alle SQL-Server ein, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).
     2. Geben Sie im Textfeld **Kennwort** das Kennwort für den Benutzernamen ein, der für die Verbindung zum SQL-Server angegeben wurde.
     3. Klicken Sie auf **OK** um die Einstellungen zu bestätigen und das Dialogfeld zu schließen.
   - Wenn Sie die Anmeldeinformationen für eine einzelne SQL Server-Datenbankinstanz festlegen möchten, klicken Sie auf den Anzeigenamen der geschützten SQL-Server-Maschine und führen Sie im Dialogfeld **Anmeldeinformationen für Instanz bearbeiten** die folgenden Schritte aus:

     1. Wählen Sie den Typ der Anmeldeinformationen aus („Standard“, „Windows“ oder „SQL“).
     2. Geben Sie im Textfeld **Benutzername** den Benutzernamen eines Benutzers mit Berechtigungen für den SQL-Server ein, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).
     3. Geben Sie im Textfeld **Kennwort** das Kennwort für den Benutzernamen ein, der für die Verbindung zum SQL-Server angegeben wurde.
     4. Klicken Sie auf **OK** um die Einstellungen zu bestätigen und das Dialogfeld zu schließen.

Erzwingen einer Protokollkürzung für eine SQL-Maschine

Die Protokollkürzung ist für Maschinen mit SQL Server verfügbar. Führen Sie die folgenden Schritte aus, um eine Protokollkürzung zu erzwingen.

NOTE: Bei einer SQL-Maschine wird der freie Speicherplatz auf einem Datenträger ermittelt, die Größe der Protokolle aber nicht verringert.

1. Wählen Sie im linken Navigationsbereich der Rapid Recovery Core Console die Maschine, für die Sie Sie das Abschneiden des Protokolls erzwingen möchten.

Die Seite **Zusammenfassung** für die geschützte Maschine wird angezeigt.

2. Klicken Sie auf der Seite **Zusammenfassung** (oder von einer beliebigen Seite für diese geschützte Maschine), oben auf der Seite auf das Drop-Down-Menü **SQL** und wählen Sie **Abschneiden des Protokolls erzwingen**.
3. Klicken Sie auf **Ja**, um zu bestätigen, dass die Protokollkürzung durchgeführt werden soll.

Über die SQL-Anfügbarkeit

Mit der SQL-Anfügbarkeitsfunktion kann der Rapid Recovery Core SQL Master-Datenbankdateien (.MDF-Dateien) und Protokoll-Datenbankdateien (.LDF-Dateien) an einen Snapshot eines geschützten SQL-Servers anfügen. Der Snapshot wird unter Verwendung einer lokalen Instanz von Microsoft SQL Server erfasst.

Zu den für SQL-Server-Maschinen schützende Rapid Recovery-Benutzer relevanten Problemen gehören, welche Instanz von SQL Server die Anfügbarkeit durchführt und die Methode der Durchführung der SQL-Anfügbarkeit (auf Anforderung oder als Teil der nächtlichen Jobs).

Mithilfe der Anfügbarkeitsprüfung kann der Core die Konsistenz der SQL-Datenbanken prüfen und es kann sichergestellt werden. dass alle MDF- und LDF-Dateien im Sicherungs-Snapshot verfügbar sind.

Anfügbarkeitsprüfungen können bei Bedarf für bestimmte Wiederherstellungspunkte oder im Rahmen eines nächtlichen Jobs ausgeführt werden.

Informationen zur Durchführung der SQL-Anfügbarkeitsprüfungen auf Anforderung finden Sie unter Erzwingen einer SQL Server-Anfügbarkeitsprüfung. Um die SQL-Anfügbarkeit einmal täglich zur angegebenen Uhrzeit für Ihre nächtliche Job-Vorgänge durchzuführen, aktivieren Sie die Option **Check attachability for SQL databases** (Anfügbarkeit für SQL-Datenbanken prüfen) bei nächtlichen Jobs. Weitere Informationen zur Einrichtung nächtlicher Jobs für den Core finden Sie unter Konfigurieren nächtlicher Jobs für den Core. Weitere Informationen zur Einrichtung nächtlicher Jobs für eine bestimmte Machine (in diesem Fall ein geschützter SQL-Server) finden Sie unter Anpassen der nächtlichen Jobs für eine geschützte Maschine.

In früheren Versionen war es für die SQL-Anfügbarkeit erforderlich, dass eine lokale Instanz von Microsoft SQL Server auf der Core-Maschine installiert und konfiguriert ist. Mit Rapid Recovery Core können Sie die Anfügbarkeitsprüfung jetzt entweder von einer SQL Server-Instanz auf dem Core oder von einer SQL Server-Instanz auf einer geschützten SQL-Maschine durchführen. Die von Ihnen ausgewählte Instanz muss eine volllizenzierte SQL Server-Version sein, die bei Microsoft oder einem lizenzierten Händler erworben wurde. Microsoft lässt keine Nutzung von passiven SQL-Lizenzen zu.

Die von Ihnen festgelegte SQL Server-Instanz wird dann für alle Anfügbarkeitsprüfungen verwendet. Die Anfügbarkeit wird zwischen Core-Einstellungen und nächtlichen Jobs synchronisiert. Wenn Sie beispielsweise festlegen, dass die Core-Instanz von SQL Server für nächtliche Jobs verwendet werde soll, nutzen On-Demand-Anfügbarkeitsprüfungen dann auch den Core. Wenn Sie umgekehrt eine SQL Server-Instanz auf einer bestimmten geschützten Maschine festlegen, nutzen alle On-Demand- und nächtlichen Anfügbarkeitsprüfungen dann die lokale Instanz auf der geschützten Maschine.

Wählen Sie die SQL Server-Instanz aus, die als Teil der allgemeinen Core-Einstellungen verwendet werden soll. Weitere Informationen finden Sie unter Verwalten von Core-SQL-Anfügbarkeitseinstellungen.

NOTE: Für das Durchführen der Anfügbarkeitsprüfung von einer geschützten SQL Server-Maschine muss die Rapid Recovery Agent-Software auf diesem Server installiert sein. Agentenloser Schutz wird für die SQL-Anfügbarkeit nicht unterstützt.

Die Anfügbarkeit in Rapid Recovery Core wird für SQL Server 2005, 2008, 2008 R2, 2012 und 2014 unterstützt. Das für den Test verwendete Konto muss über die sysadmin-Rolle für die SQL Server-Instanz verfügen.

Das SQL Server-Speicherformat auf der Festplatte ist in den 64-Bit- und 32-Bit-Umgebungen identisch, sodass die Anfügbarkeit in beiden Versionen funktioniert. Eine Datenbank, die von einer in einer Umgebung aktiven Serverinstanz getrennt wurde, kann an eine in einer anderen Umgebung aktive Serverinstanz angefügt werden.

NOTE: Die SQL Server-Version auf dem Core muss gleich oder höher sein als die SQL Server-Version auf allen geschützten Maschinen, auf denen SQL Server installiert ist.

Erzwingen einer SQL Server-Anfügbarkeitsprüfung

Damit eine Anfügbarkeitsprüfung zu erzwingen, muss eine SQL-Datenbank auf einem geschützten Volume vorhanden sein. Falls Rapid Recovery nicht feststellen kann, dass eine Datenbank vorhanden ist, wird die Anfügbarkeitsprüffunktion nicht in der Core Console angezeigt.

Führen Sie die folgenden Schritte aus, damit das System eine Anfügbarkeitsprüfung für einen bestimmten SQL Server-Wiederherstellungspunkt durchführt.

1. Wählen Sie im linken Navigationsbereich der Rapid Recovery Core Console die geschützte SQL Server-Maschine aus, für die Sie die Anfügbarkeitsprüfung erzwingen möchten, und klicken Sie dann auf das Menü **Recovery Points** (Wiederherstellungspunkte).
2. Scrollen Sie zum Fensterbereich **Wiederherstellungspunkte**.
3. Navigieren Sie durch die Wiederherstellungspunkte, um den gewünschten Wiederherstellungspunkt zu suchen. Optional können Sie auf den Pfeil ▸ rechts neben einem Wiederherstellungspunkt in der Liste klicken, um die Ansicht zu erweitern.

   In den erweiterten Wiederherstellungspunktinformationen werden im Wiederherstellungspunkt eingeschlossene Volumes angezeigt.
4. Klicken Sie im Fensterbereich **Wiederherstellungspunkte** auf der Zeile für den entsprechenden Wiederherstellungspunkt auf  und wählen Sie aus dem Drop-Down-Menü die Option **Anfügbarkeitsprüfung erzwingen**.
5. Bestätigen Sie im darauffolgenden Dialogfeld durch Klicken, dass Sie eine Anfügbarkeitsprüfung erzwingen möchten.

   Das Dialogfeld wird geschlossen. Das System führt die Anfügbarkeitsprüfung durch.

Informationen zum Anzeigen des Status der Überprüfung der Bereitstellungsfähigkeit finden Sie unter Anzeigen von Ereignissen mithilfe von Aufgaben, Warnungen und Journalseiten.

Verwalten geschützter Maschinen

In diesem Kapitel wird beschrieben, wie geschützte Maschinen in der Rapid Recovery-Umgebung angezeigt, konfiguriert und verwaltet werden.

Informationen über das Verwalten geschützter Maschinen

Sie können geschützte Maschinen über denRapid Recovery Core Console verwalten, einschließlich der folgenden Aufgaben:

- Sie können geschützte Maschinen im Rapid Recovery Core Console mithilfe der unter beschriebenen Optionen anzeigen.
- Sie können die Einstellungen für eine bestimmte Maschine konfigurieren, die die Standardeinstellungen des Core überschreiben. Zu den Konfigurationsaufgaben zählen das Ändern der Hypervisor Host- oder VM-Einstellungen, Zugriff auf Systeminformationen, Ändern von Übertragungseinstellungen, Anpassen der nächtlichen Jobs oder zum Konfigurieren von Benachrichtigungen für Ereignisse. Weitere Informationen finden Sie unter Konfigurieren von Maschineneinstellungen.
- Sie können durch Anzeigen der Protokolldatei für eine geschützte Maschine eine Maschine oder ein Cluster aus dem Schutz entfernen, Lizenzinformationen für eine geschützte Maschine anzeigen oder Probleme diagnostizieren. Für weitere Informationen zu dieser und anderen Aufgaben siehe Verwalten von Maschinen.
- Sie können im Core gespeicherte Daten anzeigen und verwalten. Weitere Informationen finden Sie unter Verwalten von Snapshots und Wiederherstellungspunkten.

Anzeigen geschützter Maschinen

Von der **Startseite** auf Rapid Recovery Core Console können beim Betrachten der Zusammenfassungstabellen Zusammenfassungsinformationen für alle Maschinen, die durch den Core geschützt sind, im Fensterbereich der geschützten Maschinen angezeigt werden.

NOTE: Ein Software-Agent erledigt für den Benutzer die jeweiligen Aktionen. Geschützte Maschinen werden bisweilen als Agenten bezeichnet, da sie die Rapid Recovery Agent Software ausführen, um Datensicherung und -replikation auf Rapid Recovery Core zu ermöglichen.

Die folgenden Informationen werden angezeigt: Status, Anzeigename der einzelnen Maschinen, das verwendete Repository, Datum und Uhrzeit des letzten Snapshots, Anzahl der vorhandenen Wiederherstellungspunkte im Repository für die Maschine sowie der insgesamt von den Snapshots belegte Speicherplatz im Repository.

Sie können eine geschützte Maschine verwalten, indem Sie zu der geschützten Maschine navigieren, die Sie anzeigen, konfigurieren oder verwalten möchten. Von der **Startseite** gibt es drei Möglichkeiten, zu einer geschützten Maschine zu navigieren:

- Sie können auf die IP-Adresse oder den Anzeigenamen einer geschützten Maschine aus dem Fensterbereich der geschützten Maschinen klicken. Daraufhin wird die Seite „Zusammenfassung“ für die ausgewählte Maschine angezeigt.
- Im linken Navigationsbereich können Sie auf den Titel des Menüs **Geschützte Maschinen** klicken. Die Seite **Geschützte Maschinen** wird angezeigt. Auf dieser Seite werden Übersichtsinformationen zu den einzelnen Maschinen angezeigt. Eine ausführliche Beschreibung dieser Seite finden Sie unter Anzeigen von zusammenfassenden Informationen für eine geschützte Maschine.
- Sie können im linken Navigationsbereich unter dem Menü „Geschützte Maschinen“ auf die IP-Adresse oder den Anzeigenamen einer geschützten Maschine klicken. Daraufhin wird die Seite **Zusammenfassung** für die ausgewählte Maschine angezeigt. Eine ausführliche Beschreibung dieser Seite finden Sie unter Anzeigen von zusammenfassenden Informationen für eine geschützte Maschine.

Anzeigen von Cluster-Übersichtsinformationen

Führen Sie die folgenden Schritte aus, um zusammenfassende Informationen für einen Cluster anzuzeigen, z. B. Informationen zum Quorum für den Cluster.

1. Klicken Sie in der Rapid Recovery Core Console unter „Geschützte Maschinen“ auf den Cluster, den Sie anzeigen möchten.

   Die Seite „Zusammenfassung“ für die Maschine wird angezeigt.
2. Auf der Seite „Zusammenfassung“ werden Informationen wie Cluster-Name, Cluster-Typ, Quorumtyp (sofern zutreffend) und Quorumpfad (sofern zutreffend) angezeigt. Auf dieser Seite werden auch Übersichtsinformationen zu den Volumes in diesem Cluster, z. B. Größe und Schutzzeitplan, angezeigt. Sofern zutreffend können auch SQL Server- oder Exchange Server-Informationen für einen anderen Cluster angezeigt werden.
3. Zum Anzeigen der aktuellsten Informationen klicken Sie auf **Aktualisieren**.

Weitere Informationen zum Anzeigen von Übersichts- und Statusinformationen für eine einzelne Maschine (Knoten) in einem Cluster finden Sie unter .

Konfigurieren von Maschineneinstellungen

Sobald Sie eine Maschine zum Schutz Rapid Recovery Core hinzugefügt haben, können Sie auf einfache Weise die Einstellungen anzeigen und ändern, die das Verhalten der geschützten Maschine bestimmen. Wenn Sie Einstellungen für eine bestimmte Maschine ändern, ersetzen diese die bisherigen Verhaltenseinstellungen auf Core-Ebene.

Sie können die folgenden Maschineneinstellungen in Rapid Recovery Core Console anzeigen und konfigurieren:

- **Allgemein**. Allgemeine Konfigurationseinstellungen für die Maschinen umfassen Anzeigename, Hostname, Port, Verschlüsselungsschlüssel, Repository und Verknüpfungen zu einem Hypervisor-Host. Informationen über das Konfigurieren von allgemeinen Einstellungen für eine Maschine finden Sie unter Anzeigen und Ändern von geschützten Maschineneinstellungen.
- **Nächtliche Jobs**. Die Teilmenge der Core Jobeinstellungen für nächtliche Jobs, die für eine bestimmte geschützte Maschine angezeigt werden, ermöglicht Ihnen, die Einstellungen für nächtliche Jobs auf

Core-Ebene zu ersetzen. Dies schließt Rollup ein, das Ihnen ein Verwalten der Aufbewahrungsrichtlinie ermöglicht. Einige Einstellungen können je nach Typ der geschützten Maschine variieren.

- **Übertragungseinstellungen.** Spezifische Einstellungen zum Verwalten von Datenübertragungsprozessen für die ausgewählte geschützte Maschine. Informationen über Datenübertragungsarten, für die diese Einstellungen gelten, finden Sie unter Informationen über das Ändern von Übertragungseinstellungen.
- **Ausgeschlossene Writer**. Mit diesen Einstellungen können Sie Writer ausschließen. Die Einstellungen sind maschinenspezifisch. Ein Writer ist eine bestimmte von Microsoft veröffentlichte API, die eine Verwendung von Microsoft Volumeschatten-Diensten (VSS) für andere Softwarekomponenten ermöglicht. Jeder Writer in Rapid Recovery, der an Volume-Snapshots teilnimmt, ist in den Einstellungen der ausgeschlossenen Writer aufgeführt. Für den Fall, dass ein Writer erfolgreiche Sicherungsübertragungen stört oder behindert, können die Writer nacheinander deaktiviert werden. Quest empfiehlt das Beibehalten dieser Einstellungen, es sei denn, ein Quest Datenschutz-Support Mitarbeiter weist Sie anderweitig an.
- **Lizenzdetails**. Dies sind Details über die Lizenz für die jeweilige geschützte Maschine. Mit diesen Einstellungen werden Informationen aus dem Core und Rapid Recovery Lizenzportal berichtet. Diese Einstellungen sind schreibgeschützt. Aktualisieren Sie zum Ändern dieser Einstellungen die Lizenzinformationen des Core mit denen des Lizenzportals. Weitere Einzelheiten erhalten Sie von Ihrem Lizenz-Administrator. Weitere Informationen finden Sie unter *Rapid Recovery Lizenzportal - Benutzerhandbuch*.

Das Verfahren zum Anzeigen oder Ändern von Einstellungen auf Maschinenebene ist identisch für allgemeine Einstellungen, ausgeschlossene Writer und Lizenzdetails. Weitere Informationen hierzu finden Sie unter Anzeigen und Ändern von geschützten Maschineneinstellungen.

Das Verfahren zum Ändern von nächtlichen Jobs für eine Maschine ist anders. Informationen über das Konfigurieren der Einstellungen für nächtliche Jobs finden Sie unter Anpassen der nächtlichen Jobs für eine geschützte Maschine.

Manchmal ist eine Anpassung der Datentransferrate für eine geschützte Maschine erforderlich. Weitere Informationen hierzu finden Sie unter Informationen über das Ändern von Übertragungseinstellungen.

Anzeigen und Ändern von geschützten Maschineneinstellungen

Maschineneinstellungen helfen, das Verhalten einer durch den Core geschützten Maschine zu bestimmen. Wenn Sie Einstellungen für eine bestimmte Maschine ändern, ersetzen diese die bisherigen Verhaltenseinstellungen auf Core-Ebene.

Genauso hat auch ein geschützter virtueller Hyper-V Host andere Maschineneinstellungen als die virtuellen Maschinen, die er verwaltet. Weitere Informationen hierzu finden Sie unter Anzeigen von zusammenfassenden Informationen für einen Host.

Führen Sie die hier beschriebenen Schritte aus, um allgemeine Einstellungen, Übertragungseinstellungen für ausgeschlossene Writer und Lizenzierungseinstellungen für eine geschützte Maschine anzuzeigen und zu ändern.

NOTE: Informationen Zum Anzeigen und Ändern von nächtlichen Aufgaben-Einstellungen finden Sie unter Anpassen der nächtlichen Jobs für eine geschützte Maschine.

1. Klicken Sie in Rapid Recovery Core Console im Menü „Geschützte Maschinen“ auf die IP-Adresse oder den Maschinennamen für die Maschine, die Sie anzeigen oder ändern möchten.

   Die Registerkarte **Zusammenfassung** für die ausgewählte Maschine wird angezeigt.
2. Klicken Sie auf das Menü **Einstellungen**.

   Die Seite **Einstellungen** wird angezeigt. Sie enthält Einstellungen für die ausgewählte Maschine. Wahlweise können Sie zum Anzeigen von Einstellungskategorien von überall auf dieser Seite auf den entsprechenden Hyperlink im linken Seitenbereich klicken.

Wenn Sie auf eine Einstellung klicken, die Sie ändern möchten, kann diese Einstellung nun bearbeitet werden. Führen Sie eine der folgenden Aktionen aus:

- Wenn das Bedienelement ein Drop-Down-Menü ist, klicken Sie auf den nach unten gerichteten Pfeil, um die Optionen anzuzeigen, und wählen Sie die gewünschte Option aus dem Menü aus.
- Wenn das Bedienelement ein Textfeld ist, geben Sie einen Wert ein.
- Wenn als Option **Ja** oder **Nein** angezeigt wird, klicken Sie auf den Wert, der durch ein Kontrollkästchen ersetzt wird. Für die Einstellung von „Ja“ aktivieren Sie das Kontrollkästchen. Für den Wert „Nein“ deaktivieren Sie das Kontrollkästchen.
- Wenn die Option einen Zeitwert anzeigt (zum Beispiel Stunden, Minuten und Sekunden), klicken Sie auf jede Komponente und geben Sie einen neuen Wert ein oder verwenden Sie die Aufwärts- und Abwärtspfeile, um die neuen Werte zu wählen.

Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf ✔, um die Änderungen zu bestätigen und zu speichern, und verlassen Sie den Bearbeitungsmodus oder klicken Sie auf ✖, um den Bearbeitungsmodus ohne Speichern zu beenden.

3. Um allgemeine Einstellungen für eine geschützte Maschine zu ändern, klicken Sie auf die entsprechende Einstellung und dann geben Sie die in der folgenden Tabelle beschriebenen Konfigurationsinformationen ein.

Tabelle 76. Allgemeine Einstellungen für eine geschützte Maschine

Textfeld	Description
Anzeigename	Geben Sie einen Anzeigenamen für die Maschine ein. Dieser Name wird für eine geschützte Maschine in der Rapid Recovery Core Console angezeigt. Sie können bis zu 64 Zeichen eingeben. Standardmäßig ist dies der Hostname für die Maschine. Sie können ihn bei Bedarf in einen aussagekräftigeren Namen ändern. Verwenden Sie weder Unzulässige Zeichen noch Unzulässige Phrasen.
Hostname	Dies ist der Name der geschützten Maschine, so wie er in den Metadaten der Maschine erscheint. **NOTE:** Ändern Sie diese Einstellung nicht, da Sie sonst die Verbindung zwischen der geschützten Maschine und dem Core unterbrechen könnten.
Repository	Diese Einstellung wird nur für geschützte Hyper-V-Cluster angezeigt, die Unterstützung für freigegebene virtuelle Festplatten bieten. Zeigt das Repository an, das auf Rapid Recovery Core konfiguriert ist, in dem Wiederherstellungspunkte für freigegebene virtuelle Festplatten für den geschützten Hyper-V-Cluster gespeichert sind.
Port	Geben Sie eine Portnummer für die Maschine ein. Der Port wird vom Rapid Recovery Core Dienst für die Kommunikation mit der Maschine genutzt. Der Standardport ist 8006.
Verschlüsselungsschlüssel	Wenn die für diesen Rapid Recovery Core definierte Verschlüsselung für die Daten aller Volumes dieser geschützten Maschine verwendet werden soll, können Sie den Verschlüsselungsschlüssel hier angeben. Der Schlüssel muss entsperrt werden. Wenn keine Verschlüsselungsschlüssel vorhanden sind, können Sie einen Verschlüsselungsschlüssel hinzufügen. Weitere Informationen zum Verwalten von Verschlüsselungsschlüsseln finden Sie im entsprechenden Abschnitt Verwalten von Verschlüsselungsschlüsseln. Wenn die Volumes dieser geschützten Maschine verschlüsselt sind, können Sie einen anderen Verschlüsselungsschlüssel auswählen. Alternativ können Sie den jeweiligen Verschlüsselungsschlüssel entfernen, indem Sie im Dropdown-Menü für den **Verschlüsselungsschlüssel(keine)** auswählen.

Textfeld	Description
	NOTE: Nachdem ein Verschlüsselungsschlüssel angewendet, geändert oder für eine geschützte Maschine entfernt wurde, erstellt Rapid Recovery beim nächsten geplanten oder erzwungenen Snapshot ein neues Basisimage.
Repository	Wählen Sie ein Repository für die Wiederherstellungspunkte aus. Zeigt das Repository im Rapid Recovery Core an, in dem die Daten für diese Maschine gespeichert werden sollen. Das Repository-Volume kann lokal (auf angeschlossenen Speicher zum Core Server) oder auf einem Volume auf einem CIFS-Freigabeverzeichnis sein. **NOTE:** Die Repository-Einstellung auf dieser Seite kann nur dann geändert werden, wenn keine Wiederherstellungspunkte vorhanden sind oder das vorherige Repository fehlt.
Hypervisor	Diese Einstellung wird nur für virtuelle Maschinen angezeigt. Der Wert für diese Einstellung gibt an, ob die ausgewählte virtuelle Maschine als untergeordnetes Element einem geschützten Hypervisor-Host zugeordnet ist. • Wenn Sie die IP-Adresse oder den Anzeigenamen eines geschützten Hosts sehen, besteht die Zuordnung. Dieses Ergebnis deutet darauf hin, dass die geschützte Maschine nicht unnötigerweise eine Lizenz aus Ihrem verfügbaren Lizenzpool verbraucht. • Wenn Sie die Zuordnung entfernen möchten, klicken Sie auf die IP-Adresse oder den Anzeigenamen des Hypervisors-Hosts, wählen Sie **Nicht verknüpft** aus dem Drop-Down-Menü aus und klicken Sie auf das Häkchen, um die Änderung zu bestätigen. Danach verbraucht diese geschützte VM eine Lizenz aus Ihrem Pool. • Wenn „Nicht verknüpft“ angezeigt wird, ist die Maschine derzeit nicht Ihrem Core als VM auf einem geschützten Host zugeordnet und benötigt eine Lizenz aus Ihrem Pool. Wenn Sie eine Lizenz speichern möchten und der Host durch Agent geschützt ist, können Sie ihn durch Anklicken von **Nicht verknüpft** und Auswahl des Hosts aus dem Drop-Down-Menü zuordnen.
Betriebssystem-Version	Diese Einstellung wird nur für virtuelle Gast-Maschinen mit Zuordnung zu einem geschützten Hypervisor-Host angezeigt. In der Regel erkennt Rapid Recovery das Betriebssystem auf der geschützten VM und zeigt dieses an.

4. Informationen zum Ändern von nächtlichen Aufgabeneinstellungen für eine geschützte Maschine finden Sie unter Anpassen der nächtlichen Jobs für eine geschützte Maschine.
5. Um Exchange-Server-Einstellungen für einen geschützten Exchange-Server zu ändern, klicken Sie im Abschnitt für Exchange-Server-Einstellungen auf **automatische Überprüfung der Bereitstellungsfähigkeit aktivieren** und führen die folgenden Schritte aus:
   - Um die automatische Überprüfung der Bereitstellungsfähigkeit zu aktivieren, markieren Sie das Kontrollkästchen und klicken dann auf ✓.
   - Um die automatische Überprüfung der Bereitstellungsfähigkeit zu deaktivieren, deaktivieren Sie das Kontrollkästchen und klicken dann auf ✕.

   Weitere Informationen zur automatischen Überprüfung der Bereitstellungsfähigkeit finden Sie unter Informationen über Überprüfungen der Bereitstellungsfähigkeit.
6. Um Übertragungseinstellungen für eine geschützte Maschine zu ändern, klicken Sie auf die entsprechende Einstellung, und dann geben Sie die in der folgenden Tabelle beschriebenen Konfigurationsinformationen ein.

NOTE: Allgemeine Informationen zu den Einstellungen für die Übertragungseinstellungen finden Sie unter Informationen über das Ändern von Übertragungseinstellungen.

Tabelle 77. Übertragungseinstellungen für eine geschützte Maschine

Textfeld	Description
Standardeinstellung wiederherstellen	Diese Steuerung stellt die gesamten Übertragungseinstellungen auf die Standardeinstellungen des Systems wieder her.
Priorität	Legt die Übertragungspriorität zwischen geschützten Maschinen fest. Sie können damit die Priorität relativ zu anderen geschützten Maschinen zuweisen. Wählen Sie eine Zahl von 1 bis 10 aus. (Dabei ist 1 die höchste Priorität.) Die Standardeinstellung für die Priorität ist 5. **NOTE:** Die Priorität wird für Übertragungen verwendet, die sich in der Warteschlange befinden.
Maximale Anzahl gleichzeitiger Streams	Legt die maximale Anzahl von TCP-Verbindungen zum Core fest, die jeweils parallel für eine einzelne geschützte Maschine verarbeitet werden (bei Maschinen, die in einem DVM-Repository geschützt werden). **NOTE:** Quest empfiehlt, diesen Wert auf 8 festzulegen. Vergrößern Sie diese Einstellung, wenn Datenpakete verloren gehen.
Maximale Anzahl gleichzeitiger Schreibvorgänge	Legt die maximale Anzahl gleichzeitiger Festplattenschreibvorgänge für jeweils eine Verbindung zu einer geschützten Maschine fest. **NOTE:** Quest empfiehlt, diese Einstellung auf denselben Wert wie für „Maximale Anzahl gleichzeitiger Streams“ festzulegen. Stellen Sie einen geringfügig kleineren Wert ein, wenn Pakete verloren gehen, z. B. auf 7, wenn „Maximale Anzahl gleichzeitiger Streams“ auf 8 festgelegt ist.
Maximale Standardanzahl der Wiederholungen von Core verwenden	Wählen Sie diese Option aus, wenn die Standardanzahl der Wiederholungen für alle geschützten Maschinen verwendet werden soll, falls Vorgänge fehlschlagen.
Maximale Segmentgröße	Gibt die größte Anzahl an Daten (in Byte) an, die ein Computer in einem einzelnen TCP-Segment empfangen kann. Die Standardeinstellung ist 4194304. Ändern Sie diese Einstellung nicht von der Standardeinstellung, außer auf Anweisung eines Quest Support-Mitarbeiters.
Maximale Tiefe der Übertragungswarteschlange	Gibt die Anzahl der Befehle an, die gleichzeitig gesendet werden kann. Die Standardeinstellung ist 64. Sie können eine höhere Zahl einstellen, wenn im System eine Vielzahl von gleichzeitigen E/A-Vorgängen durchgeführt wird.
Ausstehende Lesevorgänge pro Stream	Gibt die Anzahl der Lesevorgänge in der Warteschlange an, die im Back-End gespeichert werden. Mit dieser Einstellung können Sie die Warteschlangenverwaltung für geschützte Maschinen steuern. Die Standardeinstellung ist 0.

Textfeld	Description
Serverport für Übertragungsdaten	Legt den Port für Übertragungen fest. Die Standardeinstellung ist 8009.
Zeitüberschreitung für Übertragungen	Gibt den Zeitraum in Minuten und Sekunden an, für den ein Paket ohne Übertragung gleich bleiben darf.
Zeitüberschreitung für Snapshots	Gibt den Zeitraum in Minuten und Sekunden an, für den auf die Erstellung eines Snapshots gewartet wird.
Zeitüberschreitung bei der Snapshotbereinigung	Gibt die maximale Zeit in Minuten und Sekunden für den Vorgang des Löschens des VSS-Snapshots auf einer geschützten Maschine an.
Zeitüberschreitung für Netzwerklesevorgänge	Gibt den Zeitraum in Minuten und Sekunden an, für den auf eine Leseverbindung gewartet wird. Wenn innerhalb dieses Zeitraums kein Netzwerklesevorgang durchgeführt werden kann, wird der Vorgang wiederholt.
Zeitüberschreitung für Netzwerkschreibvorgänge	Gibt die maximale Zeit in Sekunden an, für die auf eine Schreibverbindung gewartet werden soll. Wenn innerhalb dieses Zeitraums kein Netzwerkschreibvorgang durchgeführt werden kann, wird der Vorgang wiederholt.
Snapshot-Daten verschlüsseln	Gibt an, ob Daten, die zwischen dem geschützten Computer und dem Core transportiert werden, verschlüsselt sind. Diese Option ist standardmäßig aktiviert. Diese Einstellung gilt für die Daten während des Transports über ein Netzwerk. Wenn diese Option aktiviert ist, werden alle Snapshot-Daten, die zu einem DVM-Repository transportiert werden, verschlüsselt. **NOTE:** Quest empfiehlt, diese Einstellung auf „Ja“ festzulegen, wenn Daten zwischen dem Core und geschützten Maschinen über das öffentliche oder nicht vertrauenswürdige Netzwerke wie das Internet übertragen werden.

7. Um Einstellungen für ausgeschlossene Writer zu ändern, klicken Sie auf die entsprechende Einstellung und wählen Sie dann einen Writer aus, den Sie ausschließen möchten.

   NOTE: Da die in der Liste angezeigten Writer spezifisch für die konfigurierte Maschine sind, werden nicht alle Writer in der Liste angezeigt.

8. Details zur Lizenz für eine geschützte Maschine sind schreibgeschützt. Detail-Informationen zur Lizenz werden in der folgenden Tabelle beschrieben.

Tabelle 78. Details zur Lizenz für eine geschützte Maschine

Textfeld	Description
Ablaufdatum	Gibt das Ablaufdatum der Lizenz für die ausgewählte geschützte Maschine an.
Lizenzstatus	Gibt den aktuellen Status der Lizenz für die ausgewählte geschützte Maschine an.
Lizenztyp	Gibt den Typ der Lizenz für die ausgewählte geschützte Maschine an.
Typ des Agenten	Gibt an, ob die aktuelle geschützte Maschine ein physischer oder virtueller Agent ist.

See also: Ändern der Einstellungen für einen Hyper-V-Host oder -Knoten
See also: Ändern der Einstellungen für eine geschützte virtuelle Hyper-V-Maschine
See also: Ändern der vSphere-Einstellungen für eine geschützte virtuelle VMware-Maschine

Ändern der Einstellungen für einen Hyper-V-Host oder -Knoten

Dieses Verfahren gilt für Hyper-V-Hosts oder -Knoten, die Rapid Recovery Rapid Snap for Virtual (agentenlosen Schutz) zum Schutz von virtuellen Maschinen (VMs) verwenden.

Ein Hyper-V-Host, der Rapid Snap for Virtual (agentenloser Schutz) zum Schutz von VMs verwendet, ist im linken Navigationsbereich durch das Host-Symbol  gekennzeichnet. Die Einstellungen für einen Hyper-V-Host mit VMs, die agentenlos geschützt werden, sind nicht mit denen einer typischen geschützten Maschine identisch. Alle Änderungen, die an den Einstellungen für einen Host vorgenommen werden, gelten für die VMs auf diesem Host.

1. Klicken Sie auf der Core Console unter „Geschützte Maschinen“ im linken Navigationsbereich auf den Hyper-V-Host, dessen Einstellungen Sie ändern möchten.

   Die Seite **Zusammenfassung** für den Host wird angezeigt.
2. Klicken Sie in der Menüleiste für den Host auf **Einstellungen**.

   Die Seite **Einstellungen** wird angezeigt.
3. Klicken Sie unter **Allgemein** auf die Einstellung, die Sie ändern möchten.

   Die ausgewählte Einstellung kann nun in einem Textfeld oder in einem Drop-Down-Menü bearbeitet werden.
4. Geben Sie die Konfigurationsinformationen ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 79. Informationen zu allgemeinen Einstellungen

Textfeld	Description
Anzeigename	Der Name, der für eine geschützte Maschine in der Rapid Recovery Core Console angezeigt wird. Sie können bis zu 64 Zeichen eingeben. Standardmäßig ist dies der Hostname der Maschine. Sie können den Anzeigenamen bei Bedarf in einen aussagekräftigeren Namen ändern. Verwenden Sie weder Unzulässige Zeichen noch Unzulässige Phrasen.
Hostname	Der Name der geschützten Maschine, so wie er in den Metadaten der Maschine erscheint. **NOTE:** Ändern Sie diese Einstellung nicht, da Sie sonst die Verbindung zwischen der geschützten Maschine und dem Core unterbrechen könnten.

5. Klicken Sie unter **Übertragungswarteschlange** auf die Einstellung für **Maximale Anzahl gleichzeitiger Übertragungen**, um die Anzahl der Übertragungs-Jobs, die gleichzeitig auf dem Host auftreten können, zu ändern.

   NOTE: Um eine optimale Leistung zu erzielen, wird empfohlen, die maximale Anzahl gleichzeitiger Übertragungen für den Hyper-V-Host oder -Knoten auf 1 zu setzen. Dies ist die Standardeinstellung.
6. Klicken Sie unter **Nächtliche Jobs** auf **Ändern**, um die Einstellungen für die verfügbaren nächtlichen Jobs zu ändern.

   Das Fenster **Nächtliche Jobs** wird angezeigt.
7. Geben Sie die Konfigurationsinformationen ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 80. Informationen über die Einstellungen nächtlicher Jobs

Textfeld	Description
Verwaistn Registrierungsschlüssel auf geschütztem Hyper-V-Host löschen	Entfernt nicht benötigte Dateien aus der Registrierung, die durch Verbinden und Trennen virtueller Laufwerke während der Datenübertragung erzeugt wurden.
Prüfen Sie die Integrität der Wiederherstellungspunkte	Führt eine Integritätsprüfung jedes Wiederherstellungspunkts durch, der für die virtuellen Maschinen auf dem Hyper-V-Host erstellt wurde.

8. Klicken Sie auf **OK**.
9. Klicken Sie unter **Auto Schutz** auf die Einstellung für **Neue Maschinen automatisch schützen**, um zu bestimmen, ob neue virtuelle Maschinen beim Hinzufügen zum Hyper-V-Host automatisch geschützt werden sollen.

Ändern der Einstellungen für eine geschützte virtuelle Hyper-V-Maschine

Dieses Verfahren gilt für virtuelle Hyper-V-Maschinen, die mit der Funktion „Rapid Snap for Virtual“ von Rapid Recovery (agentenloser Schutz) geschützt sind.

Eine Hyper-V-VM, die durch Rapid Snap for Virtual geschützt wird (agentenloser Schutz) ist im linken Navigationsbereich durch das Host-Symbol gekennzeichnet. Die Einstellungen für eine agentenlose Hyper-V-VM sind die gleichen wie für eine typische geschützte Maschine mit Ausnahme des Hyper-V-Abschnitts am unteren Rand der Seite Einstellungen. Die folgende Task enthält Anweisungen, die nur für den Abschnitt Hyper-V der Seite „Einstellungen“ gelten. Für alle anderen geschützten Maschineneinstellungen siehe Anzeigen und Ändern von geschützten Maschineneinstellungen.

1. Klicken Sie auf der Core Console unter **Geschützte Maschinen** im linken Navigationsbereich auf die Hyper-V-VM, deren Einstellungen Sie ändern möchten.

   Die Seite **Zusammenfassung** für die VM wird angezeigt.
2. Klicken Sie in der Menüleiste für den Host auf **Einstellungen**.

   Die Seite **Einstellungen** wird angezeigt.
3. Klicken Sie in der Liste auf der linken Seite auf **Hyper-V**.

   Die ausgewählte Einstellung kann nun in einem Textfeld oder in einem Drop-Down-Menü bearbeitet werden.
4. Klicken Sie unter **Hyper-V** auf **Snapshot-Konfiguration**.

   Die ausgewählte Einstellung kann nun in einem Dropdown-Menü bearbeitet werden.
5. Wählen Sie aus dem Dropdown-Menü eine der in der folgenden Tabelle beschriebenen Optionen aus.

Tabelle 81. Informationen zu Hyper-V-Einstellungen

Textfeld	Description
Versuchen Sie, einen VSS-Snapshot während der Übertragung zu erstellen, wenn	Wenn der VSS-Snapshot erfolgreich ist, wird der Wiederherstellungspunkt ist in einem anwendungskonsistenten Zustand erstellt. Wenn der VSS-Snapshot fehlschlägt und ein

Textfeld	Description
dies fehlschlägt, erstellen Sie einen Prüfpunkt.	Prüfpunkt erstellt wird, liegt der Wiederherstellungspunkt in einem absturzkonsistenten Zustand vor.
Erstellen Sie den VSS-Snapshot nicht während der Übertragung.	Erzeugt einen Wiederherstellungspunkt in einem absturzkonsistenten Zustand.
Verwenden Sie nur VSS-Snapshots während der Übertragungen. Wenn der VSS-Snapshot fehlschlägt, schlägt die gesamte Übertragung fehl.	Erzeugt nur anwendungskonsistente Wiederherstellungspunkte. Wenn der VSS-Snapshot fehlschlägt, wird kein Wiederherstellungspunkt erstellt.

Ändern der vSphere-Einstellungen für eine geschützte virtuelle VMware-Maschine

Dieses Verfahren gilt für virtuelle VMware ESXi-Maschinen (VMs), die mit der Funktion „Rapid Snap for Virtual“ (agentenloser Schutz) geschützt sind.

Der Einstellungen für eine VMware-VM, die agentenlos geschützt ist, schließt die gleichen Einstellungen wie für eine typische geschützte Maschine ein, wobei es jedoch eine Ausnahme gibt. Der Abschnitt **vSphere** der Seite **Einstellungen** enthält Einstellungen, die nur für agentenlose geschützte VMware-VMs gelten. Die folgende Task enthält Anweisungen, die für nur den Abschnitt **vSphere** der Seite **Einstellungen** gelten. Für alle anderen geschützten Maschineneinstellungen siehe Anzeigen und Ändern von geschützten Maschineneinstellungen.

1. Klicken Sie auf der Core Console unter „Geschützte Maschinen“ im linken Navigationsbereich auf den Hyper-V-Host, dessen Einstellungen Sie ändern möchten.

   Die Seite **Zusammenfassung** für den Host wird angezeigt.
2. Klicken Sie in der Menüleiste für den Host auf **Einstellungen**.

   Die Seite **Einstellungen** wird angezeigt.
3. Klicken Sie in der Liste auf der linken Seite auf **vSphere**.

   Die ausgewählte Einstellung kann nun in einem Textfeld oder in einem Drop-Down-Menü bearbeitet werden.
4. Klicken Sie unter **vSphere** auf die Einstellung, die Sie ändern möchten.

   Die ausgewählte Einstellung kann nun in einem Textfeld oder in einem Drop-Down-Menü bearbeitet werden.
5. Geben Sie die Konfigurationsinformationen ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 82. Informationen zu den vSphere-Einstellungen

Textfeld	Description
Rapid Recovery gestatten, den in VMware erstellten Benutzer zu löschen	Die Standardeinstellung ist „Nein“.
Übertragung für Volumes mit einer ungültigen verwendeten Kapazität zulassen	Die Standardeinstellung ist „Ja“.
Stillgelegte Snapshots gestatten	Die Standardeinstellung ist „Ja“.

Informationen über das Ändern von Übertragungseinstellungen

In Rapid Recovery können Sie die Einstellungen für die Verwaltung der Datenübertragung für eine geschützte Maschine ändern. Die in diesem Abschnitt beschriebenen Übertragungseinstellungen werden auf der Ebene der geschützten Maschinen festgelegt. Informationen zur Übertragung auf Core-Ebene finden Sie unter Ändern der Einstellungen für die Übertragungswarteschlange.

Es stehen drei Übertragungsarten in Rapid Recovery zur Auswahl:

- **Snapshot.** Sichert die Daten der geschützten Maschine. Es sind zwei verschiedenartige Snapshots möglich: Basisimage aller geschützten Daten und inkrementelle Snapshots für Daten, die seit dem letzten Snapshot aktualisiert wurden. Bei einer derartigen Übertragung werden Wiederherstellungspunkte erstellt, die im Repository des Core gespeichert werden. Weitere Informationen hierzu finden Sie unter Verwalten von Snapshots und Wiederherstellungspunkten.
- **Export einer virtuellen Maschine**. Erstellt aus einem Wiederherstellungspunkt eine virtuelle Maschine (VM), die alle Daten der Sicherung der geschützten Maschine sowie Betriebssystem und Treiber und zugehörige Daten enthält, damit die VM gestartet werden kann. Weitere Informationen hierzu finden Sie unter VM-Export.
- **Wiederherstellen**. Stellt die gesicherten Informationen für eine geschützte Maschine wieder her. Weitere Informationen hierzu finden Sie unter Informationen über das Wiederherstellen von Volumes aus Wiederherstellungspunkten.

  NOTE: Bei der Wiederherstellung von Windows-Systemen mit EFI-Systempartitionen wird immer das gesamte Volume zurückgeschrieben.

Bei der Datenübertragung in Rapid Recovery wird ein Daten-Volume über ein Netzwerk von geschützten Maschinen zum Core übertragen. Bei einer Replikation werden Daten auch vom Ursprungs- oder Quell-Core zum Ziel-Core übertragen.

Die Datenübertragung kann für das jeweilige System über bestimmte Optionseinstellungen für die Leistung optimiert werden. Diese Einstellungen steuern die genutzte Bandbreite bei der Sicherung von geschützten Maschinen, bei VM-Exportvorgängen bzw. bei einer Wiederherstellung. Die Datenübertragungsleistung wird u. a. durch folgende Faktoren beeinflusst:

- Anzahl der gleichzeitigen Datenübertragungen von Agenten
- Anzahl der gleichzeitigen Datenstreams
- Umfang der geänderten Daten auf den Datenträgern
- Verfügbare Netzwerkbandbreite
- Leistung des Festplattensubsystems d für das Repository
- Verfügbarer Arbeitsspeicher zum Puffern von Daten

Sie können die Leistungsoptionen an die jeweiligen Anforderungen anpassen und die Leitung für die jeweilige Umgebung optimieren. Weitere Informationen hierzu finden Sie unter Einschränkung der Übertragungsrate.

Einschränkung der Übertragungsrate

Bei der Übertragung von Sicherungsdaten oder replizierten Wiederherstellungspunkten zwischen geschützten Maschinen und Cores über das Netzwerk können Sie die Übertragungsrate reduzieren. Dieser Prozess ist bekannt als Einschränkung.

Bei Einschränkung der Übertragungsrate schränken Sie die Netzwerkbandbreite für die Übertragung von Dateien über Rapid Recovery ein. Beim Einrichten der Replikation kann eine Einschränkung beispielsweise die

Wahrscheinlichkeit reduzieren, dass die Übertragung von früheren Wiederherstellungspunkten zum replizierten Core die gesamte Netzwerkbandbreite verbraucht.

CAUTION: Eine Einschränkung der Übertragungsrate ist nicht immer erforderlich oder empfehlenswert. Diese Informationen dienen einer Lösung von möglichen Probleme mit der Leistung in Ihrer Rapid Recovery-Umgebung. Manchmal kann eine Einschränkung beispielsweise Probleme im Zusammenhang mit wiederholten Übertragungsfehlern oder einer Netzwerkverlangsamung durch Übertragung einer erheblichen Menge an Daten für geschützte oder replizierte Cores lösen.

Es gibt verschiedene Faktoren bei der Bestimmung der besten Vorgehensweise bei der Einschränkung. Der Typ der geschützten Maschine spielt eine wesentliche Rolle. Beispielsweise hat ein ausgelasteter Microsoft Exchange Server eine viel höhere Änderungsrate als ein selten benutzter Legacy-Webserver.

Die Eingabe- und Ausgabefunktionen des Speicher-Volumes auf Ihren geschützten Maschinen können auch zu einer geringeren oder größeren Effizienz beitragen.

Die Geschwindigkeit Ihres Netzwerks ist ein weiterer kritischer Faktor mit vielen Variablen. Der verwendete Netzwerk-Backbone (zum Beispiel: 1 GbE im Vergleich zu 10 GbE), die Architektur, die Konfiguration, eine absichtliche Nutzung von NIC-Teaming und sogar der verwendete Kabeltyp können Auswirkungen auf die Übertragungsrate im Netzwerk haben. Wenn Ihre Umgebung über ein langsameres Fernnetz verfügt und Übertragungsjobs nicht gesichert oder repliziert werden können, können Sie mithilfe einiger dieser Einstellungen die Übertragungsrate einschränken.

Eine Einschränkung des Netzwerkes erfolgt letztendlich durch systematisches Ausprobieren. Quest empfiehlt ein Anpassen und Testen Ihrer Übertragungseinstellungen sowie ein regelmäßiges Überprüfen der Einstellungen, um sicherzustellen, dass die Einstellungen weiterhin auf Ihre Anforderungen abgestimmt sind.

Ein Anpassen der Übertragungsrate sollte für jede Maschine einzeln erfolgen. Navigieren Sie in der Core Console zu einer bestimmten Maschine, wählen Sie "Einstellungen" aus und passen Sie die Übertragungsgeschwindigkeit an. Spezifische Informationen über das Anzeigen und Ändern dieser Einstellungen finden Sie unter Anzeigen und Ändern von geschützten Maschineneinstellungen.

Dieser Abschnitt enthält auch Beschreibungen zu den für die Einschränkung verwendeten Einstellungen. Diese Beschreibungen können nützlich sein, um zu bestimmen, mit welchen Einstellungen Sie zuerst experimentieren sollten.

Die vier wichtigsten Einstellungen für eine Einschränkung der Übertragungsrate werden in der folgenden Tabelle beschrieben:

Einstellung auf Maschinenebene	Standardeinstellung	Vorgeschlagene Einstellung zur Einschränkung
Maximale Anzahl gleichzeitiger Streams	8	4
Maximale Anzahl gleichzeitiger Schreibvorgänge	8	4
Maximale Segmentgröße	4194304	2097152
Ausstehende Lesevorgänge pro Stream	0	Starten Sie bei 24

Quest empfiehlt ein Anpassen und Testen der anderen Einstellungen vor Änderung der Standardeinstellung für ausstehende Lesevorgänge pro Stream, es sei denn, Sie wurden durch einen Ansprechpartner beim Quest Support anderweitig angewiesen. Starten Sie beim Anpassen und Testen dieser Einstellung mit einem Wert von 24.

Wenn Sie Beschränkungen der Übertragungsparameter der geschützten Maschinen festlegen, gelten diese Einschränkungen pro Job. Wenn zwei Übertragungsjobs gleichzeitig auftreten oder sich überschneiden, wird die

doppelte Bandbreite verwendet. Wenn sich vier Übertragungsjobs im Netzwerk überschneiden, wird die vierfache Bandbreite verwendet; und so weiter.

Anpassen der nächtlichen Jobs für eine geschützte Maschine

Nächtliche Jobs können auf Core-Ebene oder für einzelne Maschinen verwaltet werden. Werden die Einstellungen für nächtliche Jobs auf der Core-Ebene festgelegt, gelten die Änderungen für alle relevanten Maschinen, die durch den betreffenden Core geschützt werden. Änderungen der nächtlichen Jobs, die auf Maschinenebene durchgeführt werden, überschreiben die auf der Core-Ebene vorgenommenen Änderungen und gelten nur für die angegebenen Maschinen.

Eine Liste aller nächtlichen Jobs jeweils mit Beschreibung und Geltungsbereich finden Sie unter Grundlegende Informationen zu nächtlichen Jobs.

Führen Sie die nachstehend beschrieben Schritte aus, um die nächtlichen Jobs für eine einzelne geschützte Maschine zu ändern.

1. In der Rapid Recovery Core Console klicken Sie unter dem Menü der Maschinen auf die IP-Adresse oder den Maschinennamen für die Maschine, für die Sie nächtliche Jobs anzeigen oder ändern möchten.

   Die Registerkarte **Zusammenfassung** für die ausgewählte Maschine wird angezeigt.
2. Klicken Sie auf das Menü **Einstellungen**.

   Die Seite **Einstellungen** wird angezeigt. Sie enthält Konfigurationseinstellungen für die ausgewählte Maschine.
3. Optional können Sie auf den Link **Nächtliche Jobs** klicken, um einen Bildlauf nach unten auf die Seite **Einstellungen** durchführen, um die Einstellungen für nächtliche Jobs anzuzeigen.
4. Unter der Überschrift „Nächtliche Jobs“ klicken Sie auf **Ändern**.

   Das Dialogfeld **Nächtliche Aufgaben** wird angezeigt.
5. Wählen Sie im Dialogfeld **Nächtliche Jobs** die Jobs, die als nächtliche Jobs ausgeführt werden sollen, oder deaktivieren Sie die Optionen, die für die betreffende Maschine nicht verwendet werden sollen.

   NOTE: Die Optionen hängen von der jeweiligen Maschine ab. Eine mit Exchange Server geschützte Maschine kann beispielsweise das Überprüfen der Prüfsumme der Exchange-Datenbanken und das Kürzen von Exchange-Protokollen enthalten.

   NOTE: Weitere Informationen zu der **Rollup**-Einstellung, einschließlich Einrichten einer benutzerdefinierten Aufbewahrungsrichtlinie, finden Sie unter Anpassen der Aufbewahrungsrichtlinieneinstellungen für eine geschützte Maschine.
6. Klicken Sie auf **OK**.

   NOTE: Die vorgenommenen Anpassungen gelten jeweils nur für die ausgewählte geschützte Maschine. Um Anpassungen für andere Maschinen durchzuführen, wiederholen Sie die aufgeführten Schritte für jede Maschine, die Sie anpassen möchten. Informationen zum Ändern der Einstellungen für nächtliche Jobs für alle durch einen Core geschützten Maschinen finden Sie unter Konfigurieren nächtlicher Jobs für den Core.

Anzeigen von Systeminformationen für eine geschützte Maschine

Die Rapid Recovery Core Console ermöglicht Ihnen einen einfachen Zugriff auf Systeminformationen über die geschützten Maschinen auf dem Core.

Beim Anzeigen von Systeminformationen für eine bestimmte geschützte Maschine enthält der Fensterbereich **Systeminformationen** allgemeine Informationen über die geschützte Maschine, einschließlich seiner Beziehung zum Core und Repository. Im Fensterbereich **Volumes** sind Informationen über die Speicher-Volumes auf der Core-Maschine aufgeführt. Der Fensterbereich **Replay Engine-Verbindungen** zeigt Volumes aller geschützten Maschinen an.

Führen Sie die folgenden Schritte aus, um detaillierte Systeminformationen für eine geschützt Maschine anzuzeigen.

1. Navigieren Sie zur Rapid Recovery Core Console und klicken Sie im Menü „Geschützte Maschinen“ im linken Navigationsbereich auf den Namen einer geschützten Maschine.

   Die Seite **Zusammenfassung** wird für die ausgewählte geschützte Maschine angezeigt.
2. Klicken Sie auf der Seite **Zusammenfassung** im unteren Bereich des Fensterbereichs **Zusammenfassung** auf **Systeminformationen**.
3. Auf der Seite **Systeminformationen** können Sie die folgenden Details zur ausgewählten geschützten Maschine anzeigen.
   - **Systeminformationen.** Dies umfasst Hostname, Betriebssystem-Version, physischen Speicher, Anzeigename, vollqualifizierter Domänenname und Typ der virtuellen Maschine (falls vorhanden).
   - **Volumes**. Dies umfasst den Namen für Volume, Geräte-ID, Dateisystem, formatierte Kapazität und genutzte Kapazität.
   - **Prozessoren**. Dies umfasst die Architektur, die Anzahl der Cores und Threads, Taktrate und Beschreibung.
   - **Netzwerkadapter**. Dies umfasst den Netzwerkadaptertyp und die Geschwindigkeit.
   - **IP-Adressen**. Dies umfasst die IP-Adresse und die Familie.

Verwalten von Maschinen

In diesem Abschnitt werden verschiedene Aufgaben beschrieben, die Sie bei der Verwaltung Ihrer geschützten Maschinen ausführen können.

- Entfernen einer Maschine
- Aufheben des Cluster-Schutzes
- Anzeigen von Lizenzinformationen für eine Maschine
- Herunterladen und Anzeigen der Protokolldatei für eine geschützte Maschine
- Konvertieren eines geschützten Cluster-Knotens in eine geschützte Maschine

Entfernen einer Maschine

Wenn Sie eine Maschine aus dem Schutz durch den Rapid Recovery Core entfernen, haben Sie zwei Wahlmöglichkeiten: Sie können die Wiederherstellungspunkte, die bisher im Core gespeichert wurden, beibehalten oder die Wiederherstellungspunkte entfernen.

Wenn Sie die Wiederherstellungspunkte beibehalten, entsteht eine „Nur Wiederherstellungspunkte“-Maschine. Wiederherstellen- und Mount-Vorgänge sind weiterhin von den erfassten Wiederherstellungspunkten von der Maschine aus zugängig, wenn diese unter Schutz gestellt wurde. Es funktionieren jedoch keine Sicherungen mehr für die geschützte Maschine.

Wenn Sie die Wiederherstellungspunkte entfernen, werden alle Snapshot-Daten für die vormals geschützte Maschine aus dem Rapid Recovery Core gelöscht.

Führen Sie die folgenden Schritte aus, um den Schutz einer Maschine in der Rapid Recovery-Umgebung aufzuheben.

1. Klicken Sie in der Rapid Recovery Core Console im linken Navigationsbereich unter „Geschützte Maschinen“ auf die Maschine, die Sie entfernen möchten.
2. Klicken Sie auf der Seite **Zusammenfassung** für die entsprechende Maschine auf **Maschine entfernen**.
3. Wenn Sie auch alle Wiederherstellungspunkte für diese Maschine aus dem Repository löschen möchten, wählen Sie im Dialogfeld **Mit Wiederherstellungspunkten entfernen** aus.
4. Klicken Sie zur Bestätigung Ihrer Auswahl zum Entfernen der Maschine auf **Ja**.

   CAUTION: Wenn die Wiederherstellungspunkte gelöscht werden, können die Daten der betreffenden Maschine nicht mehr wiederhergestellt werden.

   Rapid Recovery entfernt die Maschine aus dem Schutz und bricht alle aktiven Aufgaben für diese Maschine ab.

Aufheben des Cluster-Schutzes

Führen Sie die folgenden Schritte aus, um den Schutz eines Cluster aufzuheben.

1. Klicken Sie in der Rapid Recovery Core Console unter „Geschützte Maschinen“ auf den Cluster, den Sie entfernen möchten.
2. Klicken Sie auf der **Übersichtsseite** für den Cluster auf **Cluster entfernen**.
3. Optional können Sie im Dialogfeld **Mit Wiederherstellungspunkten entfernen** auswählen, um alle aktuell gespeicherten Wiederherstellungspunkte für diesen Cluster aus dem Repository zu entfernen.

   CAUTION: Wenn die Wiederherstellungspunkte gelöscht werden, können die Daten der betreffenden Cluster nicht mehr wiederhergestellt werden.
4. Klicken Sie im Dialogfeld **Ja**, um den Vorgang zu bestätigen.

Aufheben des Schutzes von Cluster-Knoten

Führen Sie die folgenden Schritte aus, um den Schutz eines Cluster aufzuheben.

Informationen zum Entfernen eines Knotens aus dem Cluster finden Sie unter Konvertieren eines geschützten Cluster-Knotens in eine geschützte Maschine.

1. Klicken Sie in der Rapid Recovery Core Console unter „Geschützte Maschinen“ auf den Cluster-Knoten, den Sie entfernen möchten.
2. Klicken Sie auf der **Übersichtsseite** für den Cluster auf **Maschine entfernen**.

   Das Dialogfeld „Remove Node“ (Knoten entfernen) wird angezeigt.
3. Optional können Sie im Dialogfeld **Mit Wiederherstellungspunkten entfernen** auswählen, um alle aktuell gespeicherten Wiederherstellungspunkte für diesen Cluster aus dem Repository zu entfernen.

   CAUTION: Wenn die Wiederherstellungspunkte gelöscht werden, können die Daten der Clusterknoten nicht mehr wiederhergestellt werden.
4. Klicken Sie im Dialogfeld **Ja**, um den Vorgang zu bestätigen.

Aufheben des Schutzes aller Knoten in einem Cluster

Führen Sie die folgenden Schritte aus, um den Schutz aller Knoten in einem Cluster aufzuheben.

CAUTION: Wenn Sie alle Cluster-Knoten entfernen, wird auch der Cluster entfernt.

1. Klicken Sie in der Rapid Recovery Core Console unter „Geschützte Maschinen“ auf den Cluster, dessen Knoten Sie entfernen möchten.
2. Klicken Sie auf der **Übersichtsseite** für den Cluster auf **Geschützte Knoten**.
3. Wählen Sie auf der Seite **Geschützte Knoten** alle Knoten aus.
4. Klicken Sie auf das Dropdownmenü **Maschinen entfernen** und wählen Sie dann eine der in der folgenden Tabelle beschriebenen Optionen aus.

Tabelle 83. Optionen für das Entfernen von Knoten

Option	Description
Entfernen und Wiederherstellungspunkte beibehalten	Um alle derzeit gespeicherten Wiederherstellungspunkte für diesen Cluster beizubehalten.
Wiederherstellungspunkte entfernen	Um alle derzeit gespeicherten Wiederherstellungspunkte für diesen Cluster aus dem Repository zu entfernen. **CAUTION: Wenn die Wiederherstellungspunkte gelöscht werden, können die Daten der betreffenden Cluster nicht mehr wiederhergestellt werden.**

5. Klicken Sie im Dialogfeld „Knoten löschen“ auf **Ja**, um den Löschvorgang zu bestätigen.

Anzeigen von Lizenzinformationen für eine Maschine

Sie können aktuelle Lizenzstatusinformationen für die auf einer geschützten Maschine installierte Rapid Recovery-Agentensoftware anzeigen.

1. Klicken Sie in der Rapid Recovery Core Console unter „Geschützte Maschinen“ auf die Maschine, die Sie ändern möchten.

   Die Seite **Summary** (Zusammenfassung) für die ausgewählte Maschine wird angezeigt.
2. Klicken Sie auf das Menü **Einstellungen**.

   Die Seite **Einstellungen** wird angezeigt. Sie enthält Konfigurationseinstellungen für die ausgewählte Maschine.
3. Klicken Sie auf den Link **Lizenzierung**, um einen Bildlauf nach unten auf der Seite „Einstellungen“ durchzuführen, um maschinenspezifische Lizenzierungseinstellungen anzuzeigen.

   Die Statusanzeige wird mit den folgenden Details zur Produktlizenzierung angezeigt:

Herunterladen und Anzeigen der Protokolldatei für eine geschützte Maschine

Falls bei einer geschützten Maschine Fehler oder Probleme auftreten, können Sie die Maschinenprotokolle herunterladen, um sie anzuzeigen oder an den Vertreter des Quest Support zu senden.

1. Klicken Sie im linken Navigationsbereich der Core Console unter dem Menü „Geschützte Maschinen“ auf den Pfeil, um das kontextabhängige Menü für die entsprechende, geschützte Maschine zu erweitern.

Führen Sie einen Bildlauf nach unten zu **Mehr** durch, erweitern Sie dieses Menü und wählen Sie dann  **Agenten-Protokoll**.

Daraufhin wird die Seite **Core-Protokoll herunterladen** angezeigt.

2. Klicken Sie auf der Seite **Agenten-Protokoll herunterladen** auf **Klicken Sie hier, um den Download zu starten**.
3. Führen Sie eine der folgenden Möglichkeiten im Dialogfeld **AgentAppRecovery.log öffnen** aus:
   - Um die Protokolldatei zu öffnen, wählen Sie die Option **Öffnen mit** und dann eine Anwendung (wie Notepad) für die Anzeige der textbasierten Protokolldatei und klicken dann auf **OK**.

     Die Datei **AgentAppRecovery.log** wird in der ausgewählten Anwendung geöffnet.
   - Zum Speichern der Datei lokal, wählen Sie **Datei speichern** und klicken dann auf **OK**.

     Die Datei **AgentAppRecovery.log** wird im Ordner „Downloads“ gespeichert. Sie kann über einen beliebigen Texteditor geöffnet werden.

See also: Herunterladen und Anzeigen der Core-Protokolldatei
See also: Herunterladen und Anzeigen der Protokolldatei für eine geschützte Maschine

Konvertieren eines geschützten Cluster-Knotens in eine geschützte Maschine

In Rapid Recovery können Sie einen geschützten Cluster-Knoten in eine geschützte Maschine konvertieren, sodass diese zwar weiterhin vom Core verwaltet wird, jedoch nicht mehr Bestandteil des Clusters ist. Dies ist beispielsweise nützlich, wenn Sie einen Cluster-Knoten aus dem Cluster entfernen müssen, der Knoten jedoch weiterhin geschützt sein soll.

1. Navigieren Sie in der Rapid Recovery Core Console zu dem Cluster mit der Maschine, die konvertiert werden soll, und klicken Sie auf **Geschützte Knoten**.
2. Wählen Sie auf der Seite **Geschützte Knoten** den gewünschten Knoten aus und klicken Sie im Dropdown-Menü „Aktionen“ auf **In Agent konvertieren**.
3. Um die Maschine wieder zum Cluster hinzuzufügen, wählen Sie die Maschine aus. Wählen Sie dann auf der Seite „Zusammenfassung“ im Menü „Aktionen“ die Option **In Cluster-Knoten konvertieren** aus und klicken Sie dann auf **Ja**, um die Aktion zu bestätigen.

Grundlegende Informationen zu benutzerdefinierten Gruppen

DieRapid Recovery Core Console enthält im linken Navigationsbereich ein Menü „Geschützte Maschinen“. Dazu gehören auch alle Maschinen oder Server-Cluster, die zum Schutz auf Ihrem Rapid Recovery Core hinzugefügt wurden. Darunter können noch weitere Menüs angezeigt werden, je nachdem, ob solche Objekte in Ihrem Core enthalten sind. Auf die gleiche Weise können Sie eine benutzerdefinierte Gruppe erstellen. Diese wird als letztes Menü im linken Navigationsbereich angezeigt.

Der wichtigste Vorteil einer benutzerdefinierten Gruppe ist die Möglichkeit, Core-Objekte in einem logischen Container zu gruppieren. Dies kann Ihnen dabei helfen, Core-Objekte für einen bestimmten Zweck (z. B. nach Organisation, Kostenstelle, Abteilung, geografischen Region, usw.) anzuordnen und zu verwalten.

Durch das Erstellen einer Gruppe wird immer ein Gruppenmitglied (z. B. eine geschützte Maschine oder ein Server-Cluster, eine replizierte Maschine oder eine Maschine mit nur Wiederherstellungspunkten) zu der neuen benutzerdefinierten Gruppe hinzugefügt. Welches Objekt hinzugefügt wird, richtet sich nach Ihrem Ursprungspunkt beim Erstellen der Gruppe. Die weiteren Gruppenmitglieder werden im Idealfall anschließend

hinzugefügt. Danach können Sie Gruppenaktionen durchführen, die für alle Mitglieder der benutzerdefinierten Gruppe gelten, (siehe Beschreibung in Durchführen von Gruppenaktionen).

Benutzerdefinierte Gruppen können geschützte Maschinen, Server-Cluster, replizierte Maschinen und Maschinen mit nur Wiederherstellungspunkten einschließen. Server-Cluster verhalten sich genauso wie geschützte Maschinen, außer dass sich ein Server-Cluster mit den zugehörigen Knoten wie ein einzelnes Objekt verhält. Wenn Sie versuchen, einen Knoten aus einem Server-Cluster zu einer Gruppe hinzuzufügen, wird der gesamte Cluster hinzugefügt.

Eine benutzerdefinierte Gruppe kann ähnliche oder unähnliche Mitglieder enthalten. Bei Gruppen ähnlicher Mitglieder gelten alle Gruppenaktionen für alle Mitglieder der Gruppe. Wenn Sie beispielsweise eine Snapshot-Erstellung für eine benutzerdefinierte Gruppe von geschützte Maschinen erzwingen, werden alle Maschinen gesichert. Bei Gruppen mit unterschiedlichen Mitgliedern (z. B. geschützte Maschinen und replizierte Maschinen) gilt eine Gruppenaktion wie beispielsweise das Erzwingen einer Replikation nur für replizierte Maschinen.

Sie können beliebig viele Gruppen erstellen. Eine einzelne geschützte Maschine bzw. eine replizierte Maschine kann in mehr als einer Gruppe enthalten sein. Auf diese Weise können Sie Maschinen des Core beliebig gruppieren und Aktionen für die jeweilige Gruppe durchführen.

Alle benutzerdefinierten Gruppen werden im linken Navigationsbereich mit der jeweils festgelegten Bezeichnung angezeigt. Gruppen mit standardmäßig geschützten Maschinen werden zuerst in der benutzerdefinierten Gruppe angezeigt; replizierte Maschinen erscheinen unter geschützten Maschinen, wo anwendbar. Wenn Sie Maschinen mit nur Wiederherstellungspunkten haben, so werden diese unter den replizierten Maschinen aufgeführt.

Im linken Navigationsbereich werden die Objekte, die auf dem Core geschützt sind, in jeweils ihrem eigenen Menü angezeigt. Von diesen Menüs werden benutzerdefinierte Gruppen zuletzt angezeigt.

Wenn Sie eine Maschine in eine Gruppe einfügen, wird sie nicht an der ursprünglichen Stelle gelöscht. Wenn beispielsweise drei geschützte Maschinen namens Agent1, Agent2 und Agent3 vorhanden sind, und Sie Agent1 zu CustomGroup1 hinzufügen, wird Agent1 an beiden Stellen angezeigt.

See also: Erstellen von benutzerdefinierten Gruppen
See also: Ändern der Namen von benutzerdefinierten Gruppen
See also: Entfernen von benutzerdefinierten Gruppen
See also: Durchführen von Gruppenaktionen
See also: Anzeigen aller Maschinen in einer benutzerdefinierten Gruppe auf einer Seite

Erstellen von benutzerdefinierten Gruppen

Wenn Sie den Cursor über den Namen einer Maschine im Menü „Geschützte Maschinen“ oder „Replizierte Maschinen“ bewegen, wird ein Pfeil angezeigt, über den ein Dropdown-Menü geöffnet wird. In diesem Menü können Sie eine benutzerdefinierte Bezeichnung erstellen.

Gehen Sie folgendermaßen vor, um eine benutzerdefinierte Gruppe zu erstellen.

1. Navigieren Sie zur Rapid Recovery Core Console.
2. Gehen Sie im Menü "Geschützte Computer", "Replizierte Computer" oder "Nur Wiederherstellungspunkte" wie folgt vor:
    a. Platzieren Sie den Cursor über einem Computer im Menü.
    b. Klicken Sie auf das Dropdown-Menü für die betreffende Maschine.
    c. Wählen Sie im Menü **Beschriften als** aus, und klicken Sie dann auf **Neue Beschriftung**.

    Das Dialogfeld **Etikett erstellen** wird angezeigt.
3. Geben Sie im Feld **Name** ein geeignetes Etikett für Ihre benutzerdefinierte Gruppe ein.

    Verwenden Sie einen aussagekräftigen Namen, der den Zweck der Gruppe beschreibt. Beispiel: Um geschützte Maschinen, replizierte Maschinen und Maschinen, die nur Wiederherstellungspunkte enthalten, nach Abteilung zu gruppieren, geben Sie `Buchhaltungsabteilung` ein. Sie können eine Gruppe später umbenennen.

NOTE: Die Bezeichnung darf höchstens 50 Zeichen umfassen. Sie können zwischen Wörtern einzelne Leerzeichen eingeben. Sie müssen eine Bezeichnung für die benutzerdefinierte Gruppe eingeben.

4. Wenn Sie mit dem Etikettennamen zufrieden sind, klicken Sie auf **OK**.

   Das Dialogfeld wird geschlossen und die benutzerdefinierte Gruppe wird als das letzte Element im linken Navigationsbereich angezeigt.
5. Optional können Sie andere geschützte Computer, replizierte Computer oder Computer-nur Wiederherstellungspunkte zu dieser Gruppe hinzufügen. Wechseln Sie zum entsprechenden Menü, klicken Sie auf das Dropdown-Menü, wählen Sie **Beschriften als** aus und klicken Sie auf den Namen der benutzerdefinierten Gruppe.

   Danach können Sie Gruppenaktionen für diese Gruppe durchführen. Weitere Informationen hierzu finden Sie unter Durchführen von Gruppenaktionen.

Ändern der Namen von benutzerdefinierten Gruppen

Wenn Sie den Namen einer benutzerdefinierten Gruppe ändern, wird nur die Bezeichnung geändert. Die Maschinennamen bleiben unverändert.

Gehen Sie folgendermaßen vor, um den Namen einer benutzerdefinierten Gruppe zu ändern.

1. Navigieren Sie zur Rapid Recovery Core Console.
2. Wählen Sie im Menü „Geschützte Maschinen“ die benutzerdefinierte Gruppe aus, die Sie ändern möchten.
3. Wählen Sie im Dropdown-Menü der betreffenden Gruppe **Bearbeiten** aus.

   Das Dialogfeld **Etikett bearbeiten** wird angezeigt, in dem der Name der benutzerdefinierten Gruppe bearbeitet werden kann.
4. Aktualisieren Sie den Text im Feld **Name** oder löschen Sie das vorhandene Etikett und geben Sie eine neue Bezeichnung für Ihre benutzerdefinierte Gruppe an.

   Verwenden Sie einen aussagekräftigen Namen, der den Zweck der Gruppe beschreibt. Beispiel: Um geschützte Maschinen, replizierte Maschinen und Nur Wiederherstellungspunkt-Maschinen nach geografischer Region zu gruppieren, geben Sie `Tokyo` ein. Sie können eine Gruppe später umbenennen.

   NOTE: Die Bezeichnung darf höchstens 50 Zeichen umfassen. Sie können zwischen Wörtern einzelne Leerzeichen eingeben. Sie müssen eine Bezeichnung für die benutzerdefinierte Gruppe eingeben.
5. Wenn Sie mit dem Etikettennamen zufrieden sind, klicken Sie auf **OK**.

   Das Dialogfeld wird geschlossen und die geänderte benutzerdefinierte Gruppe wird als das letzte Element im linken Navigationsbereich angezeigt.
6. Optional können Sie andere geschützte Computer, replizierte Computer oder Computer-nur Wiederherstellungspunkte zu dieser Gruppe hinzufügen. Wechseln Sie zum entsprechenden Menü, klicken Sie auf das Dropdown-Menü, wählen Sie **Beschriften als** aus und klicken Sie auf den Namen der benutzerdefinierten Gruppe.

Entfernen von benutzerdefinierten Gruppen

Beim Entfernen einer benutzerdefinierten Gruppe wird die betreffende Gruppe aus dem Menü „Geschützte Maschinen“ gelöscht. Die in der Gruppe enthaltenen Maschinen werden nicht gelöscht. Sie befinden sich weiterhin im entsprechenden Standardmenü.

Gehen Sie folgendermaßen vor, um eine benutzerdefinierte Gruppe zu entfernen.

1. Navigieren Sie zur Rapid Recovery Core Console.
2. Wählen Sie im Menü „Geschützte Maschinen“ die benutzerdefinierte Gruppe aus, die Sie entfernen möchten.
3. Wählen Sie im Dropdown-Menü der betreffenden Gruppe **Beschriftung entfernen** aus.

   Daraufhin wird eine Meldung mit der Aufforderung angezeigt, das Entfernen der Gruppe zu bestätigen.
4. Bestätigen Sie das Entfernen der benutzerdefinierten Gruppe.

   Das Dialogfeld wird geschlossen und die benutzerdefinierte Gruppe wird nicht mehr im Navigationsbereich angezeigt.

Durchführen von Gruppenaktionen

Sie können für jede Gruppe, die im linken Navigationsbereich der Rapid Recovery Core Console angezeigt wird, Gruppenaktionen durchführen. Wenn die Gruppe unterschiedliche Mitglieder enthält (z. B. replizierte Maschinen und Maschinen, die nur Wiederherstellungspunkte enthalten), werden die ausgewählten Aktionen nur für die relevanten Gruppenmitglieder ausgeführt.

Gehen Sie folgendermaßen vor, um Gruppenaktionen für eine benutzerdefinierte Gruppe durchzuführen.

1. Navigieren Sie zur Rapid Recovery Core Console.
2. Wählen Sie im Menü „Geschützte Maschinen“ die benutzerdefinierte Gruppe aus, für die Sie eine Gruppenaktion durchführen möchten.
3. Klicken Sie auf das Dropdown-Menü der betreffenden Gruppe, und wählen Sie dann eine der folgenden Aktionen aus:
    - Um einen inkrementellen Snapshot oder ein Basisimage für einen geschützten Agenten zu erzwingen, klicken Sie auf **Snapshot erzwingen** bzw. auf **Basisimage erzwingen**.
    - Um den Schutz für alle geschützten Maschinen in der Gruppe vorübergehend zu deaktivieren, klicken Sie auf **Schutz vorübergehend deaktivieren**. Geben Sie anschließend die Parameter für die Fortsetzung an.
    - Um den Schutz für alle geschützten Maschinen in der Gruppe, für die der Schutz vorübergehend deaktiviert wurde, wieder zu aktivieren, klicken Sie auf **Schutz wieder aktivieren** und bestätigen Sie, dass der Schutz wieder aktiviert werden soll.
    - Zum Aktualisieren der Informationen für alle Objekte in der Gruppe, klicken Sie auf **Metadaten aktualisieren**.
    - Um die Replikation für alle replizierten Maschinen in dieser Gruppe vorübergehend zu deaktivieren, klicken Sie unter „Replikation“ auf **Vorübergehend deaktivieren**.
    - Um die Replikation für alle geschützten Maschinen in der Gruppe, für die die Replikation vorübergehend deaktiviert wurde, wieder aufzunehmen, klicken Sie unter „Replikation“ auf **Wieder aufnehmen**.
    - Um die Replikation für alle replizierten Maschinen in dieser Gruppe zu erzwingen, klicken Sie unter „Replikation“ auf **Erzwingen**.
    - Um die Replikation für alle replizierten Maschinen in dieser Gruppe zu entfernen, klicken Sie unter „Replikation“ auf **Entfernen**.
    - Um Maschinen, die nur Wiederherstellungspunkte enthalten, von diesem Core zu entfernen und die Wiederherstellungspunkte zu verwerfen, klicken Sie unter „Nur Wiederherstellungspunkte“ auf **Wiederherstellungspunkte entfernen**.
    - Wählen Sie **Bearbeiten** aus, um die Bezeichnung für eine benutzerdefinierte Gruppe zu ändern (nur für benutzerdefinierte Gruppen möglich).
    - Um die benutzerdefinierte Gruppe aus dem Navigationsmenü zu entfernen (nur für benutzerdefinierte Gruppen möglich), wählen Sie **Beschriftung entfernen** aus.

See also: Erzwingen eines Snapshots
See also: Erzwingen einer Replikation
See also: Anhalten und Fortsetzen der Replikation
See also: Vorübergehendes Deaktivieren und erneutes Aktivieren der Schutzfunktion
See also: Eingehende Replikation vom Ziel-Core entfernen
See also: Ändern der Namen von benutzerdefinierten Gruppen
See also: Entfernen von benutzerdefinierten Gruppen

Anzeigen aller Maschinen in einer benutzerdefinierten Gruppe auf einer Seite

Wenn Sie auf den Namen einer benutzerdefinierten Gruppe klicken, wird die Seite „Maschinen“ angezeigt, auf der alle Maschinen in dieser benutzerdefinierten Gruppe aufgelistet werden. Dort können Sie einige Funktionen im Menü „Aktionen“ für alle Maschinen durchführen. Sie können Funktionen auch einzeln ausführen, indem Sie Befehle für die jeweilige Maschine auswählen.

Snapshots und Wiederherstellungspunkte

Dieser Abschnitt beschreibt die Verwendung und Verwaltung der Snapshots und Wiederherstellungspunkte, die von Rapid Recovery erstellt werden. Er enthält Informationen zum Bereitstellen, Anzeigen und Erzwingen sowie zum Migrieren und Löschen von Wiederherstellungspunkten.

Verwalten von Snapshots und Wiederherstellungspunkten

Bei einem Wiederherstellungspunkt handelt es sich um eine Gruppe von Snapshots der einzelnen Datenträger-Volumes, die im Repository gespeichert sind. Snapshots erfassen und speichern den Zustand eines Datenträger-Volumes zu einem bestimmten Zeitpunkt, während die Anwendungen, die die Daten generieren, genutzt werden. In Rapid Recovery können Sie einen Snapshot erzwingen, Snapshots vorübergehend deaktivieren, Listen mit aktuellen Wiederherstellungspunkten im Repository anzeigen und diese bei Bedarf löschen. Wiederherstellungspunkte werden für die Wiederherstellung geschützter Maschinen oder für die Bereitstellung in einem lokalen Dateisystem verwendet.

Die von Rapid Recovery erfassten Snapshots werden auf Blockebene erstellt und sind anwendungskonsistent. Das heißt, dass alle offenen Transaktionen und laufenden Transaktionsprotokolle abgeschlossen und die Cache-Speicher auf der Festplatte abgelegt werden, bevor der Snapshot erstellt wird.

Rapid Recovery verwendet einen hardwarenahen Volume-Filtertreiber, der den bereitgestellten Volumes zugeordnet wird und alle Änderungen auf Blockebene für den nächsten bevorstehenden Snapshot protokolliert. Mithilfe der Microsoft Volumeschattenkopie-Dienste (VSS) werden anwendungs- und absturzkonsistente Snapshots ermöglicht.

Anzeigen der Seite „Wiederherstellungspunkte“ einer geschützten Maschine

Führen Sie die folgenden Schritte aus, um die vollständige Liste der Wiederherstellungspunkte für eine geschützte Maschine anzuzeigen.

NOTE: Wenn Sie Daten eines DAG- oder CCR-Server-Clusters schützen, werden die zugehörigen Wiederherstellungspunkte nicht auf Cluster-Ebene angezeigt. Sie sind nur auf Knoten- oder Maschinenebene sichtbar.

1. Navigieren Sie in der Rapid Recovery Core Console zu der geschützten Maschine, für die Sie Wiederherstellungspunkte anzeigen möchten.
2. Klicken Sie im Menü am oberen Rand der Seite auf **Wiederherstellungspunkte**.

Die Seite **Wiederherstellungspunkte** wird angezeigt. Sie enthält einen Fensterbereich “Zusammenfassung der Wiederherstellungspunkte und einen Fensterbereich „Wiederherstellungspunkte“.

Sie können die in der folgenden Tabelle beschriebenen Übersichtsinformationen für die Wiederherstellungspunkte der Maschine anzeigen.

Tabelle 84. Übersichtsinformationen für Wiederherstellungspunkte

Info	Description
Wiederherstellungspunkte, gesamt	Führt die Gesamtzahl der Wiederherstellungspunkte an, die im Repository für diese Maschine gespeichert werden.
Geschützte Daten, gesamt	Zeigt die Menge des im Repository für diese Wiederherstellungspunkte verwendeten Speicherplatzes an.
Repository	Führt den Namen des Repository auf, in dem diese Wiederherstellungspunkte gespeichert sind.
Repositorystatus	Zeigt eine grafische Ansicht der Menge an Speicherplatz an, die von den Wiederherstellungspunkten verbraucht wurde. Zeigt den Prozentsatz des belegten Repositorys, die Menge an Speicherplatz, und den Gesamtspeicherplatz des Repositorys an. Klicken Sie auf das Diagramm, um die verbleibende Menge an Speicherplatz anzuzeigen.

Sie können die in der folgenden Tabelle beschriebenen Informationen für die Wiederherstellungspunkte der Maschine anzeigen.

Tabelle 85. Informationen für Wiederherstellungspunkte

Info	Description
Symbol	Grafische Darstellung eines Wiederherstellungspunkts oder, wenn erweitert, eines Volumes innerhalb des Wiederherstellungspunkts . Wiederherstellungspunkte weisen ein nach rechts zeigenden Pfeil auf, was darauf hinweist, dass die Details erweitert werden können.
Verschlüsselt	Zeigt an, ob der Wiederherstellungspunkt verschlüsselt ist.
Status	Zeigt den aktuellen Status des Wiederherstellungspunkts an.
Inhalt	Zeigt eine Liste der im Wiederherstellungspunkt enthaltenen Volumes an. • Klicken Sie auf (Informationen), um die Speicherplatznutzung und das Dateisystem anzuzeigen. • Für Exchange Server klicken Sie auf , um Informationen über den Server anzuzeigen.
Typ	Gibt an, ob der Wiederherstellungspunkt ein Basisimage oder ein inkrementeller (differenzieller) Snapshot ist.
Erstellungsdatum	Zeigt das Datum an, an dem der Wiederherstellungspunkt erstellt wurde.
Größe	Zeigt den Speicherplatz an, den der Wiederherstellungspunkt im Repository belegt.

Info	Description
	Über das Dropdown-Menü „Mehr“ können Sie bestimmte Aufgaben für den ausgewählten Wiederherstellungspunkt ausführen.

3. Sie können auf Wunsch einen Wiederherstellungspunkt erweitern, um die geschützten Volumes anzuzeigen.

Zugehörige Verweise

See also: Anzeigen von Wiederherstellungspunkten für eine Maschine

Grundlegende Informationen zu Statusanzeigen für Wiederherstellungspunkte

Wenn ein Wiederherstellungspunkt für einen geschützten SQL- oder Exchange-Server erstellt wurde, zeigt die Anwendung eine entsprechende Farb-Statusanzeige im Raster der Wiederherstellungspunkte an. Dieses Raster wird im Fensterbereich **Wiederherstellungspunkte** beim Anzeigen von Wiederherstellungspunkten für eine bestimmte Maschine aufgerufen. Die angezeigte Farbe basiert auf den Überprüfungseinstellungen für die geschützte Maschine und dem Erfolg bzw. Fehlschlagen dieser Überprüfungen, wie in den folgenden Tabellen beschrieben.

NOTE: Weitere Informationen zum Anzeigen von Wiederherstellungspunkten finden Sie unter Anzeigen der Seite „Wiederherstellungspunkte“ einer geschützten Maschine.

Statusfarbe von Wiederherstellungspunkten für Exchange-Datenbanken

Die folgende Tabelle enthält eine Liste der Statusanzeigen für Exchange-Datenbanken.

Tabelle 86. Statusanzeigen für Exchange-Datenbanken

Statusfarbe	Description
Weiß	Zeigt an, dass eine Exchange-Datenbank innerhalb Wiederherstellungspunkt, Volume oder Volume Group nicht erkannt wird.
Gelb	Zeigt an, dass Bereitstellbarkeitsprüfungen für die Exchange-Datenbank noch nicht durchgeführt wurden.
Rot	Zeigt an, dass die Bereitstellbarkeitsprüfungen oder die Prüfsummenprüfungen für mindestens eine Datenbank fehlgeschlagen sind.
Grün	Zeigt an, dass der Wiederherstellungspunkt eine oder mehrere Datenbanken enthält, und dass Bereitstellbarkeitsprüfungen aktiviert sind, und dass die Bereitstellbarkeitsprüfung bzw. die Prüfsummen-Überprüfung erfolgreich war.

Statusfarbe von Wiederherstellungspunkten für SQL-Datenbanken

Die folgende Tabelle enthält eine Liste der Statusanzeigen für SQL-Datenbanken.

Tabelle 87. Statusanzeigen für SQL-Datenbanken

Statusfarbe	Description
Weiß	Zeigt an, dass eine SQL-Datenbank innerhalb Wiederherstellungspunkt, Volume oder Volume Group nicht erkannt wird.

Statusfarbe	Description
Gelb	SQL-Datenbank war offline, was darauf hinweist, dass Anfügbarkeitsprüfungen nicht möglich waren und nicht durchgeführt wurden.
Rot	Zeigt an, dass die Anfügbarkeitsprüfung fehlgeschlagen ist, oder die SQL-Datenbank offline ist.
Grün	Zeigt an, dass die Anfügbarkeitsprüfung erfolgreich war.

NOTE: Wiederherstellungspunkte, denen keine Exchange- oder SQL-Datenbank zugeordnet ist, werden mit einer weißen Statusanzeige angezeigt. In Situationen, in denen es für den Wiederherstellungspunkt sowohl eine Exchange- als auch eine SQL-Datenbank gibt, wird die schwerwiegendste Statusanzeige für den Wiederherstellungspunkt angezeigt.

Bereitstellen eines Wiederherstellungspunkts

In Rapid Recovery können Sie einen Wiederherstellungspunkt für eine Windows-Maschine bereitstellen, um über ein lokales Dateisystem auf gespeicherte Daten zuzugreifen.

NOTE: Informationen zum Bereitstellen eines Linux-Wiederherstellungspunkts mit dem Dienstprogramm `local_mount` finden Sie unter Bereitstellen eines Wiederherstellungspunkt-Volumes für eine Linux-Maschine.

NOTE: Beim Bereitstellen von Wiederherstellungspunkten aus Daten, die aus einer Maschine wiederhergestellt wurden, für die die Deduplizierung von Daten aktiviert ist, müssen Sie die Deduplizierung auch im Core-Server aktivieren.

1. Navigieren Sie in der Rapid Recovery Core Console zu der Maschine, die in einem lokalen Dateisystem bereitgestellt werden soll.

   Die Seite **Zusammenfassung** wird für die ausgewählte geschützte Maschine angezeigt.

2. Klicken Sie auf das Menü **Wiederherstellungspunkte**.

   Die Seite **Wiederherstellungspunkte** wird für die ausgewählte Maschine angezeigt.

3. Optional klicken Sie im Fensterbereich **Wiederherstellungspunkte** in der Liste der Wiederherstellungspunkte auf das Symbol der Nach-Rechts-Taste , um die Wiederherstellungspunktdetails mit den im Wiederherstellungspunkt eingeschlossenen Volumes anzuzeigen.

4. Klicken Sie in der Zeile für den Wiederherstellungspunkt, den Sie bereitstellen möchten, auf und wählen Sie aus dem Drop-down-Menü **Bereitstellen** aus.

   Der **Bereitstellungsassistent** mit der Seite **Volumes** wird angezeigt.

5. Wählen Sie auf der Seite **Volumes** die Volumes des Wiederherstellungspunkts aus, die Sie bereitstellen möchten, und klicken Sie dann auf **Weiter**.

   Die Seite **Bereitstellungsoptionen** des Bereitstellungsassistenten wird angezeigt.

6. Bearbeiten Sie auf der Seite **Bereitstellen** die Einstellungen für die Bereitstellung eines Wiederherstellungspunkts, wie in der folgenden Tabelle beschrieben.

Tabelle 88. Einstellungen für Bereitstellungsoptionen

Option	Description
Lokaler Ordner	Geben Sie den Pfad an, der für den Zugriff auf den bereitgestellten Wiederherstellungspunkt verwendet wird. Wählen Sie beispielsweise `C:\ProgramData\AppRecovery\MountPoints\MountPoint1`.
Bereitstellungstyp	Geben Sie an, wie der Datenzugriff für den bereitgestellten Wiederherstellungspunkt erfolgen soll: • Nur-Lesen • Schreibgeschützt mit vorherigen Schreibvorgängen • Beschreibbar
Windows-Freigabe für diese Bereitstellung erstellen	Aktivieren Sie optional dieses Kontrollkästchen, um festzulegen, ob der bereitgestellte Wiederherstellungspunkt freigegeben wird, und legen Sie dann Zugriffsrechte dafür fest, einschließlich Freigabename und Zugriffsgruppen.

7. Klicken Sie auf **Fertig stellen**, um den Wiederherstellungspunkt bereitzustellen.

   NOTE: Wenn Sie Verzeichnisse oder Dateien eines bereitgestellten Wiederherstellungspunkts auf eine andere Windows-Maschine kopieren möchten, können Sie sie in Windows-Explorer mit den Standardberechtigungen oder den ursprünglichen Dateizugriffsberechtigungen kopieren. Entsprechende Details finden Sie in den Abschnitten Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer bis Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer und Beibehalten der Berechtigungen.

8. Während die Aufgabe verarbeitet wird, können Sie optional den Fortschritt im Drop-Drop-Down-Menü **Aktive Aufgaben** der Core Console sowie ausführliche Informationen auf der Seite **Ereignisse** anzeigen. Weitere Informationen zur Überwachung von Rapid Recovery Ereignissen finden Sie unter Anzeigen von Ereignissen mithilfe von Aufgaben, Warnungen und Journalseiten.

Aufheben der Bereitstellung von Wiederherstellungspunkten

Führen Sie die folgenden Schritte aus, um die Bereitstellung von Wiederherstellungspunkten aufzuheben, die im Core bereitgestellt wurden.

NOTE: Das Aufheben der Bereitstellung eines remote bereitgestellten Wiederherstellungspunkts wird auch Trennen genannt.

1. Klicken Sie in Rapid Recovery Core Console auf der Symbolleiste auf (Mehr) und wählen Sie dann **Bereitstellungen**.

   Die Seite **Bereitstellungen** wird angezeigt. Sie enthält einen Bereich für lokale Bereitstellungen (im Core bereitgestellte Wiederherstellungspunkte) und einen Bereich für Remote-Bereitstellungen (mit dem Local Mount Utility bereitgestellte Wiederherstellungspunkte). In der Liste des jeweiligen Fensterbereichs werden die jeweils bereitgestellten Wiederherstellungspunkte angezeigt.

2. Um die Bereitstellung lokaler Bereitstellungen im Fensterbereich **Lokale Bereitstellungen** aufzuheben, gehen Sie wie folgt vor:

a. Wählen Sie dir lokalen Bereitstellungspunkt oder Punkte, deren Bereitstellung Sie aufheben möchten.

- Um die Bereitstellung aller Wiederherstellungspunkte aufzuheben, klicken Sie auf das Kontrollkästchen in der Titelleiste der lokalen Bereitstellungstabelle zum Auswählen aller Bereitstellungspunkte.
- Um die Bereitstellung eines oder mehrerer Wiederherstellungspunkte aufzuheben, klicken Sie auf das Kontrollkästchen in der ersten Spalte jeder Zeile, die den Bereitstellungspunkt repräsentiert, den Sie trennen möchten.

b. Klicken Sie auf **Bereitstellung aufheben**.

Ein Bestätigungsdialogfeld wird angezeigt.

c. Klicken Sie hier, um zu bestätigen, dass Sie die Bereitstellung der ausgewählten Wiederherstellungspunkte aufheben möchten.

Die Bereitstellung der lokalen Wiederherstellungspunkte wird aufgehoben.

NOTE: Wenn Popup-Warnungen aktiviert sind, wird möglicherweise eine Warnung angezeigt, dass die Bereitstellung der entsprechenden Bereitstellungspunkte aufgehoben wird.

3. Um remote bereitgestellte Wiederherstellungspunkte im Fensterbereich **Remote-Bereitstellungen** zu trennen, gehen Sie wie folgt vor:
   a. Wählen Sie den Remote Bereitstellungspunkt oder die Wiederherstellungspunkten, die Sie trennen möchten.
   - Um alle Wiederherstellungspunkte zu trennen, klicken Sie auf das Kontrollkästchen in der Titelleiste der Fern-Bereitstellungstabelle zum Auswählen aller Bereitstellungspunkte.
   - Um einen oder mehrere Wiederherstellungspunkte zu trennen, klicken Sie auf das Kontrollkästchen in der ersten Spalte jeder Zeile, die den Bereitstellungspunkt repräsentiert, den Sie trennen möchten.

   b. Klicken Sie auf **Bereitstellung aufheben**.

   Ein Bestätigungsdialogfeld wird angezeigt.

   c. Klicken Sie hier, um zu bestätigen, dass Sie die gewählten Wiederherstellungspunkte trennen möchten.

   Die lokalen Wiederherstellungspunkte werden getrennt.

   NOTE: Wenn Popup-Warnungen aktiviert sind, wird möglicherweise eine Warnung angezeigt, dass die entsprechenden Bereitstellungspunkte getrennt werden.
4. Vergewissern Sie sich, dass die zuvor bereitgestellten Wiederherstellungspunkte nicht mehr in der Liste „Lokale Bereitstellungen“ bzw. „Remote-Bereitstellungen“ angezeigt werden.

Arbeiten mit Linux-Wiederherstellungspunkten

Die empfohlene und unterstützte Methode zum Bereitstellen und Aufheben der Bereitstellung von Wiederherstellungspunkten auf einem geschützten Linux-Computer ist die Verwendung des Dienstprogramms **local_mount**.

Die nachfolgend aufgelisteten Verfahren behandeln insbesondere das Bereitstellen und Aufheben der Bereitstellung von Linux-Wiederherstellungspunkten mit local_mount.

NOTE: Informationen zur anderen Verwaltungsmöglichkeiten für Linux-Wiederherstellungspunkte finden Sie unter Verwalten von Snapshots und Wiederherstellungspunkten, da alle anderen Verwaltungsaufgaben in der Kern-Konsole durchgeführt werden können.

- Bereitstellen eines Wiederherstellungspunkt-Volumes für eine Linux-Maschine
- Aufheben der Bereitstellung eines Wiederherstellungspunkts auf einer Linux-Maschine

Bereitstellen eines Wiederherstellungspunkt-Volumes für eine Linux-Maschine

Mit dem Dienstprogramm local_mount in Rapid Recovery können Sie ein Volume per Fernzugriff aus einem Wiederherstellungspunkt als lokales Volume auf einem Linux-Computer bereitstellen.

NOTE: Versuchen Sie dabei nicht, Wiederherstellungspunkte im Ordner „/tmp“ bereitzustellen, da dieser die aavdisk-Dateien enthält.

1. Erstellen Sie ein neues Verzeichnis für die Bereitstellung des Wiederherstellungspunkts (z. B. mit dem Befehl `mkdir`).
2. Vergewissern Sie sich, dass das Verzeichnis vorhanden ist (z. B. mit dem Befehl `ls`).
3. Führen Sie das Rapid Recovery Dienstprogramm local_mount als Root oder als Superuser aus, z. B.:

   ```
   sudo local_mount
   ```
4. Geben Sie den folgenden Befehl in die Rapid Recovery Bereitstellungsaufforderung ein, um die geschützten Computer aufzulisten.

   ```
   lm
   ```
5. Wenn Sie dazu aufgefordert werden, geben Sie die IP-Adresse oder den Hostnamen Ihres Rapid Recovery Core-Servers an.
6. Geben Sie die Anmeldeinformationen (Benutzername und Kennwort) für den Core-Server ein.

   Daraufhin wird eine Liste der Computer angezeigt, die vom Rapid Recovery Server geschützt werden. Die Liste enthält für jede Maschine die folgenden Informationen: laufende Zeilennummer, Host/IP-Adresse und ID-Nummer für die Maschine.

   Beispiel: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba
7. Geben Sie den folgenden Befehl ein, um die für eine bestimmte Maschine verfügbaren Wiederherstellungspunkte anzuzeigen:

   ```
   lr <line_number_of_machine>
   ```

   NOTE: Sie können in diesem Befehl auch die ID-Nummer der Maschine anstelle der laufenden Zeilennummer angeben.

   Daraufhin werden die Basiswiederherstellungspunkte und die inkrementellen Wiederherstellungspunkte für die Maschine aufgelistet. Die Liste umfasst die laufende Zeilennummer, Datum und Zeitstempel, Speicherort des Volumes, Größe des Wiederherstellungspunkts und eine ID-Nummer für das Volume mit einer laufenden Nummer am Ende, die den Wiederherstellungspunkt kennzeichnet,

   Zum Beispiel: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2
8. Geben Sie den folgenden Befehl ein, um den angegebenen Wiederherstellungspunkt auszuwählen und im angegebenen Bereitstellungspunkt/-pfad bereitzustellen.

   ```
   m <volume_recovery_point_ID_number> <volume-letter> [flag] <path>
   ```

Das Flag im Befehl bestimmt, wie der Wiederherstellungspunkt bereitgestellt wird. Sie können eine der folgenden Optionen verwenden:

- [r] - schreibgeschützt bereitstellen (Standard). Dieses Flag bietet die Möglichkeit, einen Wiederherstellungspunkt zu mounten, aber keine Möglichkeit, daran Änderungen vorzunehmen.
- [w] - mit Schreibzugriff bereitstellen. Dieses Flag bietet die Möglichkeit, einen Wiederherstellungspunkt zu mounten und daran Änderungen vorzunehmen.
- [v] - Schreibgeschützt bereitstellen mit vorherigen Schreibvorgängen. Dieses Flag bietet die Möglichkeit, einen Wiederherstellungspunkt zu mounten und alle Änderungen einzubeziehen, die bei einer früheren Bereitstellung mit Schreibzugriff durchgeführt wurden, aber nicht im Wiederherstellungspunkt vorhanden sind.
- [n] - NBD-Gerät nicht in <Pfad> bereitstellen. Ein NBD-Gerät (Network Block Device) stellt bei einer lokalen Bereitstellung eine Socket-Verbindung zwischen dem Core und der geschützten Maschine her. Mit diesem Flag können Sie den Wiederherstellungspunkt bereitstellen, ohne das NBD-Gerät bereitzustellen. Dies ist nützlich, wenn Sie das Dateisystem des Wiederherstellungspunks manuell überprüfen möchten.

NOTE: Sie können im Befehl auch die Zeilennummer anstelle der ID-Nummer für den Wiederherstellungspunkt angeben, um den Wiederherstellungspunkt anzugeben. In diesem Fall müssen Sie die Zeilennummer für die Maschine (in der lm-Ausgabe), gefolgt von der Zeilennummer des Wiederherstellungspunkts und dem Volume-Buchstaben und dahinter den Pfad angeben, z. B. „m <Zeilennummer_für_Maschine> <Zeilennummer_für_Wiederherstellungspunkt> <Volume-Buchstabe> <Pfad>“. Wenn die `lm`-Ausgabe beispielsweise drei geschützte Maschinen auflistet, Sie den Befehl `lr` für Nummer 2 eingeben und Sie das 23. Wiederherstellungspunktvolume B in /tmp/mount_dir bereitstellen, lautet der Befehl:

```
m 2 23 b /tmp/mount_dir
```

NOTE: Wenn Sie ein BTRFS-Volume auf einem kompatiblen Betriebssystem bereitstellen (siehe Abschnitt „Rapid Recovery Version 6.1 Betriebssystem-Installations- und Kompatibilitätsmatrix“ im Rapid Recovery-Installations und -Aktualisierungshandbuch), müssen Sie die folgenden Parameter einschließen:

```
mount -o nodatasum,device=/dev/xxx /dev/xxx /mnt/yyy
```

9. Um festzustellen, ob die Bereitstellung erfolgreich durchgeführt wurde, geben Sie den folgenden Befehl ein, der das angehängte Remote-Volume auflisten sollte:

   ```
   l
   ```

Aufheben der Bereitstellung eines Wiederherstellungspunkts auf einer Linux-Maschine

Führen Sie die folgenden Schritte aus, um die Bereitstellung eines Wiederherstellungspunkt auf einer Linux-Maschine aufzuheben.

1. Führen Sie das Rapid Recovery Dienstprogramm local_mount als Root oder als Superuser aus, z. B.:

   ```
   sudo local_mount
   ```

2. Geben Sie den folgenden Befehl in die Rapid Recovery Bereitstellungsaufforderung ein, um die geschützten Maschinen aufzulisten.

   ```
   lm
   ```

3. Wenn Sie dazu aufgefordert werden, geben Sie die IP-Adresse oder den Hostnamen Ihres Rapid Recovery Core Core-Servers an.
4. Geben Sie die Anmeldeinformationen (Benutzername und Kennwort) für den Core-Server ein.

Daraufhin wird eine Liste der Maschinen angezeigt, die vom Rapid Recovery Core Server geschützt werden.

5. Geben Sie den folgenden Befehl ein, um die für eine bestimmte Maschine verfügbaren Wiederherstellungspunkte anzuzeigen:

   ```
   lr <line_number_of_machine>
   ```

   NOTE: Sie können in diesem Befehl auch die ID-Nummer der Maschine anstelle der laufenden Zeilennummer angeben.

   Daraufhin werden die Basiswiederherstellungspunkte und die inkrementellen Wiederherstellungspunkte für die betreffende Maschine aufgelistet. Die Liste umfasst die laufende Zeilennummer, Datum/Zeitstempel, Speicherort des Volume, Größe des Wiederherstellungspunkts und eine ID-Nummer für das Volume mit einer laufenden Nummer am Ende, die den Wiederherstellungspunkt kennzeichnet.

   Beispiel: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2

6. Führen Sie den Befehl `l or list` aus, um eine Liste der bereitgestellten NBD-Geräte (Network Block Device) abzurufen. Wenn Sie einen Wiederherstellungspunkt bereitstellen, wird nach der Ausführung des Befehls `l or list` ein Pfad zum NBD-Gerät ausgegeben.
7. Geben Sie den folgenden Befehl ein, um die Bereitstellung eines Wiederherstellungspunkts aufzuheben.

   ```
   unmount path_of_nbd-device>
   ```

8. Führen Sie den Befehl `l or list` aus, um zu überprüfen, ob die Bereitstellung des Wiederherstellungspunkts erfolgreich aufgehoben wurde.

Erzwingen eines Snapshots

Durch das Erzwingen eines Snapshots können Sie eine Datenübertragung für die aktuelle geschützte Maschine erzwingen. Wenn Sie eine Snapshot-Erstellung erzwingen, wird die Übertragung entweder sofort gestartet oder zur Warteschlange hinzugefügt, wenn andere Jobs ausgeführt werden.

Sie können zwei Typen von Snapshots wählen.

Wenn Sie einen inkrementellen Snapshot auswählen und kein vorheriger Wiederherstellungspunkt vorhanden ist, wird ein Basisimage erfasst. Ein Erzwingen eines Snapshots ändert nicht den Zeitplan für geplante Snapshots.

NOTE: Rapid Recovery unterstützt Windows 8, Windows 8,1, Windows Server 2012, Windows Server 2012 R2 und Windows Server 2016 für Basis- und inkrementelle Übertragungen.

- Ein Basisimage ist ein Snapshot aller Daten in den ausgewählten Volumes der Maschine.
- Ein inkrementeller Snapshot erfasst alle Daten, die seit dem letzten Snapshot geändert wurden.

1. Navigieren Sie in der Rapid Recovery Core Console zu der Maschine oder dem Cluster mit dem Wiederherstellungspunkt, für den Sie einen Snapshot erzwingen möchten.
2. Klicken Sie auf der Seite "Zusammenfassung" im Fensterbereich "Zusammenfassung" auf **Snapshot erzwingen**.

   Das Dialogfeld "Snapshot erzwingen" wird angezeigt.
3. Klicken Sie im Dialogfeld "Snapshot erzwingen" im Kontrollkästchen auf ein oder mehrere Volumes oder Schutzgruppen.
4. Klicken Sie auf **Snapshot erzwingen** bzw. "Basisimage erzwingen".
5. Wenn Sie ein Basisimage ausgewählt haben, bestätigen Sie, dass Sie ein Basisimage erstellen möchten.

   Ein Basisimage kann ja nach Menge der Daten in den Volumes, die Sie sichern möchten, längere Zeit in Anspruch nehmen.
   Der ausgewählte Snapshot wird in die Warteschlange eingereiht und wird gestartet, sobald andere Jobs abgeschlossen sind.

Entfernen von Wiederherstellungspunkten

Sie können Wiederherstellungspunkte für eine bestimmte Maschine einfach aus dem Repository entfernen. Beim Löschen von Wiederherstellungspunkten in Rapid Recovery können Sie eine der folgenden Optionen angeben.

- **Alle Wiederherstellungspunkte löschen**. Entfernt alle Wiederherstellungspunkte für die ausgewählte geschützte Maschine aus dem Repository.
- **Bereich von Wiederherstellungspunkten löschen**. Entfernt alle Wiederherstellungspunkte in einem angegebenen Bereich vor dem aktuellen, bis einschließlich zum Basisimage, d. h. alle Daten auf der Maschine sowie alle Wiederherstellungspunkte nach dem aktuellen bis hin zum nächsten Basisimage.

NOTE: Gelöschte Wiederherstellungspunkte können nicht wiederhergestellt werden. Wenn Sie die in den Wiederherstellungspunkten gespeicherten Daten benötigen, ziehen Sie in Betracht, die Daten vorher zu archivieren.

1. Klicken Sie in der Rapid Recovery Core Console unter dem Menü **Geschützte Maschinen** auf den Namen oder die IP-Adresse der Maschine, für die Sie Wiederherstellungspunkte anzeigen und entfernen möchten.

   Die Anzeige „Zusammenfassung“ für die ausgewählte Maschine wird aufgerufen.
2. Klicken Sie neben der Maschine oder der IP-Adresse auf das Menü **Wiederherstellungspunkte**.

   Die Seite **Wiederherstellungspunkt** für die ausgewählte Maschine wird angezeigt.
3. Scrollen Sie zum Fensterbereich **Wiederherstellungspunkte**.

   Unter dem Fensterbereichstitel werden Optionen angezeigt, einschließlich „Aktualisieren“, „Löschen“ und „Alle löschen“.
4. Um alle derzeit gespeicherten Wiederherstellungspunkte zu löschen, klicken Sie unter dem Fensterbereich „Wiederherstellungspunkte“ auf **Alle löschen** und in das Bestätigungsdialogfeld, um den Löschvorgang zu bestätigen.
5. Um einen Satz Wiederherstellungspunkte in einem bestimmten Datenbereich zu löschen, gehen Sie folgendermaßen vor:
   a. Klicken Sie unter dem Fensterbereichstitel „Wiederherstellungspunkte“ auf **Bereich löschen**.

   Das Dialogfeld **Löschen von Wiederherstellungspunkten innerhalb des Bereichs** wird angezeigt.

   b. Wählen Sie im Dialogfeld **Löschen von Wiederherstellungspunkten innerhalb des Bereichs** im Feld **Von** Datum und Uhrzeit für den Start des Löschens von Wiederherstellungspunkten.
   c. Im Feld **Bis** wählen Sie Datum und Uhrzeit aus, um den letzten Wiederherstellungspunkt zu definieren, den Sie löschen möchten.
   d. Klicken Sie auf **Löschen**.
   e. Klicken Sie im Bestätigungsdialogfeld, um die Löschung zu bestätigen.

Löschen einer verwaisten Wiederherstellungspunktkette

Bei einem verwaisten Wiederherstellungspunkt handelt es sich um einen inkrementellen Snapshot, der keinem Basisimage zugeordnet ist. Nachfolgende Snapshots bauen jedoch weiterhin auf diesem Wiederherstellungspunkt auf. Ohne das Basisimage sind die entstehenden Wiederherstellungspunkte jedoch unvollständig und enthalten höchstwahrscheinlich nicht die erforderlichen Daten für eine Wiederherstellung. Diese

Wiederherstellungspunkte werden als Teil der verwaisten Wiederherstellungspunktkette angesehen. In dieser Situation sollte idealerweise die Kette gelöscht und ein neues Basisimage erstellt werden.

Weitere Informationen zum Erzwingen eines Basisimage finden Sie unter Erzwingen eines Snapshots.

1. Navigieren Sie in der Rapid Recovery Core Console zu der geschützten Maschine, für die Sie die verwaiste Wiederherstellungspunktkette löschen möchten.
2. Klicken Sie im Menü am oberen Rand der Seite auf **Wiederherstellungspunkte**.
3. Erweitern Sie im Fensterbereich „Wiederherstellungspunkte“ den verwaisten Wiederherstellungspunkt.

   Ein solcher Wiederherstellungspunkt weist in der Spalte „Typ“ den Eintrag „Inkrementell, Verwaist“ auf.
4. Klicken Sie neben „Aktionen“ auf **Löschen**.

   Das Fenster „Wiederherstellungspunkte löschen“ wird angezeigt.
5. Klicken Sie im Dialogfeld „Wiederherstellungspunkte löschen“ auf **Ja**.

   CAUTION: Durch Löschen dieses Wiederherstellungspunkts wird die gesamte Wiederherstellungspunktkette mit allen inkrementellen Wiederherstellungspunkten davor oder danach bis zum nächsten Basisimage gelöscht. Dieser Vorgang kann nicht rückgängig gemacht werden.

   CAUTION: Die verwaiste Wiederherstellungspunktkette wird gelöscht.

Migrieren von Wiederherstellungspunkten in ein anderes Repository

Wenn Sie die Wiederherstellungspunkte einer geschützten Maschine aus einem Repository entfernen möchten, ohne sie zu löschen, können Sie sie gemäß folgendem Verfahren in ein anderes Repository migrieren. Dieser Vorgang umfasst Archivierung von Wiederherstellungspunkten vom Quell-Repository, und anschließendem Importieren des Archivs in das Ziel-Repository.

Sie können beispielsweise dieses Verfahren durchführen, wenn Ihr vorhandenes Repository vollständig belegt ist, oder wenn sich Ihre Anforderungen ändern und Sie eine Maschine mit einem anderen Core und Repository möchten.

CAUTION: Wenn Ihr Repository zuvor von AppAssure **5.3 oder 5.4 aktualisiert und Replikation verwendet wurde, empfiehlt** Quest **die Durchführung des Check-Repository-Jobs auf jedem Repository in diesem Ziel-Core vor der Migration. Die Durchführung dieses Jobs kann jedoch Kopieren von Daten-Unregelmäßigkeiten auf ein neues Ziel-Repository ausschließen. Der Check-Repository-Job ist nur in der Benutzeroberfläche verfügbar, wenn er auf den Core angewendet werden kann, und könnte einen erheblichen Teil der Zeit für die Ausführung erfordern. Informationen zu diesem Job finden Sie unter Informationen über das Überprüfen der Integrität der DVM Repositorys. Informationen zur Durchführung dieses Jobs finden Sie unter Ausführen einer Integritätsprüfung auf einem DVM-Repository.**

1. Deaktivieren Sie in der Rapid Recovery Core Console vorübergehend die Schutzfunktion für die geschützten Maschinen, deren Wiederherstellungspunkte Sie migrieren möchten. Weitere Informationen hierzu finden Sie unter Vorübergehendes Deaktivieren und erneutes Aktivieren der Schutzfunktion.
2. Brechen Sie alle Vorgänge für die geschützten Maschinen ab, oder für Maschinen deren Wiederherstellungspunkte Sie migrieren möchten oder warten Sie, bis alles abgeschlossen ist.
3. Archivieren Sie die Wiederherstellungspunkte für die Maschinen, die vorübergehend deaktiviert wurden. Weitere Informationen hierzu finden Sie unter Erstellen eines Archivs.
4. Nach der Archivierung und Überprüfung des Archivs entfernen Sie die vorhandenen Wiederherstellungspunkte für die geschützte Maschine, die Sie migrieren möchten. Weitere Informationen hierzu finden Sie unter Entfernen von Wiederherstellungspunkten.

   NOTE: Ohne Entfernen der vorhandenen Wiederherstellungspunkte können Sie keine Änderungen an Repositorys für eine geschützte Maschine ändern.
5. Erstellen Sie ein neues Repository für die migrierten Wiederherstellungspunkte oder stellen Sie sicher, dass ein neues Ziel-Repository vorhanden ist. Weitere Informationen hierzu finden Sie unter Erstellen eines DVM-Repository.

   - Fahren Sie mit Schritt 6 fort, wenn ein vorhandenes Repository verwendet werden soll.
6. Ändern Sie das Repository für die einzelnen deaktivierten Maschinen, indem Sie die folgenden Schritte durchführen:
   a. Klicken Sie in der Navigationsstruktur der Core Console auf die geschützte Maschine.
   b. Klicken Sie auf der Seite **Zusammenfassung** der geschützten Maschine auf **Einstellungen**.
   c. Klicken Sie auf der Seite **Einstellungen** im Fensterbereich **Allgemein** auf die Drop-Down-Liste **Repository** und wählen Sie anschließend den Namen des Repositorys, das Sie in Schritt 4 erstellt haben.

   - Wählen Sie den Namen eines bestehenden Repositorys aus, wenn ein bestehendes Repository verwendet werden soll.

     NOTE: Achten Sie bei der Migration von Wiederherstellungspunkten in ein bestehendes Repository darauf, dass im bestehenden Repository genügend freier Speicherplatz für die migrierten Wiederherstellungspunkte vorhanden ist.

   d. Klicken Sie auf **OK**.
7. Aktivieren Sie wieder die Schutzfunktion für die Maschinen, deren Schutz vorübergehend deaktiviert wurde. Weitere Informationen hierzu finden Sie unter Vorübergehendes Deaktivieren und erneutes Aktivieren der Schutzfunktion.
8. Erstellen Sie ein Basisimage für jede verschobene geschützte Maschine. Weitere Informationen finden Sie unter Erzwingen eines Snapshots und verwenden Sie die Option „Basisimage erzwingen“.
9. Importieren Sie die archivierten Daten für die Maschinen, die Sie migrieren möchten. Weitere Informationen hierzu finden Sie unter Importieren eines Archivs.

Replikation

In diesem Kapitel wird beschrieben, wie die Replikation geschützter Daten für die Notfallwiederherstellung von einem Rapid Recovery Ziel-Core auf einen Rapid Recovery Ziel-Core konfiguriert und verwaltet wird.

Replikation mit Rapid Recovery

Dieser Abschnitt enthält konzeptionelle und prozedurale Informationen, um Sie beim Verständnis und der Konfiguration der Replikation in Rapid Recovery zu unterstützen.

Replikation ist der Vorgang des Kopierens von Wiederherstellungspunkten von einem Rapid Recovery Core und deren Übertragung an einen anderen Rapid Recovery Core zur Notfall-Wiederherstellung. Dafür ist eine gekoppelte Quelle-Ziel-Beziehung zwischen zwei oder mehr Cores erforderlich.

Der Quell-Core kopiert die Wiederherstellungspunkte bestimmter geschützter Maschinen und überträgt anschließend diese inkrementellen Snapshot-Daten asynchron und kontinuierlich an den Ziel-Core.

Wenn Sie das Standardverhalten durch Einrichten eines Replikationszeitplans nicht ändern, startet der Core einen Replikationsjob sofort nach Abschluss jedes Sicherungs-Snapshots, jeder Prüfsummen-Überprüfung, jeder Bereitstellbarkeitsprüfung und jeder Anfügbarkeitsprüfung. Protokollkürzungen jeglicher Art sowie eine Überprüfung der Integrität von Wiederherstellungspunkten oder einer Oracle Datenbank lösen ebenfalls einen Replikationsjob aus. Wenn irgendwelche dieser Aktionen in nächtlichen Jobs enthalten sind, dann löst auch der Abschluss der nächtlichen Jobs einen Replikationsjob aus. Weitere Informationen hierzu finden Sie unter Planen der Replikation.

NOTE: Wenn Sie Daten für einen Cluster replizieren, müssen Sie den gesamten Cluster replizieren. Wenn Sie zum Beispiel einen Knoten zum Replizieren auswählen, wird der Cluster automatisch ausgewählt. Wenn Sie entsprechend den Cluster auswählen, werden alle Knoten in diesem Cluster ebenfalls aktiviert.

Für eine optimale Datensicherheit verwenden Administratoren in der Regel einen Ziel-Core an einem Remote-Notfallwiederherstellungsstandort. Sie können die ausgehende Replikation in einem unternehmenseigenen Rechenzentrum oder am Remote-Notfallwiederherstellungsstandort (ein „selbstverwalteter“ Ziel-Core) konfigurieren. Sie können eine ausgehende Replikation auch an einen Drittanbieter, der verwaltete Dienste bereitstellt, (MSP) oder einen Cloud-Anbieter konfigurieren, der externe Sicherungs- und Notfallwiederherstellungsdienste anbietet. Bei der Replikation auf den Ziel-Core eines Drittanbieters können Sie integrierte Arbeitsabläufe verwenden, mit denen Sie Verbindungen anfordern und automatische Rückmeldungen erhalten können.

Die Replikation wird auf jeder geschützten Maschine einzeln verwaltet. Alle in einem Quell-Core geschützten oder auf einen Quell-Core replizierten Maschinen können für die Replikation auf einen Ziel-Core konfiguriert werden.

Mögliche Szenarien für die Replikation sind:

- **Replikation auf einen lokalen Speicherort.** Der Ziel-Core befindet sich in einem lokalen Rechenzentrum oder vor Ort und die Replikation wird immer vorgenommen. In dieser Konfiguration ist eine Wiederherstellung auch möglich, wenn ein Core verloren geht.
- **Replikation auf einen externen Speicherort.** Der Ziel-Core befindet sich in einer externen Einrichtung zur Notfallwiederherstellung, um im Verlustfall eine Wiederherstellung zu ermöglichen.
- **Gegenseitige Replikation.** Zwei Rechenzentren an zwei unterschiedlichen Standorten enthalten jeweils einen Core, die Maschinen schützen und gegenseitig als externe Sicherung für eine

Notfallwiederherstellung dienen. In diesem Szenario repliziert jeder Core die geschützten Maschinen auf den Core im anderen Rechenzentrum.

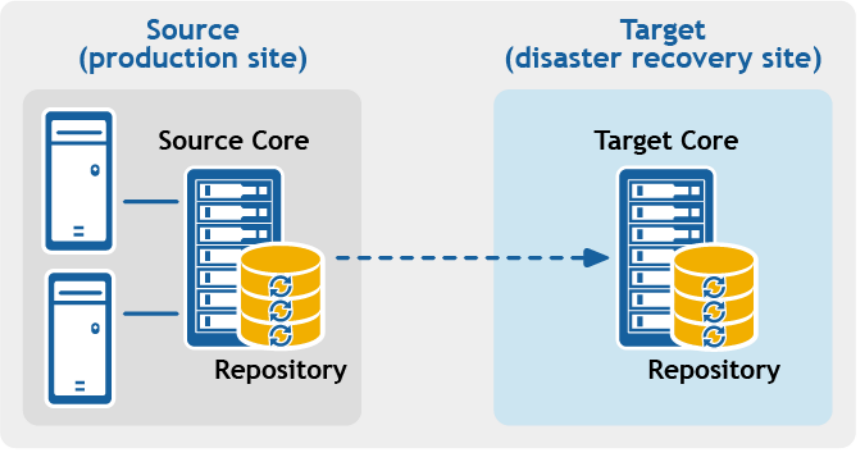
- **Gehostete Replikation und Cloud-Replikation.** Rapid Recovery-MSP-Partner unterhalten mehrere Ziel-Cores in einem Rechenzentrum oder in einer öffentlichen Cloud. Auf diesen Cores können Kunden des MSP-Partners gegen Gebühr Wiederherstellungspunkte von einem Quell-Core am Kundenstandort auf den Ziel-Core des MSP replizieren.

  NOTE: In diesem Szenario haben Kunden nur Zugriff auf ihre eigenen Daten.

Mögliche Replikationskonfigurationen sind:

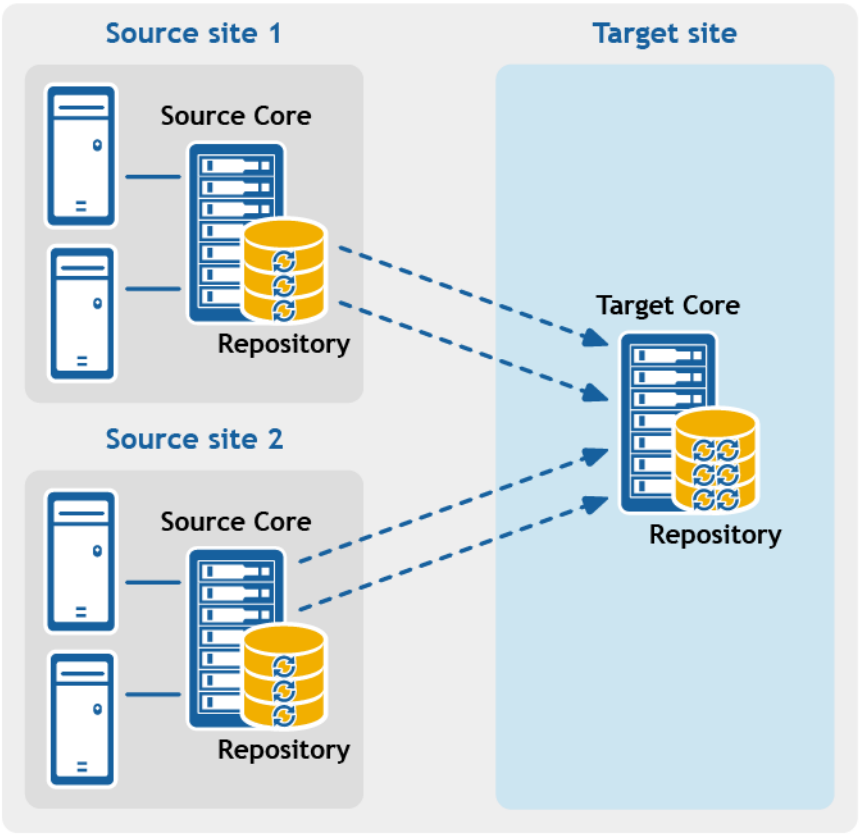
- **Punkt-zu-Punkt Replikation**. Eine einzelne geschützte Maschine wird von einem einzelnen Quell-Core auf einen einzelnen Ziel-Core repliziert.

Abbildung 1. Konfiguration der Punkt-zu-Punkt-Replikation



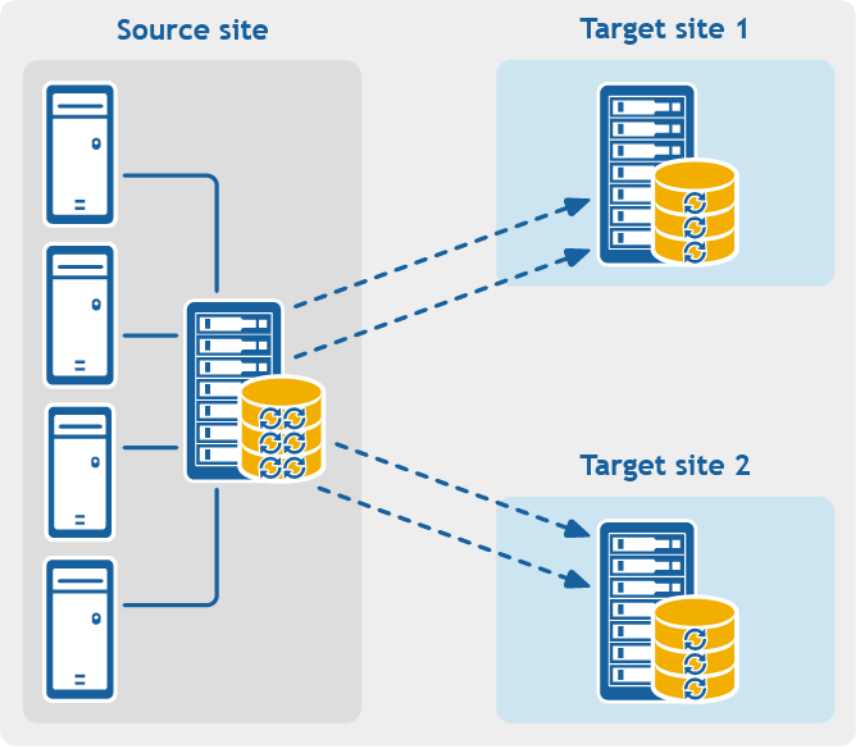
- **Multi-Punkt-zu-Punkt-Replikation**. Geschützte Maschinen werden von mehreren Quell-Cores auf einen einzelnen Ziel-Core repliziert.

Abbildung 2. Konfiguration der Multi-Punkt zu-Punkt-Replikation



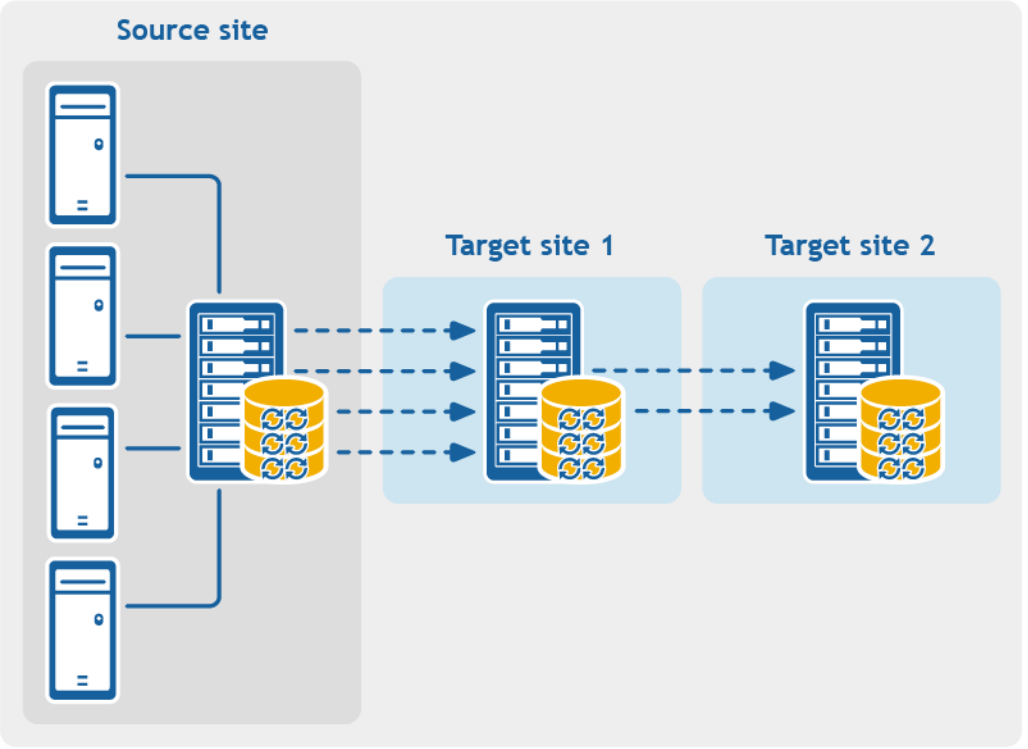
- **Punkt-zu-Multi-Punkt-Replikation**. Eine oder mehrere geschützte Maschine/n wird/werden von einem einzelnen Quell-Core auf mehrere Ziel-Cores repliziert.

Abbildung 3. Konfiguration der Punkt-zu-Multi-Punkt-Replikation



- **Multi-Hop-Replikation.** Eine oder mehrere geschützte Maschine/n wird/werden von einem Ziel-Core auf einen weiteren Ziel-Cores repliziert, wodurch zusätzliche Failover- oder Wiederherstellungsoptionen auf dem replizierten Core geschaffen werden.

Abbildung 4. Konfiguration der Multi-Hop-Replikation



Bei Verwendung von Sicherungs-Appliances der DL-Serie muss auf dem Ziel-Core, auf den Sie replizieren, eine gültige Softwarelizenz konfiguriert sein. Beim Kauf dieser Hardwaregeräte erhalten Sie eine Replikationsziel-Lizenz. Überprüfen Sie Ihren Lizenzschlüssel in der Willkommens-E-Mail, die Sie beim Kauf des Geräts erhalten haben. Wenn Sie Hilfe benötigen, besuchen Sie die Website mit Hilfestellungen zum Thema „Lizensierung“ unter https://support.quest.com/contact-us/licensing oder wenden Sie sich per E-Mail an license@quest.com.

Wiederherstellungspunkt-Ketten und -Waisen

Rapid Recovery erfasst Snapshots einer geschützten Maschine und speichert die Daten in einem Repository als Wiederherstellungspunkt. Der erste im Core gespeicherte Wiederherstellungspunkt wird als Basisimage bezeichnet. Das Basisimage umfasst das Betriebssystem, Anwendungen und Einstellungen jedes Volume, das Sie zum Schutz angeben, sowie alle Daten auf diesen Volumes. Nachfolgende Sicherungen werden inkrementelle Snapshots bezeichnet und enthalten lediglich die Daten auf den geschützten Volumes, die seit der letzten Sicherung geändert wurden. Das Basisimage plus alle inkrementellen Snapshots formen zusammen eine vollständige Wiederherstellungspunkt-Kette.

Aus einer vollständigen Wiederherstellungspunkt-Kette können Sie Daten einfach und zuverlässig wiederherstellen, wozu Ihnen die gesamte Palette von Wiederherstellungsoptionen in Rapid Recovery zur Verfügung steht. Diese Optionen umfassen Wiederherstellung auf Dateiebene, Wiederherstellung auf Volume-Ebene und Bare-Metal-Wiederherstellung.

Da Sie logischerweise keine Daten wiederherstellen können, die nicht vorhanden sind, können Sie im Falle einer unvollständigen Wiederherstellungspunkt-Kette keine Daten auf der Volume-Ebene wiederherstellen oder eine Bare-Metal-Wiederherstellung durchführen. In solchen Fällen können Sie weiterhin alle Daten wiederherstellen, die in einem Wiederherstellungspunkt auf Dateiebene vorliegen.

Wenn die Informationen, die Sie von einem Wiederherstellungspunkt wiederherstellen möchten, in einer vorherigen Sicherung vorliegen, die dem Core nicht zur Verfügung steht (ein früherer inkrementeller Snapshot oder das Basisimage, so wird der Wiederherstellungspunkt alsverwaist bezeichnet. Verwaiste Wiederherstellungspunkte sind typisch für einige Replikationsszenarien.

Wenn Sie beispielsweise erstmals eine Replikation einrichten, sind Ihre Optionen für das Wiederherstellen von Daten aus replizierten Wiederherstellungspunkten beschränkt. Bis alle Sicherungsdaten vom Quell-Core auf den Ziel-Core übertragen wurden, kann die Erstellung vollständiger Wiederherstellungspunkt-Ketten aus den Waisen nur auf Dateiebene erfolgen.

Wenn die Replikation startet

Standardmäßig werden Replikationsübertragungs-Jobs nach jedem Abschluss einer regelmäßig geplanten Backup-Übertragung vom Core automatisch in eine Warteschlange gestellt. Sofern der Replikationszeitplan für eine geschützte Maschine also nicht angepasst wurde, basiert dieser auf dem standardmäßigen Sicherungs-Snapshot-Zeitplan.

Wenn Sie die Replikation erstmals einrichten, beginnt der Replikationsvorgang sofort, wenn ein oder mehrere Wiederherstellungspunkte auf dem Quell-Core vorliegen, es sei denn:

- Sie wählen die Option, die Replikation vorerst anzuhalten, oder
- Sie aktivieren die Option, ein Seed-Laufwerk für die Erstübertragung zu verwenden.

Wenn Sie eine Replikation zunächst anhalten, beginnt die Replikation erst, wenn Sie sie explizit wieder aufnehmen.

Wenn Sie beim Einrichten der Replikation die Verwendung eines Seed-Laufwerks angeben, beginnt die Replikation auf den Ziel-Core beim nächsten regelmäßig geplanten Sicherungs-Snapshot.

NOTE: Sie können auch eine Sicherung der geschützten Maschine erzwingen, nachdem Sie eine Replikation eingerichtet haben. Dies führt dazu, dass die Replikation unmittelbar nach Abschluss des Snapshots der geschützten Maschine beginnt.

Wenn Sie beim Einrichten der Replikation ein Seed-Laufwerk angeben, werden nur zukünftige Sicherungs-Übertragungen repliziert. Wenn Sie möchten, dass vorhandene Wiederherstellungspunkte der ursprünglichen geschützten Maschine auf dem Ziel-Core bestehen, müssen Sie Daten von der geschützten Maschine übertragen. Zum Übertragen von Daten erstellen Sie ein Seed-Laufwerk aus dem Quell-Core und konsumieren dann das Seed-Laufwerk auf dem Ziel-Core.

Sie können auch den Replikationszeitplan für eine geschützte Maschine anpassen. Wenn Sie zum Beispiel den Standard-Schutzzeitplan von einer Sicherung pro Stunde verwenden, können Sie angeben, dass die Replikation des Quell-Core auf den Ziel-Core unter einem anderen Zeitplan (z. B. einmal täglich um 2 Uhr) stattfindet.

Bestimmen der Seeding-Anforderungen und -Strategie

Die folgenden Kapitel beschreiben das Wiederherstellen von replizierten Daten und ob Sie Wiederherstellungspunktdaten vom Quell-Core mit einem Seeding-Vorgang übertragen müssen.

Wenn das Seeding von Daten erforderlich ist

Wenn Sie das erste Mal eine Replikation einrichten, beginnt der Quell-Core mit der Übertragung aller Wiederherstellungspunkte für die ausgewählten Maschinen auf den Ziel-Core, es sei denn, Sie geben Sie die Verwendung eines Seed-Laufwerks an. Die Übertragung Ihrer Daten über das Netzwerk kann viel Zeit in Anspruch nehmen. Beeinflusst wird dies von Faktoren wie die Geschwindigkeit Ihres Netzwerks, die Robustheit

der Netzwerkarchitektur und die Menge der Daten, die auf den Ziel-Core übertragen werden sollen. Wenn die Sicherungsdaten auf dem Quell-Core beispielsweise 10 GB umfassen und die WAN-Verbindung 24 MBit/s übertragen kann, so dauert die Übertragung ungefähr eine Stunde.

Basierend auf der Menge an Informationen, die Sie auf den Ziel-Core kopieren möchten, kann sich das Seed-Laufwerk auf Hunderte oder Tausende Gigabytes von Daten summieren. Viele Organisationen entscheiden sich dafür, nicht die hierfür benötigte Netzwerkbandbreite zu konsumieren, und ziehen stattdessen das Definieren und Konsumieren eines Seed-Laufwerks vor. Weitere Informationen finden Sie unter Überlegungen zur Übertragungsleistung für Replikationsdaten.

Wenn Sie bei der Definition der Replikation die Verwendung eines Seed-Laufwerks angeben, werden nur Wiederherstellungspunkte, die nach der Einrichtung der Replikation auf dem Quell-Core gespeichert wurden, auf den Ziel-Core repliziert. Sicherungen, die vor der Einrichtung der Replikation auf dem Quell-Core gespeichert waren, sind im Anschluss nicht auf dem Ziel-Core vorhanden, es sei denn, Sie geben mit folgendem Vorgang ein explizites Seeding der Daten an.

Um eine Beeinträchtigung der Netzwerkgeschwindigkeit durch einen umfangreichen Transfer historischer Daten zu vermeiden, sollten Sie Ihre vorherigen Sicherungsdaten mithilfe eines **Seed-Laufwerks** auf den Ziel-Core übertragen. Ein Seed-Laufwerk ist eine Archivdatei, die eine Reihe von deduplizierten Basisimages und inkrementellen Snapshots vom Quell-Core **kopiert**. Die Seed-Laufwerksdatei enthält den vollständigen Satz von vorherigen Wiederherstellungspunkten für die geschützten Maschinen, die Sie vom Quell-Core auf den Ziel-Core replizieren möchten.

Verschieben Sie die Seed-Laufwerksdatei in ein Speichervolume, das Sie dann dem Ziel-Core zur Verfügung stellen. Anschließend **konsumieren** Sie die Informationen des Seed-Laufwerks. Dies umfasst das Anhängen des Volumes mit dem Seed-Laufwerksimage an den Ziel-Core und das Importieren der Daten in das Repository von der Core Console. Dieser Prozess repariert Waisen, indem inkrementelle Snapshots, die auf den Ziel-Core repliziert wurden, mit ihren Basisimages vereint werden, um eine oder mehrere vollständige Wiederherstellungspunkt-Ketten zu bilden. Dieser Prozess wird mitunter auch als „copy-consume“ bezeichnet.

Das Seeding von Daten von Ihrem Quell-Core ist nicht immer erforderlich. Beispiel:

- Wenn Sie Replikation für einen neuen Rapid Recovery Core einrichten, ist Seeding nicht erforderlich.
- Wenn die Daten aus früheren Snapshots nicht kritisch für Ihre replizierten Daten sind und Sie nur Daten wiederherstellen müssen, die nach der Einrichtung von Replikation gespeichert wurden, ist Seeding nicht erforderlich.

  NOTE: In diesem Fall empfiehlt Quest, dass Sie unmittelbar vor oder unmittelbar nach dem Einrichten der Replikation ein neues Basisimage erfassen. Dieser Schritt gewährleistet, dass eine vollständige Wiederherstellungspunkt-Kette auf dem Ziel-Core vorhanden ist, die Sie zur Wiederherstellung von Daten in Zukunft benötigen.
- Wenn Sie ein BasisImage unmittelbar vor dem Einrichten der Replikation erfasst haben und nur Daten wiederherstellen müssen, die nach diesem Zeitpunkt erfasst wurden, ist Seeding nicht erforderlich.
- Wenn Sie die Replikation ohne Angabe eines Seed-Laufwerks eingerichtet haben, werden die Snapshot-Daten über das Netzwerk vom Quell-Core zum Ziel-Core übertragen.

Wenn eine der folgenden Situationen auf Sie zutrifft, ist kein Seeding der Daten erforderlich. In solchen Fällen kann die Replikation vollständig vom Quell-Core aus abgeschlossen werde.

Wenn Sie die Replikation für einen Core mit vorhandenen Wiederherstellungspunkten eingerichtet haben und eventuell eine Wiederherstellung auf Volume-Ebene durchführen müssen, wenn Sie eine BMR (Bare-Metal-Wiederherstellung) durchführen oder Daten von einem früheren Basisimage oder inkrementellen Snapshot wiederherstellen möchten, dann ist Seeding erforderlich. In diesen Fällen sollten Sie Ihre Seeding-Anforderungen und -Strategie überdenken. Überprüfen Sie die Informationen in diesem Thema und entscheiden, ob Sie ein Seeding auf Ihren Ziel-Core benötigen und welchen Ansatz Sie verwenden.

Ansätze in Hinblick auf das Seeding von Daten

Wenn Sie möchten, dass die replizierten Maschinen auf einem Ziel-Core Zugriff auf Daten erhalten, die zuvor auf dem ursprünglichen Quell-Core gespeichert waren, ist ein Seeding auf den Ziel-Core über eines der folgenden Verfahren erforderlich:

1. **Seeding auf den Ziel-Core über eine Netzwerkverbindung** Legen Sie beim Definieren der Replikation die Verwendung eines Seed-Laufwerks fest. Sie können dann den Ordner mit dem Seed-Laufwerk an den Ziel-Core freigeben und die Seed-Laufwerksdatei über das Netzwerk konsumieren. Für große Datenmengen oder langsame Verbindungen kann das Seeding anhand dieser Methode geraume Zeit dauern und erhebliche Netzwerkbandbreite beanspruchen.

   NOTE: Quest rät vom Seeding großer Datenmengen über eine Netzwerkverbindung ab. Beim ersten Seeding müssen u. U. sehr viele Daten übertragen werden, was eine typische WAN-Verbindung überlasten kann.

2. **Übertragen von Sicherungsdaten vom Quell-Core unter Verwendung physischer Speichermedien** Übertragen Sie die Seed-Laufwerksdatei auf einen portablen, externen Wechseldatenträger. Dieser Ansatz ist üblicherweise bei umfangreichen Datensets oder Standorten mit langsamen Netzwerkverbindungen nützlich. Zum Seeding anhand dieser Methode müssen Sie die folgenden Schritte ausführen:
   a. Erstellen Sie ein Seed-Archiv vom Quell-Core und speichern Sie dieses auf einem Wechseldatenträger.
   b. Bringen Sie das Seed-Laufwerk zum physischen Standort des Ziel-Core.
   c. Verbinden Sie das Laufwerk mit dem Ziel-Core.
   d. Konsumieren Sie die Daten vom Seed-Laufwerk auf dem Repository des Ziel-Core.

   Bei der Replikation auf einen Core eines Drittanbieters verbindet ein Vertreter des Rechenzentrums normalerweise das Medium, sobald dieses vom MSP empfangen wurde, und benachrichtigt Sie, sobald Sie die Seed-Daten im Core konsumieren (oder in diesem importieren) können.

   NOTE: Da große Datenmengen auf das Speichergerät kopiert werden müssen, wird eine eSATA-, USB 3.0- oder eine andere Hochgeschwindigkeitsverbindung empfohlen. Wenn die Gesamtgröße des Seed-Datenarchivs den auf dem Wechseldatenträger verfügbaren Speicherplatz überschreitet, kann sich das Archiv über mehrere Geräte erstrecken.

3. **Für Quell- und Ziel-Cores, die auf virtuellen Hosts gespeichert sind, übertragen Sie Sicherungsdaten mit einer virtuellen Festplatte**. Wenn sich Ihre Quell- und Ziel-Cores beide auf einem virtuellen Host befinden, können Sie ein Seed-Laufwerk auf virtuellen Speichermedien definieren und konsumieren. Zum Seeding anhand dieser Methode müssen Sie die folgenden Schritte ausführen:
   a. Erstellen Sie eine Seed-Laufwerksdatei vom Quell-Core und speichern Sie diese auf einem virtuellen Speichervolume.
   b. Trennen Sie das Volume vom Quell-Core und verbinden Sie es mit dem Ziel-Core.
   c. Konsumieren Sie die Daten vom Seed-Laufwerk auf dem Repository des Ziel-Core.

NOTE: Während die Replikation von inkrementellen Snapshots zwischen Quell- und Ziel-Cores erfolgen kann, bevor das Seeding abgeschlossen ist, bleiben die replizierten Snapshots, die von der Quelle auf das Ziel übertragen werden, solange „verwaist“, bis die ursprünglichen Daten konsumiert sind und die Snapshots mit den replizierten Basisabbildern kombiniert werden.

Zugehörige Links

- Einzelheiten zum Prozess des Konsumierens des Seed-Laufwerks finden Sie unter dem Thema Konsumieren des Seed-Laufwerks auf einem Ziel-Core.
- Weitere Informationen zu verwaisten Wiederherstellungspunkten finden Sie unter Löschen einer verwaisten Wiederherstellungspunktkette.
- Weitere Informationen zum Vorbereiten eines Seed-Laufwerks finden Sie unter Grundlegendes zu Seed-Laufwerken und Konsumieren des Seed-Laufwerks auf einem Ziel-Core.

See also: Konsumieren des Seed-Laufwerks auf einem Ziel-Core
See also: Löschen einer verwaisten Wiederherstellungspunktkette

Überlegungen zur Übertragungsleistung für Replikationsdaten

Wenn die Bandbreite zwischen den Quell- und Ziel-Cores die Übertragung von gespeicherten Wiederherstellungspunkten nicht aufnehmen kann, richten Sie eine Replikation ein und legen Sie die Verwendung eines Seed-Laufwerks fest. Dieser Prozess führt ein Seeding des Ziel-Cores mit Basisabbildern und Wiederherstellungspunkten von den ausgewählten Servern durch, die auf dem Quell-Core geschützt sind. Der Seeding-Vorgang kann jederzeit durchgeführt werden. Ein Seeding kann als Bestandteil der anfänglichen Datenübertragung durchgeführt werden, was als Grundlage für eine regelmäßige, geplante Replikation dient. Sie können auch ein Daten-Seeding für eine zuvor replizierte Maschine durchführen, wenn die Replikation angehalten oder gelöscht wurde. In diesem Fall können Sie mit der Option „Wiederherstellungspunktkette erstellen“ noch nicht replizierte Wiederherstellungspunkte auf ein Seed-Laufwerk replizieren.

Beim Vorbereiten der Replikation sollten Sie die folgenden Faktoren beachten:

- **Änderungsrate.** Die Änderungsrate ist die Rate, mit der sich der Umfang der geschützten Daten vergrößert. Die Rate hängt vom Datenvolumen ab, das auf geschützten Volumes geändert wird und vom Schutzintervall der Volumes. Einige Maschinentypen weisen typischerweise eine höhere Änderungsrate auf, z. B. ein Exchange E-Mail-Server. Eine Möglichkeit zur Reduzierung der Änderungsrate ist die Verringerung des Schutzintervalls.
- **Bandbreite.** Die Bandbreite ist die verfügbare Übertragungsgeschwindigkeit zwischen dem Quell- und dem Ziel-Core. Die Bandbreite muss unbedingt größer als die Änderungsrate sein, damit die Replikation mit den Wiederherstellungspunkten Schritt halten kann, die im Rahmen der Snapshots erstellt werden. Aufgrund der zwischen den Cores übertragenen Datenmenge sind eventuell mehrere parallele Streams mit Leitungsgeschwindigkeit erforderlich, um die Geschwindigkeit einer 1-GB-Ethernetverbindung zu erreichen.

  NOTE: Die von ISPs angegebene Bandbreite ist in der Regel die verfügbare Gesamtbandbreite. Alle Geräte im Netzwerk nutzen die ausgehende Bandbreite gemeinsam. Es muss sichergestellt sein, dass für die Replikation ausreichend freie Bandbreite für die Änderungsrate zur Verfügung steht.
- **Anzahl der geschützten Maschinen.** Es muss berücksichtigt werden, wie viele Maschinen pro Quell-Core geschützt werden und wie viele davon auf den Ziel-Core repliziert werden sollen. Es ist nicht erforderlich, jede auf dem Quell-Core geschützte Maschine zu replizieren. Mit Rapid Recovery können Sie jede geschützte Maschine einzeln replizieren, sodass Sie auch nur bestimmte Maschinen zur Replikation auswählen können. Wenn alle geschützten Maschinen auf einem Quell-Core repliziert werden müssen, ist die Änderungsrate in der Regel höher. Dieser Faktor ist relevant, wenn die Bandbreite zwischen Quell- und Ziel-Cores für die Menge und Größe der replizierten Wiederherstellungspunkte nicht ausreicht.

Die folgende Tabelle „Maximale Änderungsrate für WAN-Verbindungstypen“ enthält einige Beispiele für die erforderliche Bandbreite pro Gigabyte für eine zumutbare Änderungsrate.

Tabelle 89. Beispiele für Bandbreite pro Gigabyte

WAN-Typ	Bandbreite	Max. Änderungsrate
DSL	768 KBit/s und mehr	330MB pro Stunde
Kabel	1 MBit/s und mehr	429MB pro Stunde
T1	1,5 MBit/s und mehr	644MB pro Stunde
Glasfaser	20 MBit/s und mehr	8,38GB pro Stunde

NOTE: Für optimale Ergebnisse befolgen Sie bitte die Empfehlungen in der nachfolgenden Tabelle.

Bei einem Verbindungsausfall während der Datenübertragung wird die Replikation vom letzten Fehlerpunkt der Übertragung wieder aufgenommen (nachdem die Verbindung wieder funktionsfähig ist).

Abhängig von der Netzwerkkonfiguration kann die Replikation ein zeitaufwendiger Vorgang sein. Stellen Sie sicher, dass Sie genügend Bandbreite für die Replikation und andere Rapid Recovery-Übertragungen wie Backups sowie für andere kritische Anwendungen zur Verfügung haben, die Sie ausführen müssen.

Wenn Probleme bei der Übertragung von Daten über das Netzwerk auftreten – insbesondere für bestimmte geschützte oder replizierte Maschinen – sollten Sie die Datenübertragungsrate für diese Maschinen anpassen. Weitere Informationen finden Sie unter Informationen über das Ändern von Übertragungseinstellungen und Einschränkung der Übertragungsrate.

Informationen zu Replikation und verschlüsselten Wiederherstellungspunkten

Das Seed-Laufwerk enthält keine Sicherungen der Registrierung und Zertifikate des Quell-Core. Es enthält allerdings die Verschlüsselungsschlüssel des Quell-Core, wenn die Wiederherstellungspunkte, die vom Quell- zum Ziel-Core repliziert werden, verschlüsselt sind. Die replizierten Wiederherstellungspunkte bleiben verschlüsselt, nachdem sie auf den Ziel-Core übertragen wurden. Die Besitzer oder Administratoren des Ziel-Core benötigen die Passphrase, um die verschlüsselten Daten wiederherzustellen.

Informationen zu Aufbewahrungsrichtlinien für die Replikation

Die Aufbewahrungsrichtlinien auf dem Quell- und dem Ziel-Core werden nicht synchronisiert. Rollup- und Ad-hoc-Löschung werden auf jedem Core bei der ersten Maßnahme unabhängig voneinander durchgeführt.

Weitere Informationen zu Aufbewahrungsrichtlinien finden Sie unter Verwalten von Aufbewahrungsrichtlinien.

Anzeigen von ein- und ausgehender Replikation

Wenn Sie auf das Symbol **Replikation** in der Symbolleiste klicken, wird die Seite **Replikation** angezeigt. Diese Seite bietet Ihnen einen Einblick in eine Replikation von der Sicht dieses Core aus. Sie umfasst zwei Fensterbereiche:

- Im Fensterbereich **Ausgehende Replikation** sind alle geschützten Maschinen in diesem Core aufgelistet, die auf einem anderen Core repliziert werden.
- Im Fensterbereich **Eingehende Replikation** werden die Maschinen aufgelistet, die auf diesen Core repliziert wurden, sowie der Quell-Core, von dem diese Maschinen repliziert werden.

In diesem Abschnitt werden die in diesen Fensterbereichen angezeigten Informationen beschrieben.

Informationen zur eingehenden Replikation von diesem Rapid Recovery Core sind in der folgenden Tabelle beschrieben.

Tabelle 90. Informationen über ausgehende Replikation

UI-Element	Description
Element auswählen	Sie können für jede Zeile in der Übersichtstabelle das Kontrollkästchen aktivieren, um Aktionen aus der Liste der Menüoptionen oberhalb der Tabelle auszuführen.
Typ	Zeigt den Maschinentyp an. Sie können einen Ziel-Core erweitern, um einzelne replizierte Maschinen anzuzeigen.
Statusanzeige	Status der Replikation. Farbige Kreise in der Statusspalte zeigen an, ob eine replizierte Maschine online oder nicht erreichbar ist. Wenn Sie den Cursor über den farbigen Kreis bewegen, wird die Statusbedingung angezeigt. Statusbedingungen sind grün (Replikation eingerichtet und online), gelb (Replikation vorübergehend deaktiviert), rot (Authentifizierungsfehler) und grau (offline oder nicht erreichbar).
Replication Name (Name der Replikation)	Der Anzeigename der Core-Maschine, auf die Maschinen aus diesem Quell-Core repliziert werden.
Maschinen	Listet die Anzahl der replizierten Maschinen auf den ausgewählten Ziel-Core auf.
Sync	Das Datum und die Uhrzeit der letzten Replikationsübertragung auf den Ziel-Core.
	Wenn Sie auf das Drop-Down-Menü „Mehr“ in dieser Spalte klicken, sehen Sie eine Liste der Aktionen, die Sie für die spezifische Replikationsbeziehung durchführen müssen.

Sie können Aktionen für zwei oder mehr Ziel-Cores durchführen, die im Raster „Ausgehende Replikation“ aufgelistet werden. Um Aktionen für mehrere Ziel-Cores durchzuführen, markieren Sie das Kontrollkästchen für jeden Core im Raster und wählen Sie aus dem Menü oberhalb des Rasters die gewünschte Aktion aus. Sie können die in folgender Tabelle beschriebenen Aktionen ausführen.

Tabelle 91. Globale Aktionen verfügbar im Fensterbereich „Ausgehende Replikation“

UI-Element	Description
Ziel-Core hinzufügen	Können Sie einen anderen Ziel-Core definieren, um auf diesem Quell-Core geschützte Maschinen zu replizieren.
Aktualisieren	Aktualisiert die in der Tabelle gezeigten Informationen.
Erzwingen	Erzwingt die Replikation.
Vorübergehend deaktivieren	Hält die Replikation vorübergehend an.
Fortsetzen	Nimmt eine angehaltene Replikation wieder auf.
Kopieren	Öffnet den Replikationsassistenten, mit dem Sie vorhandene Wiederherstellungspunkte für ausgewählte geschützte Maschinen auf ein Seed-Laufwerk kopieren können.
Löschen	Löscht die ausgehende Replikation.
Seed-Laufwerke	Diese Menüoption wird angezeigt, wenn Daten auf ein Seed-Laufwerk kopiert wurden, wenn Replikation eingerichtet war.

UI-Element	Description
	Zeigt Informationen über die Seed-Laufwerksdatei an, einschließlich Datum und Uhrzeit des Speicherns des Seed-Laufwerks. Reduzierbare Menüs zeigen den Ziel-Core und die geschützten Maschinen an, aus denen die Seed-Laufwerksdateien erzeugt wurden.
	Wenn Sie auf das Drop-Down-Menü „Mehr“ in dieser Spalte klicken, sehen Sie eine Liste der Aktionen, die Sie für die spezifische Replikationsbeziehung durchführen müssen.

Informationen zur eingehenden Replikation von einem anderen Core sind in der folgenden Tabelle beschrieben.

Tabelle 92. Informationen über eingehende Replikation

UI-Element	Description
Element auswählen	Sie können für jede Zeile in der Übersichtstabelle das Kontrollkästchen aktivieren, um Aktionen aus der Liste der Menüoptionen oberhalb der Tabelle auszuführen.
Typ	Zeigt den Maschinentyp an. Sie können einen Quell-Core erweitern, um einzelne replizierte Maschinen anzuzeigen.
Statusanzeige	Status der Replikation. Farbige Kreise in der Statusspalte zeigen an, ob eine replizierte Maschine online oder nicht erreichbar ist. Wenn Sie den Cursor über den farbigen Kreis bewegen, wird die Statusbedingung angezeigt. Statusbedingungen sind grün (Replikation eingerichtet und online), gelb (Replikation vorübergehend deaktiviert), rot (Authentifizierungsfehler) und grau (offline oder nicht erreichbar).
Replication Name (Name der Replikation)	Der Anzeigename der Quell-Core-Maschine mit geschützten Maschinen, die auf diesen Ziel-Core repliziert werden. Dieser Name kann beim Einrichten der Replikation auf dem Quell-Core mithilfe des Replikationsassistenten optional angegeben werden.
Maschinen	Listet die Anzahl der geschützten Maschinen auf dem Quell-Core auf, die auf diesen Ziel-Core repliziert werden.
Sync	Das Datum und die Uhrzeit der letzten Replikationsübertragung vom Quell-Core.
	Wenn Sie auf das Drop-Down-Menü „Mehr“ in dieser Spalte klicken, sehen Sie eine Liste der Aktionen, die Sie für die spezifische Replikationsbeziehung durchführen müssen.

Sie können Aktionen für zwei oder mehr Quell-Cores durchführen, die im Raster „Eingehende Replikation“ aufgelistet werden. Um Aktionen für mehrere Quell-Cores durchzuführen, markieren Sie das Kontrollkästchen für jeden Core im Raster und wählen Sie aus dem Menü oberhalb des Rasters die gewünschte Aktion aus. Sie können die in folgender Tabelle beschriebenen Aktionen ausführen.

Tabelle 93. Globale Aktionen verfügbar im Fensterbereich "Eingehende Replikation"

UI-Element	Description
Aktualisieren	Aktualisiert die in der Tabelle gezeigten Informationen.
Erzwingen	Erzwingt die Replikation.
Vorübergehend deaktivieren	Hält die Replikation vorübergehend an.

UI-Element	Description
Fortsetzen	Nimmt eine angehaltene Replikation wieder auf.
Löschen	Löscht die eingehende Replikation.

Konfigurieren der Replikation

Um Daten mit Rapid Recovery zu replizieren, müssen Sie den Quell-Core und den Ziel-Core für die Replikation konfigurieren. Nachdem die Replikation konfiguriert wurde, können Sie die Daten der geschützten Maschine replizieren, die Replikation überwachen und verwalten sowie Wiederherstellungen durchführen.

NOTE: Wenn Sie Daten für einen Cluster replizieren, müssen Sie den gesamten Cluster replizieren. Wenn Sie zum Beispiel einen Knoten zum Replizieren auswählen, wird der Cluster automatisch ausgewählt. Wenn Sie entsprechend den Cluster auswählen, werden alle Knoten in diesem Cluster ebenfalls aktiviert.

Zur Durchführung von Replikationen in Rapid Recovery müssen Sie die folgenden Vorgänge ausführen:

- Einrichten eines Repositorys auf dem Ziel-Core. Weitere Informationen zum Hinzufügen eines Repositorys zum Ziel-Core finden Sie unter Erstellen eines DVM-Repository.
- Konfigurieren der selbstverwalteten Replikation. Weitere Informationen zur Replikation auf einen selbstverwalteten Ziel-Core finden Sie unter Replikation auf einen selbstverwalteten Ziel-Core.
- Konfigurieren der Replikation zu einem externen Anbieter. Weitere Informationen zur Replikation auf den Ziel-Core eines externen Anbieters finden Sie unter Replikation auf den Ziel-Core eines externen Anbieters.
- Replikation einer vorhandenen geschützten Maschine. Weitere Informationen zum Replizieren einer geschützten Maschine, die bereits vom Quell-Core geschützt wird, finden Sie unter Hinzufügen einer Maschine zu einer bestehenden Replikation.
- Konsumieren des Seed-Laufwerks. Weitere Informationen zum Konsumieren der Seed-Laufwerksdaten auf dem Ziel-Core finden Sie unter Konsumieren des Seed-Laufwerks auf einem Ziel-Core.
- Festlegen der Replikationspriorität für eine geschützte Maschine. Weitere Informationen zum Priorisieren der Replikation von geschützten Maschinen finden Sie unter Festlegen der Replikationspriorität für eine geschützte Maschine.
- Festlegen eines Replikationszeitplans für eine geschützte Maschine. Weitere Informationen zum Festlegen eines Replikationszeitplans finden Sie unter Planen der Replikation.
- Bedarfsabhängige Überwachung der Replikation. Weitere Informationen zur Überwachung der Replikation finden Sie unter Anzeigen von ein- und ausgehender Replikation.
- Bedarfsabhängige Verwaltung der Replikationseinstellungen. Weitere Informationen zur Verwaltung der Replikationseinstellungen finden Sie unter Verwalten der Replikationseinstellungen.
- Wiederherstellen replizierter Daten im Notfall oder bei Datenverlust. Weitere Informationen zur Wiederherstellung replizierter Daten finden Sie unter Wiederherstellen von replizierten Daten.

Replikation auf einen selbstverwalteten Ziel-Core

Diese Konfiguration gilt für die Replikation an einen externen Standort sowie für die gegenseitige Replikation. Die folgenden Schritte sind Voraussetzung:

- Der Rapid Recovery Core muss auf allen Quell- und Zielmaschinen installiert sein.
- Wenn Sie Rapid Recovery für eine Mehrpunkt-zu-Punkt Replikation konfigurieren, müssen Sie diese Aufgabe auf allen Quell-Cores sowie auf dem Ziel-Core ausführen. Beschreibungen zu diesen Replikationskonfigurationen finden Sie unter Replikation.
- Wenn Sie ein Seed-Laufwerk erstellen und an ein physisches Wechselspeicher-Volume übertragen müssen, um die Erstübertragung vorhandener Wiederherstellungspunkte durchzuführen, müssen Sie geeignetes tragbares Speichergerät zur Hand haben. Außerdem müssen Sie über direkten Zugriff auf die Quell-Core-Maschine verfügen, um das Laufwerk für die Kopie des Seed-Laufwerkarchivs anzuschließen.
- Bei Verwendung eines Seed-Laufwerks in einem selbstverwaltenden Ziel-Core müssen Sie oder ein vertrauenswürdiger Administrator über physischen Zugang zum Ziel-Core verfügen.

Ein selbstverwalteter Ziel-Core ist ein Core, zu dem Sie Zugang haben. Zum Beispiel wird ein selbstverwalteter Core häufig von Ihrem Unternehmen an einem externen Standort verwaltet oder an einem anderen geographischen Ort als der Quell-Core gehostet. Die Replikation kann vollständig im Quell-Core eingerichtet werden, sofern kein Daten-Seeding mithilfe eines Seed-Laufwerks notwendig ist. In diesen Fällen müssen Sie ein Seed-Laufwerk unter Verwendung dieses Verfahrens erstellen und später befestigen das Seed-Laufwerk mit dem Ziel-Core verbinden, um die archivierten Wiederherstellungspunkt-Daten zu konsumieren. Weitere Informationen hierzu finden Sie unter Bestimmen der Seeding-Anforderungen und -Strategie.

Führen Sie die folgenden Schritte aus, um den Quell-Core für die Replikation auf einen selbstverwalteten Ziel-Core zu konfigurieren.

1. Navigieren Sie zu Rapid Recovery Core Console des Quell-Cores.
2. Klicken Sie auf der Schaltflächenleiste auf **Replizieren**.

   Der **Replikationsassistent** wird geöffnet.
3. Wenn Sie die Replikation mit einem Ziel-Core aufbauen, der zuvor mit diesem Quell-Core gekoppelt wurde, wählen Sie auf der Seite **Target Core** (Ziel-Core) des Replikationsassistenten die Option **Use an existing target Core** (Einen vorhandenen Ziel-Core auswählen) und anschließend den entsprechenden Ziel-Core aus der Dropdownliste aus. Fahren Sie mit Schritt 5 fort.
4. Wenn Sie die Replikation mit einem Ziel-Core zum ersten Mal von diesem Quell-Core aufbauen, wählen Sie auf der Seite **Target Core** (Ziel-Core) des Replikationsassistenten die Option **I have my own Target Core** (Ich habe meinen eigenen Ziel-Core) aus und geben Sie anschließend die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 94. Informationen zum Ziel-Core

Textfeld	Description
Hostname	Geben Sie den Hostnamen oder die IP-Adresse der Core-Maschine ein, auf die Daten repliziert werden.
Port	Geben Sie die Portnummer ein, über die der Rapid Recovery Core mit der Maschine kommuniziert. Die Standardportnummer ist 8006.

Textfeld	Description
Benutzername	Geben Sie den Benutzernamen für den Zugriff auf den Core ein.
Kennwort	Geben Sie das Kennwort für den Zugriff auf den Core ein.

5. Klicken Sie auf **Weiter**.

   NOTE: Wenn auf dem Ziel-Core kein Repository vorhanden ist, wird eine Warnung mit dem Hinweis angezeigt, dass Sie den Quell-Core zwar mit dem Ziel-Core koppeln können, Agenten (geschützte Maschinen) aber erst dorthin replizieren können, nachdem ein Repository eingerichtet wurde. Weitere Informationen über die Einrichtung eines Repository für einen Core finden Sie unter Erstellen eines DVM-Repository.

6. Geben Sie auf der Seite **Request** (Anforderung) einen Namen für diese Replikationskonfiguration ein, z. B. „SourceCore1“. Hierbei handelt es sich um den Anzeigenamen für den Bereich „Incoming Replication“ (Eingehende Replikation) auf der Replikationsseite des Ziel-Core.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Protected Machines** (Geschützte Maschinen) die geschützten Maschinen aus, die repliziert werden sollen, und wählen Sie in den Dropdown-Listen in der Spalte „Repository“ ein Repository für jede geschützte Maschine aus.
9. Führen Sie die folgenden Schritte aus, wenn Sie ein Seeding für die Übertragung der Basisdaten durchführen möchten: Wenn Sie kein Seeding Ihrer Daten durchführen möchten fahren Sie mit dem nächsten Schritt fort.

   NOTE: Da große Datenmengen auf den Wechseldatenträger kopiert werden müssen, empfiehlt Quest eine eSATA-, USB 3.0- oder eine andere Hochgeschwindigkeitsverbindung zum Wechseldatenträger.

   a. Wählen Sie auf der Seite **Protected Machines** (Geschützte Maschinen) die Option **Use a seed drive to perform the initial transfer** (Ein Seed-Laufwerk für Erstübertragung verwenden) aus.

   - Wenn derzeit eine oder mehr geschützte Maschinen auf einen Ziel-Core replizieren, können Sie diese geschützten Maschinen in das Seed-Laufwerk einbeziehen, indem Sie **Include already replicated recovery points in the seed drive** (Bereits replizierte Wiederherstellungspunkte im Seed-Laufwerk einbeziehen) auswählen.
   - Wählen Sie **Replikation vorerst anhalten** aus, wenn die Replikation nicht sofort nach Abschluss dieses Verfahrens beginnen soll.

     NOTE: Wenn Sie diese Option auswählen, beginnt die Replikation erst, bis Sie sie explizit fortzusetzen. Weitere Informationen hierzu finden Sie unter Anhalten und Fortsetzen der Replikation.

   b. Klicken Sie auf **Weiter**.
   c. Wählen Sie auf der Seite **Seed Drive Location** (Seed-Laufwerkspeicherort) des Replikationsassistenten in der Dropdownliste **Location type** (Typ des Speicherorts) einen der folgenden Zieltypen aus:

   - Lokal
   - Netzwerk
   - Cloud

   d. Geben Sie im Feld „Speicherort“ die in der folgenden Tabelle beschriebenen Details für die Seed-Laufwerkdatei auf Basis der Position, die Sie in Schritt c ausgewählt haben, ein.

Tabelle 95. Archivierungsdetails

Option	Textfeld	Description
Lokal	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Seed-Laufwerkarchiv gespeichert werden soll, z. B. `D:\work\archive`.
Netzwerk	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Seed-Laufwerkarchiv gespeichert werden soll, z. B. `\\servername\sharename`.
	Benutzername	Geben Sie einen Benutzernamen ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
	Kennwort	Geben Sie ein Kennwort für den Netzwerkpfad ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **NOTE:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen hierzu finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.
	Ordnername	Geben Sie einen Namen für den Ordner ein, in dem die archivierten Daten gespeichert werden sollen. Der Standardname lautet „Rapid-Recovery-Archive-[ERSTELLUNGSDATUM]-[ERSTELLUNGSZEIT]“.

e. Klicken Sie auf **Weiter**.

f. Geben Sie auf der Seite **Seed Drive Options** (Seed-Laufwerkoptionen) des Replikationsassistenten die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 96. Seed-Laufwerkoptionen

Element	Description
Maximale Größe	Umfangreiche Datenarchive können in mehrere Segmente aufgeteilt werden. Wählen Sie die maximale Größe des Segments aus, die zum Erstellen des Seed-Laufwerks reserviert werden soll. Führen Sie dazu einen der folgenden Schritte aus: • Wählen Sie **Entire Target** (Gesamtes Ziel) aus, um den gesamten verfügbaren Speicherplatz im Pfad, der auf der Seite „Seed Drive Location“ (Seed-Laufwerkspeicherort) für das Ziel angegeben wurde, zu reservieren. Wenn z. B. der Speicherort `D:\work\archive` ist, wird der gesamte verfügbare Speicherplatz auf Laufwerk D: reserviert, wenn dieser zum Kopieren des Seed-Laufwerks benötigt wird. Er wird jedoch nicht unmittelbar nach dem Start des Kopiervorgangs reserviert. • Geben Sie in das Textfeld einen Wert ein und wählen Sie dann eine Maßeinheit in der Dropdownliste aus, um den maximal reservierten Speicherplatz festzulegen. Der Standardwert ist 250MB.

Element	Description
Recyclingaktion	Falls der Pfad bereits ein Seed-Laufwerk enthält, wählen Sie eine der folgenden Optionen aus: • **Do not reuse** (Nicht wiederverwenden). Vorhandene Seed-Daten am Speicherort werden nicht überschrieben oder gelöscht. Wenn der Speicherort nicht leer ist, können keine Daten in das Seed-Laufwerk geschrieben werden. • **Replace this Core** (Diesen Core ersetzen). Alle bereits vorhandenen Daten auf dem Core werden überschrieben. Die Daten anderer Cores bleiben aber unverändert. • **Erase completely** (Vollständig löschen). Alle Seed-Daten werden aus dem Verzeichnis gelöscht, bevor das Seed-Laufwerk geschrieben wird.
Anmerkung	Geben Sie eine Anmerkung ein, die das Seed-Laufwerk beschreibt.
Alle Agenten zum Seed-Laufwerk hinzufügen	Wählen Sie diese Option aus, um alle geschützten Maschinen im Quell-Core mit dem Seed-Laufwerk zu replizieren. Diese Option ist standardmäßig ausgewählt.
„Build recovery point chains (fix orphans)“ (Wiederherstellungspunktketten erstellen (Waisen korrigieren))	Wählen Sie diese Option aus, um die gesamte Wiederherstellungspunktkette auf das Seed-Laufwerk zu replizieren. Hierdurch werden einige bereits replizierte Wiederherstellungspunkte zum Seed-Laufwerk hinzugefügt, um zu verhindern, dass Waisen auftreten. Diese Option ist standardmäßig ausgewählt. **NOTE:** Beim Seeding in AppAssure 5.4 werden normalerweise nur die letzten Wiederherstellungspunkte auf das Seed-Laufwerk repliziert, um Zeitaufwand und Speicherplatz zum Erstellen des Seed-Laufwerks zu verringern. Wenn Wiederherstellungspunktketten auf dem Seed-Laufwerk erstellt werden sollen, muss auf dem Seed-Laufwerk genügend Speicherplatz zum Speichern der letzten Wiederherstellungspunkte der angegebenen geschützten Maschine oder Maschinen vorhanden sein. Dieser Vorgang kann entsprechend länger dauern.

g. Führen Sie eine der folgenden Aktionen aus:

- Wenn Sie die Markierung des Kontrollkästchens **Alle Agenten dem Seed-Laufwerk hinzufügen** entfernt haben, klicken Sie auf **Weiter**.
- Wenn Sie **Alle Agenten zum Seed-Laufwerk hinzufügen** aktiviert haben, gehen Sie weiter zu Schritt 10.

10. Klicken Sie auf **Fertig stellen**.
11. Transportieren Sie ggf. das erstellte Seed-Laufwerk zum Ziel-Core.

    Damit ist die Kopplung von Quell- und Ziel-Core abgeschlossen.

Wenn Sie die Option zum anfänglichen Anhalten der Replikation nicht ausgewählt haben, wird der Replikationsvorgang gleich gestartet.

1. Wenn Sie die Option für die Verwendung eines Seed-Laufwerks ausgewählt haben, erstellt die Replikation verwaiste Wiederherstellungspunkte auf dem Ziel-Core, bis das Seed-Laufwerk belegt ist, und stellt die erforderlichen Basisabbilder bereit.
2. Wenn Sie die Nutzung eines Laufwerks angegeben haben, übertragen Sie die Archivdatei des Seed-Laufwerks auf ein Volume (freigegebener Ordner, virtuelles Laufwerk oder Wechselspeichermedien). Belegen Sie dann das Seed-Laufwerk.

See also: Hinzufügen eines Cloud-Kontos
See also: Erstellen eines DVM-Repository
See also: Replikation mit Rapid Recovery
See also: Bestimmen der Seeding-Anforderungen und -Strategie

See also: Replikation

Replikation auf den Ziel-Core eines externen Anbieters

Bei einem Core eines externen Anbieters handelt es sich um einen Ziel-Core, der von einem MSP unterhalten und verwaltet wird. Für eine Replikation auf einen Core, der von einem externen Anbieter verwaltet wird, muss der Kunden keinen Zugriff auf den Ziel-Core haben.

Bei der Replikation auf den Core eines externen Anbieters müssen vom Kunden und vom externen Anbieter bestimmte Aufgaben ausgeführt werden. Nachdem ein Kunde eine Replikationsanforderung für einen Quell-Core gesendet hat, muss der MSP die Konfiguration im Ziel-Core vornehmen, indem er die Anforderung überprüft.

NOTE: Diese Konfiguration gilt für gehostete und Cloud-Replikation. Der Rapid Recovery Core muss auf allen Quell-Core-Maschinen installiert sein. Wenn Sie Rapid Recovery für eine Mehrpunkt-zu-Punkt Replikation konfigurieren, müssen Sie diese Aufgabe auf allen Quell-Cores ausführen.

Sie müssen die folgenden Aufgaben ausführen, um Daten auf einen Ziel-Core zu replizieren, der von einem externen Anbieter verwaltet wird:

- Senden einer Replikationsanforderung an einen externen Dienstanbieter
- Überprüfen einer Replikationsanforderung von einem Kunden
- Ignorieren einer Replikationsanforderung von einem Kunden

Senden einer Replikationsanforderung an einen externen Dienstanbieter

Führen Sie als Endbenutzer, der einen Core abonniert hat, der extern verwaltet wird, z. B. durch einen MSP, die nachstehend aufgeführten Schritte aus, um eine Replikationsanforderung an den externen Dienstanbieter zu senden.

1. Navigieren Sie zum Rapid Recovery Core.
2. Klicken Sie auf der Symbolleiste auf **Replizieren**.

   Der **Replikationsassistent** wird geöffnet.
3. Wählen Sie auf der Seite **Ziel-Core** des Replikationsassistenten **Ich habe ein Abonnement bei einem Drittanbieter für Offsite-Sicherungs- und Notfallwiederherstellungsdienste** und geben Sie die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 97. Informationen zum externen Ziel-Core

Textfeld	Description
Hostname	Geben Sie den Hostnamen, die IP-Adresse oder FQDN für die externe Core-Maschine ein.
Port	Geben Sie die Portnummer ein, die Sie vom externen Dienstanbieter erhalten haben. Die Standardportnummer ist 8006.

- Wenn der Core, der hinzugefügt werden soll, zuvor mit diesem Quell-Core gepaart wurde, können Sie wie folgt vorgehen:

1. Wählen Sie **Vorhandenen Ziel-Core verwenden** aus.
2. Wählen Sie den Ziel-Core in der Dropdown-Liste aus.
3. Klicken Sie auf **Weiter**.
4. Fahren Sie mit Schritt 7 fort.

4. Klicken Sie auf **Weiter**.
5. Geben Sie auf der Seite **Anforderung** des Replikationsassistenten die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 98. Details zum externen Ziel-Core

Textfeld	Description
E-Mail-Adresse	Geben Sie die E-Mail-Adresse für das Abonnement des externen Dienstes an.
Kunden-ID (optional)	Geben Sie die Kundennummer ein, die vom Dienstanbieter zugewiesen wurde (optional).

6. Klicken Sie auf **Weiter**.
7. Wählen Sie auf der Seite **Geschützte Maschinen** die geschützten Maschinen aus, die auf den externen Core repliziert werden sollen.
8. Führen Sie die folgenden Schritte aus, wenn Sie ein Seeding für die Übertragung der Basisdaten durchführen möchten:

NOTE: Da große Datenmengen auf den Wechseldatenträger kopiert werden müssen, wird eine eSATA-, USB 3.0- oder eine andere Hochgeschwindigkeitsverbindung zum Wechseldatenträger empfohlen.

a. Wählen Sie auf der Seite **Geschützte Maschinen** des Replikationsassistenten die Option **Seed-Laufwerk für Erstübertragung verwenden** aus.

- Wenn derzeit geschützte Maschinen auf einen Ziel-Core replizieren, können Sie diese Maschinen in das Seed-Laufwerk einbeziehen, indem Sie die Option **Include already replicated recovery points in the seed drive** (Bereits replizierte Wiederherstellungspunkte auf Seed-Laufwerk einbeziehen) auswählen.

b. Klicken Sie auf **Weiter**.

c. Wählen Sie auf der Seite **Seed-Laufwerkspeicherort** des Replikationsassistenten in der Dropdown-Liste **Speicherort** einen der folgenden Zieltypen aus:

- Lokal
- Netzwerk
- Cloud

d. Geben Sie die in der folgenden Tabelle beschriebenen Details für das Archiv auf Basis der Position, die Sie in Schritt c ausgewählt haben, ein.

Tabelle 99. Archivierungsdetails

Option	Textfeld	Description
Lokal	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. `D:\Arbeit\Archiv`
Netzwerk	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. `\\Servername\Freigabename`.

Option	Textfeld	Description
	Benutzername	Geben Sie einen Benutzernamen ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
	Kennwort	Geben Sie ein Kennwort für den Netzwerkpfad ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **NOTE:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen hierzu finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.
	Ordnername	Geben Sie einen Namen für den Ordner ein, in dem die archivierten Daten gespeichert werden sollen. Der Standardname lautet „Rapid-Recovery-Archive-[ERSTELLUNGSDATUM]-[ERSTELLUNGSZEIT]“.

e. Klicken Sie auf **Weiter**.

f. Geben Sie auf der Seite **Seed-Laufwerkoptionen** des Replikationsassistenten die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 100. Seed-Laufwerkoptionen

Element	Description
Maximale Größe	Umfangreiche Datenarchive können in mehrere Segmente aufgeteilt werden. Wählen Sie den maximalen Speicherplatz aus, der zum Erstellen des Seed-Laufwerks reserviert werden soll. Führen Sie dazu einen der folgenden Schritte aus: • Wählen Sie **Gesamtes Ziel** aus, um den gesamten verfügbaren Speicherplatz im Pfad, der auf der Seite „Seed-Laufwerkspeicherort“ angegeben wurde, zu reservieren. (Wenn beispielsweise „D:\Arbeit\Archiv“ als Speicherort angegeben wurde, wird der gesamte verfügbare Speicherplatz auf dem Laufwerk D: reserviert.) • Geben Sie in das leere Textfeld einen Wert ein und wählen Sie dann eine Maßeinheit in der Dropdown-Liste aus, um den maximal reservierten Speicherplatz festzulegen.
Recyclingaktion	Falls der Pfad bereits ein Seed-Laufwerk enthält, wählen Sie eine der folgenden Optionen aus: • **Do not reuse** (Nicht wiederverwenden). Vorhandene Seed-Daten am Speicherort werden nicht überschrieben oder gelöscht. Wenn der Speicherort nicht leer ist, können keine Daten in das Seed-Laufwerk geschrieben werden. • **Replace this Core** (Diesen Core ersetzen). Alle bereits vorhandenen Daten auf dem Core werden überschrieben. Die Daten anderer Cores bleiben aber unverändert. • **Erase completely** (Vollständig löschen). Alle Seed-Daten werden aus dem Verzeichnis gelöscht, bevor das Seed-Laufwerk geschrieben wird.

Element	Description
Anmerkung	Geben Sie eine Anmerkung ein, die das Seed-Laufwerk beschreibt.
Alle Agenten zum Seed-Laufwerk hinzufügen	Wählen Sie diese Option aus, um alle geschützten Maschinen im Quell-Core mit dem Seed-Laufwerk zu replizieren. Diese Option ist standardmäßig ausgewählt.
Wiederherstellungspunktkette erstellen (Waisen korrigieren)	Wählen Sie diese Option aus, um die gesamte Wiederherstellungspunktkette auf das Seed-Laufwerk zu replizieren. Diese Option ist standardmäßig ausgewählt. **NOTE:** Beim Seeding in AppAssure 5.4 werden normalerweise nur die letzten Wiederherstellungspunkte auf das Seed-Laufwerk repliziert, um Zeitaufwand und Speicherplatz zum Erstellen des Seed-Laufwerks zu verringern. Wenn Wiederherstellungspunktketten auf dem Seed-Laufwerk erstellt werden sollen, muss auf dem Seed-Laufwerk genügend Speicherplatz zum Speichern der letzten Wiederherstellungspunkte der angegebenen geschützten Maschinen vorhanden sein. Dieser Vorgang kann entsprechend länger dauern.

g. Führen Sie eine der folgenden Aktionen aus:

- Wenn Sie die Markierung des Kontrollkästchens **Alle Agenten dem Seed-Laufwerk hinzufügen** entfernt haben, klicken Sie auf **Weiter**.
- Wenn Sie **Alle Agenten zum Seed-Laufwerk hinzufügen** aktiviert haben, gehen Sie weiter zu Schritt 9.

h. Wählen Sie auf der Seite **Maschinen** des Replikationsassistenten die geschützten Maschinen aus, die mit dem Seed-Laufwerk auf den Ziel-Core repliziert werden sollen.

9. Klicken Sie auf **Fertig stellen**.
10. Senden Sie ggf. das erstellte Seed-Laufwerk an den externen Dienstanbieter. Befolgen Sie dazu dessen Anweisungen.

Überprüfen einer Replikationsanforderung von einem Kunden

Nachdem ein Benutzer die Schritte in Senden einer Replikationsanforderung an einen externen Dienstanbieter durchgeführt hat, wird von Quell-Core eine Replikationsanforderung an den externen Ziel-Core gesendet. Der externe Anbieter kann die Anforderung überprüfen und genehmigen, damit die Replikation für den Kunden durchgeführt wird, oder die Anforderung ablehnen, sodass keine Replikation stattfindet.

Wählen Sie eine der folgenden Optionen aus:

- Genehmigen einer Replikationsanforderung
- Ablehnen einer Replikationsanforderung

Genehmigen einer Replikationsanforderung

Führen Sie die folgenden Schritte aus, um eine Replikationsanforderung auf einem externen Ziel-Core zu genehmigen.

1. Auf dem Ziel-Core navigieren Sie zur Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Replikation).

Die Seite **Replikation** wird angezeigt.

3. Klicken Sie auf der Seite **Replikation** auf **Anforderung (#)**.

   Der Abschnitt **Anstehende Replikationsanforderungen** wird angezeigt.

4. Klicken Sie unter „Anstehende Replikationsanforderungen“ auf das Dropdown-Menü neben der Anforderung, die überprüft werden soll, und klicken Sie dann auf **Überprüfen**.

   Das Fenster **Replikationsanfragen überprüfen** wird angezeigt.

   NOTE: Die im Abschnitt „Quell-Core-Identität“ dieses Fensters angezeigten Informationen stammen aus der Anforderung des Kunden.

5. Führen Sie unter „Quell-Core-Identität“ eine der folgenden Aktionen aus:

   - Wählen Sie **Vorhandenen replizierten Kern ersetzen** aus, und wählen Sie dann einen Kern aus der Dropdown-Liste aus.
   - Wählen Sie **Neuen Quell-Core erstellen** aus und überprüfen Sie dann, ob Core-Name, E-Mail-Adresse des Kunden und Kunden-ID richtig sind. Bearbeiten Sie ggf. die Informationen.

6. Wählen Sie unter „Agenten“ die Maschinen aus, für die die Genehmigung gilt, und wählen Sie in den Dropdown-Listen in der Spalte „Repository“ das entsprechende Repository für die einzelnen Agenten aus.
7. Geben Sie optional im Textfeld **Anmerkung** eine Beschreibung oder Nachricht ein, die in die Antwort an den Kunden aufgenommen werden soll.
8. Klicken Sie auf **Antwort senden**.

   Die Replikation wird akzeptiert.

Ablehnen einer Replikationsanforderung

Führen Sie die folgenden Schritte aus, um eine Replikationsanforderung abzulehnen, die von einem Kunden an einen externen Core gesendet wurde.

Informationen zum Ablehnen einer Anforderung, ohne sie zu überprüfen, finden Sie unter Ignorieren einer Replikationsanforderung von einem Kunden.

1. Auf dem Ziel-Core navigieren Sie zur Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Replikation).

   Die Seite **Replikation** wird angezeigt.

3. Klicken Sie auf der Seite **Replikation** auf **Anforderung (#)**.

   Der Abschnitt **Anstehende Replikationsanforderungen** wird angezeigt.

4. Klicken Sie unter „Anstehende Replikationsanforderungen“ auf das Dropdown-Menü neben der Anforderung, die überprüft werden soll, und klicken Sie dann auf **Überprüfen**.

   Das Fenster **Replikationsanfragen überprüfen** wird angezeigt.

5. Klicken Sie auf **Ablehnen**.

   Die Replikation wird abgelehnt. Unter „Benachrichtigungen“ auf der Seite „Ereignisse“ des Quell-Core wird eine entsprechende Benachrichtigung angezeigt.

Ignorieren einer Replikationsanforderung von einem Kunden

Als externen Dienstanbieter für einen Ziel-Core können Sie eine von einem Kunden gesendete Replikationsanforderung ignorieren. Diese Möglichkeit kann genutzt werden, wenn eine Anforderung irrtümlicherweise gesendet wurde ohne eine Anforderung ohne Überprüfung abgelehnt werden soll.

Weitere Informationen zu Replikationsanforderungen finden Sie unter Überprüfen einer Replikationsanforderung von einem Kunden.

Führen Sie die folgenden Schritte aus, um eine Replikationsanforderung von einem Kunden zu ignorieren.

1. Auf dem Ziel-Core navigieren Sie zur Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Replikation).

   Die Seite **Replikation** wird angezeigt.
3. Klicken Sie auf der Seite **Replikation** auf **Anforderung (#)**.

   Der Abschnitt **Anstehende Replikationsanforderungen** wird angezeigt.
4. Klicken Sie unter „Anstehende Replikationsanforderungen“ auf das Dropdown-Menü neben der Anforderung, die ignoriert werden soll, und klicken Sie dann auf **Ignorieren**.
5. Klicken Sie im Dialogfeld **Anforderung ignorieren** auf **Ja**, um das Löschen zu bestätigen.

   An den Quelle-Core wird eine Benachrichtigung gesendet, dass die Anforderung ignoriert wurde, und die Anforderung wird von der Seite „Replikation“ des Ziel-Core entfernt.

Hinzufügen einer Maschine zu einer bestehenden Replikation

Nachdem die Replikation zwischen einen Quell- und einem Ziel-Core eingerichtet wurde, besteht die Möglichkeit, neue geschützte Maschinen hinzuzufügen und auf das Ziel zu replizieren. Führen Sie die folgenden Schritte aus, um eine neue geschützte Maschine zu einem gekoppelten Ziel-Core hinzuzufügen und zu replizieren.

Weitere Informationen zur Replikation finden Sie unter Replikation und Replikation auf einen selbstverwalteten Ziel-Core.

1. Navigieren Sie zur Rapid Recovery Core Console des Quell-Core.
2. Klicken Sie auf der Schaltflächenleiste auf **Replizieren**.

   Die Seite **Protected Machines** (Geschützte Maschinen) des Replikationsassistenten wird geöffnet.
3. Wählen Sie auf der Seite **Protected Machines** (Geschützte Maschinen) die geschützten Maschinen aus, die repliziert werden sollen, und wählen Sie in den Dropdown-Listen in der Spalte „Repository“ ein Repository für jede geschützte Maschine aus.
4. Führen Sie die folgenden Schritte aus, wenn Sie ein Seeding für die Übertragung der Basisdaten durchführen möchten:

   NOTE: Da große Datenmengen auf den Wechseldatenträger kopiert werden müssen, wird eine eSATA-, USB 3.0- oder eine andere Hochgeschwindigkeitsverbindung zum Wechseldatenträger empfohlen.

a. Wählen Sie auf der Seite **Geschützte Maschinen** des Replikationsassistenten die Option **Seed-Laufwerk für Erstübertragung verwenden** aus.

- Wenn derzeit eine oder mehr geschützte Maschinen auf einen Ziel-Core replizieren, können Sie diese Maschinen in das Seed-Laufwerk einbeziehen, indem Sie die Option **Include already replicated recovery points in the seed drive** (Bereits replizierte Wiederherstellungspunkte im Seed-Laufwerk einbeziehen) auswählen.

b. Klicken Sie auf **Weiter**.

c. Wählen Sie auf der Seite **Seed Drive Location** (Seed-Laufwerkspeicherort) des Assistenten in der Dropdownliste **Location type** (Typ des Speicherorts) einen der folgenden Zieltypen aus:

- Lokal
- Netzwerk
- Cloud

d. Geben Sie die in der folgenden Tabelle beschriebenen Details für das Archiv auf Basis der Position, die Sie in Schritt c ausgewählt haben, ein.

Tabelle 101. Archivierungsdetails

Option	Textfeld	Description
Lokal	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. D:\Arbeit\Archiv.
Netzwerk	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. \ \Servername\Freigabename.
	Benutzername	Geben Sie einen Benutzernamen ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
	Kennwort	Geben Sie ein Kennwort für den Netzwerkpfad ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **NOTE:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen hierzu finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.
	Ordnername	Geben Sie einen Namen für den Ordner ein, in dem die archivierten Daten gespeichert werden sollen. Der Standardname lautet „Rapid-Recovery-Archive-[ERSTELLUNGSDATUM]-[ERSTELLUNGSZEIT]“.

e. Klicken Sie auf **Weiter**.

f. Geben Sie auf der Seite **Seed Drive Options** (Seed-Laufwerkoptionen) des Assistenten die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 102. Seed-Laufwerkoptionen

Element	Description
Maximale Größe	Umfangreiche Datenarchive können in mehrere Segmente aufgeteilt werden. Wählen Sie den maximalen Speicherplatz aus, der zum Erstellen des Seed-Laufwerks reserviert werden soll. Führen Sie dazu einen der folgenden Schritte aus: • Wählen Sie **Gesamtes Ziel** aus, um den gesamten verfügbaren Speicherplatz im Pfad, der auf der Seite „Seed-Laufwerkspeicherort“ angegeben wurde, zu reservieren. (Wenn beispielsweise „D:\Arbeit\Archiv“ als Speicherort angegeben wurde, wird der gesamte verfügbare Speicherplatz auf dem Laufwerk D: reserviert.) • Geben Sie in das leere Textfeld einen Wert ein und wählen Sie dann eine Maßeinheit in der Dropdown-Liste aus, um den maximal reservierten Speicherplatz festzulegen.
Recyclingaktion	Falls der Pfad bereits ein Seed-Laufwerk enthält, wählen Sie eine der folgenden Optionen aus: • Nicht wiederverwenden. Vorhandene Seed-Daten am Speicherort werden nicht überschrieben oder gelöscht. Wenn der Speicherort nicht leer ist, können keine Daten in das Seed-Laufwerk geschrieben werden. • Diesen Core ersetzen. Alle bereits vorhandenen Daten auf dem Core werden überschrieben. Die Daten anderer Cores bleiben aber unverändert. • Vollständig löschen. Alle Seed-Daten werden aus dem Verzeichnis gelöscht, bevor das Seed-Laufwerk geschrieben wird.
Anmerkung	Geben Sie eine Anmerkung ein, die das Seed-Laufwerk beschreibt.
Alle Agenten zum Seed-Laufwerk hinzufügen	Wählen Sie diese Option aus, um alle geschützten Maschinen im Quell-Core mit dem Seed-Laufwerk zu replizieren. Diese Option ist standardmäßig ausgewählt.
„Build recovery point chains (fix orphans)“ (Wiederherstellungspunktkette erstellen (Waisen korrigieren))	Wählen Sie diese Option aus, um die gesamte Wiederherstellungspunktkette auf das Seed-Laufwerk zu replizieren. Diese Option ist standardmäßig ausgewählt. **NOTE:** Beim Seeding in Rapid Recovery 5.4 werden normalerweise nur die letzten Wiederherstellungspunkte auf das Seed-Laufwerk repliziert, um Zeitaufwand und Speicherplatz zum Erstellen des Seed-Laufwerks zu verringern. Wenn Wiederherstellungspunktketten auf dem Seed-Laufwerk erstellt werden sollen, muss auf dem Seed-Laufwerk genügend Speicherplatz zum Speichern der letzten Wiederherstellungspunkte der angegebenen geschützten Maschinen vorhanden sein. Dieser Vorgang kann entsprechend länger dauern.

g. Führen Sie eine der folgenden Aktionen aus:

- Wenn Sie die Markierung des Kontrollkästchens **Alle Agenten dem Seed-Laufwerk hinzufügen** entfernt haben, klicken Sie auf **Weiter**.
- Wechseln Sie zu **Schritt 5**, wenn Sie Alle Agenten zum Seed-Laufwerk hinzufügen ausgewählt haben.

h. Wählen Sie auf der Seite **Protected Machines** (Geschützte Maschinen) des Assistenten die geschützten Maschinen aus, die mit dem Seed-Laufwerk auf den Ziel-Core repliziert werden sollen.

5. Klicken Sie auf **Fertig stellen**.

Konsumieren des Seed-Laufwerks auf einem Ziel-Core

Führen Sie die folgenden Schritte aus, um die Daten des Seed-Laufwerks auf dem Ziel-Core zu konsumieren.

NOTE: Diese Schritte sind nur erforderlich, wenn im Rahmen von Replikation auf einen selbstverwalteten Ziel-Core oder Replikation auf den Ziel-Core eines externen Anbieters ein Seed-Laufwerk erstellt wurde.

1. Wenn das Seed-Laufwerk auf einem Wechseldatenträger, wie z. B. ein USB-Laufwerk, gespeichert wurde, verbinden Sie das Laufwerk mit dem Ziel-Core.
2. Öffnen Sie im Ziel-Core die Rapid Recovery Core Console und klicken Sie auf der Symbolleiste auf (Replikation).

   Die Seite **Replikation** wird angezeigt.
3. Klicken Sie auf der Registerkarte **Replikation** unter „Eingehende Replikation“ im Dropdown-Menü der zugehörigen Quell-Core auf **Konsumieren**.

   Das Dialofeld **Konsumieren** wird angezeigt.
4. Wählen Sie für **Speicherorttyp** eine der folgenden Optionen aus der Drop-Down-Liste aus:
   - Lokal
   - Netzwerk
   - Cloud
5. Geben Sie die in der folgenden Tabelle beschriebenen Details für das Archiv auf Basis der Position, die Sie in Schritt 4 ausgewählt haben, ein.

Tabelle 103. Archivierungsdetails

Option	Textfeld	Description
Lokal	Speicherort	Geben Sie das Kennwort für das Archiv ein.
Netzwerk	Speicherort	Geben Sie das Kennwort für das Archiv ein.
	Benutzername	Geben Sie den Benutzernamen ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
	Kennwort	Geben Sie das Kennwort für den Netzwerkpfad ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **NOTE:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen hierzu finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.

Option	Textfeld	Description
	Ordnername	Geben Sie den Namen des Ordners ein, in dem die archivierten Daten gespeichert sind, z. B. „Rapid-Recovery-Archive-[ERSTELLUNGSDATUM]-[ERSTELLUNGSZEIT]“.

6. Klicken Sie auf **Datei überprüfen**.

   Der Core sucht nach der Datei.

   Nachdem die Datei gefunden wurde, werden in die folgenden Textfelder des Fensters „Konsumieren“ die in Schritt 4, Schritt 5 und aus der Datei erfassten Daten eingetragen. In „Datumsbereich“ werden die Datumsangaben der ältesten und neuesten Wiederherstellungspunkte im Seed-Laufwerk angezeigt. Anmerkungen, die beim Erstellen des Seed-Laufwerks eingegeben wurden, werden automatisch importiert.

7. Wählen Sie im Dialogfeld **Konsumieren** unter „Agenten“ die Maschinen aus, für die Daten konsumiert werden sollen.
8. Klicken Sie auf **Konsumieren**.
9. Um den Fortschritt der Datenkonsumierung zu überwachen, zeigen Sie die Seite „Ereignisse“ an.

Entfernen eines Seed-Laufwerks

Wenn Sie ein Seed-Laufwerk mit der Absicht erstellen, es auf dem Ziel-Core zu konsumieren, jedoch später beschließen, es nicht zu konsumieren, können Sie das Seed-Laufwerk aufgeben.

Bis Sie das Seed-Laufwerk aufgeben oder verbrauchen bleibt ein Link für das ausstehende Seed-Laufwerk im Seitenbereich „Ausgehende Replikation“ des Quell-Core.

Bis Sie Informationen vom Seed-Laufwerk übertragen, können verwaiste Wiederherstellungspunkte (die auf der ursprünglichen geschützten Maschine, aber nicht im Ziel-Core vorliegen) nicht zum Wiederherstellen von Daten verwendet werden.

CAUTION: Wenn Sie das Seed-Laufwerk aufgeben, werden die ursprünglichen Wiederherstellungspunkte (in der Seed-Laufwerksdatei definiert) während des nächsten Replikationsauftrags über das Netzwerk auf den Ziel-Core übertragen. Die Übertragung alter Wiederherstellungspunkte über das Netzwerk kann das Netzwerk erheblich verlangsamen. Dies gilt insbesondere dann, wenn es viele Wiederherstellungspunkte gibt.

Führen Sie die folgenden Schritte aus, um ein ausstehendes Seed-Laufwerk aufzugeben.

NOTE: Des Aufgeben des Seed-Laufwerks in der Core Console hat keine Auswirkungen auf die Seed-Laufwerksdatei an ihrem ursprünglichen Speicherort.

1. Öffnen Sie im Quell-Core die Rapid Recovery Core Console und klicken Sie auf der Symbolleiste auf (Replikation).

   Die Seite **Replikation** wird angezeigt.
2. Klicken Sie auf der Seite **Replikation** im Fensterbereich „Ausgehende Replikation“ auf **Seed-Laufwerke (Zahl)**.

   Im Fensterbereich „Ausgehende Replikation“ wird ein Abschnitt mit Informationen über die ausstehenden Seed-Laufwerke angezeigt.
3. Klicken Sie optional auf den Pfeil , um das reduzierbare Menü zu erweitern.

   Es werden Informationen über ausstehende Seed-Laufwerke, einschließlich des Ziel-Core, und den Datumsbereich der im Seed-Laufwerk enthaltenen Wiederherstellungspunkte angezeigt.
4. Für die Seed-Laufwerksdatei, die Sie aufgeben möchten, klicken Sie auf (Weitere Optionen) und wählen Sie **Aufgeben**.
5. Bestätigen Sie im Bestätigungsfenster, dass Sie das Seed-Laufwerk aufgeben möchten.

Das Seed-Laufwerk wird entfernt.

Wenn auf dem Quell-Core keine Seed-Laufwerke mehr vorhanden sind, werden der Link „Seed-Laufwerke (Zahl)“ und der Abschnitt „Ausstehende Seed-Laufwerke“ von der Registerkarte „Replikation“ entfernt.

Verwalten der Replikationseinstellungen

Rapid Recovery bietet die Möglichkeit, die Replikation auf Gesamtebene, Core-Ebene und Ebene der geschützten Maschinen zu überwachen, zu planen und anzupassen.

Sie können die folgenden Replikationseinstellungen bearbeiten:

- Informationen zum Planen von Replikationsjobs finden Sie unter Planen der Replikation.
- Informationen zum Erstellen eines Seed-Laufwerks für eine geschützte Maschine, die bereits für die Replikation gepaart wurde, finden Sie unter Erstellen eines Seed-Laufwerks mit der Kopierfunktion
- Informationen zum Überwachen des Fortschritts eines Replikationsjobs finden Sie unter Anzeigen von ein- und ausgehender Replikation.
- Informationen zum Anhalten oder Fortsetzen eines angehaltenen Replikationsjobs finden Sie unter Anhalten und Fortsetzen der Replikation.
- Informationen zum Erzwingen einer Replikation einer ein- oder ausgehenden geschützten Maschine finden Sie unter Erzwingen einer Replikation.
- Informationen zum Verwalten der Einstellungen für alle Ziel-Cores und Replikationsverfahren finden Sie unter Verwalten der Einstellungen für die ausgehende Replikation.
- Informationen zum Verwalten der Einstellungen für einen bestimmten Ziel-Core finden Sie unter Ändern der Ziel-Core-Einstellungen.
- Informationen zum Verwalten der Prioritätseinstellungen für eine bestimmte geschützte Maschine, die auf einen Ziel-Core repliziert wird, finden Sie unter Festlegen der Replikationspriorität für eine geschützte Maschine.

Planen der Replikation

Wenn Sie das Standardverhalten durch Einrichten eines Replikationszeitplans nicht ändern, startet der Core einen Replikationsjob sofort nach Abschluss jedes Sicherungs-Snapshots, jeder Prüfsummen-Überprüfung, Anfügbarkeitsprüfung und nach den nächtlichen Jobs.

Sie können den Replikationszeitplan ändern, um die Arbeitslast im Netzwerk zu verringern.

Führen Sie die hier beschriebenen Schritte aus, um einen Replikationszeitplan für alle replizierten Maschinen festzulegen.

1. Öffnen Sie im Ziel-Core die Rapid Recovery Core Console und klicken Sie auf der Symbolleiste auf (Replikation).

   Die Seite **Replikation** wird angezeigt.
2. Klicken Sie im Fensterbereich „Ausgehende Replikation“ auf den Core, für den Sie eine Replikation planen möchten, auf (Weitere Optionen) und wählen Sie **Zeitplan**.

Das Dialogfeld **Replikationszeitplan für [Core-Name]** wird geöffnet.

3. Wählen Sie eine der drei folgenden Optionen aus:

   - **Jederzeit**. Nach jedem neuen Snapshot, nach jeder Prüfsummenprüfung und jeder Anfügbarkeitsprüfung sowie nach Abschluss der nächtlichen Jobs wird eine Replikation durchgeführt.
   - **Täglich (Replikation nur im angegebenen Zeitraum starten)**. Die Replikation wird nur im angegebenen Zeitraum gestartet.

     1. Geben Sie im Textfeld **Von** den frühesten Zeitpunkt für den Beginn der Replikation ein.
     2. Geben Sie im Textfeld **Bis** den spätesten Zeitpunkt für den Beginn der Replikation ein.

     NOTE: Wenn die Replikation am Ende der geplanten Zeit noch läuft, wird der Replikationsjob nach dem zugewiesenen Zeitraum beendet.

   - **Benutzerdefiniert**. Beginnt die Replikation erst innerhalb des angegebenen Zeitraums, wobei Sie einen Zeitraum für Werktage und einen anderen Zeitraum für Wochenenden angeben können.

     1. Geben Sie neben „Wochentage“ im Textfeld **Von** den frühesten Zeitpunkt und im Textfeld **Bis** den spätesten Zeitpunkt für die Replikation an Wochentagen ein.
     2. Geben Sie neben „Wochenenden“ im Textfeld **Von** den frühesten Zeitpunkt und im Textfeld **Bis** den spätesten Zeitpunkt für die Replikation an Wochenenden ein.

4. Klicken Sie auf **Speichern**.

   Der Zeitplan wird für alle Replikationen zum ausgewählten Ziel-Core verwendet.

Erstellen eines Seed-Laufwerks mit der Kopierfunktion

Wenn Sie sich beim Konfigurieren der Replikation entschieden haben, kein Seed-Laufwerk zu erstellen, können Sie mit der Funktion „Kopieren“ im Dropdown-Menü der geschützten Maschine ein Seed-Laufwerk erstellen.

1. Öffnen Sie im Quell-Core die Rapid Recovery Core Console und klicken Sie auf der Symbolleiste auf (Replikation).

   Die Seite **Replikation** wird angezeigt.

2. Klicken Sie auf der Seite **Replikation** im Fensterbereich „Ausgehende Replikation“ auf), um den Core zu erweitern, der die Maschine schützt, für die Sie ein Seed-Laufwerk erstellen möchten.

   Die Auswahl wird erweitert und zeigt jede geschützte Maschine im angegebenen Core an.

3. Klicken Sie in der ersten Zeile der Tabelle, um jede Maschine auszuwählen, für die Sie ein Seed-Laufwerk erstellen möchten.
4. Klicken Sie im Menü unter dem Fensterbereich „Ausgehende Replikation auf **Kopieren**.

   Der **Replikationsassistent** wird geöffnet.

5. Wählen Sie auf der Seite **Seed-Laufwerkspeicherort** in der Dropdown-Liste **Speicherort** einen der folgenden Zieltypen aus:

   - Lokal
   - Netzwerk
   - Cloud

6. Geben Sie die Details für das Seed-Laufwerksarchiv, wie in der folgenden Tabelle beschrieben, auf Basis des im vorherigen Schritt ausgewählten Speicherorttyps ein.

Tabelle 104. Archivierungsdetails

Option	Textfeld	Description
Lokal	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. D:\Arbeit\Archiv.
Netzwerk	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. \\Servername \Freigabename.
	Benutzername	Geben Sie einen Benutzernamen ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
	Kennwort	Geben Sie ein Kennwort für den Netzwerkpfad ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **NOTE:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen hierzu finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.
	Ordnername	Geben Sie einen Namen für den Ordner ein, in dem die archivierten Daten gespeichert werden sollen. Der Standardname lautet „Rapid-Recovery-Archive-[ERSTELLUNGSDATUM]-[ERSTELLUNGSZEIT]“.

7. Klicken Sie auf **Weiter**.
8. Geben Sie auf der Seite „Seed-Laufwerkoptionen“ die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 105. Seed-Laufwerkoptionen

Element	Description
Maximale Größe	Umfangreiche Datenarchive können in mehrere Segmente aufgeteilt werden. Wählen Sie den maximalen Speicherplatz aus, der zum Erstellen des Seed-Laufwerks reserviert werden soll. Führen Sie dazu einen der folgenden Schritte aus: • Wählen Sie **Gesamtes Ziel** aus, um den gesamten verfügbaren Speicherplatz im Pfad, der auf der Seite „Seed-Laufwerkspeicherort“ angegeben wurde, zu reservieren. (Wenn beispielsweise „D:\Arbeit\Archiv“ als Speicherort angegeben wurde, wird der gesamte verfügbare Speicherplatz auf dem Laufwerk D: reserviert.) • Geben Sie in das leere Textfeld einen Wert ein und wählen Sie dann eine Maßeinheit in der Dropdown-Liste aus, um den maximal reservierten Speicherplatz festzulegen.

Element	Description
Recyclingaktion	Falls der Pfad bereits ein Seed-Laufwerk enthält, wählen Sie eine der folgenden Optionen aus: • **Nicht wiederverwenden.** Vorhandene Seed-Daten am Speicherort werden nicht überschrieben oder gelöscht. Wenn der Speicherort nicht leer ist, können keine Daten in das Seed-Laufwerk geschrieben werden. • **Replace this Core** (Diesen Core ersetzen). Alle bereits vorhandenen Daten auf dem Core werden überschrieben. Die Daten anderer Cores bleiben aber unverändert. • **Erase completely** (Vollständig löschen). Alle Seed-Daten werden aus dem Verzeichnis gelöscht, bevor das Seed-Laufwerk geschrieben wird.
Anmerkung	Geben Sie eine Anmerkung ein, die das Seed-Laufwerk beschreibt.
Alle Agenten zum Seed-Laufwerk hinzufügen	Wählen Sie diese Option aus, um alle geschützten Maschinen im Quell-Core mit dem Seed-Laufwerk zu replizieren. Diese Option ist standardmäßig ausgewählt.
„Build recovery point chains (fix orphans)“ (Wiederherstellungspunktkette erstellen (Waisen korrigieren))	Wählen Sie diese Option aus, um die gesamte Wiederherstellungspunktkette auf das Seed-Laufwerk zu replizieren. Diese Option ist standardmäßig ausgewählt. **NOTE:** Beim Seeding in Rapid Recovery 5.4.x werden normalerweise nur die letzten Wiederherstellungspunkte auf das Seed-Laufwerk repliziert, um Zeitaufwand und Speicherplatz zum Erstellen des Seed-Laufwerks zu verringern. Wenn Wiederherstellungspunkt-Ketten auf dem Seed-Laufwerk erstellt werden sollen, muss auf dem Seed-Laufwerk genügend Speicherplatz zum Speichern der letzten Wiederherstellungspunkte der angegebenen geschützten Maschinen vorhanden sein. Dieser Vorgang kann entsprechend länger dauern.

9. Führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie die Markierung des Kontrollkästchens **Alle Agenten dem Seed-Laufwerk hinzufügen** entfernt haben, klicken Sie auf **Weiter**.
   - Wenn Sie **Alle Agenten zum Seed-Laufwerk hinzufügen** aktiviert haben, gehen Sie weiter zu Schritt 10.
10. Wählen Sie auf der Seite **Geschützte Maschinen** die geschützten Maschinen aus, für die Sie ein Seed-Laufwerk erstellen wollen.
11. Klicken Sie auf **Fertig stellen**.

Überwachen der Replikation

Wenn die Replikation eingerichtet wurde, können Sie den Status der Replikationsaufgaben für Quell- und Ziel-Core überwachen. Sie können die Statusinformationen aktualisieren, Replikationsdetails anzeigen usw.

1. Öffnen Sie im Quell-Core die Rapid Recovery Core Console und klicken Sie auf der Symbolleiste auf (Replikation).

   Die Seite **Replikation** wird angezeigt.
2. Auf dieser Registerkarte können Sie Informationen zum Status der Replikationsaufgaben abrufen und Replikationsaufgaben überwachen (siehe Beschreibung in der folgenden Tabelle).

Tabelle 106. Replikationsaufgaben

Abschnitt	Description	Verfügbare Aktionen
Seed Drives (#) (Seed-Laufwerke (#))	Nach dem Festlegen der Verwendung eines Seed-Laufwerks bei der Definition der Replikation wird ein Link namens **Seed Drives (#)** (Seed-Laufwerke(#)) im Bereich „Outgoing Replication“ (Ausgehende Replikation) angezeigt, bis Sie den Vorgang aufgeben oder die Laufwerke belegt sind. Die angezeigte Zahl gibt an, wie viele Seed-Laufwerke ausstehen. **NOTE:** Dieser Link wird nur angezeigt, wenn ein Seed-Laufwerk aussteht. Durch Klicken auf diesen Link werden die Seed-Laufwerke aufgelistet, die bereits geschrieben, aber noch nicht vom Ziel-Core belegt wurden. Erweitern Sie das reduzierbare Menü, um Informationen zu ausstehenden Seed-Laufwerken einschließlich des Ziel-Cores und des Datumsbereichs der Wiederherstellungspunkte im Seed-Laufwerk anzuzeigen.	Klicken Sie im Dropdown-Menü auf **Abandon** (Aufgeben), um den Seeding-Vorgang aufzugeben oder abzubrechen.
Ausgehende Replikation	In diesem Bereich werden alle Ziel-Cores aufgelistet, auf die der Quell-Core repliziert. Angezeigt werden der Name des Ziel-Cores, Status, Anzahl der replizierten Maschinen und der Fortschritt einer Replikationsübertragung.	Auf einem Quell-Core im Drop-Down-Menü ... (Mehr) können Sie folgende Optionen auswählen: • Unter **Details** (Einzelheiten) sind ID, URL, Anzeigename, Status, Kunden-ID, E-Mail-Adresse und Anmerkungen zum replizierten Core aufgeführt. • **Einstellungen ändern.** Hier wird der Anzeigename aufgeführt und Host und Port für den Ziel-Core können bearbeitet werden. • **Zeitplan.** Diese Option bietet die Möglichkeit, einen angepassten Zeitplan für die Replikation zum betreffenden Ziel-Core festzulegen. • **Maschinen hinzufügen.** Bietet die Möglichkeit, einen Host in einer Dropdown-Liste auszuwählen, geschützte Maschinen für die Replikation auszuwählen und ein Seed-Laufwerk für die Erstübertragung der neuen geschützten Maschine zu erstellen. Sie können optional auch Wiederherstellungspunkte für Maschinen hinzufügen, die

Abschnitt	Description	Verfügbare Aktionen
		bereits zur Replikation hinzugefügt wurden. • **Löschen.** Hiermit können Sie die Replikationsbeziehung zwischen Quell- und Ziel-Cores löschen. Dadurch wird jegliche Replikation auf diesen Core beendet.
Eingehende Replikation	In diesem Bereich werden alle Quellmaschinen aufgelistet, von denen das Ziel replizierte Daten empfängt. Angezeigt werden Name des Remote Cores, Status, Maschinen und Fortschritt. In diesem Bereich werden alle Quell-Cores aufgelistet, von denen das Ziel replizierte Daten empfängt. Der Anzeigename für die aufgeführten Quell-Cores wird mit dem Wert im Replikationsassistenten bei der Definition der Replikation gefüllt. Angezeigt werden ein Statusindikator, der Remote-Core-Name und der Fortschritt einer Replikationsübertragung.	Auf einem Ziel-Core im Drop-Down-Menü ... (Mehr) können Sie folgende Optionen auswählen: • **Details.** Listet ID, Hostnamen, Kunden-ID, E-Mail-Adresse und Anmerkungen für den replizierten Core auf. • **Konsumieren.** Konsumiert die Anfangsdaten vom Seed-Laufwerk und speichert sie im lokalen Repository. • **Löschen.** Hiermit können Sie die Replikationsbeziehung zwischen Ziel- und Quell-Cores löschen. Dadurch wird jegliche Replikation von diesem Core beendet.
Anstehende Replikationsanforderungen	Diese Informationen gelten nur für Anbieter von verwalteten Diensten. Wenn ein Kunde auf den Link **Anfragen** im Bereich „Incoming Replication“ (Eingehende Replikation) klickt, wird ein Übersichtstabellenabschnitt mit der Kunden-ID, der E-Mail-Adresse und dem Hostnamen für die Anforderung angezeigt.	Klicken Sie im Dropdownmenü auf **Ignore** (Ignorieren), um die Anforderung zu ignorieren oder abzulehnen, oder auf **Review** (Überprüfen) zur Überprüfung der ausstehenden Anforderung.

Anhalten und Fortsetzen der Replikation

Sie können die Replikation für die Quell-Cores (ausgehend) oder für die Ziel-Cores (eingehend) vorübergehend deaktivieren.

Die Option zum Anhalten der Replikation ist nur verfügbar, wenn die Replikation aktiv ist. Die Option zum Wiederaufnehmen der Replikation ist nur verfügbar, wenn die Replikation angehalten wurde.

Führen Sie die folgenden Schritte aus, um eine Replikation vorübergehend zu deaktivieren und wieder zu aktivieren.

1. Öffnen Sie die Rapid Recovery Core Console und klicken Sie auf der Symbolleiste auf (Replikation).

   Die Seite **Replikation** wird angezeigt.
2. Um die Replikation für alle replizierten Maschinen anzuhalten, gehen Sie wie folgt vor:
   a. Klicken Sie auf das Kontrollkästchen am oberen Rand der Übersichtstabelle, um den Quell- oder Ziel-Core auszuwählen.

b. Klicken Sie im der Übersichtstabelle vorangestellten Menü auf **Anhalten**.

Die Replikation für alle geschützten Maschinen im ausgewählten Core wird angehalten.

3. Um die Replikation für bestimmte replizierte Maschinen anzuhalten, gehen Sie wie folgt vor:
   a. Klicken Sie auf den Pfeil ▸ rechts von einem beliebige Core.

   Die Ansicht wird erweitert und alle vom ausgewählten Core geschützten Maschinen, die repliziert werden, werden angezeigt.

   b. Klicken Sie in der ersten Spalte auf die jeweiligen Maschinen, für die Sie die Replikation anhalten möchten. Klicken Sie erneut auf eine beliebige Auswahl, um das Kontrollkästchen für Maschinen, die Sie nicht anhalten möchten, zu deaktivieren.
   c. Klicken Sie im der Übersichtstabelle vorangestellten Menü auf **Anhalten**.

   Die Replikation für die ausgewählten geschützten Maschinen wird angehalten.

4. Um die Replikation für alle replizierten Maschinen fortzusetzen, gehen Sie wie folgt vor:
   a. Klicken Sie auf das Kontrollkästchen am oberen Rand der Übersichtstabelle, um den Quell- oder Ziel-Core auszuwählen.
   b. Klicken Sie im Menü über der Übersichtstabelle auf **Fortsetzen**.

   Die Replikation für alle geschützten Maschinen im ausgewählten Core wird fortgesetzt.

5. Um die Replikation für bestimmte replizierte Maschinen fortzusetzen, gehen Sie wie folgt vor:
   a. Klicken Sie auf den Pfeil ▸ rechts von einem beliebige Core.

   Die Ansicht wird erweitert und alle vom ausgewählten Core geschützten Maschinen, die repliziert werden, werden angezeigt.

   b. Klicken Sie in der ersten Spalte auf die jeweiligen Maschinen, für die Sie die Replikation fortsetzen möchten. Klicken Sie erneut auf eine beliebige Auswahl, um das Kontrollkästchen für Maschinen, die Sie nicht fortsetzen möchten, zu deaktivieren.
   c. Klicken Sie im Menü über der Übersichtstabelle auf **Fortsetzen**.

   Die Replikation für die ausgewählten geschützten Maschinen wird fortgesetzt.

Erzwingen einer Replikation

Vom Quell-Core können Sie die Replikation zu einem beliebigen Zeitpunkt erzwingen, statt darauf zu warten, dass ein Replikationsjob nach einem bestimmten Ereignis wie z. B. einer Sicherung oder Anfügbarkeitsprüfung in die Warteschlange eingereiht wird.

Führen Sie die folgenden Schritte aus, um die Replikation vom Quell-Core oder vom Ziel-Core aus zu erzwingen.

1. Öffnen Sie im Quell-Core die Rapid Recovery Core Console und klicken Sie auf der Symbolleiste auf (Replikation).

   Die Seite **Replikation** wird angezeigt.

2. Führen Sie eine der folgenden Aktionen aus:
   - Um die Replikation auf einem Quell-Core zu erzwingen, wählen Sie im Bereich **Ausgehende Replikation** einen Core aus und klicken Sie im Menü über der Übersichtstabelle auf **Erzwingen**.
   - Um die Replikation auf einem Ziel-Core zu erzwingen, wählen Sie im Bereich **Eingehende Replikation** einen Core aus und klicken Sie im Menü über der Übersichtstabelle auf **Erzwingen**.

   Das Dialogfeld „Force Replication“ (Replikationen erzwingen) wird angezeigt.
3. Optional können Sie verwaiste Wiederherstellungspunktketten korrigieren, indem Sie **restore orphaned recovery point chains** (Verwaiste Wiederherstellungspunktketten wiederherstellen) auswählen.
4. Klicken Sie zur Bestätigung im Dialogfeld „Force Replication“ (Replikationen erzwingen) auf **Yes** (Ja).

Das Dialogfeld wird geschlossen und die Replikation wird erzwungem.

Verwalten der Einstellungen für die ausgehende Replikation

Änderungen dieser Einstellungen wirken sich auf die Datenübertragung auf alle Ziel-Cores aus, diese diesem Quell-Core zugeordnet sind.

1. Öffnen Sie im Quell-Core die Rapid Recovery Core Console und klicken Sie auf der Symbolleiste auf (Replikation).

   Die Seite **Replikation** wird angezeigt.

2. Klicken Sie im Fensterbereich **Ausgehende Replikation** am oberen Rand der Übersichtstabelle auf (Einstellungen).

   Das Dialogfeld **Replikationseinstellungen** wird angezeigt.

3. Bearbeiten Sie im Dialogfeld **Replikationseinstellungen** die Einstellungen, wie in der folgenden Tabelle beschrieben:

Tabelle 107. Replikationseinstellungen

Option	Description
Cache-Lebensdauer (Sekunden)	Geben Sie den Zeitraum zwischen zwei Statusabfragen an den Ziel-Core durch den Quell-Core an.
Zeitüberschreitung für Volume-Image-Sitzung (Minuten)	Geben Sie die Dauer an, während der der Quell-Core versucht, ein Volume-Abbild auf den Ziel-Core zu übertragen.
Maximale Anzahl paralleler Streams	Geben Sie die Anzahl der zulässigen Netzwerkverbindungen an, die eine einzelne geschützte Maschine für die Replikation der Daten der betreffenden Maschine gleichzeitig verwenden darf.
Max. Übertragungsgeschwindigkeit (MB/s)	Geben Sie die maximale Geschwindigkeit für die Übertragung der replizierten Daten an.
Maximale Größe der übertragenen Daten (GB)	Geben Sie die maximale Größe in GB für die Übertragungsblöcke der replizierten Daten an.
Standardeinstellungen wiederherstellen	Wählen Sie diese Option aus, um alle Replikationseinstellungen zu den Standardeinstellungen des Systems zu ändern. **NOTE:** Notieren Sie alle benutzerdefinierten Einstellungen, bevor Sie diese Option auswählen. Sie werden nicht aufgefordert, diese Aktion zu bestätigen

4. Wenn Sie zufrieden sind, klicken Sie auf **Speichern** zum Speichern der Replikationseinstellungen und zum Schließen des Dialogfelds.

Ändern der Ziel-Core-Einstellungen

Sie können den Host und die Anschlusseinstellungen einzelner Ziel-Cores vom Quell-Core aus ändern.

1. Öffnen Sie im Quell-Core die Rapid Recovery Core Console und klicken Sie auf der Symbolleiste auf (Replikation). .

   Die Seite **Replikation** wird angezeigt.

   Im Bereich **Outgoing Replication** (Ausgehende Replikation) enthält die Übersichtstabelle eine Zeile für jeden Ziel-Core, der für die Replikation von Wiederherstellungspunkten von diesem Quell-Core konfiguriert wurde.

2. Klicken Sie auf das Drop-Down-Menü (Einstellungen) für den Ziel-Core, den Sie ändern möchten, und klicken Sie dann auf **Einstellungen ändern**.

   Das Dialogfeld **Einstellungen** wird angezeigt.

3. Bearbeiten Sie die der in der folgenden Tabelle beschriebenen Optionen.

Tabelle 108. Einstellungen für den Ziel-Core

Option	Description
Host	Geben Sie den Host für den Ziel-Core ein.
Port	Geben Sie einen Port für die Kommunikation zwischen Ziel-Core und Quell-Core ein. **NOTE:** Die Standardportnummer ist 8006.

4. Klicken Sie auf **Speichern**.

Festlegen der Replikationspriorität für eine geschützte Maschine

Die Replikationspriorität bestimmt, welche Replikationsaufgaben zuerst an den Core gesendet werden. Priorisierung wird als Ordinalzahl auf einer Skala von 1 bis 10 eingestellt, wobei eine Priorität von 1 die höchste und eine Priorität von 10 die niedrigste Priorität angibt. Wenn Sie das erste Mal eine Replikation für jede Maschine einrichten, ist seine Priorität auf 5 gesetzt. Sie können die Priorität auf der Ebene der geschützten Maschinen vom Quell-Core anzeigen und ändern.

In manchen Fällen ist es möglich, dass einige Replikationsaufgaben aufgegeben werden. Zum Beispiel können Replikationsaufgaben aufgegeben werden, wenn in Ihrer Umgebung ungewöhnlich hohe Änderungsraten auftreten oder wenn Ihr Netzwerk nicht über genügend Bandbreite verfügt. Diese Situation ist besonders wahrscheinlich, wenn Sie Zeitpläne festlegen, welche die Stunden, in denen die Replikation in Ihrer Umgebung stattfinden kann, beschränken. Weitere Informationen zum Festlegen von Zeitplänen für die Replikation finden Sie unter Planen der Replikation.

Um sicherzustellen, dass die Replikation für wichtige Maschinen zuerst erfolgt, stellen Sie zunächst kritische Server auf eine Priorität mit einer niedrigeren Zahl (zwischen 1 und 5). Stellen Sie die Priorität für weniger wichtige Maschinen auf eine höhere Zahl (zwischen 6 und 10) ein.

Durch Einstellen der Replikationspriorität auf 4 für eine beliebige Maschine wird sichergestellt, dass ihre Replikationsaufgabe vor einer Maschine mit der Standard-Replikationspriorität von 5 gestartet wird. Replikationsaufgaben für Maschinen mit der Priorität 3 werden vor 4 in die Warteschlange gestellt usw. Je niedriger die Prioritätsnummer, desto schneller werden die entsprechenden Replikationsaufgaben gesendet. Es

ist leicht zu merken, dass Priorität 1 die höchste Priorität ist. Maschinen mit einer Replikationspriorität von 1 sind die ersten Maschinen, die zur Replikation anstehen.

Führen Sie die folgenden Schritte aus, um die Prioritätseinstellungen für die Replikation einer geschützten Maschine zu bearbeiten.

1. Öffnen Sie im Quell-Core die Rapid Recovery Core Console und klicken Sie auf der Symbolleiste auf (Replikation).

   Die Seite **Replikation** wird angezeigt.
2. Klicken Sie im Fensterbereich **Ausgehende Replikation** auf den Pfeil rechts von jedem Quell-Core.

   Die Ansicht wird erweitert und alle geschützten Maschinen von diesem Quell-Core, die auf den angegebenen Ziel-Core repliziert werden, werden angezeigt.
3. Klicken Sie auf das Dropdown-Menü (Mehr) für die geschützte Maschine, die Sie priorisieren möchten, und klicken Sie dann auf **Einstellungen ändern**.

   Ein Dialogfeld wird angezeigt.
4. Klicken Sie auf die Drop-Down-Liste **Priorität** und wählen Sie eine Priorität zwischen **1 (höchste)** und **10 (niedrigste)**, basierend auf Ihren Anforderungen.
5. Klicken Sie auf **Speichern**.

   Das Dialogfeld wird geschlossen und die Replikationspriorität für die ausgewählte Maschine aktualisiert.

Entfernen einer ausgehenden Replikation vom Quell-Core

Führen Sie die folgenden Schritte aus, um eine oder mehrere geschützte Maschine(n) aus der Replikation auf dem Quell-Core zu entfernen.

1. Öffnen Sie im Quell-Core die Rapid Recovery Core Console und klicken Sie auf der Symbolleiste auf (Replikation).

   Die Seite **Replikation** wird angezeigt.

   Im Bereich **Outgoing Replication** (Ausgehende Replikation) enthält die Übersichtstabelle eine Zeile für jeden Ziel-Core, der für die Replikation von Wiederherstellungspunkten von diesem Quell-Core konfiguriert wurde.
2. Klicken Sie optional auf den Pfeil rechts von einem beliebigen Ziel-Core.

   Die Ansicht wird erweitert und alle geschützten Maschinen von diesem Quell-Core, die auf den angegebenen Ziel-Core repliziert werden, werden angezeigt.
3. Wählen Sie die geschützten Maschinen, die Sie aus der ausgehenden Replikation entfernen möchten, wie folgt:
   - Um die vorhandene Replikationsbeziehung zwischen diesem Quell-Core und allen Ziel-Cores vollständig zu entfernen, klicken Sie auf das Drop-Down-Menü (Mehr) und wählen Sie dann **Löschen**.
   - Um die ausgehende Replikation für eine Teilmenge der Maschinen im angegebenen Ziel-Core zu entfernen, erweitern Sie die Ansicht, bis alle replizierten Maschinen angezeigt werden, und aktivieren Sie das Kontrollkästchen für jedes replizierte Maschine, die Sie entfernen möchten. Deaktivieren Sie das Kontrollkästchen für jede Maschine, die Sie weiter replizieren möchten. Klicken Sie anschließend im Menü über der Übersichtstabelle auf **Löschen**.

Eine Bestätigungsmeldung wird angezeigt, in der Sie gefragt werden, ob Sie die Replikationsbeziehungen entfernen möchten.

4. Klicken Sie im darauffolgenden Dialogfeld auf **Ja**, um die Entfernung zu bestätigen.

Eingehende Replikation vom Ziel-Core entfernen

Führen Sie die folgenden Schritte aus, um eine oder mehrere geschützte Maschinen auf dem Quell-Core aus der Replikation zu entfernen.

NOTE: Sie können die Replikation von geschützten Maschinen auch aus dem Fensterbereich „Ausgehende Replikation“ auf der Seite „Replikation“ des Quell-Core entfernen. Weitere Informationen hierzu finden Sie unter Entfernen einer ausgehenden Replikation vom Quell-Core

1. Öffnen Sie im Ziel-Core die Rapid Recovery Core Console und klicken Sie auf der Symbolleiste auf (Replikation).

   Die Seite **Replikation** wird angezeigt. Im Fensterbereich „Eingehende Replikation“ enthält die Übersichtstabelle eine Zeile für jeden Quell-Core mit geschützten Maschinen, die dieser Ziel-Core repliziert.

2. Wählen Sie die replizierten Maschinen, die Sie entfernen möchten, wie folgt aus:

   - Um **alle** vom Quell-Core auf den Ziel-Core replizierten Maschinen zu löschen, markieren Sie im Fensterbereich „Eingehende Replikation“ das Kontrollkästchen für diesen Core.
   - Um eine kleinere Untermenge von Maschinen des gleichen Quell-Core zu löschen, gehen Sie wie folgt vor:

     a. Klicken Sie auf den Pfeil rechts vom Quell-Core.

   Die Ansicht erweitert sich und zeigt allen Maschinen vom ausgewählten Quell-Core an, die auf Ihren Ziel-Core repliziert wurden.

     b. Markieren Sie das Kontrollkästchen für jede replizierte Maschine, die Sie entfernen möchten.

     c. Auf der übergeordneten Zeile des ausgewählten Quell-Core klicken Sie auf das Drop-Down -Menü (Mehr) und wählen Sie dann **Löschen**.

   Das Dialogfeld **Replikation entfernen** wird angezeigt.

3. Führen Sie im Dialogfeld **Replikation entfernen** einen der folgenden Schritte aus:

   - Wenn Sie die replizierten Wiederherstellungspunkte auf dem Ziel-Core belassen wollen, heben Sie die Markierung der Option **Vorhandene Wiederherstellungspunkte löschen** auf.
   - Wählen Sie **Vorhandene Wiederherstellungspunkte löschen** aus, wenn alle replizierten Wiederherstellungspunkte, die von der betreffenden Maschine empfangen wurden, zusammen mit dem Quell-Core gelöscht werden sollen.

4. Klicken Sie auf **Ja**, um den Löschvorgang zu bestätigen.

   WARNING: Wenn Sie diese Option auswählen, werden alle auf diesen Core replizierten Wiederherstellungspunkte gelöscht.

   Die ausgewählten Maschinen, die auf dem Quell-Core geschützt sind, werden aus der Replikation auf diesen Ziel-Core entfernt. Wenn Sie optional die Option zum Löschen von Wiederherstellungspunkten ausgewählt haben, werden auch diese aus dem Repository dieses Core entfernt.

Wiederherstellen von replizierten Daten

Die alltägliche Replikationsfunktion wird auf dem Quell-Core verwaltet. Auf dem Ziel-Core können nur die für eine Notfallwiederherstellung notwendigen Funktionen durchgeführt werden.

Für eine Notfallwiederherstellung kann der Ziel-Core die replizierten Wiederherstellungspunkte verwenden, um die geschützten Maschinen wiederherzustellen. Sie können die folgenden Wiederherstellungsoptionen auf dem Ziel-Core durchführen:

- **Wiederherstellungspunkte bereitstellen**. Weitere Informationen finden Sie unter Bereitstellen eines Wiederherstellungspunkts.
- **Rollback auf Wiederherstellungspunkte durchführen**. Weitere Informationen finden Sie unter Informationen über das Wiederherstellen von Volumes aus Wiederherstellungspunkten bzw. Wiederherstellen von Volumes einer Linux-Maschine über die Befehlszeile.
- **Export einer virtuellen Maschine (VM) durchführen**. Weitere Informationen finden Sie unter Exportieren auf virtuelle Maschinen mit Rapid Recovery.
- **BMR-Wiederherstellung (Bare Metal Restore) durchführen**. Weitere Informationen finden Sie unter Durchführen einer BMR-Wiederherstellung für Windows-Computer.

Ereignisse

DasRapid Recovery Core umfasst vordefinierte Sätze von Ereignissen. Diese Ereignisse können verwendet werden, um Administratoren über entscheidende Probleme im Core oder über Probleme mit Jobs im Zusammenhang mit Sicherungen, virtuellem Export, Replikation usw. zu benachrichtigen.

In diesem Abschnitt wird beschrieben, wie Ereignisse auf der Rapid Recovery Core Console angezeigt werden. Sie können auch mehr über Methoden und Konfiguration von Ereignis-Benachrichtigungen, einschließlich der Einrichtung von E- Mail-Benachrichtigungen, erfahren. Darüber hinaus können Sie Benachrichtigungen konfigurieren, um die Zeit, die Ereignisprotokolle beibehalten werden, zu ändern und wiederholte Ereignisbenachrichtigungen zu reduzieren.

Anzeigen von Ereignissen mithilfe von Aufgaben, Warnungen und Journalseiten

Aus der Core Console können Sie Ereignisse für den Core anzeigen und Sie können Ereignisse für bestimmte geschützte oder replizierte Maschine anzeigen.

Auf den Seiten **Ereignisse** der Core Console wird ein Protokoll aller Systemereignisse für den Rapid Recovery Core angezeigt. Für den Zugriff auf und die Anzeigen von Ereignissen für den Core klicken Sie auf (Ereignisse).

Die Seiten **Ereignisse** für eine bestimmte geschützte oder replizierte Maschine zeigen ein Protokoll der Ereignisse in Bezug auf die entsprechende Maschine an. Für den Zugriff auf und die Anzeige von Ereignissen für eine ausgewählte Maschine klicken Sie auf den Maschinennamen im Menü „Geschützte Maschinen“ und von der Seite Maschine-**Zusammenfassung** klicken Sie auf der Menü **Ereignisse**.

Die Seiten „Ereignisse“ (auf dem Core oder einer bestimmten Maschine) sind in drei Ansichten verfügbar: Aufgaben, Warnungen und Journal.Alle in einer der Kategorien angezeigten Elemente bilden ein Ereignis. Über diese Ansichten können Sie Filter-Details über verschiedene Teilmengen der Ereignisse, je nach Bedarf anzeigen. Die Standardansicht ist, wenn Tasks angezeigt werden

- Ein **Task** ist ein Ereignis im Zusammenhang mit einem Job. Ein **Job** ist ein Prozess, den der Rapid Recovery Core durchführen müssen. Jeder Job verfügt über einen aktuellen Status, eine Start- und Endzeit und ein Datum. Manche Tasks werden manuell gestartet oder durch den Benutzer geplant. Beispiele umfassen das Erzwingen eines Snapshots, das Planen einer Sicherung oder das Durchführen einer Wiederherstellung von einem Wiederherstellungspunkt. Andere Tasks sind automatische Funktionen, wie zum Beispiel nächtliche Jobs oder das Durchführen eines Rollup unter Verwendung der Standard-Aufbewahrungsrichtlinie.
- Eine **Warnung** ist ein Prioritätsereignis, z. B. ein Fehler, eine Warnung oder eine wichtige informative Meldung. Wenn Sie Benachrichtigungen über bestimmte Ereignisse anfordern, erscheinen diese Benachrichtigungen in der Teilmenge „Warnungen“.
- Das **Journal** zeigt eine vollständige Liste aller protokollierten Ereignisse an (für den Core oder die ausgewählte Maschine). Diese Liste ist umfassender und zeigt Jobs, Ereignisse mit hoher Priorität und Ereignisse mit niedriger Priorität an. Diese Kategorie schließt passive und Nicht-Job-Ereignisse ein (wie z. B. erfolgreicher Start des Core oder Statusberichte vom Lizenzportal).

Führen Sie die Schritte in den folgenden Verfahren aus, um Aufgaben, Benachrichtigungen oder ein Journal aller Ereignisse anzuzeigen:

- Anzeigen von Aufgaben
- Anzeigen von Benachrichtigungen
- Anzeigen eines Journals aller protokollierten Ereignisse
- Anzeigen von laufenden Tasks von einer beliebigen Core Console-Seite
- Navigieren zwischen Aufgaben, Warnungen und dem Ereignisjournal

Anzeigen von Aufgaben

Eine Aufgabe ist ein Job, den der Rapid Recovery Core durchführen muss, z. B. die Übertragung von Daten in einer regelmäßig geplanten Sicherung oder die Wiederherstellung aus einem Wiederherstellungspunkt.

NOTE: Aktive Aufgaben werden im Dropdown-Menü **Aktive Aufgaben** oben in der Core Console aufgelistet. Das Klicken auf eine laufende Aufgabe öffnet das Dialogfeld **Aktive Aufgabe überwachen**. Von hier aus können Sie eine oder mehrere laufende Aufgaben abbrechen. Weitere Informationen dazu finden Sie unter Anzeigen von laufenden Tasks von einer beliebigen Core Console-Seite. Sie können auch die Planung zukünftiger Aufgaben auf dem Core aufheben. Dies ist nützlich, wenn Sie beispielsweise BS-Aktualisierungen oder Serverwartung durchführen müssen. Weitere Informationen zur dieser Funktion finden Sie im Abschnitt Unterbrechen oder Wiederaufnehmen geplanter Aufgaben.

Führen Sie die folgenden Schritte zum Anzeigen der Aufgaben für den Rapid Recovery Core oder zum Anzeigen der Warnhinweise für eine bestimmte Maschine aus.

1. Zum Anzeigen aller Aufgaben für den Rapid Recovery Core klicken Sie auf der Symbolleiste auf (Ereignisse). Die Standardansicht zeigt alle Aufgaben für den Core an.

   Wenn Sie Aufgaben für eine bestimmte geschützte Maschine anzeigen möchten, navigieren Sie zu der Seite **Zusammenfassung** der angegebenen Maschine und klicken dann auf das Menü **Ereignisse**. Die Standardansicht zeigt alle Aufgaben für die ausgewählte Maschine an.

2. Optional können Sie die Liste der Aufgaben nach Stichwort, Startdatum und/oder Enddatum filtern. Gehen Sie dazu folgendermaßen vor und drücken Sie dann **Eingabe**:

   a. Geben Sie ein Stichwort in das Textfeld **Stichwortsuche** ein, um nach Stichwort zu filtern.

   Sie können beispielsweise nach Schlagwörtern wie „Rollup“, „Archiv“, „Export“ oder „Übertragung“ filtern.

   b. Geben Sie wie folgt Startdatum und -zeit ein, um nach Startdatum und -zeit zu filtern:

   - Geben Sie im Textfeld **Von** Datum und Uhrzeit im Format MM/TT/JJJJ HH:MM AM/PM ein. Geben Sie beispielsweise 1/1/2016 08:00 AM ein, wenn die Suche am ersten Tag des Januars im Jahr 2016 um 08:00 Uhr beginnen soll.
   - Klicken Sie auf das Widget **Kalender** im Textfeld **Von** und klicken Sie dann auf das aktuelle Datum. Die aktuelle Uhrzeit wird automatisch angezeigt.
   - Klicken Sie auf das Widget **Kalender**, wählen Sie das Datum und klicken Sie dann auf das Widget Uhr und wählen Sie die gewünschte Uhrzeit mithilfe der Steuerelemente. Klicken Sie außerhalb des Kalenders, um die ausgewählten Änderungen zu akzeptieren.

   c. Um die Liste der angezeigten Aufgaben weiter einzugrenzen, können Sie auch ein Enddatum und eine Endzeit angeben.

   Die Liste der Aufgaben wird sofort abhängig von den ausgewählten Kriterien gefiltert.

3. Optional können Sie die in der Liste angezeigten Aufgaben wie folgt filtern:

Option	Description
	Klicken Sie auf das Symbol **Aktive Aufgaben**, damit nur aktive Aufgaben angezeigt werden.
	Klicken Sie auf das Symbol **Aufgaben in Warteschlange**, damit nur Aufgaben angezeigt werden, die in der Warteschlange auf Durchführung warten.
	Klicken Sie auf das Symbol **Wartende Aufgaben**, damit nur Aufgaben angezeigt werden, die auf ihre Ausführung warten.
	Klicken Sie auf das Symbol **Abgeschlossene Aufgaben**, damit nur Aufgaben angezeigt werden, die beendet wurden.
	Klicken Sie auf das Symbol **Fehlgeschlagene Aufgaben**, damit nur Aufgaben angezeigt werden, die fehlgeschlagen sind.
	Um alle Ereignisse anzuzeigen, einschließlich der Service-Ereignisse für den Core, die nicht standardmäßig angezeigt werden, klicken Sie auf das Symbol **Service**.

4. Wählen Sie ein Format in der Liste aus, um die Liste der Aufgaben zu exportieren, und klicken Sie auf **Export**. Bestätigen Sie im folgenden Dialogfeld das Exportieren und klicken Sie dann **OK**.

   Sie können die folgenden Formate für den Export auswählen:

Tabelle 109. Exportformate

Die verfügbaren Ausgabeformate, in die Sie einen Bericht herunterladen können.

Format	Description
PDF	Portable Document Format (Standard-Exportformat)
HTML	Webseiten-Format
CSV	Werte mit Kommas als Trennzeichen
XLS	Arbeitsmappe Microsoft Excel 1997 - 2003
XLSX	Excel-Arbeitsmappe

   Die Datei vom Typ den Sie ausgewählt haben, wird in das Standardverzeichnis auf dem Core-Server heruntergeladen.

5. Klicken Sie auf das Symbol **Jobdetails** für eine Aufgabe, um ein neues Fenster mit Aufgabendetails zu öffnen.

Zugehörige Tasks

See also: Anzeigen von Aufgaben
See also: Unterbrechen oder Wiederaufnehmen geplanter Aufgaben
See also: Anzeigen von Benachrichtigungen

See also: Anzeigen eines Journals aller protokollierten Ereignisse
See also: Anzeigen von laufenden Tasks von einer beliebigen Core Console-Seite
See also: Navigieren zwischen Aufgaben, Warnungen und dem Ereignisjournal

Anzeigen von laufenden Tasks von einer beliebigen Core Console-Seite

Zum Durchführen dieses Verfahrens muss sichergestellt werden, dass gerade eine Aufgabe auf dem Rapid Recovery Core ausgeführt wird.

Rapid Recovery bietet eine schnelle Möglichkeit, um von jeder Seite der Core Console aus Aufgaben, die gerade auf dem Core ausgeführt werden, anzuzeigen.

Auf der rechten Seite der Schaltflächenleiste befindet sich die Warteschlange **Ausgeführte Tasks**. Bei niedrigeren Bildschirmauflösungen oder wenn das Browserfenster nicht vollständig erweitert ist, erscheint die Warteschlange möglicherweise als ein Symbol  . Wenn eine oder mehrere Aufgaben ausgeführt werden, erscheint neben der Warteschlange eine Zahl, die die Anzahl der gerade auf dem Core ausgeführten Tasks angibt, und das Symbol wird animiert. Sie können auf die Warteschlange klicken, um eine Dropdown-Liste der laufenden Aufgaben anzuzeigen und die im folgenden Verfahren beschriebenen Aktionen auszuführen.

1. Klicken Sie in der Core Console auf **Ausgeführte Tasks** oder das Symbol für ausgeführte Tasks, während eine Aufgabe ausgeführt wird.

   Eine kleine Box wird eingeblendet und zeigt den Typ der ausgeführten Tasks und deren Fortschritt an und bietet Optionen zum Abbrechen einer oder mehrerer Tasks oder zur Anzeige weiterer Informationen.
2. Zum Abbrechen einer oder mehrerer der ausgeführten Tasks, wählen Sie eine der folgenden Optionen:
   - Zum Abbrechen einer einzigen Task klicken Sie auf das **X** neben der Task-Beschreibung.
   - Zum Abbrechen aller laufenden Tasks klicken Sie auf **Alle abbrechen**.
3. Um weitere Details über eine laufende Aufgabe anzuzeigen, klicken Sie auf die Task-Beschreibung.

   Das Fenster **Aktiven Task überwachen** wird geöffnet und zeigt Einzelheiten wie z. B. Fortschritt und Startzeit an.

Zugehörige Tasks

See also: Anzeigen von Aufgaben
See also: Navigieren zwischen Aufgaben, Warnungen und dem Ereignisjournal
See also: Unterbrechen oder Wiederaufnehmen geplanter Aufgaben

Unterbrechen oder Wiederaufnehmen geplanter Aufgaben

Zum Fortsetzen des Core-Scheduler muss dieser zuerst angehalten werden, wie in Schritt 3 beschrieben.

Der Core verfolgt Aufgaben auf Grundlage eines Zeitplans. Übertragungen für Sicherung, Replikation und Archivierung können alle geplant werden. Berichte können wöchentlich oder monatlich usw. erstellt werden. Wenn die Zeit für eine geplante Aufgabe ansteht, wird der Job in eine Warteschlange platziert. Die Jobs werden dann nacheinander oder gleichzeitig, basierend auf der Priorität, ausgeführt. Diese Funktion wird auch als Core Scheduler bezeichnet.

Benutzer können nun den Core anweisen, den Scheduler zu unterbrechen. Wenn angehalten, werden zukünftige Aufträge, die sonst automatisch nach Plan auf dem Core ausgeführt werden würden, vorübergehend in eine Warteschlange gestellt, und es werden keine neuen Aufgaben geplant. Diese Funktion ist hilfreich in Situationen, wie z. B. die Durchführung von BS-Aktualisierungen, Installationen oder Wartung auf dem Core Server. Wenn aufgehoben, sammeln sich die Jobs in der Warteschlange an, werden aber nicht gestartet, bis die Core Scheduler-Funktion explizit wieder aufgenommen wird. In der Zwischenzeit wird ein Banner über der Core Console angezeigt, der darauf hinweist, dass der Core-Scheduler angehalten ist.

NOTE: Diese Funktion verhindert, dass Aufgaben, die in Kürze geplant sind, ausgeführt werden. Informationen zum Anzeigen oder Stornieren von Aufgaben, die sich bereits in der Warteschlange befinden, ohne zukünftige Aufgaben anzuhalten, finden Sie im Thema Anzeigen von laufenden Tasks von einer beliebigen Core Console-Seite.

Führen Sie die folgenden Schritte aus, um die Core Scheduler-Funktion aufzuheben oder wiederaufzunehmen.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Ereignisse).

   Die Seite **Aufgaben** wird angezeigt.
3. Zum Aufheben der Core Scheduler-Funktion gehen Sie wie folgt vor:
   a. Klicken Sie auf **Scheduler aufheben**.
   b. Wenn Sie alle laufenden Aufgaben abbrechen und zukünftige Aufgaben aufheben möchten, wählen Sie **Aktive Aufgaben abbrechen und aufheben** im Dialogfeld.
   c. Um nur zukünftige Aufgaben aufzuheben, klicken Sie auf **Aufheben**.

   Aufgaben werden angehalten, und es wird ein Banner über der Core Console angezeigt, der darauf hinweist, dass der Core-Scheduler angehalten ist.
4. Zum Fortsetzen der aufgehobenen Aufgaben klicken Sie auf der Seite **Aufgaben** auf **Scheduler fortsetzen**.

   NOTE: Wenn der Scheduler angehalten ist, können Sie auch auf **Wiederaufnehmen** im Banner oben auf der Core Console klicken.

Zugehörige Tasks

See also: Anzeigen von laufenden Tasks von einer beliebigen Core Console-Seite
See also: Anzeigen von Aufgaben
See also: Unterbrechen oder Wiederaufnehmen geplanter Aufgaben
See also: Anzeigen von Benachrichtigungen
See also: Anzeigen eines Journals aller protokollierten Ereignisse
See also: Navigieren zwischen Aufgaben, Warnungen und dem Ereignisjournal

Anzeigen von Benachrichtigungen

Eine Warnung ist eine Prioritätsbenachrichtigung eines Ereignisses. Jedes Ereignis, für das Sie ausdrücklich eine Benachrichtigung angefordert haben, wird zusammen mit Fehlern, Warnungen oder wichtigen Informationsmeldungen in der Liste der Warnungen angezeigt.

Rapid Recovery Core enthält bei der Auslieferung einen Standardsatz von Ereignissen, die als Warnungen priorisiert sind. Sie können durch Bearbeiten der Standard-Benachrichtungsgruppe (oder durch Einrichten einer neuen Benachrichtigungsgruppe) die Ereignisse anpassen, die als Warnhinweise angezeigt werden. Zusätzlich zu diesen Ereignissen, die auf der Seite **Warnhinweise** erscheinen, können Sie auch die Methoden zur Benachrichtigung ändern, indem Sie die Benachrichtigungsoptionen ändern. Weitere Informationen zum Ändern der Ereignisse, die als Warnhinweise angezeigt werden, oder zum Ändern der Benachrichtigungsoptionen finden Sie unter dem Thema Grundlegendes zu Ereignisbenachrichtigungen in Rapid Recovery.

Führen Sie die folgenden Schritte zum Anzeigen der Warnungen für den Rapid Recovery Core oder zum Anzeigen der Warnungen für eine bestimmte Maschine aus.

1. Zum Anzeigen von Warnungen für den Rapid Recovery Core klicken Sie auf der Symbolleiste auf (Ereignisse). Klicken Sie auf das Drop-Down-Menü rechts vom Titel der Seite „Aufgaben“ und wählen Sie **Warnungen** aus.

   Wenn Sie Warnhinweise für eine bestimmte geschützte Maschine anzeigen möchten, navigieren Sie zur Seite **Zusammenfassung** der angegebenen Maschine. Klicken Sie auf das Menü **Ereignisse** und dann auf **Warnungen**.

Die Liste der Ereignisse wird so gefiltert, dass nur wichtige Warnhinweise für den Core bzw. für die ausgewählte Maschine angezeigt werden.

2. Wahlweise können Sie zum Filtern der Liste der wichtigen Warnhinweise nach Startdatum, Enddatum, Beschreibung der Warnungsmeldung oder einer beliebiger Kombination davon die folgenden Schritte ausführen:
    a. Um nach Warnkategorie (Fehler, Informationsmeldungen oder Warnungen) zu filtern, klicken Sie auf das Status-Drop-Down-Menü und wählen Sie die Statusbedingung oder Bedingungen aus. Die Filteroptionen für die Warnkategorie umfassen  Fehler  Informationsmeldungen und  Warnungen oder eine beliebigen Kombination aller drei.
    b. Geben Sie wie folgt Startdatum und -zeit ein, um nach Startdatum und -zeit zu filtern:
    - Geben Sie im Textfeld **Von** Datum und Uhrzeit im Format MM/TT/JJJJ HH:MM AM/PM ein. Geben Sie beispielsweise 1/1/2016 08:00 AM ein, wenn die Suche am ersten Tag des Januars im Jahr 2016 um 08:00 Uhr beginnen soll.
    - Klicken Sie auf das Widget  **Kalender** im Textfeld **Von** und klicken Sie dann auf das aktuelle Datum. Die aktuelle Uhrzeit wird automatisch angezeigt.
    - Klicken Sie auf das Widget  **Kalender**, wählen Sie das Datum und klicken Sie dann auf das Widget  Uhr und wählen Sie die gewünschte Uhrzeit mithilfe der Steuerelemente. Klicken Sie außerhalb des Kalenders, um die ausgewählten Änderungen zu akzeptieren.

    c. Um nach der Beschreibung der Warnmeldung zu filtern, geben Sie die Beschreibung in das Textfeld **Meldung suchen** ein.

    Beispiel: Um nur Warnhinweise im Zusammenhang mit Agenten zu sehen, geben Sie „Agent“ ein, für Warnungen im Zusammenhang mit Übertragungen geben Sie „Übertragung“ ein usw.

    d. Um die Liste der angezeigten Warnhinweise weiter einzugrenzen, können Sie auch ein Enddatum und eine Endzeit im gleichen Format angeben.

    Die Liste der Warnhinweise wird sofort abhängig von den ausgewählten Kriterien gefiltert.
3. Wenn Sie alle Benachrichtigungen löschen möchten, können Sie ggf. auf **Alle schließen** klicken.

Zugehörige Tasks

See also: Konfigurieren von Benachrichtigungsgruppen
See also: Anzeigen von Aufgaben
See also: Unterbrechen oder Wiederaufnehmen geplanter Aufgaben
See also: Anzeigen von Benachrichtigungen
See also: Anzeigen eines Journals aller protokollierten Ereignisse
See also: Anzeigen von laufenden Tasks von einer beliebigen Core Console-Seite
See also: Navigieren zwischen Aufgaben, Warnungen und dem Ereignisjournal

Zugehörige Verweise

See also: Grundlegendes zu Ereignisbenachrichtigungen in Rapid Recovery

Anzeigen eines Journals aller protokollierten Ereignisse

Das Journal listet alle protokollierten Ereignisse auf. Diese Liste ist umfangreich, und schließt Job- und Nicht-Job-bezogene Ereignisse ein. Es enthält bestimmte Ereignisse, für die Sie eine Benachrichtigung angefordert haben. Das Journal führt auch passive Ereignisse und Statusereignisse vom Core, dem Lizenzportal usw. auf.

NOTE: Wenn in Ihrer Umgebung die Wiederholungsreduzierung verwendet wird, werden einige wiederholte Ereignisse möglicherweise nicht bei jedem Auftreten des Ereignisses protokolliert. Weitere Informationen zu dieser Funktion finden Sie unter Informationen zur Reduzierung von Wiederholungen

Führen Sie die folgenden Schritte zum Anzeigen eines Journals aller Ereignisse für den Rapid Recovery Core oder zum Anzeigen eines Journals aller Ereignisse für eine bestimmte Maschine aus.

1. Um ein Journal aller für den Rapid Recovery Core protokollierten Ereignisse anzuzeigen, klicken Sie auf der Symbolleiste auf (Ereignisse). Klicken Sie auf das Drop-Down-Menü rechts vom Titel der Seite „Aufgaben“ und wählen Sie **Journal** aus.

   Wenn Sie ein Journal aller Ereignisse für eine bestimmte geschützte Maschine anzeigen möchten, navigieren Sie zur Seite **Zusammenfassung** der angegebenen Maschine. Klicken Sie auf das Menü **Ereignisse** und anschließend auf **Journal**.

2. Wahlweise können Sie zum Filtern der Liste aller Ereignisse, nach Startdatum, Enddatum, Beschreibung der Warnungsmeldung oder einer beliebiger Kombination davon die folgenden Schritte ausführen:

   a. Um nach Ereigniskategorie (Fehler, Informationsmeldungen oder Warnungen) zu filtern, klicken Sie auf das Status-Drop-Down-Menü und wählen Sie die Statusbedingung oder Bedingungen aus. Die Filteroptionen für die Ereigniskategorie umfassen Fehler Informationsmeldungen und Warnungen oder eine beliebigen Kombination aller drei.

   b. Geben Sie wie folgt Startdatum und -zeit ein, um nach Startdatum und -zeit zu filtern:

   - Geben Sie im Textfeld **Von** Datum und Uhrzeit im Format MM/TT/JJJJ HH:MM AM/PM ein. Geben Sie beispielsweise 1/1/2016 08:00 AM ein, wenn die Suche am ersten Tag des Januars im Jahr 2016 um 08:00 Uhr beginnen soll.
   - Klicken Sie auf das Widget **Kalender** im Textfeld **Von** und klicken Sie dann auf das aktuelle Datum. Die aktuelle Uhrzeit wird automatisch angezeigt.
   - Klicken Sie auf das Widget **Kalender**, wählen Sie das Datum und klicken Sie dann auf das Widget Uhr und wählen Sie die gewünschte Uhrzeit mithilfe der Steuerelemente. Klicken Sie außerhalb des Kalenders, um die ausgewählten Änderungen zu akzeptieren.

   c. Um nach der Beschreibung der Warnmeldung zu filtern, geben Sie die Beschreibung in das Textfeld **Meldung suchen** ein.

   Beispiel: Um nur Warnhinweise im Zusammenhang mit Agenten zu sehen, geben Sie „Agent“ ein, für Warnungen im Zusammenhang mit Übertragungen geben Sie „Übertragung“ ein.

   d. Um die Liste der angezeigten Aufgaben weiter einzugrenzen, können Sie auch ein Enddatum und eine Endzeit im gleichen Format angeben.

   Die Liste der Ereignisse wird sofort abhängig von den ausgewählten Kriterien gefiltert.

Zugehörige Konzepte

See also: Informationen zur Reduzierung von Wiederholungen

Zugehörige Tasks

See also: Anzeigen von Aufgaben
See also: Unterbrechen oder Wiederaufnehmen geplanter Aufgaben
See also: Anzeigen von Benachrichtigungen
See also: Anzeigen eines Journals aller protokollierten Ereignisse
See also: Anzeigen von laufenden Tasks von einer beliebigen Core Console-Seite
See also: Navigieren zwischen Aufgaben, Warnungen und dem Ereignisjournal

Navigieren zwischen Aufgaben, Warnungen und dem Ereignisjournal

Ereignisse, die in den Core-Protokollen aufgezeichnet werden, sind in der Core Console sichtbar und in drei Kategorien unterteilt: Aufgaben, Warnungen und ein Journal aller protokollierten Ereignisse.

Unabhängig davon, ob Sie Ereignisse für den Core einer bestimmten Maschine anzeigen, ist die Standardansicht für Ereignisse ist die Seite **Aufgaben**. Durch Klicken auf das Drop-Down-Menü rechts von dem Seitentitel können Sie eine andere Ansicht der Ereignisse auswählen.

Führen Sie folgende Schritte durch, um Ereignisse anzuzeigen und zwischen Aufgaben, wichtigen Warnungen und einem Journal aller Ereignisse zu navigieren.

Sie können durch Klicken auf (Ereignisse) auf der Symbolleiste Ereignisse anzeigen, die sich auf den Core beziehen.

Wenn Sie zuerst zu einer geschützten oder replizierten Maschine navigieren und dann **Ereignisse** aus dem Menü oben auf der Seite wählen, können Sie Ereignisse für die angegebene Maschine anzeigen.

Unabhängig davon, ob Sie Ereignisse für den Core einer bestimmten Maschine anzeigen, ist die Standardansicht für Ereignisse ist die Seite **Aufgaben**. Durch Klicken auf das Drop-Down-Menü rechts von dem Seitentitel können Sie eine andere Ansicht der Ereignisse auswählen.

1. Zum Anzeigen aller Aufgaben für den Rapid Recovery Core klicken Sie auf der Symbolleiste auf (Ereignisse).

   Die Standardansicht zeigt alle Aufgaben für den Core an. Fahren Sie mit Schritt 3 fort.
2. Wenn Sie Aufgaben für eine bestimmte geschützte Maschine anzeigen möchten, navigieren Sie zu der Seite **Zusammenfassung** der angegebenen Maschine und klicken dann auf das Menü **Ereignisse**.

   Die Standardansicht zeigt alle Aufgaben für die ausgewählte Maschine an. Fahren Sie mit Schritt 3 fort.
3. Klicken Sie oben links im Fenster **Tasks** auf (den nach unten gerichteten Pfeil rechts vom Tasks-Titel).

   Ein Drop-Down-Menü wird angezeigt.
4. Wählen Sie eine der folgenden Optionen:

Option	Description
Aufgabe	Eine Aufgabe ist ein Job, den der Rapid Recovery Core durchführen muss, z. B. die Übertragung von Daten in einer regelmäßig geplanten Sicherung oder die Wiederherstellung aus einem Wiederherstellungspunkt.
Warnung	Bei einer Warnung handelt es sich um eine Prioritätsbenachrichtigung in Zusammenhang mit einer Aufgabe oder einem Ereignis, z. B. ein Fehler, eine Warnung oder eine wichtige informative Meldung.
Journal	Das Journal zeigt eine vollständige Liste aller protokollierten Ereignisse an. Diese Liste ist umfassender als die in die Warnungen eingeschlossene Teilgruppe.

Die ausgewählte Ansicht der Ereignisse wird angezeigt. Wenn Sie zum Beispiel **Warnungen** ausgewählt haben, wird die Seite „Warnungen“ angezeigt

5. Um eine andere Ansicht zu sehen, kehren Sie zum Dropdown-Menü auf der rechten Seite des Fensterbereichs „Tasks“, „Warnungen“ oder „Journal“ zurück und wählen Sie die Option für die Sie gewünschte Ansicht.

   Der Liste der Ereignisse wird gefiltert und zeigt nun nur den relevanten Satz von Ereignissen für die aktuelle Ansicht an.

Zugehörige Tasks

See also: Anzeigen von Aufgaben
See also: Anzeigen von Benachrichtigungen
See also: Anzeigen eines Journals aller protokollierten Ereignisse
See also: Anzeigen von laufenden Tasks von einer beliebigen Core Console-Seite

Grundlegendes zu Ereignisbenachrichtigungen in Rapid Recovery

Die Rapid Recovery Core verfolgt viele Ereignisse und protokolliert die Informationen für Diagnose- und betriebliche Zwecke.

Sie können die Benachrichtigung bestimmter Ereignisse einrichten. Rapid Recovery ermöglicht Ihnen, die Methode der Benachrichtigung und den Zeitraum, währenddessen das System eine Aufzeichnung dieser Ereignisse aufbewahren sollte, zu wählen. Mithilfe der Reduzierungsfunktion für Wiederholungen können Sie sogar die Häufigkeit der Benachrichtigung über das gleiche Ereignis einstellen.

Auf dem Core nachverfolgte Jobs und Ereignisse werden standardmäßig 30 Tage lang gespeichert. Angaben zum Ändern der Aufbewahrungsdauer für die Verfolgung von Ereignissen finden Sie unter Konfigurieren der Ereignisaufbewahrung

Sie können von Ereignissen über verschiedene Methoden benachrichtigt werden. Die verfügbaren Benachrichtigungsmethoden sind in der folgenden Tabelle aufgelistet.

Tabelle 110. Unterstützte Ereignis-Benachrichtigungsmethoden

Optionstyp	Description	Standardeinstellung
E-Mail	Benachrichtigt den angegebenen Benutzer per E-Mail unter Verwendung der SMTP Konfigurationseinstellungen im Core und basierend auf der verwendeten E- Mail-Benachrichtigungsvorlage.	Aus
Windows-Ereignisprotokoll	Protokolliert Ereignisse mithilfe der Windows Ereignisprotokoll-API. Dieses Protokoll kann vom Windows Event Viewer oder speziellen Anwendungen gelesen werden.	Ein
syslogd	Protokolliert Ereignisse, die auf einem Linux-Protokollserver gelesen werden sollen, der auch das Syslog Message-Protokoll unterstützt.	Aus
Pop-up-Warnung	Wenn diese Benachrichtigungsmethode ausgewählt ist, werden Meldungen kurz in einem Popup-Fenster in der rechten unteren Ecke der Rapid Recovery Core Console angezeigt.	Ein
SNMP-Trap	Wenn Sie den Rapid Recovery Core als einen SNMP-Agent konfigurieren und diese Benachrichtigungsmethode ausgewählt ist, werden	Ein

Optionstyp	Description	Standardeinstellung
	Ereignisse an einen Protokollserver unter Verwendung der im Dialogfeld „Benachrichtigungsoptionen“ angegebenen Trap-Nummer gesendet.	

Benachrichtigungsgruppen ermöglichen Ihnen die Arten von Ereignissen festzulegen, über die Sie benachrichtigt werden möchten, und die Benachrichtigungsmethode anzugeben.

Rapid Recovery Core erfordert mindestens eine Benachrichtigungsgruppe und wird mit einer Standardgruppe ausgeliefert, die automatisch angewandt wird. Sie können die Standardeinstellungen verwenden oder sie bearbeiten.

Optional können Sie zusätzliche Benachrichtigungsgruppen hinzufügen und konfigurieren. Sie können beispielsweise die Standardgruppe unverändert verwenden und eine andere Gruppe einrichten, die E-Mail-Benachrichtigungen verwendet.

Ein weiteres Beispiel wäre, dass Sie eine benutzerdefinierte Benachrichtigungsgruppe für einen Ereignistyp einrichten (zum Beispiel Microsoft Exchange) und alle zugehörigen Warnungsbenachrichtigungen an einen Exchange-Administrator senden.

Weitere Informationen finden Sie unter Konfigurieren von Benachrichtigungsgruppen.

E- Mail-Benachrichtigungen sind standardmäßig deaktiviert. Um Benachrichtigungen per E-Mail zu senden, müssen Sie einen E-Mail-Server einrichten und bearbeiten oder eine Benachrichtigungsgruppe mit aktivierter Option **Per E-Mail benachrichtigen** hinzufügen. Diese Einstellung erfordert die Eingabe der E-Mail-Adresse, an die die Benachrichtigungen gesendet werden. Weitere Informationen finden Sie unter Konfigurieren eines E-Mail-Servers.

Wenn Sie einen Exchange Server verwenden, müssen Sie Relay auf dem Server einrichten. Andernfalls werden trotz erfolgreicher E-Mail-Tests keine E-Mail-Benachrichtigungen gesendet. Weitere Informationen erhalten Sie von Ihrem Exchange Server-Administrator.

Der Core verwendet eine E-Mail-Benachrichtigungsvorlage. Die Vorlage enthält eine Betreffzeile und spezifische Inhalte für den Nachrichtentext. Eine Standard E-Mail-Benachrichtigungsvorlage ist eingeschlossen. Die Vorlage identifiziert den Core und den Server-Host, das Datum und die Uhrzeit des Ereignisses, die Art des Ereignisses sowie Fehlerdetails, falls relevant. Optional können Sie die Standardvorlage ändern oder Anpassungen rückgängig machen, um die Standardeinstellungen wiederherzustellen. Weitere Informationen finden Sie unter Konfigurieren einer E-Mail-Benachrichtigungsvorlage.

Sie können die Anzahl der Ereignisse des gleichen Typs und Bereichs, die protokolliert und in der Core Console angezeigt werden, mithilfe der Reduzierungsfunktion für Wiederholungen reduzieren. Diese Option ist standardmäßig aktiviert. Sie können diese Funktion deaktivieren oder den Zeitraum, für den Ereignisse im Ereignisprotokoll zu einem einzelnen Vorkommen zusammengefasst werden, steuern. Weitere Informationen finden Sie unter Informationen zur Reduzierung von Wiederholungen.

Zugehörige Konzepte

See also: Informationen zur Reduzierung von Wiederholungen

Zugehörige Tasks

See also: Konfigurieren von Benachrichtigungsgruppen
See also: Konfigurieren der Ereignisaufbewahrung

Zugehörige Verweise

See also: Grundlegende Informationen zu E-Mail-Benachrichtigungen

Konfigurieren von Benachrichtigungsgruppen

NOTE: Sie müssen zunächst SMTP-Servereinstellungen (Simple Mail Transfer Protocol) konfigurieren, wenn Benachrichtigungen als E-Mail-Nachrichten gesendet werden sollen (siehe nachstehende Beschreibung). Weitere Informationen zum Festlegen von Konfigurationseinstellungen für E-Mail-Server finden Sie unter Konfigurieren eines E-Mail-Servers.

Benachrichtigungsgruppen bieten die Möglichkeit, bestimmte Ereignisse zu definieren, über die Benutzer benachrichtigt werden, sowie festzulegen, wir die Benachrichtigung erfolgen soll. Sie können zum Senden von Benachrichtigungen folgende Methoden konfigurieren:

- E-Mail
- Windows-Ereignisprotokoll
- Syslogd
- Pop-up-Warnungen
- Benachrichtigungen
- SNMP-Traps

Rapid Recovery Core wird mit einer standardmäßigen Benachrichtigungsgruppe für den Core geliefert. Sie können diese Gruppe gemäß Ihren Bedürfnissen bearbeiten. Sie können optional mehr als eine Benachrichtungsgruppe mit unterschiedlichen Benachrichtigungsparametern konfigurieren.

Benachrichtungsgruppen können auf Core-Ebene oder für einzelne geschützte Maschinen festgelegt werden.

Führen Sie die folgenden Schritte aus, um Benachrichtigungsgruppen für Benachrichtigungen zu konfigurieren.

1. Um Benachrichtigungen auf Core-Ebene einzustellen, klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Benachrichtigungen**.

   Die Seite **Benachrichtigungen** wird angezeigt. Fahren Sie mit Schritt 3 fort.
2. Zum Einstellen von Benachrichtigungen für eine bestimmte geschützte Maschine, führen Sie die folgenden Schritte aus:
   a. Klicken Sie im Menü „Geschützte Maschinen“ auf die geschützte Maschine, für die Sie Benachrichtigungen angeben möchten.

   Die Seite **Zusammenfassung** wird angezeigt.

   b. Wählen Sie auf der Seite **Zusammenfassung** der geschützten Maschine die Option **Benachrichtigungen** aus dem Drop-Down-Menü **Mehr**.

   Die Seite **Benutzerdefinierte Benachrichtigungsgruppen** wird angezeigt.
3. Wenn Sie eine neue Benachrichtigungsgruppe hinzufügen möchten, klicken Sie auf **+Gruppe hinzufügen**. Fahren Sie mit Schritt 5 fort.

   Das Dialogfeld **Benachrichtigungsgruppe hinzufügen** wird angezeigt. Es enthält einen allgemeinen Beschreibungsbereich und zwei Registerkarten:
4. Wenn Sie die Standard-Benachrichtigungsgruppe oder eine vorhandene Benachrichtigungsgruppe bearbeiten möchten, klicken Sie im Fensterbereich „Benachrichtigungsgruppen“ auf das Drop-Down-Menü (Mehr) für die entsprechende Benachrichtigungsgruppe und wählen Sie **Bearbeiten**.

   Das Dialogfeld **Benachrichtigungsgruppe bearbeiten** wird angezeigt. Es enthält einen allgemeinen Beschreibungsbereich und zwei Registerkarten:
5. Geben Sie im Bereich „Allgemein“ die in der folgenden Tabelle beschriebenen grundlegenden Informationen für die Benachrichtigungsgruppe ein.

Option	Description
Name	Geben Sie einen Namen für die Ereignisbenachrichtigungsgruppe ein. Diese Information ist erforderlich. **CAUTION: Der für den Benachrichtigungsgruppennamen eingegebene Wert kann später nicht mehr geändert werden.**

Option	Description
Description	Geben Sie eine Beschreibung ein, die den Zweck der Ereignisbenachrichtigungsgruppe verdeutlicht. Diese Information ist optional.

6. Konfigurieren Sie auf der Registerkarte **Benachrichtigungen aktivieren** die Benachrichtigungen, die zu Warnungen führen sollen. Diese werden auf der Seite **Warnungen** beim Anzeigen von Ereignissen in der Core Console angezeigt. Sie können Gruppen von Ereignissen auswählen, wie in der folgenden Tabelle beschrieben.

Option	Description
Alle Benachrichtigungen	Wählen Sie zum Erstellen von Warnungen für alle Ereignisse
Fehler	Zum Erstellen von Warnungen für Fehler klicken Sie im Menü **Typen auswählen** auf **Fehler**. Wird durch ein rotes X gekennzeichnet.
Warnung	Zum Erstellen von Warnungen für Fehler klicken Sie im Menü **Typen auswählen** auf **Warnung**. Wird dies durch ein gelbes Ausrufezeichen gekennzeichnet.
Info	Zum Erstellen von Warnungen für Informationsmeldungen klicken Sie im Menü **Typen auswählen** auf **Info**. Dies ist durch ein blaues „i“ gekennzeichnet.
Standardeinstellungen wiederherstellen	oder die vorgegebene Core-Benachrichtigungsgruppe aus und klicken Sie auf **Standardeinstellungen zurücksetzen** im Menü **Typen auswählen**, um die Gruppe von Ereignissen, die als Warnungen angezeigt werden sollen, auf die Standardeinstellung zurückzusetzen. **NOTE:** Diese Option ist nur beim Bearbeiten der vorgegebenen Core-Benachrichtigungsgruppe verfügbar. Sie ist nicht verfügbar für neue Core-Benachrichtigungsgruppen oder für Konfigurationsbenachrichtigungen für eine bestimmte geschützte Maschine.

7. Zum Erstellen von Warnungen für einen bestimmten Ereignistyp (Fehler, Warnung oder informative Meldung), gehen Sie wie folgt vor:
    a. Wenn die Option **Alle Warnungen** keine Warnungsgruppen anzeigt, klicken Sie auf die rechte spitze Klammer **>** vor dem Etikett „Alle Warnungen“. Das Symbol ändert sich zu einem nach unten zeigenden Pfeil, und die Ansicht erweitert sich auf die Anzeige von Gruppen.

b. Klicken Sie dann auf die rechte spitze Klammer **>** neben einer bestimmten Warnungsgruppe, um zugehörige Ereignisse in der Gruppe anzuzeigen.

- Um Warnungen für alle Ereignisse in jeder Gruppe zu definieren, markieren Sie das Kontrollkästchen für **Alle Warnungen**.
- Um Benachrichtigungen für alle Ereignisse in einer beliebigen Warnungsgruppe zu definieren, markieren Sie das Kontrollkästchen neben der betreffenden Gruppe.
- Um nur einige Warnungstypen innerhalb einer Warnungsgruppe auszuwählen, erweitern Sie die Gruppe und wählen Sie dann nur diejenigen Ereignisse, für die Sie Warnungen protokollieren, melden und festlegen möchten.

8. Klicken Sie auf die Registerkarte **Benachrichtigungsoptionen**.
9. Geben Sie auf der Registerkarte **Benachrichtigungsoptionen** an, wie die Benachrichtigung erfolgen soll.

Option	Description
Per E-Mail benachrichtigen	Geben Sie die Empfänger der E-Mail-Benachrichtigung an. Sie können entweder mehrere getrennte E-Mail-Adressen sowie BCC- und CC-Empfänger angeben. **NOTE:** Bei der Verwendung von Exchange Server muss SMTP-Relay auf dem Server eingerichtet sein. Andernfalls werden Ereignisbenachrichtigungen nicht an die angegebene E- Mail-Adresse gesendet. Weitere Informationen erhalten Sie von Ihrem Exchange Server-Administrator.
Über Windows-Ereignisprotokoll benachrichtigen	Wählen Sie diese Option, wenn Benachrichtigungen über das Windows-Ereignisprotokoll gemeldet werden sollen.
Über syslogd benachrichtigen	Wählen Sie diese Option, wenn Benachrichtigungen durch syslogd gemeldet werden sollen. Geben Sie die Details für syslogd in den folgenden Textfeldern an: • Host: • Port:
Über Popupbenachrichtigungen benachrichtigen	Wählen Sie diese Option aus, wenn die Benachrichtigung als Popupmeldungen in der unteren rechten Ecke des Bildschirms angezeigt werden soll.
Über SNMP-Trap benachrichtigen	Der Rapid Recovery Core fungiert als SNMP-Agent, der Traps (Benachrichtigungen zu bestimmten Ergebnissen) an einen SNMP-Manager sendet, um Core-Informationen wie Ereignisbenachrichtigungen, Repositorystatus und geschützte Maschinen zu melden. Wählen Sie diese Option aus, wenn Core-Ereignisse über SNMP-Traps gemeldet werden sollen. Sie müssen außerdem eine Trap Nummer angeben, die vom SNMP-Manager verwendet wird.

10. Klicken Sie auf **OK**.

Beim Erstellen einer neuen Gruppe wird eine Meldung mit dem Hinweis angezeigt, dass der festgelegte Name der Benachrichtigungsgruppe nicht mehr geändert werden kann, nachdem die Gruppe erstellt wurde. Die anderen Eigenschaften der Benachrichtigungsgruppe können jederzeit geändert werden.

- Bestätigen Sie die Meldung, wenn Sie den eingegebenen Gruppennamen verwenden möchten, um die Einstellungen zu speichern.
- Klicken Sie auf **Nein**, wenn Sie den Gruppennamen ändern möchten, um zum Fenster zum Erstellen der Benachrichtigungsgruppe zurückzukehren. Aktualisieren Sie dort den Gruppenname und ggf. andere Einstellungen für die Benachrichtigungsgruppe und speichern Sie die Einstellungen.

Die Benachrichtigungsgruppe wird in der Übersichtstabelle angezeigt. Sie können verschiedene Benachrichtigungsgruppen unter Verwendung einer beliebigen Anzahl an Parametern erstellen.

Grundlegende Informationen zu E-Mail-Benachrichtigungen

Sie können Rapid Recovery Core so konfigurieren, dass Sie eine Benachrichtigung zu bestimmten Ereignissen in Form einer E-Mail-Nachricht an eine von Ihnen festgelegte E-Mail-Adresse erhalten. Die Ereignisse, die Benachrichtigungen auslösen, und die Benachrichtigungsmethoden werden in der Benachrichtigungsgruppe definiert.

NOTE: Benachrichtigungsgruppen müssen unabhängig davon eingerichtet werden, ob die Benachrichtigung per E-Mail erfolgt. Weitere Informationen hierzu finden Sie unter Konfigurieren von Benachrichtigungsgruppen.

Rapid Recovery verwendet eine E-Mail-Benachrichtigungsvorlage, welche die in jeder Benachrichtigung gesendeten Informationen festlegt. Die Vorlage definiert die E-Mail-Betreffzeile der einzelnen Benachrichtigungen sowie den Inhalt der E-Mail-Nachrichten. Die Vorlage verfügt über Standardeinstellungen, die Sie unverändert übernehmen oder überprüfen und Ihren Anforderungen entsprechend ändern können. Sie können zu einem beliebigen Zeitpunkt nach der Anpassung der Mail-Benachrichtigungsvorlage die Option „Standardeinstellungen wiederherstellen“ wählen, um zur Verwendung der Standardvorlage zurückzukehren. Weitere Informationen über das Anzeigen und Anpassen der E-Mail-Benachrichtigungsvorlage finden Sie unter Konfigurieren einer E-Mail-Benachrichtigungsvorlage.

Wenn Sie E-Mails als eine Ihrer Benachrichtigungsoptionen auswählen, müssen Sie zuerst einen SMTP-Server für E-Mails konfigurieren. Der Rapid Recovery Core verwendet den von Ihnen festgelegten Server zum Senden von Benachrichtigungen basierend auf den Parametern in der Benachrichtigungsgruppe.

Um E- Mail-Benachrichtigungen zu erhalten, müssen Sie außerdem die Option **Per E-Mail benachrichtigen** Option innerhalb der Benachrichtigungsgruppe aktivieren. Die Benachrichtigungsoption ist standardmäßig deaktiviert. Die Einstellung **Per E-Mail benachrichtigen** erfordert, dass als Minimum eine Adresse „An“ definiert ist. Optional können Sie CC- und BCC-Adressen hinzufügen, falls gewünscht.)

In diesem Abschnitt werden folgende Themen behandelt:

- Konfigurieren eines E-Mail-Servers
- Konfigurieren einer E-Mail-Benachrichtigungsvorlage

Konfigurieren eines E-Mail-Servers

Führen Sie die folgenden Schritte aus, um einen E-Mail-Server zu konfigurieren.

NOTE: Darüber hinaus müssen Sie Einstellungen für Benachrichtigungsgruppen konfigurieren, z. B. die Option **Per E-Mail benachrichtigen** aktivieren, damit E-Mail-Benachrichtigungen gesendet werden können. Weitere Informationen zum Angeben von Ereignissen, für die E-Mail-Benachrichtigungen erstellt werden sollen, finden Sie unter Konfigurieren von Benachrichtigungsgruppen.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite „Einstellungen“ auf **SMTP-Server**.
   - Scrollen Sie auf der rechten Seite der Seite „Einstellungen“ nach unten, bis sie die Überschrift **SMTP-Server** sehen können.
3. Klicken Sie auf die Einstellung, die Sie ändern möchten.

   Die ausgewählte Einstellung wird bearbeitbar.
4. Geben Sie die Konfigurationsinformationen ein (siehe Beschreibung in der folgenden Tabelle).

Option	Description
SMTP-Server	Geben Sie den Namen des E-Mail-Servers an, der von der E-Mail-Benachrichtigungsvorlage verwendet werden soll. Angegeben werden müssen Hostname, Domäne und Suffix, z.B. smtp.gmail.com.
Von	Geben Sie eine Absender-E-Mail-Adresse ein. Diese Option wird zur Angabe der Absender-E-Mail-Adresse für die E-Mail-Benachrichtigungsvorlage verwendet, z. B. noreply@localhost.com.
Benutzername	Geben Sie einen Benutzernamen für den E-Mail-Server ein.
Kennwort	Geben Sie das erforderliche Kennwort für den Benutzernamen für den Zugriff auf den E-Mail-Server ein.
Port	Geben Sie eine Portnummer ein. Sie wird zur Angabe des Ports für den E-Mail-Server verwendet, z. B. Port 587 für Gmail. Die Standardeinstellung ist 25.
Zeitlimit (Sekunden)	Geben Sie einen ganzzahligen Wert für den Zeitraum ein, in dem eine Verbindung zum E-Mail-Server hergestellt werden soll. Der Zeitraum vor einer Zeitüberschreitung wird in Sekunden angegeben. Die Standardeinstellung ist 60 Sekunden.
TLS	Wählen Sie diese Option aus, wenn der E-Mail-Server eine sichere Verbindung verwendet, z. B.

Option	Description
	Transport Layer Security (TLS) oder Secure Sockets Layer (SSL).

5. Klicken Sie für jede Einstellung nach Fertigstellung einer Änderung auf , um die Änderungen zu speichern und den Bearbeitungsmodus zu beenden, oder klicken Sie auf , um den Bearbeitungsmodus ohne Speichern zu beenden.

   CAUTION: Wenn Sie nicht jede einzelne Änderung bestätigen, werden Ihre Einstellungen nicht geändert.

6. Klicken Sie auf **Test-E-Mail senden** und führen Sie die folgenden Aktionen aus:
   a. Geben Sie im Dialogfeld **Test-E-Mail senden** eine E-Mail-Zieladresse für die Testnachricht ein und klicken Sie auf **Senden**.
   b. Schließen Sie das Fehlerdialogfeld und das Dialogfeld **Test-E-Mail senden**, wenn die Testnachricht fehlschlägt, und ändern Sie die Konfigurationseinstellungen für den E-Mail-Server. Senden Sie dann die Testnachricht erneut.
   c. Klicken Sie auf **OK**, wenn die Testnachricht erfolgreich gesendet wurde, um dies zu bestätigen.
   d. Überprüfen Sie das E-Mail-Konto, an das die Test-E-Mail-Nachricht gesendet wurde.

Konfigurieren einer E-Mail-Benachrichtigungsvorlage

Wenn Sie Benachrichtigungen von Rapid Recovery Ereignissen per E-Mail aktivieren, wird standardmäßig ein Standardschema für Sie erstellt. Der für den Core definierte SMTP-E-Mail Server verwendet diese Vorlage zum Senden von Benachrichtigungen bezüglich Rapid Recovery Ereignissen per E-Mail.

Dieses Thema beschreibt den Prozess der Konfiguration der standardmäßigen E- Mail-Benachrichtigungsvorlage oder das Anpassen des Inhalts. Unter Verwendung der Wiederherstellungs-Standardoption können Sie Änderungen an der standardmäßigen Benachrichtigungsvorlage jederzeit wiederherstellen.

CAUTION: Ändern Sie die Vorlage auf eigenes Risiko. Sie sind verantwortlich für die Prüfung sämtliche Modifizierungen der Vorlage. Nur die Standardvorlage wird unterstützt.

Führen Sie die folgenden Schritte aus, um eine E-Mail-Benachrichtigungsvorlage zu konfigurieren.

NOTE: Darüber hinaus müssen Sie einen E-Mail-Server und Einstellungen für Benachrichtigungsgruppen konfigurieren, z. B. die Option **Per E-Mail benachrichtigen** aktivieren, damit E-Mail-Warnmeldungen gesendet werden können. Weitere Informationen zum Konfigurieren eines E-Mail-Servers zum Senden von Warnmeldungen finden Sie unter Konfigurieren eines E-Mail-Servers. Weitere Informationen zum Angeben von Ereignissen, für die E-Mail-Benachrichtigungen erstellt werden sollen, finden Sie unter Konfigurieren von Benachrichtigungsgruppen.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Benachrichtigungen**.

   Die Seite **Benachrichtigung** wird angezeigt.

3. Klicken Sie im Bereich „E-Mail-Einstellungen“ auf **Ändern**.

   Das Dialogfeld **Edit Email Notification Configuration** (Konfiguration der E-Mail-Benachrichtigung bearbeiten) wird angezeigt.

4. Wählen Sie **E-Mail-Benachrichtigungen aktivieren** aus.

   Die E- Mail-Vorlage ist aktiviert und sichtbar. Die Werte der standardmäßigen E-Mail-Vorlage werden im folgenden Schritt beschrieben.

5. Überprüfen Sie den Inhalt im Dialogfeld „Konfiguration der E-Mail-Benachrichtigung bearbeiten“ und stellen Sie fest, ob der Standardinhalt sich für Ihre Anforderungen eignet.

Option	Description
E-Mail-Benachrichtigungen aktivieren	Diese Einstellung aktiviert oder deaktiviert der E-Mail-Benachrichtigungsvorlage. • Um E-Mail-Benachrichtigungen zu aktivieren, wählen Sie diese Option. • Zum Deaktivieren von Benachrichtigung per E-Mail, löschen Sie diese Option.
E-Mail-Betreff	Der Inhalt dieses Textfeld steuert die Betreffzeile für E-Mail-Nachrichten, die als Benachrichtigungen von Systemereignissen gesendet wurden. Die standardmäßige E-Mail-Betreffzeile lautet wie folgt: `<hostName> <level>: <Name> für <agentName>`
E-Mail	Der Inhalt dieses Textbereichs steuert den Textkörper für E-Mail-Nachrichten, die als Benachrichtigungen von Systemereignissen gesendet wurden. Die standardmäßige E-Mail-Textkörper-Nachricht lautet wie folgt: `<shortCompanyName> <coreProductName> auf <hostName> meldete das <level> Ereignis „<Name> Datum/Zeit: <localTimestamp> <message> <if(details.errorDetails)> <details.ErrorDetails.Message> <details.ErrorDetails.Details> <endif> --- Über dieses Ereignis: <description> <coreAdminUrl>`
Test-E-Mail senden	Durch Klicken auf diese Schaltfläche wird eine Test-E-Mail an die E- Mail-Adresse gesendet, die Sie im resultierenden Dialogfeld **Test-Email senden** angeben.
Standardeinstellungen wiederherstellen	Durch Klicken auf diese Schaltfläche werden besondere Änderungen aus der E-Mail-Vorlage entfernt und der E-Mail-Betreff und die E-Mail-Felder mit dem in dieser Tabelle beschriebenen Standard-Inhalt wiederhergestellt.
OK	Durch Klicken auf diese Schaltfläche werden die Einstellungen im Dialogfeld „Konfiguration der E-Mail-Benachrichtigung bearbeiten“ bestätigt und speichert.

Option	Description
Abbrechen	Durch Klicken auf diese Schaltfläche werden Änderungen im Dialogfeld „Konfiguration der E-Mail-Benachrichtigung bearbeiten“ abgebrochen.

6. Wenn Sie die E-Mail-Vorlage anpassen möchten, nehmen Sie die Änderungen an Text oder Variablen vor, die im vorherigen Schritt beschrieben werden. Die standardmäßig verwendeten Variablen werden in der folgenden Tabelle beschrieben.

Option	Description
hostName	Der Hostname des Core
Details	Das Detail-Objekt des spezifischen Ereignisses.
agentName	Der Name der geschützten Maschine im Zusammenhang mit diesem Ereignis, wenn das Ereignis den Umfang einer einzelnen geschützten Maschine hat.
repositoryName	Der Name des Repository im Zusammenhang mit diesem Ereignis, wenn das Ereignis einen Repository-Umfang hat.
jobSummary	Die Zusammenfassung des mit diesem Ereignis verknüpften Jobs, wenn das Ereignis einen Job-Umfang hat.
remoteSlaveCoreName	Der Name des Remoteziels im Zusammenhang mit diesem Ereignis, wenn das Ereignis einen Remoteziel-Umfang hat.
remoteMasterCoreName	Der Name der Remote-Quelle im Zusammenhang mit diesem Ereignis, wenn das Ereignis einen Quell-Core-Umfang hat.
productName	Der Name des Produkts, z. B. „AppAssure Core“ oder „Rapid Recovery Core“. Dieser Produktname kann für das Branding mit White-Labeling geändert werden.
companyName	Der Name des Unternehmens, das das Produkt verkauft.

7. Geben Sie in das Textfeld **E-Mail-Betreff** einen Betreff für die E-Mail-Vorlage ein.

   Der E-Mail-Betreff wird zur Definition des Betreffs der E-Mail-Benachrichtigungsvorlage verwendet, z. B. <Hostname> - <Level>: <Name>.

8. Geben Sie im Textfeld **E-Mail** die Informationen für den Nachrichtentext der Benachrichtigung ein, der das Ereignis, den Zeitpunkt, zu dem das Ereignis aufgetreten ist, und den Schweregrad beschreibt.
9. Klicken Sie auf **Test-E-Mail senden** und führen Sie die folgenden Aktionen aus:
   a. Geben Sie im Dialogfeld Test-E-Mail senden eine E-Mail-Zieladresse für die Testnachricht ein und klicken Sie auf **Senden**.
   b. Wenn die Test-Nachricht nicht erfolgreich versendet wird, beenden Sie das Fehler-Dialogfeld und das Dialogfeld „Test-E-Mail senden“, klicken Sie auf **OK**, um die aktuellen E-Mail-Einstellungen

zu speichern. Ändern Sie dann Ihre E-Mail-Server-Einstellungen wie im Verfahren Konfigurieren eines E-Mail-Servers beschrieben. Stellen Sie sicher, dass Sie das Kennwort für dieses Konto wieder eingeben. Speichern Sie die Einstellungen und kehren Sie hierher zurück.

c. Klicken Sie auf **OK**, wenn die Testnachricht erfolgreich gesendet wurde, um dies zu bestätigen.

d. Überprüfen Sie das E-Mail-Konto, an das die Test-E-Mail-Nachricht gesendet wurde.

Kehren Sie wieder zum Dialogfeld „Konfiguration der E-Mail-Benachrichtigung bearbeiten“ zurück, wenn Sie mit den Testergebnissen zufrieden sind, und klicken Sie auf **Speichern**, um das Dialogfeld zu schließen und die Änderungen zu speichern.

Konfigurieren von Ereigniseinstellungen

Sie können die für Ereignisse spezifischen Einstellungen konfigurieren.

Sie können beispielsweise Wiederholungsreduzierungseinstellungen festlegen und dadurch die Menge an Benachrichtigungen reduzieren, die Sie für identische wiederholte Ereignisse sehen.

Sie können auch den Zeitraum in Tagen festlegen, den Ereignisdatensätze in der Datenbank beibehalten werden.

Zeigen Sie die folgenden Themen an, um Näheres über das Konfigurieren von Ereigniseinstellungen zu erfahren.

- Informationen zur Reduzierung von Wiederholungen
- Konfigurieren der Ereignisaufbewahrung

Zugehörige Verweise

See also: Anzeigen von Ereignissen mithilfe von Aufgaben, Warnungen und Journalseiten
See also: Grundlegendes zu Ereignisbenachrichtigungen in Rapid Recovery

Informationen zur Reduzierung von Wiederholungen

Die Möglichkeit, dass Administratoren über das Auftreten bestimmter Ereignisse benachrichtigt werden, ist von entscheidender Bedeutung. Gleichwohl kann die wiederholte Benachrichtigung über Ereignisse, die bereits gemeldet wurden, frustrierend oder lästig sein. Selbst wenn eine Benachrichtigung aufgrund eines Fehlers der Umgebungsbedingungen generiert wird, den Sie sofort kennen möchten, ist es möglich, dass dieselbe Fehlerbedingung Hunderte oder Tausende von Ereignissen im Ereignisprotokoll generiert. Zur Reduzierung von Wiederholung im Ereignisprotokoll und zur Reduzierung des Empfangs wiederholter Popup-Warnungen oder E-Mail-Benachrichtigungen für das gleiche Ereignis in der Core Console enthält Rapid Recovery eine Wiederholungsreduzierungs-Einstellung, die standardmäßig aktiviert wird und auf 5 Minuten eingestellt ist. Diese Einstellung kann im Bereich von 1 Minute bis 60 Minuten festgelegt werden. Sie kann auch komplett deaktiviert werden.

Wenn die Reduzierung von Wiederholungen deaktiviert ist, wird jedes Vorkommen eines Ereignisses des gleichen Typs und Bereichs in der Datenbank protokolliert. Unabhängig vom vergangenen Zeitraum seit dem vorherigen Auftreten des Ereignisses wird jedes neue Vorkommen im Bereich „Benachrichtigungen“ der Seite „Ereignisse“ angezeigt.

Wenn die Wiederholungsreduzierung konfiguriert ist (z. B. mit dem Standardzeitraum von 5 Minuten), wird das erste Vorkommen dieses bestimmten Ereignisses in der Ereignisdatenbank protokolliert und im Warnmeldungsprotokoll angezeigt. Wird nachfolgend innerhalb des festgelegten Zeitraums erneut ein Ereignis des gleichen Typs und Bereichs protokolliert, wird der Zähler für das Ereignis in der Datenbank für jedes wiederholte Auftreten im festgelegten Zeitraum um 1 erhöht. Das Protokoll wird im Warnungen-Teil der Seite „Ereignisse“ angezeigt. Jedoch wird das Ereignis nur einmal mit dem Datum und der Uhrzeit für das aktuellste Auftreten angezeigt. Das Ereignisprotokoll wird nicht mit dem gleichen Ereignis aktualisiert, bis der Schwellenwert

ab dem ersten Auftreten abläuft. Beispiel: Wenn die Einstellung 5 Minuten ist und das Ereignis 6 Minuten später erneut eintritt, erscheint es im Protokoll und Sie erhalten eine weitere Benachrichtigung.

Konfigurieren der Reduzierung der Wiederholungen

Führen Sie die folgenden Schritte aus, um die Reduzierung der Wiederholungen für Ereignisse zu konfigurieren.

1. Navigieren Sie zu dem Rapid Recovery Core Console. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Benachrichtigungen**.

   Die Seite **Benachrichtigung** wird angezeigt.
2. Im Fensterbereich „Wiederholungsreduzierung“ zeigen Sie die vorhandenen Einstellungen.
3. Zum Aktivieren, Deaktivieren oder Ändern der gespeicherten Ereignis-Schwellenwert-Zeit klicken Sie auf **Ändern**.

   Das Dialogfeld **Wiederholungsreduzierung aktivieren** wird angezeigt.
4. Führen Sie eine der folgenden Aktionen aus:
   - Zum Deaktivieren der Wiederholungsreduzierung, entfernen Sie die Markierung aus der Option **Wiederholungsreduzierung aktivieren**.
   - Zum Aktivieren der Wiederholungsreduzierung, aktivieren Sie die Markierung der Option **Wiederholungsreduzierung aktivieren**.
   - Um den Schwellwert für Zeit (in Minuten) zu ändern, für die die wiederholten identischen Ereignisse ignoriert werden, geben Sie im Textfeld **__ minute(s)** eine Zahl zwischen 1 und 60 ein.

   NOTE: Die Option **Wiederholungsreduzierung aktivieren** muss ausgewählt sein, um diesen Wert zu ändern.
5. Klicken Sie auf **OK** um die Einstellungen zu speichern und das Dialogfeld zu schließen.

Konfigurieren der Ereignisaufbewahrung

Auf dem Core nachverfolgte Ereignisse und Jobs werden für einen bestimmten Zeitraum gespeichert. Die Standardeinstellung beträgt 30 Tage. Dieser Wert kann auf 0 bis 3652 Tage (ca. 10 Jahre) eingestellt werden.

Führen Sie die folgenden Schritte aus, um die Aufbewahrung von Ereignissen zu konfigurieren.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite „Einstellungen“ auf **Datenbankverbindung**.
   - Scrollen Sie auf der rechten Seite der Seite „Einstellungen“ nach unten, bis sie die Überschrift **Database Connection** (Datenbankverbindung) sehen können.

   Die Datenbankverbindungseinstellungen werden angezeigt.
3. Um die Anzahl der Tage für die Speicherung von Ereignisinformationen in der Datenbank zu ändern, klicken Sie auf das Textfeld **Aufbewahrungsdauer (Tage)**, geben Sie einen Wert zwischen 0 und 3652 ein und klicken Sie dann auf das , um die Änderung zu speichern.

   Der Ereignis-Aufbewahrungszeitraum wird wie gewünscht angepasst.

Berichterstellung

Dieser Abschnitt enthält eine Übersicht über die Berichtsfunktion in der Rapid Recovery Core Console.

Informationen über Berichte von Rapid Recovery

Sie können diese Berichte über die Rapid Recovery Core Console generieren. Andere Berichte sind ebenfalls voraussichtlich über die Datenschutz-Portal verfügbar.

Die über die Core Console verfügbaren Berichte sind in der folgenden Tabelle aufgeführt.

Tabelle 111. Berichte von Rapid Recovery

Berichtstyp	Description
Jobbericht	Bietet einen Bericht über den Status erfolgreicher, fehlgeschlagener und fehlerhafter Jobs. Fehlgeschlagene Jobs können im Fehlerbericht genauer angezeigt werden. • Der Bericht enthält standardmäßig die Daten für die letzten 31 Tage. Dies kann individuell angepasst werden. • Bei Ausführung aus der Core Console kann dieser Bericht Angaben für einen oder mehrere Cores enthalten.Standardmäßig umfasst dieser Informationssatz die Jobs für alle Maschinen, d.h. Datenbankserver, geschützte Maschinen, replizierte Maschinen und Maschinen, die nur Wiederherstellungspunkte enthalten, in den angegebenen Cores. In den Berichtparametern können Sie den Bericht anpassen. Verwenden Sie die Filter, um Computer auszuwählen- oder auszuschließen. Sie können auch computerunabhängige Jobs auswählen oder ausschließen, in diesem Fall zeigt der Bericht nur den Status für Core-Jobs an. Weitere Informationen zu dieser Berichtsart, siehe Grundlegende Informationen zu Jobberichten.
Jobübersichtsbericht	Bietet einen detaillierteren Bericht über den Status der erfolgreichen Jobs, fehlgeschlagene Jobs und Jobs mit Fehlern, mit einer separaten Zeile im Bericht für jeden Jobtyp, wodurch eine bessere Diagnose potenzieller Probleme ermöglicht wird. • Der Bericht enthält standardmäßig die Daten für die letzten 31 Tage. Dies kann individuell angepasst werden. • Im Gegensatz zum Jobbericht enthält dieser Bericht keine Auswahl der Cores als Parameter. • Standardmäßig umfasst dieser Informationssatz die Jobs für alle Maschinen, d.h., Datenbankserver, geschützte Maschinen, replizierte Maschinen und Maschinen, die nur Wiederherstellungspunkte enthalten, und Jobs, die maschinenabhängig sind, nach Jobtyp. Sie können den Bericht anpassen. Verwenden Sie die Filter, um

Berichtstyp	Description
	Computer auszuwählen- oder auszuschließen. Sie können auch Jobs auswählen oder ausschließen, die maschinenabhängig sind. • Bei Ausführung aus der Perspektive eines geschützten Computers in der Core Console zeigt der daraus resultierende Bericht nur den Status von Jobs für diesen geschützten Computer an. Weitere Informationen zu dieser Berichtsart, siehe Grundlegende Informationen zu Jobübersichtsberichten.
Fehlerbericht	Enthält Informationen über fehlgeschlagene Core-Jobs entsprechend der angegebenen Kriterien. Dieser Bericht kann Details zu geschützten Maschine ein- oder ausschließen. Genau wie der Jobbericht kann dieser Bericht nur von einem im Core ausgewählten geschützten Computer ausgeführt werden. Der daraus resultierende Bericht zeigt nur für den ausgewählten geschützten Computer die Einzelheiten zu fehlgeschlagenen Jobs an. Weitere Informationen zu dieser Berichtsart, siehe Grundlegende Informationen zu Fehlerberichten.
Zusammenfassender Bericht	Stellt zusammenfassende Informationen bereit.Standardmäßig umfasst dieser Informationssatz die Jobs für alle Computer, d.h., jeden geschützten Computer, jeden replizierten Computer und jeder "Computer-nur Wiederherstellungspunkte" in den angegebenen Cores. In den Berichtparametern können Sie den Bericht anpassen. Verwenden Sie die Filter, um Computer auszuwählen- oder auszuschließen. Sie können auch computerunabhängige Jobs auswählen oder ausschließen, in diesem Fall zeigt der Bericht nur den Status für Core-Jobs an. Dieser Bericht ist nicht aus der Perspektive eines einzelnen geschützten Computers verfügbar. Die Informationskategorien in diesem Bericht umfassen Core, Lizenz und Repository. Die Daten können in Form einer Liste, eines Diagramms oder einer Tabelle ausgegeben werden. Weitere Informationen zu dieser Berichtsart, siehe Grundlegende Informationen zu Zusammenfassungsberichten.
Repository-Bericht	Dieser Berichttyp bietet Ihnen einen Bericht über alle Repositorys auf einem oder mehreren ausgewählten Cores. Sie können auch ein beliebiges einzelnes Repository wählen, das dem Core zur Verfügung steht. Dieser Bericht stellt lediglich die Perspektive des Core dar. Weitere Informationen zu dieser Berichtsart, siehe Grundlegende Informationen zu Repositoryberichten.
Klassischer Übersichtsbericht	Dieser Bericht bietet eine Übersicht über Statistiken zu erfolgreichen Jobs, Repository-Zusammenfassungen in GB, erfolgreichen Snapshots, Repository-Nutzungstrends und eine Zusammenfassung der geschützten Maschinen auf Ihrem Core. Berichtparameter beinhalten den Datumsbereich und den relevanten Core.
Geplanter Bericht	Sie können auch jeden dieser Berichte in der Core Console planen. Das Planen eines Berichts führt dazu, dass der festgelegte Bericht mehrmals entsprechend dem von Ihnen definierten Zeitplan generiert wird. Optional können Sie jedes Mal eine E-Mail-Benachrichtigung erhalten, wenn ein Bericht erstellt wird. Weitere Informationen zum Planen, Ändern, Anhalten oder Löschen von Berichten finden Sie unter Verwalten von geplanten Berichten über die Core Console.

Basierend auf der ausgewählten Berichtsart und den Parametern, die Sie auswählen, können Sie einen Bericht auf einem oder mehreren Rapid Recovery Cores oder für eine oder mehrere geschützte Maschinen generieren.

Erstellen eines Berichts von der Core Console

Sie können Berichte bedarfsweise aus der Kern-Konsole generieren. Es gelten die folgenden Regeln:

- Alle Berichte können aus der Perspektive des Kerns erzeugt werden.
- Zusätzlich können zwei Jobarten (der Jobbericht und der Fehlerbericht) aus der Perspektive eines geschützten Computers erzeugt werden. Für diese Berichte werden die Daten nur im Zusammenhang mit dem ausgewählten Computer erzeugt.
- Fehlerberichte enthalten nur dann Daten, wenn Jobs auf den ausgewählten Kernen (oder geschützten Computern) fehlgeschlagen sind.

Die Methode für die bedarfsweise Generierung von Berichten ist dieselbe, unabhängig davon, ob der Bericht aus der Perspektive des Kerns oder aus der Perspektive eines geschützten Computers erstellt wird. Jedoch unterscheidet sich die Navigation leicht.

Sie können auch das wiederholte Erzeugen von Berichte planen. Weitere Informationen zum Planen, Ändern, Anhalten oder Löschen von Berichten finden Sie unter Verwalten von geplanten Berichten über die Core Console.

Bedarfsweise Generierung eines Core-Berichts

Im Abschnitt Informationen über Berichte von Rapid Recovery können Sie die gesamte Palette der in der Core Console zur Verfügung stehenden Berichte generieren.

Führen Sie die hier beschriebenen Schritte aus, um einen Bericht aus der Perspektive des Rapid Recovery Core zu generieren.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Berichte**.

   Die Seite **Job-Bericht** wird angezeigt. Rechts neben dem Berichtsnamen in der Seitenüberschrift wird ein nach unten zeigender Pfeil angezeigt, über den Sie eine andere Berichtsart auswählen können.

   Wenn Sie einen Job-Bericht erzeugen möchten, fahren Sie mit Schritt 6 fort, um die Bericht-Kriterien festzulegen.
3. Wenn Sie eine andere Berichtsart auswählen möchten, klicken Sie auf den Pfeil rechts vom Berichtsnamen, um ein Menü der verfügbaren Berichte anzuzeigen.
4. Für das Festlegen geplanter Berichte finden Sie Informationen unter Planen eines Berichts.
5. Um einen Bericht nur über Repositorys zu erstellen, fahren Sie mit Schritt 11 fort.
6. Um einen Job-, Jobübersichts-, Fehler-, zusammenfassenden oder (klassischen) Core-Bericht zu erstellen, wählen Sie einen Datumsbereich aus dem Drop-Down-Menü **Datumsbereich** aus.

   Wenn Sie keinen Datumsbereich wählen, wird die Standardoption (letzte 31 Tage) verwendet. Sie können aus den Optionen in der folgenden Tabelle wählen.

Option	Description
Letzte 24 Stunden	Bericht über Aktivitäten für den vergangenen Tag im Verhältnis zu dem Zeitpunkt, zu dem Sie den Bericht generieren.

Option	Description
Letzte 7 Tage	Bericht über Aktivitäten für die vergangene Woche im Verhältnis zu dem Zeitpunkt, zu dem Sie den Bericht generieren.
Letzte 31 Tage	Bericht über Aktivitäten für letzten 31 Tage im Verhältnis zu dem Zeitpunkt, zu dem Sie den Bericht generieren.
Letzte 90 Tage	Bericht über Aktivitäten für letzten 90 Tage im Verhältnis zu dem Zeitpunkt, zu dem Sie den Bericht generieren.
Letzte 365 Tage	Bericht über Aktivitäten für das vergangene Jahr im Verhältnis zu dem Zeitpunkt, zu dem Sie den Bericht generieren.
Alle Zeiten	Dieser Zeitraum erstreckt sich über die Lebensdauer des Core.
Angepasst	Für diesen Zeitraum müssen Sie das Start- und Enddatum genauer angeben.
Monat bis heute	Bericht über Aktivitäten ab dem ersten Tag des aktuellen Kalendermonats bis zum Datum, an dem Sie den Bericht generieren.
Jahr bis heute	Bericht über Aktivitäten ab dem ersten Tag des aktuellen Kalenderjahrs bis zum Datum, an dem Sie den Bericht generieren.

NOTE: In Fällen, in denen keine Berichtsdaten verfügbar sind, bevor die Core-Software bereitgestellt wurde, oder aus der Zeit bevor Computer vom Core geschützt wurden.

7. Wählen Sie für einen Job-, Fehler- oder (klassischen) Core-Bericht aus dem Drop-Down-Menü **Ziel-Cores** den bzw. die entsprechenden Core(s) aus, für die Sie einen Bericht erstellen möchten.

   Die Standardauswahl umfasst alle verfügbaren Cores.

8. Wählen Sie aus dem Drop-Down-Menü **geschützte Computer** den Computer aus, für den Sie einen Bericht generieren möchten.

   Standardmäßig umfasst dieser Informationssatz die Jobs für alle Computer, d.h., jeden geschützten Computer, jeden replizierten Computer und jeder "Computer-nur Wiederherstellungspunkte" in den angegebenen Cores. In den Berichtparametern können Sie den Bericht anpassen. Verwenden Sie die Filter, um Computer auszuwählen- oder auszuschließen. Sie können auch computerunabhängige Jobs auswählen oder ausschließen, in diesem Fall zeigt der Bericht nur den Status für Core-Jobs an.

   Sie haben folgende Auswahlmöglichkeiten:

Option	Description
Alles auswählen	Diese Option wählt alle geschützten Computer aus, die von diesem Core geschützt werden. **NOTE:** Sie können alle Computer auswählen und anschließend einige der Optionen zur Angabe eines Teils aller Computer entfernen.

Option	Description
Maschinenunabhängig	Wählen Sie diese Option aus, um einen Bericht zu erstellen, der Jobs aus Perspektive des Core anzeigt. Jobtypen wie z. B. das Erstellen oder Löschen eines Repositorys oder das Erstellen einer Start-CD stehen nicht im Zusammenhang mit einem bestimmten Computer. Wenn Sie die Bereitstellung der Agentensoftware auf einem noch nicht geschützten Computer vornehmen, wird dieser Jobtyp auch als computerunabhängig angesehen. Bei diesen Jobs wird kein geschützter Computer in der Spalte "geschützter Computer" des generierten Berichts angegeben. Im Gegensatz dazu wird beim Bereitstellen der Agent-Software auf einem Computer, der bereits durch den Core geschützt wird, der Name des geschützten Computers im Bericht aufgeführt. Dies wird nicht als computerunabhängig angesehen.
Geschützte Computer	Diese Option führt die Computer auf, die von diesem Core geschützt werden. Sie können alle oder einen Teil der geschützten Computer auswählen.
Nur Wiederherstellungspunkte	Diese Option führt Computer auf, die zuvor geschützt wurden, von denen nun aber nur noch Wiederherstellungspunkte im Repository gespeichert sind.
[Quell-Cores]	Wenn Ihr Core ein Ziel-Core ist und Wiederherstellungspunkte für einen durch einen Quell-Core geschützten Computer repliziert, wird der Name dieses Quell-Core angezeigt (in Großbuchstaben). Diese Option führt alle geschützten Computer auf diesem Quell-Core auf. Sie können entweder alle replizierten Computer in diesem Ziel-Core oder einen Teil davon wählen.
[Benutzerdefinierte Gruppen]	Wenn Sie benutzerdefinierte Gruppen auf diesem Core erstellt haben, wird der Name jeder benutzerdefinierten Gruppe als Option angezeigt. Jedes Objekt in dieser benutzerdefinierten Gruppe wird angezeigt. Sie können entweder alle Objekte in der Gruppe oder einen Teil davon wählen.

9. Für die Generierung eines zusammenfassenden Berichts fahren Sie mit Schritt 12 fort.
10. Wählen Sie für einen Jobübersichts- oder Fehlerbericht die entsprechenden Jobtypen aus dem Dropdown-Menü **Jobtypen** aus.

    Standardmäßig enthält dieser Informationssatz alle Jobs für die ausgewählten geschützten Computer. In den Berichtparametern können Sie den Bericht anpassen. Verwenden Sie Filter zum Auswählen oder Ausschließen jedes Jobs in den Hauptjobkategorien und jedes Job in den anderen Jobkategorien. Alternativ können Sie jede dieser Kategorien bei der Definition der Jobparameter erweitern und nur die Jobtypen jeder Kategorie wählen, die Sie im Bericht angezeigt haben möchten. Klicken Sie auf das Kontrollkästchen für einen beliebigen Jobtyp, um diesen Typ zu aktivieren oder zu deaktivieren. Sie können einige oder alle Jobs in jeder Kategorie wählen.

Sie können aus folgenden **andere** Jobtypen wählen:

11. Wählen Sie für einen Repository-Bericht aus dem Menü "Repositorys" ein oder mehrere Repositorys, die Sie im Bericht aufgeführt haben möchten.

    Die Standardauswahl umfasst alle verfügbaren Repositorys.

12. Klicken Sie auf **Vorschau** zum Generieren eines Berichts mit den angegebenen Kriterien.

    Wenn das Bericht-Kriterium, das Sie gewählt haben, nicht gefunden wird, wird der Bericht trotzdem generiert, enthält aber nur eine leere Zeile. Beispiel: Wenn keine Fehler vorliegen, wird der Inhalt der Spalte Fehler im Bericht als leer angezeigt.

13. Führen Sie eine der folgenden Aktionen aus:

    - Online-Anzeige des erzeugten Berichts.
    - Aktualisieren Sie den Bericht dynamisch durch Änderung eines beliebigen Kriteriums, klicken Sie anschließend erneut auf **Vorschau**.
    - Verwenden Sie das Menü **Berichte** zum Auswählen eines Exportformats (einschließlich des Standardformats PDF) und klicken Sie auf , um den Bericht zu exportieren. Weitere Informationen zum Bericht-Menü finden Sie unter Verwendung des Bericht-Menüs.
    - Verwenden Sie die **Symbolleiste "Berichte"** zum Anzeigen, Bearbeiten oder Drucken des Berichts. Weitere Informationen zur Bericht-Symbolleiste finden Sie unter Verwendung der Symbolleiste für Berichte.

Generieren eines bedarfsorientierten Berichts zu einer geschützten Maschine

Sie können einen Jobbericht oder einen Fehlerbericht für eine beliebige Maschine generieren.

Führen Sie die hier beschriebenen Schritte aus, um einen Bericht für eine geschützte Maschine zu generieren.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie im Menü „Geschützte Maschinen“ auf die geschützte Maschine, für die Sie einen Bericht anzeigen möchten.

   Die Seite **Summary** (Zusammenfassung) für die ausgewählte geschützte Maschine wird angezeigt.

3. Klicken Sie oben auf der Seite in den Menüoptionen neben dem Namen der geschützten Maschine auf den nach unten zeigenden Pfeil neben „Berichte“ und wählen Sie dann einen Berichtstyp aus.

   - Wenn Sie einen Bericht zu allen Aufgaben im Zusammenhang mit dieser geschützten Maschine generieren möchten, einschließlich fehlgeschlagener Jobs, klicken Sie auf **Jobbericht** und legen Sie die Berichtskriterien fest.
   - Wenn Sie lediglich eine Liste der fehlgeschlagenen Jobs im Zusammenhang mit dieser geschützten Maschine generieren möchten, klicken Sie auf **Fehlerbericht** und legen Sie die Berichtskriterien fest.

4. Für einen Job- oder Fehlerbericht wählen Sie einen Datumsbereich aus dem Drop-Down-Menü **Datumsbereich**.

   Wenn Sie keinen Datumsbereich wählen, wird die Standardoption (letzte 31 Tage) verwendet. Sie können aus den Optionen in der folgenden Tabelle wählen.

Option	Description
Letzte 24 Stunden	Bericht über Aktivitäten für den vergangenen Tag im Verhältnis zu dem Zeitpunkt, zu dem Sie den Bericht generieren.

Option	Description
Letzte 7 Tage	Bericht über Aktivitäten für die vergangene Woche im Verhältnis zu dem Zeitpunkt, zu dem Sie den Bericht generieren.
Letzte 31 Tage	Bericht über Aktivitäten für letzten 31 Tage im Verhältnis zu dem Zeitpunkt, zu dem Sie den Bericht generieren.
Letzte 90 Tage	Bericht über Aktivitäten für letzten 90 Tage im Verhältnis zu dem Zeitpunkt, zu dem Sie den Bericht generieren.
Letzte 365 Tage	Bericht über Aktivitäten für das vergangene Jahr im Verhältnis zu dem Zeitpunkt, zu dem Sie den Bericht generieren.
Alle Zeiten	Dieser Zeitraum erstreckt sich über die Lebensdauer des Core.
Angepasst	Für diesen Zeitraum müssen Sie das Start- und Enddatum genauer angeben.
Monat bis heute	Bericht über Aktivitäten ab dem ersten Tag des aktuellen Kalendermonats bis zum Datum, an dem Sie den Bericht generieren.
Jahr bis heute	Bericht über Aktivitäten ab dem ersten Tag des aktuellen Kalenderjahrs bis zum Datum, an dem Sie den Bericht generieren.

NOTE: In Fällen, in denen keine Berichtsdaten verfügbar sind, bevor die Core-Software bereitgestellt wurde, oder aus der Zeit bevor Computer vom Core geschützt wurden.

5. Wählen Sie aus dem Dropdown-Menü **Jobtypen** die entsprechenden Jobtypen aus.

   Standardmäßig enthält dieser Informationssatz alle Jobs für die ausgewählten geschützten Computer. In den Berichtparametern können Sie den Bericht anpassen. Verwenden Sie Filter zum Auswählen oder Ausschließen jedes Jobs in den Hauptjobkategorien und jedes Job in den anderen Jobkategorien. Alternativ können Sie jede dieser Kategorien bei der Definition der Jobparameter erweitern und nur die Jobtypen jeder Kategorie wählen, die Sie im Bericht angezeigt haben möchten. Klicken Sie auf das Kontrollkästchen für einen beliebigen Jobtyp, um diesen Typ zu aktivieren oder zu deaktivieren. Sie können einige oder alle Jobs in jeder Kategorie wählen.

6. Klicken Sie auf **Vorschau** zum Generieren eines Berichts mit den angegebenen Kriterien.

Wenn das Bericht-Kriterium, das Sie gewählt haben, nicht gefunden wird, wird der Bericht trotzdem generiert, enthält aber nur eine leere Zeile. Beispiel: Wenn keine Fehler vorliegen, wird der Inhalt der Spalte Fehler im Bericht als leer angezeigt.

7. Führen Sie eine der folgenden Aktionen aus:
   - Online-Anzeige des erzeugten Berichts.
   - Aktualisieren Sie den Bericht dynamisch durch Änderung eines beliebigen Kriteriums, klicken Sie anschließend erneut auf **Vorschau**.
   - Wählen Sie über das **Menü „Berichte“** ein Exportformat aus und exportieren Sie den Bericht. Weitere Informationen zum Bericht-Menü finden Sie unter Verwendung des Bericht-Menüs.
   - Verwenden Sie die **Symbolleiste "Berichte"** zum Anzeigen, Bearbeiten oder Drucken des Berichts. Weitere Informationen zur Bericht-Symbolleiste finden Sie unter Verwendung der Symbolleiste für Berichte.

Verwalten von geplanten Berichten über die Core Console

Sie können jeden in der Kern-Konsole verfügbaren Bericht planen. Das Planen eines Berichts führt dazu, dass er in Zukunft mehrmals generiert wird. Der Zeitplan legt fest, ob der Bericht täglich, wöchentlich oder monatlich generiert wird.

Optional ermöglicht Rapid Recovery das Senden einer E-Mail-Benachrichtigung an einen oder mehrere Empfänger, sobald ein Bericht erstellt wurde. In der E-Mail werden die Berichtsart, das Berichtsformat und der Datumsbereich angegeben und der Bericht als Anlage beigefügt.

NOTE: Bevor Sie Berichte per E-Mail senden können, müssen Sie einen SMTP-Server für den Kern konfigurieren. Weitere Informationen hierzu finden Sie unter Konfigurieren eines E-Mail-Servers.

Unabhängig davon, ob Sie das Versenden von E-Mail-Benachrichtigungen wählen, können Sie die erstellten Berichte lokal oder auf einem Netzwerkstandort speichern, der für den Kern-Server zugänglich ist.

Sie müssen die E-Mail-Benachrichtigung und -Zustellung angeben oder einen Speicherort zum Speichern der Berichte angeben. Sie können auch beide Optionen auswählen.

In diesem Abschnitt werden folgende Themen behandelt:

- Planen eines Berichts
- Ändern eines Berichtszeitplans
- Anhalten, Wiederaufnehmen oder Löschen eines geplanten Berichts

Zugehörige Konzepte

See also: Anhalten, Wiederaufnehmen oder Löschen eines geplanten Berichts

Zugehörige Tasks

See also: Planen eines Berichts
See also: Ändern eines Berichtszeitplans

Planen eines Berichts

Sie können einen Bericht in der Core Console planen. Der Bericht wird dann gemäß des von Ihnen definierten Zeitplans generiert, bis Sie den Bericht anhalten oder löschen.

Sie müssen die E-Mail-Benachrichtigung und -Zustellung angeben oder einen Speicherort zum Speichern der Berichte angeben. Sie können auch beide Optionen auswählen.

Führen Sie die folgenden Schritte aus, um einen Bericht zu planen.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Berichte**.

   Die Seite **Job-Bericht** wird angezeigt. Ein nach unten zeigender Pfeil wird rechts neben dem aktuellen Namen des Berichts angezeigt.
3. Klicken Sie auf den Pfeil rechts vom Namen des Berichts, und wählen Sie **Geplante Berichte** aus dem Drop-Down-Menü.

   Die Seite **Geplante Berichte** wird angezeigt.
4. Um einen Zeitplan festzulegen, nach dem ein Bericht wiederholt generiert wird, klicken Sie auf **Hinzufügen**.

   Der **Assistent zum Festlegen des Berichtszeitplans** wird angezeigt.
5. Geben Sie auf der Seite **Konfiguration** des Assistenten die Einzelheiten für den Bericht ein, den Sie planen möchten, und klicken Sie dann auf **Weiter**. Die Konfigurationsinformationen werden in der folgenden Tabelle beschrieben.

Tabelle 112. Konfigurationsoptionen für geplanten Bericht

Maschine	Verfügbare Berichte
Name	Geben Sie den Anzeigenamen ein, der diesem bestimmten Zeitplan zugewiesen werden soll. Der Standardname lautet „Geplanter Bericht 1“. Beschränken Sie den Namen auf 64 oder weniger Zeichen. Verwenden Sie weder Unzulässige Zeichen noch Unzulässige Phrasen.
Berichtformat	Wählen Sie ein Ausgabeformat für den Bericht. Wenn Sie keinen Wert wählen, wird das Standardformat (pdf) verwendet.
Berichtstyp	Wählen Sie den Berichtstyp aus, den Sie auf wiederholter Basis erstellen möchten.
Labels	Wählen Sie die Bezeichnungen aus, die auf Ihrem geplanten Bericht angezeigt werden sollen. Mindestens eine Bezeichnung ist erforderlich. Mit der Funktion „Benutzerdefinierte Gruppen“ können Sie Core-Objekte in einem logischen Container gruppieren, für den Sie eine Bezeichnung definieren. Mithilfe des Parameters „Bezeichnungen“ im Assistenten zum Festlegen des Berichtszeitplans können Sie eine benutzerdefinierte Gruppe auswählen, für die geplante Berichte ausgeführt werden. Wenn keine benutzerdefinierten Bezeichnungen vorhanden sind, schließt das Drop-Down-Menü „Bezeichnungen“ die Optionen „Alle auswählen“ und „Geschützte Maschinen“ ein. Wenn benutzerdefinierte Gruppen angezeigt werden, wird jede Gruppe als Option angezeigt. Sie könne jede dieser Optionen aktivieren oder deaktivieren, um diese Objekte in den geplanten Bericht ein- oder daraus auszuschließen.
Geschützte Maschine	Wählen Sie eine oder mehrere geschützten Maschinen aus, die in den Bericht eingeschlossen werden sollen. Diese Option ist nicht für den Repository-Bericht verfügbar.
Jobtypen	Wählen Sie die Jobtypen aus, die im Bericht angezeigt werden sollen.

Maschine	Verfügbare Berichte
	Standardmäßig umfasst dieser Informationssatz die Jobs für alle Computer, d.h., jeden geschützten Computer, jeden replizierten Computer und jeder "Computer-nur Wiederherstellungspunkte" in den angegebenen Cores. In den Berichtparametern können Sie den Bericht anpassen. Verwenden Sie die Filter, um Computer auszuwählen- oder auszuschließen. Sie können auch computerunabhängige Jobs auswählen oder ausschließen, in diesem Fall zeigt der Bericht nur den Status für Core-Jobs an. Die Parameter „Jobtypen“ ist nicht für die folgenden Typen von geplanten Berichten verfügbar: Core-Zusammenfassung und Repository.

6. Wählen Sie auf der Seite **Ziel** des Assistenten ein Ziel für die geplanten Berichte aus. Sie müssen eine der folgenden Optionen auswählen, können jedoch auch beide auswählen. Klicken Sie auf **Weiter**, wenn die Angaben in Ordnung sind.
   - Geben Sie im Feld **Send email to addresses** (An E-Mail-Adressen senden) eine oder mehrere gültige E- Mail-Adressen ein, um Benutzern per E-Mail zu benachrichtigen, wenn ein geplanter Bericht erstellt wird.

     NOTE: Wenn Sie keine E-Mail-Benachrichtigung und -Zustellung angeben, müssen Sie einen Speicherort festlegen.
   - Wählen Sie zum Speichern der erzeugten Berichtsdateien an dem von Ihnen bestimmten Speicherort **Als Datei speichern** aus und wählen Sie dann im Drop-Down-Menü **Speicherorttyp** eine die Option für einen lokalen, Netzwerk- oder Cloud-Speicher aus. Geben Sie dann im Feld **Speicherort** die in der folgenden Tabelle beschriebenen zusätzlichen Informationen ein.

Tabelle 113. Speicherortoptionen für geplante Berichte

Typ des Speicherorts	Beschreibung des Speicherorttyps	Speicherort
Lokal	Wählen Sie den Speicherorttyp „Lokal“, um generierte Berichte in einem lokalen, für den Core zugänglichen Pfad zu speichern.	Geben Sie den Pfad in das Feld „Speicherort“ ein. Geben Sie einen Speicherort ein, der für den Core lokal zugänglich ist. Um Berichte beispielsweise im Ordner „Berichte“ auf dem Laufwerk D zu speichern, geben Sie `D:\Berichte\` ein.
Netzwerk	Wählen Sie den Speicherorttyp „Netzwerk“, um generierte Berichte in einem für den Core zugänglichen Pfad auf dem Netzwerk zu speichern. Geben Sie den Pfad in das Feld „Speicherort“ ein.	Geben Sie den Pfad in das Feld „Speicherort“ ein. Geben Sie einen Speicherort ein, der für den Core auf dem Netzwerk zugänglich ist. Verwenden Sie das Format \\Servername \Freigabename. Um Berichte beispielsweise auf dem Datenserver im freigegebenen Ordner „Berichte“ zu speichern, geben Sie `\\Daten\Berichte\` ein. Geben Sie die Anmeldeinformationen des Netzwerks in die Felder „Benutzername“ und „Kennwort“ ein.
Cloud	Wählen Sie den Speicherorttyp „Cloud“, um generierte Berichte in einem im Core konfigurierten Cloud-Speicherkonto zu speichern.	Wählen Sie im Feld „Konto“ das entsprechende Cloud-Speicherkonto zum Speichern der generierten Berichte. Geben Sie im Feld „Container“ einen entsprechenden Container im Speicherkonto an.

Typ des Speicherorts	Beschreibung des Speicherorttyps	Speicherort
	Das Speicherkonto muss vor der Durchführung dieses Schritts bereits definiert sein. Informationen zum Einrichten eines Cloud-Speicherkontos für den Core finden Sie unter Cloud-Konten.	Geben Sie im Feld „Ordnername“ einen Ordner an, in dem zukünftig generierte Berichte gespeichert werden sollen.

7. Wenn Sie mit Ihren Ziel-Optionen zufrieden sind, klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Zeitplan** des Assistenten aus dem Menü **Daten senden** eine Option, um festzulegen, wie häufig der angegebene Bericht generiert werden soll. Sie können Berichte täglich, wöchentlich oder monatlich generieren. Jede Option hat ihre eigenen Parameter, wie in der folgenden Tabelle beschrieben.

Tabelle 114. Optionen zum Festlegen der Häufigkeit für die Generierung geplanter Berichte

Wie häufig	Frequenzdetails	Frequenzparameter
Täglich	Generiert und speichert oder sendet den angegebenen Bericht einmal täglich zur angegebenen Uhrzeit. Standardzeit für diese Aktion ist 00:00 Uhr (basierend auf der Uhrzeit auf dem Core-Server).	Zum Ändern der standardmäßigen Uhrzeit, zu der der Bericht generiert wird, geben Sie im Textfeld „Zeit“ einen neuen Wert ein oder verwenden Sie die Steuerelemente, um Stunde, Minute und AM oder PM auszuwählen.
Wöchentlich	Generiert und speichert oder sendet den angegebenen Bericht einmal pro Woche zur angegebenen Uhrzeit des angegebenen Tages. Standardzeit für diese Aktion ist 00:00 Uhr sonntags (basierend auf der Uhrzeit auf dem Core-Server).	Zum Ändern des standardmäßigen Tags, an dem der Bericht generiert wird, wählen Sie im Menü „Wochentag“ einen Wochentag aus. Zum Ändern der standardmäßigen Uhrzeit, zu der der Bericht generiert wird, geben Sie im Textfeld „Zeit“ einen neuen Wert ein oder verwenden Sie die Steuerelemente, um Stunde, Minute und AM oder PM auszuwählen.
Monatlich	Generiert und speichert oder sendet den angegebenen Bericht einmal pro Monat an einem bestimmten Datum und zu einer bestimmten Uhrzeit. Standarddatum für diese Aktion ist am ersten jedes Monats um 00:00 Uhr (basierend auf der Uhrzeit auf dem Core-Server).	Zum Ändern des standardmäßigen Datums, an dem der Bericht generiert wird, wählen Sie im Menü „Tag des Monats“ ein Datum aus. Zum Ändern der standardmäßigen Uhrzeit, zu der der Bericht generiert wird, geben Sie im Textfeld „Zeit“ einen neuen Wert ein oder verwenden Sie die Steuerelemente, um Stunde, Minute und AM oder PM auszuwählen.

9. Optional können Sie auf der Seite **Zeitplan** des Assistenten **Reporting anfänglich anhalten** auswählen, wenn der geplante Bericht zunächst nicht generiert werden soll, bis Sie angehaltene Berichte wieder aufnehmen.

   Wenn Sie wollen, dass dieser Bericht wie geplant generiert wird, heben Sie die Markierung dieser Option auf.
10. Wenn Sie mit dem Zeitplan zufrieden sind, klicken Sie auf **Fertig stellen**, um den Assistenten zu beenden und Ihre Arbeit zu speichern.

    Der neue Berichtszeitplan wird in der Übersichtstabelle für Zusammenfassungsberichte angezeigt.

Ändern eines Berichtszeitplans

Wenn ein Bericht geplant wurde, können Sie seine Parameter oder Einzelheiten ändern. Sie können die Konfigurationsinformationen des Berichts bearbeiten (Berichtname, Ausgabeformat, Berichtsart, enthaltene Repositorys). Sie können auch die E-Mail-Benachrichtigungsoptionen und das Ziel zum Speichern des erzeugten Berichts ändern. Darüber hinaus können Sie auch den Zeitplan des Berichts ändern.

Führen Sie die hier beschriebenen Schritte aus, um Parameter für einen geplanten Bericht zu ändern.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Berichte**.

   Die Seite **Job-Bericht** wird angezeigt. Ein nach unten zeigender Pfeil wird rechts neben dem aktuellen Namen des Berichts angezeigt.
3. Klicken Sie auf den Pfeil rechts vom Namen des Berichts, und wählen Sie **Geplante Berichte** aus dem Drop-Down-Menü.

   Die Seite **Geplante Berichte** wird angezeigt.
4. Klicken Sie in der zusammenfassenden Tabelle der geplanten Berichte in der Zeile für den Bericht, den Sie bearbeiten möchten, auf (Weitere Optionen) und wählen Sie dann **Bearbeiten** aus.

   Der **Assistent zum Festlegen des Berichtszeitplans** wird angezeigt.
5. Navigieren Sie durch die Seiten dieses Assistenten und ändern Sie die erforderlichen Parameter. Weitere Informationen zu den Parametern in diesem Assistenten finden Sie im Abschnitt Planen eines Berichts.
6. Klicken Sie auf der Seite **Zeitplan** des Assistenten auf **Fertig stellen,** um den Assistenten zu schließen und Ihre Änderungen zu speichern.

   Der Assistent wird geschlossen und der Berichterstellungszeitplan wird geändert.

Anhalten, Wiederaufnehmen oder Löschen eines geplanten Berichts

Wenn ein Bericht geplant wurde, wird er gemäß dem definierten Zeitplan generiert. Wenn Sie die Generierung eines geplanten Berichts vorübergehend anhalten möchten, können Sie den Zeitplan pausieren.

Wenn ein geplanter Bericht angehalten wurde, und Sie die Generierung des Berichts wiederaufnehmen möchten, können Sie dies gemäß der Beschreibung in diesem Verfahren tun.

Wenn Sie derzeit die Generierung eines Berichts geplant haben, diesen Bericht aber nicht mehr benötigen, können Sie ihn löschen.

Um festzustellen, ob ein geplanter Bericht angehalten wurde, überprüfen Sie die Spalte "Status" in der Übersichtstabelle der geplanten Berichte. Eine grüne Kugel zeigt einen aktiven geplanten Bericht an, eine gelbe Kugel zeigt einen angehaltenen Zeitplan an und die rote Kugel weist auf einen Fehler hin.

Führen Sie die folgenden Schritte aus, um den Zeitplan für einen Bericht anzuhalten, wiederaufzunehmen und zu löschen.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Mehr) und wählen Sie dann **Berichte**.

   Die Seite **Job-Bericht** wird angezeigt. Ein nach unten zeigender Pfeil wird rechts neben dem Namen des aktuellen Berichts angezeigt.
3. Klicken Sie auf den Pfeil rechts vom Namen des Berichts, und wählen Sie **Geplante Berichte** aus dem Drop-Down-Menü.

   Die Seite **Geplante Berichte** wird angezeigt.

4. In der Übersichtstabelle der geplanten Berichte können Sie sich den Status aller geplanten Berichte mit den farbigen Anzeigen ansehen.
5. Wählen für jeden Bericht, den Sie anhalten oder wiederaufnehmen möchten, das Kontrollkästchen in der ersten Spalte.
6. Führen Sie aus den Optionen zu geplanten Berichten oberhalb der Übersichtstabelle die folgenden Aktionen aus:
   - Zum Anhalten der Generierung der ausgewählten Berichte klicken Sie auf **Anhalten**.
   - Zur Wiederaufnahme der Generierung der geplanten Berichte, die angehalten wurden, klicken Sie auf **Fortsetzen**.
   - Zum Löschen der ausgewählten Zeitpläne für vorhandene geplante Berichte klicken Sie auf **Löschen**.

     Das Löschen eines geplanten Berichts verhindert lediglich eine Generierung künftiger Berichte. Wenn vorherige geplante Berichte gespeichert wurden, werden diese nicht entfernt.

Verwendung des Bericht-Menüs

Das Bericht-Menü wird am oberen Rand der Seite bei der Anzeige von Berichten eingeblendet. Dieses Menü enthält einen Berichttitel, der zudem ein Drop-Down-Menü ist, über das die verfügbaren Berichtsarten angezeigt werden können. Unter diesem Menü finden Sie einen oder mehrere Filter, mit deren Hilfe Sie die Berichtskriterien festlegen können.

Die spezifischen Filter richten sich nach der Berichtsart. Weitere Informationen zu den Parametern, die für die jeweilige Berichtsart gelten, finden Sie im Abschnitt über Grundlegendes zu dieser Berichtsart.

Auf der rechten Seite im Bericht-Menü werden einige Steuerelemente angezeigt. Diese Steuerelemente, die in der folgenden Tabelle beschrieben werden, helfen Ihnen beim Erstellen und Exportieren des Berichts.

Tabelle 115. Steuerelemente des Bericht-Menüs

UI-Element	Description
Vorschau-Schaltfläche	Klicken Sie auf die Schaltfläche "Vorschau", um einen Bericht auf Basis der ausgewählten Berichtsart und den in den Filtern festgelegten Bericht-Parametern zu erstellen.
Exportformat Drop-Down-Menü	Im Export Drop-Down-Menü können Sie das Berichtausgabeformat wählen. Wenn Sie keinen Wert wählen, wird das Standardformat (pdf) verwendet.
Download-Schaltfläche/ Symbol	Die Schaltfläche "Download" exportiert den erzeugten Bericht im Format, das im Menü "Exportieren" ausgewählt wurde.

Berichte enthalten Maßeinheiten, damit Sie leichter feststellen können, ob eine Spalte in GB, TB oder in Sekunden dargestellt wird.

Wenn Sie mit der Darstellung eines generierten oder exportierten Berichts nicht zufrieden sind, können Sie die Schriftart in den Berichten ändern. Weitere Informationen finden Sie unter Verwalten von Berichteinstellungen.

Sobald ein Bericht erstellt wurde, können Sie die Symbolleiste "Berichte" verwenden.

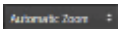
See also: Grundlegende Informationen zu Jobberichten
See also: Grundlegende Informationen zu Fehlerberichten
See also: Grundlegende Informationen zu Zusammenfassungsberichten

Verwendung der Symbolleiste für Berichte

Nach dem Erzeugen eines Berichts aus dem Menü "Berichte" wird dieser unterhalb einer Symbolleiste "Berichte" angezeigt. Die Symbolleiste kann Ihnen dabei helfen, die Berichtausgabe zu manipulieren sowie diese zu speichern und zu drucken.

Auf der linken Seite der Symbolleiste befindet sich ein Umschalter für die Randleiste. Dieses Tool erweitert oder verkleinert die Randleiste, die Zugang zu einigen weiteren Anzeigeoptionen bietet. Rechts in der Symbolleiste erweitert sich die Option "Werkzeuge" in ein Drop-Down-Menü und bietet eine Berichtsnavigation. Die Elemente der Symbolleiste "Berichte" werden in der folgenden Tabelle beschrieben.

Tabelle 116. Symbole der Symbolleiste für Berichte

Symbol	Description
	**Randleiste umschalten**. Alle Berichtseiten werden als Miniaturansichten angezeigt. Andere Optionen in der Randleiste werden nicht unterstützt.
	**Seitenleiste: Miniaturen einblenden**. Dies ist die Standardansicht für alle Seiten eines generierten Berichts.
	**Seitenleiste: Dokumentengliederung anzeigen**. Diese Funktion wird nicht unterstützt.
	**Seitenleiste: Anhänge anzeigen**. Es sind keine Anhänge für Berichte verfügbar. Diese Funktion wird nicht unterstützt.
	**Finden**. Ermöglicht Ihnen die Suche nach Text innerhalb des generierten Berichts. Enthält Optionen zum Markieren des gesamten Texts, der den Kriterien entspricht, die Sie eingeben, sowie dem Beachten oder Ignorieren der Groß-/Kleinschreibung.
	**Vorherige Seite**. Gehen Sie zur vorherigen Seite der Berichtsansicht.
	**Nächste Seite**. Gehen Sie zur nächsten Seite in der Berichtsansicht.
	**Seitennummer eingeben**. Klicken Sie auf das Textfeld "Seitenzahl", geben Sie eine gültige Seitenzahl ein und drücken Sie die Eingabetaste, um zu dieser Seite in der Berichtsansicht zu gehen.
	**Verkleinern**. Hiermit können Sie die Ansicht des generierten Berichts verkleinern. Mit jedem mal Klicken auf "Verkleinern" wird die Ansicht verkleinert, bis das Minimum von 25 % erreicht ist.
	**Vergrößern**. Hiermit können Sie die Ansicht des generierten Berichts vergrößern. Mit jedem mal Klicken auf "Vergrößern" wird die Ansicht vergrößert, bis das Maximum von 1000 % erreicht ist.
	**Automatische Vergrößerung**. Hiermit können Sie die Vergrößerung der Ansicht des generierten Berichts steuern, einschließlich der Anzeige in der tatsächlichen Größe, an

Symbol	Description
	Seitengröße anpassen, volle Breite, oder nach Prozentsatz, einschließlich 50 %, 75 %, 100 %, 125 %, 150 %, 200 %, 300 %, oder 400 %.
	**Datei öffnen**. Hiermit können Sie durch Ihr Dateisystem navigieren, um einen gespeicherten Bericht zu suchen und zu öffnen.
	**Drucken**. Hiermit können Sie den erzeugten Bericht drucken.
	**Werkzeuge**. Das Drop-Down-Menü "Werkzeuge" erweitert oder verkleinert sich, wenn Sie auf dieses Symbol klicken. Die Werkzeug-Optionen werden nachfolgend beschrieben.
	**Tools: Zur ersten Seite gehen**. Wechseln Sie zur ersten Seite des erzeugten Berichts.
	**Tools: Zur letzten Seite gehen**. Wechseln Sie zur letzten Seite des erzeugten Berichts.
	**Tools: Im Uhrzeigersinn drehen**. Diese Option dreht die Ansicht des generierten Berichts im Uhrzeigersinn.
	**Tools: Gegen den Uhrzeigersinn drehen**. Diese Option dreht die Ansicht des generierten Berichts gegen den Uhrzeigersinn.
	**Tools: Hand-Werkzeug**. Wenn Sie dieses Werkzeug auswählen, können Sie den Bericht durch Klicken und Ziehen über den Bildschirm verschieben.
	**Tools: Dokumenteigenschaften**. Enthält Informationen über die Dokumenteigenschaften des generierten Berichts. Klicken Sie auf **Schließen**, um das Fenster zu schließen.

Informationen zum Erstellen von Berichten finden Sie unter Erstellen eines Berichts von der Core Console.

Grundlegende Informationen zu Jobberichten

Der Jobbericht steht für den Rapid Recovery Core und die vom Core geschützten Maschinen zur Verfügung. Mit diesem Bericht können Sie den Status von Jobs anzeigen, die von einem bestimmten Core oder geschützten Computer durchgeführt wurden. Datenzeilen oder -spalten, die im Bericht ohne Daten angezeigt werden, geben an, dass der getestete Parameter Null war. Wenn zum Beispiel in einer Spalte (wie "Fehlermeldung") keine Daten angezeigt werden; sind keine Fehler beim ausgewählten Datensatz aufgetreten. Wenn der Bericht eine leere Zeile erzeugt, umfasst der Job für den ausgewählten Datensatz computerunabhängige Aktivitäten.

Informationen zum Erstellen von Berichten aus dem Core finden Sie unter Bedarfsweise Generierung eines Core-Berichts. Informationen zum Erstellen von Berichten für einen geschützten Computer finden Sie unter Generieren eines bedarfsorientierten Berichts zu einer geschützten Maschine.

Beim Erstellen eines Jobberichts umfassen die Einzelheiten des Berichts Folgendes:

- Auswahlkriterien für den Bericht
- Eine Übersichtstabelle, in der für jeden Job im von Ihnen angegeben Datumsbereich eine Zeile enthalten ist Zusätzlich zur Auflistung des entsprechenden Core, geschützten Computers und Jobtyp enthält jede Zeile:
  - Eine Zusammenfassung des Jobs
  - Den Job-Status
  - Etwaige Fehler in Bezug auf den Job
  - Das Start- und Enddatum des Jobs
  - Die Jobdauer in Sekunden
  - Die gesamte Arbeit in MB

Wenn Informationen für eine bestimmte Kategorie nicht relevant sind, wird diese Zelle ohne Daten im Bericht angezeigt. Beispiel: Wenn der Core für einen bestimmten geschützten Computer keine Fehler aufweist, ist diese Zeile im Bericht in der Spalte "Fehlermeldung" leer.

Grundlegende Informationen zu Jobübersichtsberichten

Der Jobübersichtsbericht ist nur verfügbar, wenn die Berichterstellung aus der Sicht des Core erfolgt; dieser Bericht ist nicht von Berichten für eine geschützte Maschine verfügbar. Dieser Bericht enthält eine einzige Zusammenfassung, die Übersichtsinformationen zu allen Jobs enthält, die auf dem Core ausgeführt werden, einschließlich der Anzahl fehlgeschlagenen, weitergeleiteten und abgebrochenen Jobs. Er zeigt mehr Details als der Jobbericht an, da er jeden Job als eine separate Zeile im Bericht angibt.

Informationen zum Erstellen von Jobübersichtsberichten finden Sie unter Erstellen eines Berichts von der Core Console.

Die Berichtparameter für diese Berichtsart umfassen:

- Datumsbereich
- Geschützte Computer
- Jobtypen

Beim Erstellen eines Jobübersichtsberichts beinhalten die Einzelheiten des Berichts Auswahlkriterien für den Bericht sowie Informationen über geschützte Computer, Volumes und Jobtypen.

Core-Informationen

Der Abschnitt „Core“ des zusammenfassenden Berichts enthält Angaben zu den Rapid Recovery Core, auf die er sich bezieht. Folgende Informationen werden angezeigt:

- Die Anzahl der geschützten Maschinen im Rapid Recovery Core
- Die Anzahl der Computer mit fehlgeschlagenen Jobs

Zusammenfassung zu geschützten Computern

Der Abschnitt zu geschützten Maschinen des zusammenfassenden Berichts enthält Daten zu allen Maschinen, die durch den ausgewählten Rapid Recovery Core geschützt werden, und die Volumes auf diesen Maschinen.

Das Diagramm zeigt eine Zeile für jeden Jobtyp für jede Maschine an, und umfasst das Verhältnis der erfolgreichen Jobs (beliebigen Typs), die Anzahl der weitergeleiteten, fehlgeschlagenen und abgebrochenen Jobs. (Abgebrochene Aufträge werden für diese Statistiken nicht berücksichtigt.)

Grundlegende Informationen zu Fehlerberichten

Der Fehlerbericht ist eine Unterkategorie der Jobberichte und steht für den Rapid Recovery Core und für die vom Core geschützten Maschinen zu Verfügung. Fehlerberichte enthalten nur die abgebrochenen und fehlgeschlagenen Jobs, die im Jobbericht aufgeführt sind. Sie werden in einem einzelnen Bericht zusammengefasst und können gedruckt sowie exportiert werden. Wenn der Bericht eine leere Zeile erzeugt, sind keine Fehler innerhalb des in Ihren Berichtkriterien festgelegten Datumsbereichs aufgetreten.

NOTE: Ergebnisse für die Parameter für Ziel-Cores und geschützte Maschinen werden nur für den Bericht auf Core-Ebene angezeigt.

Informationen zum Erstellen von Berichten aus dem Core finden Sie unter Bedarfsweise Generierung eines Core-Berichts. Informationen zum Erstellen von Berichten für einen geschützten Computer finden Sie unter Generieren eines bedarfsorientierten Berichts zu einer geschützten Maschine.

Beim Erstellen eines Fehlerberichts wird eine Übersichtstabelle angezeigt, in der für jeden Job im von Ihnen angegeben Datumsbereich eine Zeile enthalten ist. Zusätzlich zur Auflistung des entsprechenden Core, geschützten Computers und Jobtyp enthält jede Zeile:

- Eine Zusammenfassung des Jobs
- Den Job-Status
- Etwaige Fehler in Bezug auf den Job
- Das Start- und Enddatum des Jobs
- Die Jobdauer in Sekunden
- Die gesamte Arbeit in MB

Grundlegende Informationen zu Zusammenfassungsberichten

Der zusammenfassende Bericht steht für einen oder mehrere Cores zur Verfügung. Dieser Bericht ist nicht aus Berichten für einen geschützten Computer verfügbar. Der zusammenfassende Bericht enthält Informationen zu den Repositorys des ausgewählten Rapid Recovery Core sowie zu den durch den Core geschützten Maschinen. Die Informationen werden in zwei Übersichten in einem Bericht angezeigt.

Informationen zum Erstellen von zusammenfassenden Berichten finden Sie unter Erstellen eines Berichts von der Core Console.

Die Berichtparameter für diese Berichtsart umfassen:

- Datumsbereich
- Geschützte Computer

Beim Erstellen eines zusammenfassenden Berichts beinhalten die Einzelheiten des Berichts Auswahlkriterien für den Bericht sowie Informationen über Repositorys und geschützte Computer.

Core-Informationen

Der Abschnitt „Core“ des zusammenfassenden Berichts enthält Angaben zu den Rapid Recovery Core, auf die er sich bezieht. Folgende Informationen werden angezeigt:

- Der Lizenzschlüssel (Bezeichner)
- Die aktuelle Version der Rapid Recovery Core-Software

Repositoryübersicht

Der Repositoryabschnitt des zusammenfassenden Berichts enthält Daten zu den Repositorys, die sich im ausgewählten Rapid Recovery Core befinden. Folgende Informationen werden angezeigt:

- Die Anzahl der Repositorys im Rapid Recovery Core
- Eine Zusammenfassung der Repositorys im Core

Zusammenfassung zu geschützten Computern

Der Abschnitt zu geschützten Maschinen des zusammenfassenden Berichts enthält Daten zu allen Maschinen, die durch den oder die ausgewählten Rapid Recovery Core Core(s) geschützt werden. Dieser beinhaltet einen Diagramm und eine Übersichtstabelle.

Das Diagramm zeigt die geschützten Computer nach dem Verhältnis der erfolgreichen Jobs (beliebigen Typs) zu den fehlgeschlagenen Jobs. (Abgebrochene Aufträge werden für diese Statistiken nicht berücksichtigt.)

Die X- oder horizontale Achse zeigt die Anzahl der geschützten Maschinen an. Die Y- oder vertikale Achse zeigt die Erfolgsebenen an. Insbesondere zeigt die Y-Achse für die einzelnen geschützten Computer an, auf wie vielen:

- Keine Aufträge durchgeführt wurden
- Weniger als 50 % Erfolgsquote vorlag
- Mehr als 50 % Erfolgsquote vorlag
- 100 % Erfolgsquote vorlag

Unter dem Diagramm werden Informationen über die geschützten Computer angezeigt. Folgende Informationen werden angezeigt:

- Die Menge der geschützten Computer
- Die Anzahl der geschützten Computer mit fehlgeschlagenen Jobs
- Eine Übersichtstabelle, nach geschützten Computern sortiert, die Folgendes enthält:
  - Name des geschützten Computers
  - Vom Computer geschützte Volumes
  - Geschützter Speicherplatz, in GB (insgesamt und aktuell)
  - Tägliche Änderungsrate (Durchschnitt und Median)
  - Jobstatistiken (erfolgreich, abgeschlossen, fehlgeschlagen, abgebrochen)
  - Ob Verschlüsselung angewendet wurde
- Die Core-Version

Grundlegende Informationen zu Repositoryberichten

Der Repositorybericht enthält Informationen zu den Repositorys des ausgewählten Rapid Recovery Core sowie zu den durch den Core geschützten Maschinen. Die Informationen werden in zwei Übersichten in einem Bericht angezeigt.

Informationen zum Erstellen von Berichten für mehrere Cores finden Sie unter Bedarfsweise Generierung eines Core-Berichts.

Die Berichtparameter für diese Berichtsart umfassen nur Repositorys.

Beim Erstellen eines Repositoryberichts umfassen die Einzelheiten des Berichts für jedes Repository eine Zusammenfassungsliste von Repositorys auf dem Core.

Grundlegende Informationen zu klassischen Übersichtsberichten

Der klassische Übersichtsbericht bietet eine Übersicht über eine Vielzahl von nützlichen Kennzahlen für den Core im gewählten Zeitraum.

Der obere Teil enthält drei Kreisdiagramme. Das erste Kreisdiagramm zeigt Jobstatistiken (erfolgreiche, abgebrochene und fehlgeschlagene Jobs). Das zweite Kreisdiagramm zeigt den Speicherplatz pro Repository in GB. Das dritte Kreisdiagramm zeigt Snapshot-Statistiken (erfolgreiche, abgebrochene und fehlgeschlagene Jobs).

Es folgt ein Trenddiagramm, das die Repository-Ausnutzung anzeigt.

Außerdem enthält der Bericht eine Übersicht der geschützten Maschinen.

Berichtsparameter für diesen Berichtstyp umfassen den Datumsbereich und den relevanten Core.

Informationen zum Erstellen dieser Art von Bericht für den Core finden Sie unter Bedarfsweise Generierung eines Core-Berichts.

VM-Export

In diesem Kapitel wird beschrieben, wie Sie einen Wiederherstellungspunkt exportieren, um eine virtuelle Maschine zu erstellen.

Exportieren auf virtuelle Maschinen mit Rapid Recovery

Sie können einen Wiederherstellungspunkt einer Windows- oder Linux-Maschine aus Rapid Recovery Core in einem der unterstützten Formate in eine virtuelle Maschine (VM) exportieren. Wenn die ursprüngliche auf dem Core geschützte Maschine ausfällt, können Sie die virtuelle Maschine starten, um sie schnell vorübergehend zu ersetzen, wodurch Sie Zeit zur Wiederherstellung der ursprünglichen geschützten Maschine ohne nennenswerte Ausfallzeiten haben. Dieser virtuelle Export resultiert in einer VM, die alle Sicherungsinformationen aus einem Wiederherstellungspunkt sowie das Betriebssystem und die Einstellungen für die geschützte Maschine beinhaltet. Die VM wird ein startfähiger Klon einer geschützten Maschine.

NOTE: Der Wiederherstellungspunkt muss Teil einer kompletten Wiederherstellungspunkt-Kette sein. Weitere Informationen über Wiederherstellungspunkt-Ketten finden Sie unter Wiederherstellungspunkt-Ketten und -Waisen.

Sie können einen virtuellen Export von der Seite **Virtual Standby** in der Core Console, aus einem bestimmten im Core angezeigten Wiederherstellungspunkt oder durch Auswählen von **VM-Export** aus dem Drop-Down-Menü **Wiederherstellen** auf der Schaltflächenleiste durchführen.

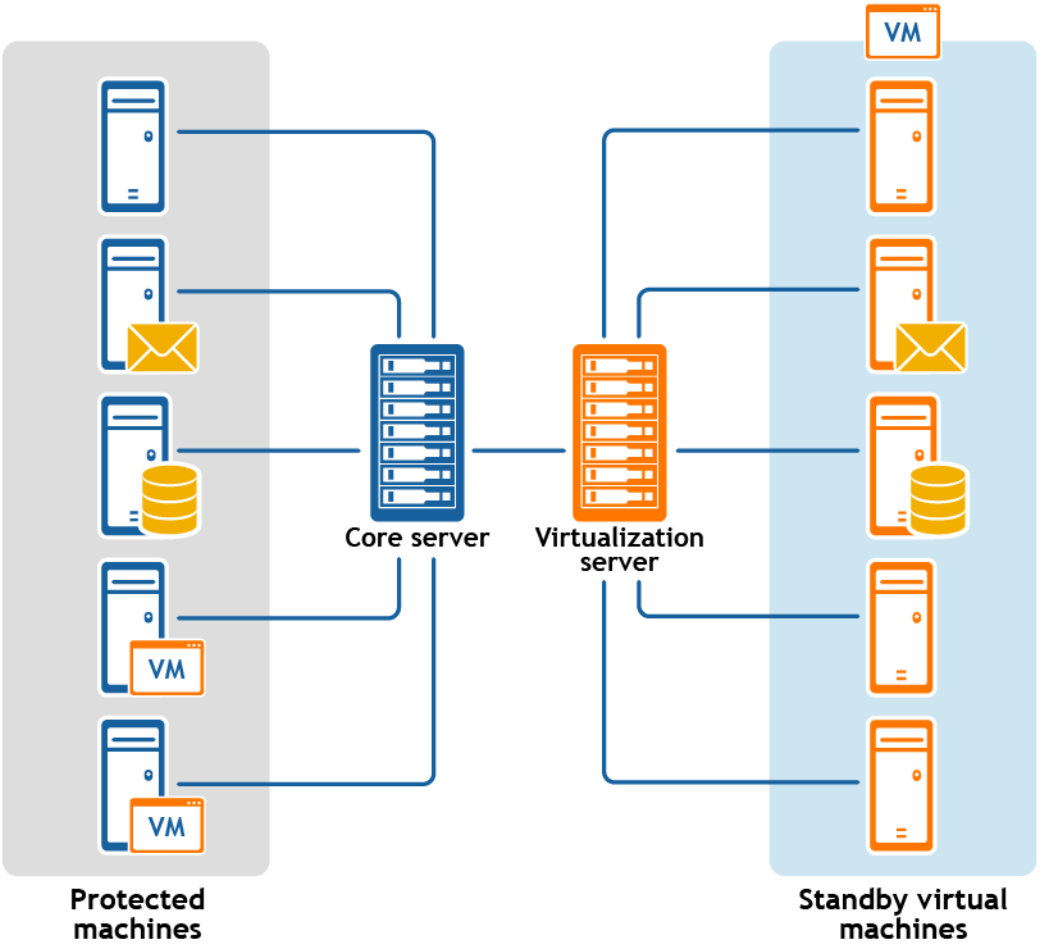
Zum Durchführen eines virtuellen Exports aus Rapid Recovery Core haben Sie zwei Möglichkeiten:

- Sie können einen **einmaligen virtuellen Export** durchführen, welcher eine startfähige VM erstellt, die einem einzelnen Snapshot der Informationen in dem Wiederherstellungspunkt entspricht. Der Exportvorgang wird sofort in die Warteschlange gestellt, und wenn er abgeschlossen ist, wird die geklonte VM an den von Ihnen gewählten Speicherort exportiert. Die für einen einmaligen Export verwendeten Konfigurationsinformationen werden nicht gespeichert.
- Sie können einen **fortlaufenden Export** einrichten. Durch diesen Vorgang entsteht eine startfähige virtuelle Maschine aus dem ursprünglichen Wiederherstellungspunkt, den Sie angegeben haben. Diese VM wird an dem von Ihnen bestimmten Speicherort gespeichert. Die Konfigurationsinformationen zur Durchführung dieses virtuellen Exports werden auf der Seite **Virtual Standby** in der Core Console gespeichert. Danach stellt der Core jedes Mal, wenn ein neuer Snapshot der geschützten Maschine aufgenommen wird, einen neuen virtuelles Exportjob in die Warteschlange, und die startfähige VM wird mit den aktualisierten Informationen aktualisiert. Da dies eine hochverfügbare Ressource für die Wiederherstellung von Daten erzeugt, wird diese Funktion auch als **Virtual Standby** bezeichnet

In dem Zeitraum, währenddessen ein virtueller Export in der Warteschlange steht, und dessen Abschluss wird der Job im Fensterbereich „Exportwarteschlange“ der Seite „Virtual Standby“ in der Core Console aufgelistet.

Das folgende Diagramm veranschaulicht eine typische Implementierung für den Export von Daten in eine virtuelle Maschine.

Abbildung 5. Virtual Standby-Implementierung



NOTE: In einer Konfiguration im Zusammenhang mit Replikationen stellt der gezeigte Core den Ziel-Core dar. Wenn zwischen zwei Cores (Quelle und Ziel) eine Replikation eingerichtet ist, können Sie nur Daten vom Ziel-Core exportieren, nachdem die Anfangsreplikation durchgeführt wurde.

Kompatible VM-Hypervisoren umfassen vCenter/ESXi, VMWare Workstation, Hyper-V, VirtualBox und Azure. Weitere Informationen über unterstützte Versionen dieser Hypervisors finden Sie im Thema „Hypervisor-Anforderungen“ in *Rapid Recovery Systemanforderungen-Handbuch*.

Bei ESXi, VMware Workstation oder Hyper-V muss die Version der virtuellen Maschine eine lizenzierte Version der virtuellen Maschinen sein. Test- oder Gratisversion werden nicht unterstützt. Der Export zu Azure setzt voraus, dass Sie ein Konto auf Azure haben und dass weitere Voraussetzungen erfüllt sind.

NOTE: Für Azure wird durch den Export und die spätere Bereitstellung eine VM mithilfe der klassischen VM-Verwaltung und nicht über das neuere Resource Manager-Modell erstellt. Das Arbeiten mit Azure umfasst Aspekte, die spezifisch für diesen Cloud-Service-Provider sind. Weitere Informationen hierzu finden Sie unter Vor dem virtuellen Export auf Azure.

Zugehörige Konzepte

See also: Exportieren von Daten in eine virtuelle ESXi-Maschine
See also: Exportieren von Daten in eine virtuelle VMware Workstation-Maschine
See also: Exportieren von Daten in eine virtuelle VirtualBox-Maschine
See also: Exportieren von Daten in eine virtuelle Azure Maschine

Zugehörige Tasks

See also: Verwalten von Exporten

Zugehörige Verweise

See also: Exportieren von Daten in eine virtuelle Hyper-V-Maschine

Exportieren von Daten in eine virtuelle ESXi-Maschine

In Rapid Recovery können Sie Daten nach ESXi exportieren, indem Sie einen einmaligen Export durchführen oder einen kontinuierlichen Export (für Virtual Standby) einrichten. Führen Sie die nachstehend aufgeführten Schritte für den jeweiligen Exporttyp aus.

Durchführen eines einmaligen ESXi-Exports

Führen Sie die folgenden Schritte aus, um einen einmaligen ESXi-Export durchzuführen.

1. Klicken Sie in der Rapid Recovery Core Console in der Schaltflächenleiste auf das Drop-Down-Menü **Wiederherstellung** und dann auf **VM-Export**.
2. Wählen Sie im Assistenten zum Exportieren virtueller Maschinen **One-time Export** (Einmaliger Export) aus.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite „Maschinen“ die geschützte Maschine aus, die Sie exportieren möchten.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite „Wiederherstellungspunkte“ den Wiederherstellungspunkt aus, den Sie für den Export verwenden möchten.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Ziel** des Exportassistenten im Dropdown-Menü Export auf eine virtuelle Maschine**ESX(i)** aus.
9. Geben Sie die Parameter für den Zugriff auf die virtuelle Maschine ein (siehe Beschreibung in der folgenden Tabelle), und klicken Sie auf **Weiter**.

Tabelle 117. Parameter für virtuelle Maschine

Optionen	Description
Hostname	Geben Sie einen Namen für die Hostmaschine ein.
Port	Geben Sie den Port für die Hostmaschine ein. Die Standardeinstellung ist 443.
Benutzername	Geben Sie den Benutzername für die Anmeldung an der Host-Maschine ein.
Kennwort	Geben Sie das Kennwort für die Anmeldung an der Hostmaschine ein.

10. Geben Sie auf der Seite „Optionen für virtuelle Maschine“ die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 118. Optionen für virtuelle Maschine

Option	Description
Ressourcenpool	Wählen Sie einen Ressourcenpool in der Dropdown-Liste aus.

Option	Description
Speicherort VM-Konfiguration	Wählen Sie einen Datenspeicher in der Dropdown-Liste aus.
Name der virtuellen Maschine	Geben Sie einen Namen für die virtuelle Maschine ein.
Speicher	Geben Sie den Arbeitsspeicher für die virtuelle Maschine an. Sie haben folgende Auswahlmöglichkeiten: • Gleiche RAM-Größe verwenden wie Quellmaschine • „Bestimmte RAM-Größe verwenden“ auswählen und Größe in MB eingeben Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.
Anzahl der Prozessoren	Die Anzahl der Prozessoren (CPUs) die Sie für die exportierte virtuelle Maschine möchten. Dieser Mindestwert beträgt 1.
Cores pro Prozessor	Die Anzahl der Cores, die Sie für jeden Prozessor möchten. Dieser Mindestwert beträgt 1.
Datenträgerbereitstellung	Wählen Sie die Art der Datenträgerbereitstellung aus den folgenden Optionen aus: • Schlank. Schlanke Speicherzuweisung (Thin Provisioning) erstellt eine virtuelle Festplatte mit der Größe des verwendeten Speicherplatzes auf den ursprünglichen Volumes, anstatt der gesamten Volume-Größe. Wenn es sich bei dem ursprünglichen Volume beispielsweise um 1 TB handelt, aber es nur 2 GB verwendeten Speicherplatz enthält, erstellt Rapid Recovery ein virtuelles Laufwerk von 2 GB. • Breit. Thick Provisioning erstellt einen neuen Datenträger oder ein neues Volume, der/das die gleiche Größe hat, wie das ursprüngliche Volume des geschützten Servers, auch wenn nur einen Teil des ursprünglichen Volume verwendet wird. Wenn es sich bei dem Volume beispielsweise um eine Größe von 1 TB handelt, aber es nur 2 GB verwendeten Speicherplatz enthält, erstellt Rapid Recovery ein virtuelles Laufwerk von 1 TB.
Datenträgerzuordnung	Wählen Sie die Art der Datenträgerzuordnung aus den folgenden Optionen aus: • Automatisch • Manuell • Mit VM
Version	Wählen Sie die Version, die von ESXi für die Erstellung der virtuellen Maschine verwendet wird, aus der Dropdown-Liste aus.

11. Klicken Sie auf **Weiter**.
12. Wählen Sie auf der Seite **Volumes** die Volumes aus, die Sie exportieren möchten, und klicken Sie dann auf **Weiter**.
13. Klicken Sie auf der Seite **Zusammenfassung** auf **Fertigstellen**, um den Assistenten zu schließen und den Export zu starten.

NOTE: Sie können Status und Fortschritt des Exports über das Anzeigen der Seiten **Virtual Standby** oder **Ereignisse** anzeigen.

Einrichten eines fortlaufenden Exports zu ESXi

Führen Sie die Schritte in diesem Verfahren aus, um einen kontinuierlichen Export an eine virtuelle ESXi-Maschine (VM) mit Rapid Recovery einzurichten. Dies wird auch als Einrichten von Virtual Standby bezeichnet.

1. Führen Sie auf der Rapid Recovery Core Console eine der folgenden Aktionen aus:
   - Klicken Sie in der Core Console auf das Dropdown-Menü **Wiederherstellen** und dann auf **VM-Export**.
     1. Wählen Sie im Assistenten zum Exportieren von virtuellen Maschinen **Dauerhaft (virtueller Standby)**.
     2. Klicken Sie auf **Weiter.**
   - Klicken Sie in der Core Console in der Symbolleiste auf (Virtual Standby).
     - Klicken Sie auf der Registerkarte **Virtual Standby** auf **Hinzufügen**, um den Assistenten zum Exportieren von virtuellen Maschinen zu starten.
2. Wählen Sie auf der Seite **Maschinen** des Assistenten zum Exportieren von virtuellen Maschinen die geschützte Maschine, die Sie exportieren möchten.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Wiederherstellungspunkte** den Wiederherstellungspunkt aus, den Sie für den Export verwenden möchten.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Ziel** im Assistenten für den Export im Dropdown-Menü „Wiederherstellung auf eine virtuelle Maschine“ die Option **ESXi** aus.
7. Geben Sie die Informationen für den Zugriff auf die virtuelle Maschine ein (siehe Beschreibung in der folgenden Tabelle), und klicken Sie auf **Weiter**.

Tabelle 119. ESXi-Anmeldeinformationen

Option	Description
Hostname	Geben Sie einen Namen für die Hostmaschine ein.
Port	Geben Sie den Port für die Hostmaschine ein. Die Standardeinstellung ist 443.
Benutzername	Geben Sie die Anmeldeinformationen für die Hostmaschine ein.
Kennwort	Geben Sie die Anmeldeinformationen für die Hostmaschine ein.

8. Geben Sie auf der Seite **Optionen für virtuelle Maschine** die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 120. Optionen für virtuelle Maschine

Option	Description
Ressourcenpool	Wählen Sie einen Ressourcenpool in der Dropdown-Liste aus.
Datenspeicher	Wählen Sie einen Datenspeicher in der Dropdown-Liste aus.

Option	Description
Name der virtuellen Maschine	Geben Sie einen Namen für die virtuelle Maschine ein.
Speicher	Geben Sie den Arbeitsspeicher für die virtuelle Maschine an. Sie haben folgende Auswahlmöglichkeiten: • Gleiche RAM-Größe verwenden wie Quellmaschine • „Bestimmte RAM-Größe verwenden“ auswählen und Größe in MB eingeben Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.
Anzahl der Prozessoren	Die Anzahl der Prozessoren (CPUs) die Sie für die exportierte virtuelle Maschine möchten. Dieser Mindestwert beträgt 1.
Cores pro Prozessor	Die Anzahl der Cores, die Sie für jeden Prozessor möchten. Dieser Mindestwert beträgt 1.
Datenträgerbereitstellung	Wählen Sie die Art der Datenträgerbereitstellung aus den folgenden Optionen aus: • Schlank. Schlanke Speicherzuweisung (Thin Provisioning) erstellt eine virtuelle Festplatte mit der Größe des verwendeten Speicherplatzes auf den ursprünglichen Volumes, anstatt der gesamten Volume-Größe. Wenn es sich bei dem ursprünglichen Volume beispielsweise um 1 TB handelt, aber es nur 2 GB verwendeten Speicherplatz enthält, erstellt Rapid Recovery ein virtuelles Laufwerk von 2 GB. • Breit. Thick Provisioning erstellt einen neuen Datenträger oder ein neues Volume, der/das die gleiche Größe hat, wie das ursprüngliche Volume des geschützten Servers, auch wenn nur einen Teil des ursprünglichen Volume verwendet wird. Wenn es sich bei dem Volume beispielsweise um eine Größe von 1 TB handelt, aber es nur 2 GB verwendeten Speicherplatz enthält, erstellt Rapid Recovery ein virtuelles Laufwerk von 1 TB.
Festplattenzuordnung	Geben Sie den Typ der Datenträgerzuordnung an („Automatisch“, „Manuell“ oder „Mit VM“).
Version	Wählen Sie die Version der virtuellen Maschine aus.
Ersten einmaligen Export durchführen	Wählen Sie diese Option aus, um den virtuellen Export sofort und nicht nach dem nächsten geplanten Snapshot durchzuführen.

9. Klicken Sie auf **Weiter**.
10. Wählen Sie auf der Seite **Volumes** die Volumes aus, die Sie exportieren möchten, und klicken Sie dann auf **Weiter**.
11. Klicken Sie auf der Seite **Zusammenfassung** auf **Fertigstellen**, um den Assistenten zu schließen und den Export zu starten.

NOTE: Sie können Status und Fortschritt des Exports über das Anzeigen der Seiten „Virtual Standby“ oder „Ereignisse“ anzeigen.

Exportieren von Daten in eine virtuelle VMware Workstation-Maschine

In Rapid Recovery können Sie Daten zur VMware Workstation exportieren, indem Sie einen einmaligen Export durchführen oder einen kontinuierlichen Export (Virtual Standby) einrichten. Führen Sie die nachstehend aufgeführten Schritte für den jeweiligen Exporttyp aus.

Durchführen eines einmaligen VMware Workstation-Exports

Führen Sie die folgenden Schritte aus, um einen einmaligen VMware Workstation-Export durchzuführen.

1. Klicken Sie in der Rapid Recovery Core Console in der Schaltflächenleiste, auf das Dropdownmenü **Restore** (Wiederherstellen) und auf **VM Export**.
2. Wählen Sie im Assistenten zum Exportieren virtueller Maschinen **One-time Export** (Einmaliger Export) aus.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Maschinen** die geschützte Maschine aus, die Sie exportieren möchten.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Wiederherstellungspunkte** den Wiederherstellungspunkt aus, den Sie für den Export verwenden möchten.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Ziel** im Assistenten für den Export im Dropdown-Menü Auf virtuelle Maschine exportieren die Option **VMware Workstation** aus und klicken Sie dann auf **Weiter**.
9. Geben Sie auf der Seite **Virtual Machine Options** (Optionen für virtuelle Maschinen) die Parameter für den Zugriff auf die virtuelle Maschine gemäß Beschreibung in der folgenden Tabelle ein.

Tabelle 121. Parameter für virtuelle Maschine

Option	Description
VM Machine Location (Speicherort virtuelle Maschine)	Geben Sie den Pfad des lokalen Ordners oder die Netzwerkfreigabe für die Erstellung der virtuellen Maschine an. **NOTE:** Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie gültige Anmeldeinformationen für ein Konto eingeben, das auf der Zielmaschine registriert ist. Das Konto muss über Lese- und Schreibberechtigungen für die Netzwerkfreigabe verfügen.
Benutzername	Geben Sie die Anmeldeinformationen für den Netzwerkspeicherort für den Export ein. • Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie einen gültigen Benutzernamen für ein Konto eingeben, das auf der Zielmaschine registriert ist. • Wenn Sie einen lokalen Pfad angegeben haben, ist kein Benutzername erforderlich.

Option	Description
Kennwort	Geben Sie die Anmeldeinformationen für den Netzwerkspeicherort für den Export ein. • Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie ein gültiges Kennwort für ein Konto eingeben, das auf der Zielmaschine registriert ist. • Wenn Sie einen lokalen Pfad angegeben haben, ist kein Kennwort erforderlich.
VM-Name	Geben Sie den Namen für die zu erstellende virtuelle Maschine ein, z. B. VM-0A1B2C3D4. **NOTE:** Standardmäßig wird der Name der Quellmaschine verwendet.
Version	Wählen Sie die VMware Workstation-Version der virtuellen Maschine aus. Sie haben folgende Auswahlmöglichkeiten: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0 • VMware Workstation 11.0 • VMware Workstation 12.0
RAM-Größe (MB)	Geben Sie den Arbeitsspeicher für die virtuelle Maschine an. Sie haben folgende Auswahlmöglichkeiten: • Gleiche RAM-Größe verwenden wie Quellmaschine • „Bestimmte RAM-Größe verwenden“ auswählen und Größe in MB eingeben Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.
Anzahl der Prozessoren	Die Anzahl der Prozessoren (CPUs) die Sie für die exportierte virtuelle Maschine möchten. Dieser Mindestwert beträgt 1.
Cores pro Prozessor	Die Anzahl der Cores, die Sie für jeden Prozessor möchten. Dieser Mindestwert beträgt 1.

10. Klicken Sie auf **Weiter**.
11. Wählen Sie auf der Seite **Volumes** die Volumes aus, die Sie exportieren möchten, z. B. C:\ und D:\, und klicken Sie dann auf **Weiter**.
12. Klicken Sie auf der Seite **Zusammenfassung** auf **Fertigstellen**, um den Assistenten zu schließen und den Export zu starten.

NOTE: Sie können Status und Fortschritt des Exports über das Anzeigen der Seiten **Virtual Standby** oder **Ereignisse** anzeigen.

Einrichten eines fortlaufenden Exports zu VMware Workstation

Führen Sie die Schritte in diesem Verfahren aus, um einen fortlaufenden Export an eine virtuelle Maschine (VM) einer VMware Workstation mit Rapid Recovery einzurichten. Dies wird auch als Einrichten von Virtual Standby bezeichnet.

1. Führen Sie auf der Rapid Recovery Core Console eine der folgenden Aktionen aus:
   - Klicken Sie in der Core Console auf das Dropdown-Menü **Wiederherstellen** und dann auf **VM-Export**.
     1. Wählen Sie im Assistenten zum Exportieren von virtuellen Maschinen **Dauerhaft (virtueller Standby)**.
     2. Klicken Sie auf **Weiter.**
   - Klicken Sie in der Core Console in der Symbolleiste auf (Virtual Standby).
     - Klicken Sie auf der Registerkarte **Virtual Standby** auf **Hinzufügen**, um den Assistenten zum Exportieren von virtuellen Maschinen zu starten.
2. Wählen Sie auf der Seite **Maschinen** des Assistenten zum Exportieren von virtuellen Maschinen die geschützte Maschine, die Sie exportieren möchten.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Wiederherstellungspunkte** den Wiederherstellungspunkt aus, den Sie für den Export verwenden möchten.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Ziel** des Exportassistenten im Dropdown-Menü „Wiederherstellung auf eine virtuelle Maschine“ **VMware Workstation** aus und klicken Sie auf **Weiter**.
7. Geben Sie auf der Seite **Virtual Machine Options** (Optionen für virtuelle Maschinen) die Parameter für den Zugriff auf die virtuelle Maschine gemäß Beschreibung in der folgenden Tabelle ein.

Tabelle 122. Parameter für virtuelle Maschine

Option	Description
Zielpfad	Geben Sie den Pfad des lokalen Ordners oder die Netzwerkfreigabe für die Erstellung der virtuellen Maschine an. **NOTE:** Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie gültige Anmeldeinformationen für ein Konto eingeben, das auf der Zielmaschine registriert ist. Das Konto muss über Lese- und Schreibberechtigungen für die Netzwerkfreigabe verfügen.
Benutzername	Geben Sie die Anmeldeinformationen für den Netzwerkspeicherort für den Export ein. • Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie einen gültigen Benutzernamen für ein Konto eingeben, das auf der Zielmaschine registriert ist. • Wenn Sie einen lokalen Pfad angegeben haben, ist kein Benutzername erforderlich.

Option	Description
Kennwort	Geben Sie die Anmeldeinformationen für den Netzwerkspeicherort für den Export ein. • Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie ein gültiges Kennwort für ein Konto eingeben, das auf der Zielmaschine registriert ist. • Wenn Sie einen lokalen Pfad angegeben haben, ist kein Kennwort erforderlich.
Virtueller Computer	Geben Sie den Namen für die zu erstellende virtuelle Maschine ein, z. B. VM-0A1B2C3D4. **NOTE:** Standardmäßig wird der Name der Quellmaschine verwendet.
Version	Wählen Sie die VMware Workstation-Version der virtuellen Maschine aus. Sie haben folgende Auswahlmöglichkeiten: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0 • VMware Workstation 11.0 • VMware Workstation 12.0
Speicher	Geben Sie den Arbeitsspeicher für die virtuelle Maschine an. Sie haben folgende Auswahlmöglichkeiten: • Gleiche RAM-Größe verwenden wie Quellmaschine • „Bestimmte RAM-Größe verwenden“ auswählen und Größe in MB eingeben Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.
Anzahl der Prozessoren	Die Anzahl der Prozessoren (CPUs) die Sie für die exportierte virtuelle Maschine möchten. Dieser Mindestwert beträgt 1.
Cores pro Prozessor	Die Anzahl der Cores, die Sie für jeden Prozessor möchten. Dieser Mindestwert beträgt 1.

8. Wählen Sie **Ersten einmaligen Export durchführen**, um den virtuellen Export sofort und nicht nach dem nächsten geplanten Snapshot durchzuführen.
9. Klicken Sie auf **Weiter**.
10. Wählen Sie auf der Seite **Volumes** die Volumes aus, die Sie exportieren möchten, z. B. C:\ und D:\, und klicken Sie dann auf **Weiter**.
11. Klicken Sie auf der Seite **Summary** (Zusammenfassung) auf **Finish** (Fertig stellen), um den Assistenten zu beenden und den Export zu starten.

NOTE: Sie können Status und Fortschritt des Exports über das Anzeigen der Seiten „Virtual Standby“ oder „Ereignisse“ anzeigen.

Exportieren von Daten in eine virtuelle Hyper-V-Maschine

In Rapid Recovery können Sie Daten nach Hyper-V-Export exportieren, indem Sie einen einmaligen Export durchführen oder einen kontinuierlichen Export (Virtual Standby) einrichten.

Weitere Informationen zu den unterstützten Host-Betriebssystemen für Hyper-V-Exporte der ersten Generation und zweiten Generation finden Sie im Thema „Hypervisor-Anforderungen“ in *Rapid Recovery Systemanforderungen-Handbuch*.

Führen Sie die nachstehend aufgeführten Schritte für den jeweiligen Exporttyp aus.

Durchführen eines einmaligen Hyper-V-Exports

Führen Sie die folgenden Schritte aus, um einen einmaligen Hyper-V-Export durchzuführen.

1. Klicken Sie in der Rapid Recovery Core Console in der Schaltflächenleiste, auf das Dropdownmenü **Restore** (Wiederherstellen) und auf **VM Export**.
2. Wählen Sie im Assistenten zum Exportieren virtueller Maschinen **One-time Export** (Einmaliger Export) aus.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Maschinen** die geschützte Maschine aus, die Sie exportieren möchten.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Wiederherstellungspunkte** den Wiederherstellungspunkt aus, den Sie für den Export verwenden möchten.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Ziel** im Drop-Down-Menü „Export auf eine virtuelle Maschine“ **Hyper-V**.
9. Klicken Sie auf **Lokale Maschine verwenden**, um den Export in eine lokale Maschine durchzuführen, der die Hyper-V-Rolle zugewiesen ist.
10. Klicken Sie auf **Remote-Host**, um anzugeben, dass sich der Hyper-V-Server auf einer Remote-Maschine befindet, und geben Sie dann die in der folgenden Tabelle beschriebenen Informationen für den Remote-Host ein.

Tabelle 123. Remote-Hostinformationen

Textfeld	Description
Hostname	Geben Sie eine IP-Adresse oder einen Hostnamen für den Hyper-V-Server ein. Dabei handelt es sich um die IP-Adresse oder den Hostnamen des Remote-Hyper-V-Servers.
Port	Geben Sie eine Portnummer für die Maschine ein. Dabei handelt es sich um den Port, über den der Core mit der Maschine kommuniziert.
Benutzername	Geben Sie den Benutzernamen für den Benutzer mit Administratorberechtigungen für die Workstation mit dem Hyper-V-Server ein. Diese Angabe dient zur Festlegung der Anmeldeinformationen für die virtuelle Maschine.

Textfeld	Description
Kennwort	Geben Sie das Kennwort für das Benutzerkonto mit den Administratorberechtigungen auf der Workstation mit Hyper-V-Server an. Diese Angabe dient zur Festlegung der Anmeldeinformationen für die virtuelle Maschine.

11. Klicken Sie auf **Weiter**.
12. Geben Sie auf der Seite **Optionen für virtuelle Maschinen** im Textfeld **Speicherort für virtuelle Maschine** den Pfad für die virtuelle Maschine ein, z. B. `D:\export`. Er wird verwendet, um den Speicherort der virtuellen Maschine anzugeben.

    NOTE: Sie müssen den Speicherort der virtuellen Maschine für lokale sowie für Remote-Hyper-V-Server angeben. Der Pfad muss ein gültiger lokaler Pfad für den Hyper-V-Server sein. Nicht vorhandene Verzeichnisse werden automatisch erstellt. Sie sollten nicht versuchen, sie manuell zu erstellen. Ein Export in freigegebene Ordner (z. B. zu `\\data\share`) ist nicht zulässig.
13. Geben Sie im Textfeld **Name der virtuellen Maschine** den Namen der virtuellen Maschine ein.

    Der Name, den Sie eingeben, wird in der Liste der virtuellen Maschinen in der Hyper-V-Manager-Konsole angezeigt.
14. Geben Sie den Arbeitsspeicher an. Sie haben folgende Auswahlmöglichkeiten:
    - **Verwenden Sie die gleiche RAM-Größe wie die Quellmaschine**. Wählen Sie diese Option aus, um anzugeben, dass die RAM-Nutzung bei virtuellen und Quellmaschinen identisch ist.
    - **Eine spezielle RAM-Größe verwenden.** Wählen Sie diese Option aus, wenn Sie die Größe des RAM-Speichers in MB angeben möchten.

      Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.
15. Klicken Sie zum Angeben der Datenträgerformats neben „Datenträgerformat“ auf eine der folgenden Optionen:
    - VHDX
    - VHD

    NOTE: Der Hyper-V-Export unterstützt VHDX-Datenträgerformate, wenn auf der Zielmaschine Windows 8 (Windows Server 2012) oder höher ausgeführt wird. Wenn VHDX für die jeweilige Umgebung nicht unterstützt wird, ist die Option deaktiviert.

    NOTE: Bei einem Export nach Hyper-V der 2. Generation wird nur das VHDX-Datenträgerformat unterstützt.
16. Klicken Sie auf eine der folgenden Optionen, um die Generation von Hyper-V anzugeben, die für den Export verwendet werden soll:
    - Generation 1
    - Generation 2

    NOTE: Nur die 2. Generation unterstützt die Option „Sicherer Start“.
17. Geben Sie den gewünschten Netzwerkadapter für die exportierte VM an.
18. Wählen Sie auf der Seite **Volumes** das/die zu exportierende/n Volume/s aus, z. B. C: \.

NOTE: Wenn die ausgewählten Volumes größer sind als die maximal zulässige Größe, die von der Anwendung unterstützt wird, oder den verfügbaren Speicherplatz überschreiten, wird eine Fehlermeldung angezeigt.

- Beim VHDX-Datenträgerformat dürfen die ausgewählten Volumes nicht größer als 64 TB sein.
- Beim VHD-Datenträgerformat dürfen die ausgewählten Volumes nicht größer als 2040 GB sein.

19. Klicken Sie auf der Seite **Volumes** auf **Fertigstellen**, um den Assistenten zu beenden und den Export zu starten.

NOTE: Sie können Status und Fortschritt des Exports über das Anzeigen der Seiten **Virtual Standby** oder **Ereignisse** anzeigen.

Einrichten eines fortlaufenden Exports zu Hyper-V

Führen Sie die Schritte in diesem Verfahren aus, um einen fortlaufenden Export zu einer virtuellen Hyper-V-Maschine (VM) mit Rapid Recovery einzurichten. Dies wird auch als Einrichten von Virtual Standby bezeichnet.

1. Führen Sie auf der Rapid Recovery Core Console eine der folgenden Aktionen aus:
   - Klicken Sie auf der Schaltflächenleiste in der Core Console auf das Drop-Down-Menü **Wiederherstellen** und dann auf **VM-Export**.
     1. Wählen Sie im Assistenten zum Exportieren von virtuellen Maschinen **Dauerhaft (virtueller Standby)**.
     2. Klicken Sie auf **Weiter.**
   - Klicken Sie in der Core Console in der Symbolleiste auf (Virtual Standby).
     - Klicken Sie auf der Registerkarte **Virtual Standby** auf **Hinzufügen**, um den Assistenten zum Exportieren von virtuellen Maschinen zu starten.
2. Wählen Sie auf der Seite **Maschinen** des Assistenten zum Exportieren von virtuellen Maschinen die geschützte Maschine, die Sie exportieren möchten.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Wiederherstellungspunkte** den Wiederherstellungspunkt aus, den Sie für den Export verwenden möchten.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Ziel** im Drop-Down-Menü „Export auf eine virtuelle Maschine“ **Hyper-V** und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie auf **Lokale Maschine verwenden**, um den Export in eine lokale Maschine durchzuführen, der die Hyper-V-Rolle zugewiesen ist.
   - Klicken Sie auf **Remote-Host**, um anzugeben, dass sich der Hyper-V-Server auf einer Remote-Maschine befindet, und geben Sie dann die in der folgenden Tabelle beschriebenen Parameter für den Remote-Host ein.

Tabelle 124. Remote-Hostinformationen

Textfeld	Description
Hostname	Geben Sie eine IP-Adresse oder einen Hostnamen für den Hyper-V-Server ein. Dabei handelt es sich um die IP-Adresse oder den Hostnamen des Remote-Hyper-V-Servers.
Port	Geben Sie eine Portnummer für die Maschine ein. Dabei handelt es sich um den Port, über den der Core mit der Maschine kommuniziert.

Textfeld	Description
Benutzername	Geben Sie den Benutzernamen für den Benutzer mit Administratorberechtigungen für die Workstation mit dem Hyper-V-Server ein. Diese Angabe dient zur Festlegung der Anmeldeinformationen für die virtuelle Maschine.
Kennwort	Geben Sie das Kennwort für das Benutzerkonto mit den Administratorberechtigungen auf der Workstation mit Hyper-V-Server an. Diese Angabe dient zur Festlegung der Anmeldeinformationen für die virtuelle Maschine.

7. Klicken Sie auf **Weiter**.
8. Geben Sie auf der Seite **Optionen für virtuelle Maschinen** im Textfeld **Speicherort für virtuelle Maschine** den Pfad für die virtuelle Maschine ein, z. B. `D:\export`. Er wird verwendet, um den Speicherort der virtuellen Maschine anzugeben.

   NOTE: Sie müssen den Speicherort der virtuellen Maschine für lokale sowie für Remote-Hyper-V-Server angeben. Der Pfad muss ein gültiger lokaler Pfad für den Hyper-V-Server sein. Nicht vorhandene Verzeichnisse werden automatisch erstellt. Sie sollten nicht versuchen, sie manuell zu erstellen. Ein Export in freigegebene Ordner (z. B. zu `\\data\share`) ist nicht zulässig.
9. Geben Sie im Textfeld **Name der virtuellen Maschine** den Namen der virtuellen Maschine ein.

   Der Name, den Sie eingeben, wird in der Liste der virtuellen Maschinen in der Hyper-V-Manager-Konsole angezeigt.
10. Geben Sie den Arbeitsspeicher an. Sie haben folgende Auswahlmöglichkeiten:
    - **Verwenden Sie die gleiche RAM-Größe wie die Quellmaschine**. Wählen Sie diese Option aus, um anzugeben, dass die RAM-Nutzung bei virtuellen und Quellmaschinen identisch ist.
    - **Eine spezielle RAM-Größe verwenden.** Wählen Sie diese Option aus, wenn Sie die Größe des RAM-Speichers in MB angeben möchten.

      Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.
11. Klicken Sie zum Angeben der Datenträgerformats neben „Datenträgerformat“ auf eine der folgenden Optionen:
    - VHDX
    - VHD

    NOTE: Der Hyper-V-Export unterstützt VHDX-Datenträgerformate, wenn auf der Zielmaschine Windows 8 (Windows Server 2012) oder höher ausgeführt wird. Wenn VHDX für die jeweilige Umgebung nicht unterstützt wird, ist die Option deaktiviert.

    NOTE: Bei einem Export nach Hyper-V der 2. Generation wird nur das VHDX-Datenträgerformat unterstützt.
12. Klicken Sie auf eine der folgenden Optionen, um die Generation von Hyper-V anzugeben, die für den Export verwendet werden soll:
    - Generation 1
    - Generation 2

    NOTE: Nur die 2. Generation unterstützt die Option „Sicherer Start“.
13. Geben Sie den gewünschten Netzwerkadapter für die exportierte VM an.
14. Wählen Sie auf der Seite **Volumes** das/die zu exportierende/n Volume/s aus, z. B. C: \.

NOTE: Wenn die ausgewählten Volumes größer sind als die maximal zulässige Größe, die von der Anwendung unterstützt wird, oder den verfügbaren Speicherplatz überschreiten, wird eine Fehlermeldung angezeigt.

- Beim VHDX-Datenträgerformat dürfen die ausgewählten Volumes nicht größer als 64 TB sein.
- Beim VHD-Datenträgerformat dürfen die ausgewählten Volumes nicht größer als 2040 GB sein.

15. Wählen Sie **Ersten einmaligen Export durchführen**, um den virtuellen Export sofort und nicht nach dem nächsten geplanten Snapshot durchzuführen.
16. Klicken Sie auf der Seite **Volumes** auf **Fertigstellen**, um den Assistenten zu beenden und den Export zu starten.

NOTE: Sie können Status und Fortschritt des Exports über das Anzeigen der Seiten **Virtual Standby** oder **Ereignisse** anzeigen.

Exportieren von Daten in eine virtuelle VirtualBox-Maschine

In Rapid Recovery können Sie Daten nach VirtualBox exportieren, indem Sie einen einmaligen Export durchführen oder einen kontinuierlichen Export (für Virtual Standby) einrichten.

Führen Sie die nachstehend aufgeführten Schritte für den jeweiligen Exporttyp aus.

NOTE: Um einen derartigen Export zu einer VirtualBox-VM auf einem Windows-Host durchführen zu können, muss VirtualBox auf der Core-Maschine installiert sein. Auf Linux gehostete VMs erfordern dies nicht.

Durchführen eines einmaligen VirtualBox-Exports

Um auf einem Remote-Windows-Host in eine VirtualBox-VM zu exportieren, sollte VirtualBox auf der Core-Maschine installiert sein. Diese Anforderung gilt nicht für VMs, die unter Linux gehostet werden.

Führen Sie die folgenden Schritte aus, um einen einmaligen VirtualBox-Export durchzuführen.

1. Klicken Sie in der Rapid Recovery Core Console in der Schaltflächenleiste, auf das Dropdownmenü **Restore** (Wiederherstellen) und auf **VM Export**.
2. Wählen Sie im Assistenten zum Exportieren virtueller Maschinen **One-time Export** (Einmaliger Export) aus.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Maschinen** die geschützte Maschine aus, die Sie exportieren möchten.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Wiederherstellungspunkte** den Wiederherstellungspunkt aus, den Sie für den Export verwenden möchten.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Ziel** im Assistenten für den Export im Dropdown-Menü Auf virtuelle Maschine exportieren die Option **VirtualBox** aus und klicken Sie dann auf **Weiter**.
9. Wählen Sie auf der Seite **Optionen für virtuelle MaschineWindows-Maschine verwenden** aus.
10. Geben Sie die Parameter für den Zugriff auf die virtuelle Maschine ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 125. Parameter für virtuelle Maschine

Option	Description
Name der virtuellen Maschine	Geben Sie den Namen für die zu erstellende virtuelle Maschine ein. **NOTE:** Standardmäßig wird der Name der Quellmaschine verwendet.
Zielpfad	Geben Sie einen lokalen oder Remote-Zielpfad für die Erstellung der virtuellen Maschine an. **NOTE:** Der Zielpfad darf kein Stammverzeichnis sein. Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie gültige Anmeldeinformationen (Benutzername und Konto) für ein Konto eingeben, das auf der Zielmaschine registriert ist. Das Konto muss über Lese- und Schreibberechtigungen für die Netzwerkfreigabe verfügen.
Speicher	Geben Sie den Arbeitsspeicher für die virtuelle Maschine an. Sie haben folgende Auswahlmöglichkeiten: • Gleiche RAM-Größe verwenden wie Quellmaschine • „Bestimmte RAM-Größe verwenden“ auswählen und Größe in MB eingeben Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.

11. Wählen Sie **Benutzerkonto für die exportierte virtuelle Maschine angeben** aus, um ein Benutzerkonto für die virtuelle Maschine anzugeben, und geben Sie die folgenden Informationen ein. Hierbei handelt es sich um ein bestimmtes Benutzerkonto, für das die virtuelle Maschine registriert wird, falls auf der virtuellen Maschine mehrere Benutzerkonten vorhanden sind. Nur der Benutzer, der sich mit diesem Benutzerkonto anmeldet, kann die betreffende virtuelle Maschine im VirtualBox-Manager sehen. Wird kein Konto angegeben, wird die virtuelle Maschine für alle vorhandenen Benutzer auf der Windows-Maschine mit VirtualBox registriert.
    - Benutzername: Geben Sie den Benutzernamen ein, für den die virtuelle Maschine registriert wird.
    - Kennwort: Geben Sie das Kennwort für dieses Konto ein.
12. Klicken Sie auf **Weiter**.
13. Wählen Sie auf der Seite **Volumes** die Volumes aus, die Sie exportieren möchten, z. B. C:\ und D:\, und klicken Sie dann auf **Weiter**.
14. Klicken Sie auf der Seite **Summary** (Zusammenfassung) auf **Finish** (Fertig stellen), um den Assistenten zu beenden und den Export zu starten.

    NOTE: Sie können Status und Fortschritt des Exports über das Anzeigen der Seiten **Virtual Standby** oder **Ereignisse** anzeigen.

Einrichten eines fortlaufenden Exports zu VirtualBox

Um auf einem Remote-Windows-Host in eine VirtualBox-VM zu exportieren, sollte VirtualBox auf der Core-Maschine installiert sein. Diese Anforderung gilt nicht für VMs, die unter Linux gehostet werden.

Führen Sie die Schritte in diesem Verfahren aus, um einen kontinuierlichen Export an eine virtuelle VirtualBox-Maschine (VM) mit Rapid Recovery durchzuführen.

1. Führen Sie in der Rapid Recovery Core Console eine der folgenden Maßnahmen aus:
   - Klicken Sie auf der Schaltflächenleiste in der Core Console auf das Drop-Down-Menü **Wiederherstellen** und dann auf **VM-Export**.
     1. Wählen Sie im Assistenten zum Exportieren von virtuellen Maschinen **Dauerhaft (virtueller Standby)**.
     2. Klicken Sie auf **Weiter.**
   - Klicken Sie in der Core Console in der Symbolleiste auf (Virtual Standby).
     - Klicken Sie auf der Registerkarte **Virtual Standby** auf **Hinzufügen**, um den Assistenten zum Exportieren von virtuellen Maschinen zu starten.
2. Wählen Sie auf der Seite **Maschinen** des Assistenten zum Exportieren von virtuellen Maschinen die geschützte Maschine, die Sie exportieren möchten.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Wiederherstellungspunkte** den Wiederherstellungspunkt aus, den Sie für den Export verwenden möchten.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Ziel** im Assistenten für den Export im Drop-Down-Menü **Auf eine virtuelle Maschine wiederherstellen** die Option **VirtualBox** aus.
7. Wählen Sie auf der Seite **Virtual Machine Options** (Optionen für virtuelle Maschine) die Option **Remote Linux Machine** (Remote-Linux-Maschine) aus.
8. Geben Sie die Informationen für die virtuelle Maschine ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 126. Einstellungen für Remote-Linux-Maschinen

Option	Description
VirtualBox-Hostname	Geben Sie eine IP-Adresse oder einen Hostnamen für den VirtualBox-Server ein. Dabei handelt es sich um die IP-Adresse oder den Hostnamen des Remote-VirtualBox-Servers.
Port	Geben Sie eine Portnummer für die Maschine ein. Diese Nummer gibt den Port an, über den der Core mit der Maschine kommuniziert.
Name der virtuellen Maschine	Geben Sie den Namen für die zu erstellende virtuelle Maschine ein. **NOTE:** Standardmäßig wird der Name der Quellmaschine verwendet.
Zielpfad	Geben Sie Zielpfad für die Erstellung der virtuellen Maschine an. **NOTE:** Es wird empfohlen, einen Stammordner im Stammverzeichnis zu erstellen, sodass die virtuelle Maschine im Stammverzeichnis ausgeführt wird. Wenn Sie nicht das Stammverzeichnis verwenden, müssen Sie den Zielordner auf der Zielmaschine manuell erstellen, bevor Sie den Export einrichten. Darüber hinaus müssen Sie die virtuelle Maschine nach dem Export manuell laden.
Benutzername	Benutzername des Kontos auf der Zielmaschine, z. B. „root“.
Kennwort	Kennwort für das Benutzerkonto auf der Zielmaschine.

Option	Description
Speicher	Geben Sie den Arbeitsspeicher für die virtuelle Maschine an. Sie haben folgende Auswahlmöglichkeiten: • Gleiche RAM-Größe verwenden wie Quellmaschine • „Bestimmte RAM-Größe verwenden“ auswählen und Größe in MB eingeben Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.

9. Wählen Sie **Ersten einmaligen Export durchführen**, um den virtuellen Export sofort und nicht nach dem nächsten geplanten Snapshot durchzuführen.
10. Klicken Sie auf **Weiter**.
11. Wählen Sie auf der Seite **Volumes** die zu exportierenden Daten-Volumes aus, und klicken Sie dann auf **Weiter**.
12. Klicken Sie auf der Seite **Summary** (Zusammenfassung) auf **Finish** (Fertig stellen), um den Assistenten zu beenden und den Export zu starten.

NOTE: Sie können Status und Fortschritt des Exports über das Anzeigen der Seiten „Virtual Standby“ oder „Ereignisse“ anzeigen.

Exportieren von Daten in eine virtuelle Azure Maschine

In Rapid Recovery können Sie Daten nach Azure exportieren, indem Sie einen einmaligen Export durchführen oder einen kontinuierlichen Export (für Virtual Standby) einrichten. Ein einmaliger Export auf die Azure Plattform beinhaltet die Bereitstellung in einem Workflow. Bei Verwendung eines fortlaufenden Exports können Sie die exportierten Dateien auch später auf einer startfähigen VM bereitstellen.

Weitere Informationen zum Arbeiten mit Azure finden Sie unter .

Weitere Informationen über die Vorbedingungen für den virtuellen Export auf Azure finden Sie unter Vor dem virtuellen Export auf Azure.

Eine detaillierte Beschreibung der einzigartigen Aspekte des virtuellen Exports für Azure finden Sie unter Exportieren und Bereitstellen von VMs für Azure.

Weitere Informationen zu den Konfigurationen und der Preisstruktur von Azure finden Sie auf der Seite Preisstruktur für virtuelle Maschinen der Azure Website.

Links zu anderen hilfreichen Verweisen auf Microsoft Websites finden Sie unter .

Eine Beschreibung der Vorgehensweisen in Bezug auf den Export oder die Bereitstellung von VMs auf Azure finden Sie über folgenden verwandten Links.

Zugehörige Konzepte

See also: Exportieren von Daten in eine virtuelle VirtualBox-Maschine

Zugehörige Tasks

See also: Einrichten eines fortlaufenden Exports zu Azure
See also: Bereitstellen einer virtuellen Maschine in Azure
See also: Durchführen eines einmaligen Azure Exports

Arbeiten mit Microsoft Azure

Microsoft Azure ist eine Abonnement-basierte Cloud-Computing-Plattform. Die folgenden Informationen werden Rapid Recovery Kunden zur Verfügung gestellt, um die Verwendung von Azure mit unserem Produkt zu vereinfachen.

- Haftungsausschluss für Azure-Schnittstelle
- Erstellen eines Containers in einem Azure Speicherkonto
- Exportieren und Bereitstellen von VMs für Azure
- Microsoft Azure Dokumentation

Haftungsausschluss für Azure-Schnittstelle

Die Microsoft Azure Schnittstelle unterliegt Änderungen.

Die Informationen in diesem Dokument über die in Azure erforderlichen Schritte waren zum Zeitpunkt der Veröffentlichung aktuell. Diese Informationen werden als Service für unsere Kunden bereitgestellt, um sie bei der Erfüllung der Azure Voraussetzungen zu unterstützen.

Bei der Arbeit mit Azure ist jedoch zu beachten, dass sich bestimmte Schritte, URLs oder sogar die Azure-Schnittstelle jederzeit ändern können, was sich unserer Kontrolle entziehen.

Wenn Sie Schwierigkeiten beim Durchführen irgendwelcher Schritte in Bezug auf Ihr Azure Konto haben, wenden Sie sich bitte an einen Microsoft Azure Ansprechpartner.

Erstellen eines Containers in einem Azure Speicherkonto

- Sie müssen über Administratorrechte für ein Konto auf Azure verfügen.
- Sie müssen innerhalb Ihres Azure Kontos ein Speicherkonto definiert haben.

Wenn Sie einen virtuellen Export durchführen, werden die Informationen in einem Container innerhalb eines Azure Kontos gespeichert. Sie können den Container über Ihr Azure Konto definieren, bevor Sie einen virtuellen Export durchführen, wie unten beschrieben. Oder Sie können den Container im Rahmen des Exportvorgangs über die Seite **Ziel** des Assistenten definieren.

Führen Sie die hier beschriebenen Schritte aus, um einen Container in einem Azure Speicherkonto zu erstellen.

1. Öffnen Sie das Microsoft Azure Dashboard.
2. Klicken Sie im linken Navigationsbereich auf **Alle Ressourcen**.
3. Klicken Sie im Bereich **Alle Ressourcen** auf den Namen des Speicherkontos, in dem Sie Daten aus Ihren virtuellen Rapid Recovery-Exporten speichern möchten.
4. Klicken Sie im Bereich **Einstellungen** auf **Blobs**.
5. Klicken Sie am oberen Rand des Fensters **Blob-Service**, in der Kopfzeile, auf **+ Container**.
6. Geben Sie im Fenster **Neuer Container** im Feld **Name** den Namen für den neuen Container ein.

   NOTE: Geben Sie einen Namen zwischen 3 und 63 Zeichen unter Verwendung von Kleinbuchstaben, Zahlen und Bindestrichen ein.
7. Wählen Sie im Fenster **Neuer Container** den entsprechenden Containertyp aus dem Dropdown-Menü **Zugriffstyp**, wodurch festlegt wird, ob öffentlich auf den Container zugegriffen werden kann. Verwenden Sie folgende Angaben als Leitfaden.

Option	Description
Privat	Diese Option schränkt den Container auf den Kontobesitzer ein.
Blob	Diese Option ermöglicht den öffentlichen Lesezugriff für Binary Large Objects (Blobs).
Container	Diese Option ermöglicht den öffentlichen Lese- und Listenzugriff auf den gesamten Container.

Wählen Sie beispielsweise **Container** aus.

8. Klicken Sie auf **Erstellen**.

   Wenn Pop-up-Warnungen aktiv sind, sollten Sie eine Meldung sehen, dass der Container erfolgreich erstellt wurde.

   Die Seite **BlobService** wird aktualisiert und der neue Containername wird in der Liste angezeigt.

Microsoft Azure Dokumentation

Microsoft hat umfangreiche Dokumentationen zur Verwendung von Azure in seinem Dokumentationscenter bereitgestellt.

Für Informationen zur Erstellung eines Azure Kontos oder dem Hochfahren einer VM für die Verwendung mit einem Rapid Recovery oder AppAssure Core, Hinzufügen eines Speicherkontos und vieles mehr finden Sie in der Microsoft-Dokumentation unter https://azure.microsoft.com/en-us/documentation.

Zum Beispiel Informationen zur Bereitstellung oder Verwalten von Windows-VMs finden Sie unter https://azure.microsoft.com/en-us/documentation/services/virtual-machines/windows/.

Online-Videos über die Verwendung von Azure finden Sie unter http://azure.microsoft.com/en-us/get-started/.

NOTE: Die Azure Website verwendet Sprachen- und Ländercodes für ihre Webadressen, die Einfluss auf die Darstellung der Inhalte haben. Zum Beispiel: `https://azure.microsoft.com/[Ländercode]/[Zielseite]/`.

NOTE: Die URLs für Azure, die in diesem Dokument verwendet werden, umfassen die Ländervorwahl für Englisch in den USA. Für andere Sprachen können basierend auf den Einstellungen Ihres Computers und den Inhalten, die Microsoft bietet, URLs in Bezug auf diese Codes abweichen.

Relevante Microsoft-Links

Einige Artikel von den Microsoft Websites sind unten aufgelistet:

- Azure Anmeldeseite (US)
- Microsoft Azure Startseite
- Microsoft Dokumentationscenter
- Virtuelle Windows-Maschinen Dokumentation
- Videos: Informationen zum Einstieg in Azure
- Preisstruktur für Azure virtuelle Maschinen
- Azure Services nach Region
- Informationen über Azure-Speicherkonten
- Erstellen eines Speicherkontos auf Azure
- Anleitung zum Anschließen einer Festplatte an eine Windows VM im Azure Portal
- Verwenden des Import/-Export-Service von Microsoft Azure zur Datenübertragung auf Blob-Speicher
- Import/Export-Preisstruktur
- Speicher: Import/Export von Festplattenlaufwerken in Windows Azure (Blogbeitrag)

Vor dem virtuellen Export auf Azure

Mit Rapid Recovery können Sie einen virtuellen Export (einmalig oder Virtual Standby) zu Microsoft Azure durchführen.

Vor dem Ausführen eines virtuellen Exports von Maschinen, die in Rapid Recovery geschützt sind, müssen Sie zuerst Ihr Azure Cloud-Konto dem Core zuordnen, wie im Thema Hinzufügen eines Cloud-Kontos beschrieben.

Sie müssen über ein angemessenes Speicherkonto auf Azure verfügen. Weitere Informationen zum Erstellen eines Speicherkontos in Azure finden Sie in den Azure Support-Informationen, auf die im Thema verwiesen wird.

In Ihrem Speicherkonto können Sie dynamisch einen Container zum Speichern der Exporte erstellen oder einen vorhandenen Container verwenden. Weitere Informationen zum Erstellen eines Speichercontainers finden Sie unter Erstellen eines Containers in einem Azure Speicherkonto.

Im Gegensatz zu anderen Formen des virtuellen Exports mit Rapid Recovery umfasst der VM-Export für Azure zwei Prozesse, die im Thema Exportieren und Bereitstellen von VMs für Azure ausführlich beschrieben werden.

Exportieren und Bereitstellen von VMs für Azure

Im Gegensatz zum virtuellen Export für andere Plattformen umfasst der virtuelle Export für Azure zwei Prozesse: Exportieren und Bereitstellen.

Wir weisen Sie darauf hin, dass Microsoft Azure Kunden für ihre eigenen Gebühren verantwortlich sind. Einige Aspekte der Integration mit Azure sind an dieser Gebührenstruktur ausgerichtet. Microsoft erhebt beispielsweise Gebühren, wenn Sie eine VM auf Azure bereitstellen und wenn Daten von Azure an eine andere Quelle übertragen werden.

NOTE: Da Microsoft die Voraussetzungen, Anforderungen, Kosten usw. ändern kann, sollten Sie solche Informationen immer bei Azure überprüfen. Weitere Informationen finden Sie auf der Azure Website oder wenden Sie sich an einen Mitarbeiter von Azure.

Um unnötige Gebühren zu vermeiden, besteht der virtuelle Export auf Azure aus zwei separaten Prozessen.

Der Prozess des **Exportierens** extrahiert die erforderlichen Dateien von Rapid Recovery, validiert sie und lädt sie auf den angegebenen Container in Azure hoch. Diese Dateien beinhalten:

- Eine VHD-Datei (Virtual Hard Disk, virtuelle Festplatte) für jedes Volume im Wiederherstellungspunkt.
- Eine XML-Datei, die Metadaten-Informationen über jede einzelne Festplatte enthält (eine Liste der Dateien auf jeder Festplatte und ein Flag, das anzeigt, ob es sich bei einem Volume um ein Systemlaufwerk handelt).
- Eine VHD-Datei mit dem Sicherungs-Snapshot.

Abgesehen von den Kosten für den erforderlichen Speicherplatz, entstehen durch den Export allein keine Gebühren bei Azure.

Der **Bereitstellungs**prozess kombiniert diese Dateien zu einer startfähigen virtuellen Maschine. Bereitstellung verwendet direkt die REST-APIs der Azure Cloud. Die ursprünglichen Dateien, die während des Exportvorgangs auf Azure abgelegt wurden, sind in Azure schreibgeschützt. Sie verbrauchen zwar Speicherplatz, aber ansonsten fallen keine Gebühren in Azure an. Wenn Sie diese Dateien bereitstellen, wird ein Duplikat davon erstellt und in einem separaten Container gespeichert, den Sie definieren, und zu einer funktionierenden virtuellen Maschine kombiniert. Aus der Perspektive des Azure Kontos werden ihnen nach der Bereitstellung Gebühren für die VM auf seinen Servern angerechnet. Da die bereitgestellte VM eine Kopie der exportierten Dateien ist, verdoppelt der Bereitstellungsprozess auch die Menge an Speicherplatz, der in Azure für diesen virtuellen Export verwendet wird.

Für einen einmaligen virtuellen Export gibt es keinen Mechanismus, die Bereitstellung als separaten Prozess durchzuführen. Um für den Export nützlich zu sein, sollten Sie also nur dann eine Bereitstellung auf Azure durchführen, wenn Sie die virtuelle Maschine nach Bedarf erstellen. Einmalige Exporte zu Azure ziehen folglich sofortige Kosten für die bereitgestellte VM nach sich.

Beim Einrichten von Virtual Standby für eine geschützte Maschine auf Azure können Sie den Exportvorgang einfach definieren, um die Gebühren für die Verwendung von zusätzlichem Speicherplatz und der VM zu sparen. Das Ergebnis ist ein anfänglicher virtueller Export auf Azure, welcher ständig aktualisiert wird. Jedes Mal, wenn eine Snapshot im Core erfasst wird, werden die exportierten Dateien in Ihrem Azure Konto mit aktualisierten Informationen aktualisiert. Bevor der virtuelle Export als startfähige VM verwendet werden kann, müssen Sie diese bereitstellen, wodurch VM-Kosten auf Azure entstehen. Wenn Sie die exportierten Dateien für eine geschützte Maschine nicht in eine startfähige VM konvertieren müssen, fallen in Ihrem Azure Konto keine VM-Kosten an.

Informationen über das Durchführen eines einmaligen Exports zu Azure, einschließlich der Bereitstellung, finden Sie unter dem Thema Durchführen eines einmaligen Azure Exports.

Informationen zum Einrichten eines fortlaufenden Exports zu Azure, ausgenommen der Bereitstellung, finden Sie in dem Thema Einrichten eines fortlaufenden Exports zu Azure.

Weitere Informationen zum Bereitstellen der aktuellsten exportierten Dateien zum Erstellen einer startfähigen virtuellen Standby-VM in Azure finden Sie unter dem Thema Bereitstellen einer virtuellen Maschine in Azure.

Durchführen eines einmaligen Azure Exports

Bevor Sie einen einmaligen Azure Export durchführen können, benötigen Sie Folgendes:

- Sie müssen über eine geschützte Maschine mit mindestens einem Wiederherstellungspunkt in einem Rapid Recovery Core verfügen, den Sie nach Azure exportieren möchten.
- Remote Access muss auf der geschützten Maschine aktiviert sein, damit die bereitgestellte VM erfolgreich starten kann.
- Sie müssen über Administratorrechte für ein Konto auf Azure verfügen.
- Optional können Sie vor dem Exportieren einen entsprechenden Container innerhalb Ihres Azure Kontos erstellen, in dem die exportierten Daten gespeichert werden. Weitere Informationen dazu finden Sie unter Erstellen eines Containers in einem Azure Speicherkonto.

Wie im Thema Exportieren und Bereitstellen von VMs für Azure beschrieben umfasst der virtuelle Export zu Azure zwei Prozesse: Exportieren und Bereitstellen.

Der Prozess des **Exportierens** extrahiert die erforderlichen Dateien von Rapid Recovery, validiert sie und lädt sie auf den angegebenen Container in Azure hoch. Diese Dateien beinhalten:

- Eine VHD-Datei (Virtual Hard Disk, virtuelle Festplatte) für jedes Volume im Wiederherstellungspunkt
- Eine XML-Datei, die Metadaten-Informationen über jede einzelne Festplatte enthält (eine Liste der Dateien auf jeder Festplatte und ein Flag, das anzeigt, ob es sich bei einem Volume um ein Systemlaufwerk handelt)
- Eine VHD-Datei mit dem Sicherungs-Snapshot

Der **Bereitstellungs**prozess kombiniert diese Dateien zu einer startfähigen virtuellen Maschine. Bereitstellung nutzt die direkten Azure Cloud REST-APIs. Die ursprünglichen Dateien, die während des Exportvorgangs auf Azure abgelegt wurden, sind in Azure schreibgeschützt. Sie verbrauchen zwar Speicherplatz, aber ansonsten fallen keine zusätzlichen Gebühren in Azure an. Wenn Sie diese Dateien bereitstellen, wird ein Duplikat davon erstellt und in einem separaten Container gespeichert, den Sie definieren, und zu einer funktionierenden virtuellen Maschine kombiniert. Aus der Perspektive eines Azure Kontos werden ihnen nach der Bereitstellung Gebühren für die VM auf seinen Servern angerechnet. Der Bereitstellungsvorgang verdoppelt auch die Menge an Speicherplatz, der in Azure für diesen virtuellen Export verwendet wird.

Für einen einmaligen virtuellen Export gibt es keinen Mechanismus, die Bereitstellung als separaten Prozess durchzuführen; damit der Export also nützlich ist, sollten Sie die Bereitstellung durchführen, wenn Sie die virtuelle Maschine nach Bedarf erstellen

Beim Einrichten von Virtual Standby für eine geschützte Maschine auf Azure können Sie den Exportvorgang einfach durchführen und den Wiederherstellungspunkt ohne die Notwendigkeit der Bereitstellung automatisch fortlaufend aktualisieren, um die Gebühren für die Verwendung von zusätzlichem Speicherplatz und der VM zu sparen. Sie können dann in Azure nur dann bereitstellen, wenn Sie die VM verwenden müssen. Weitere Informationen zum Bereitstellen eines Virtual Standby in Azure auf einer funktionierenden VM finden Sie unter dem Thema „Bereitstellen von Virtual Standby-Daten auf einer VM auf Azure“.

Führen Sie die folgenden Schritte aus, um einen einmaligen Export zu Azure bei Bedarf durchzuführen, einschließlich der Bereitstellung auf einer VM.

1. Klicken Sie in der Rapid Recovery Core Console auf das Drop-Down-Menü **Wiederherstellen** und klicken Sie dann auf **VM-Export**.

   Der Assistent zum Exportieren von virtuellen Maschinen wird gestartet.
2. Klicken Sie im Assistenten auf der Seite **Exporttyp auswählen** auf **Einmaliger Export** und dann auf **Weiter**.

   Die Seite **Computer** des Assistenten wird angezeigt.
3. Wählen Sie auf der Seite **Computer** die geschützte Maschine aus, die Sie wiederherstellen möchten, und klicken Sie auf **Weiter**.
4. Führen Sie auf der Seite **Wiederherstellungspunkte** ggf. einen Bildlauf durch die Liste der Wiederherstellungspunkte durch und wählen Sie den Wiederherstellungspunkt aus, den Sie für den Export verwenden möchten Klicken Sie anschließend auf **Weiter**.
5. Wählen Sie auf der Seite **Ziel** im Dropdown-Menü Export auf eine virtuelle Maschine die Option **Azure**.
6. Geben Sie die Parameter für den Zugriff auf die virtuelle Maschine ein (siehe Beschreibung in der folgenden Tabelle), und klicken Sie auf **Weiter**.

Tabelle 127. Azure Anmeldeinformationen

Optionen	Description
Veröffentlichungseinstellungendatei	Bei der Veröffentlichungseinstellungendatei handelt es sich um ein auf Azure generiertes XML-Dokument, das die Verwaltungszertifikate für Azure Abonnementinformationen enthält.

Optionen	Description
	NOTE: Veröffentlichungseinstellungen müssen pro Azure Konto nur einmal über die Core-UI definiert werden. Danach werden sie im Cache gespeichert. Wenn Sie nach dieser Datei gefragt werden, melden Sie sich bei Ihrem Azure Konto an und laden Sie sie aus Ihrer VM unter https://manage.windowsazure.com/publishsettings/index?client=powershell herunter. Die Datei definiert die AzureServiceManagement-API und Informationen zu Ihrem Azure Abonnement, einschließlich sicherer Anmeldeinformationen. Diese Datei muss im Rapid Recovery Core definiert werden, bevor können Sie eine Verbindung mit Ihrem Konto herstellen und einen virtuellen Export durchführen können. Aus Sicherheitsgründen sollten Sie die Datei nach der Verwendung in diesem Verfahren an einem sicheren Ort speichern oder sie löschen.
Abonnement	Wenn Sie soeben eine Veröffentlichungseinstellungsdatei hinzugefügt haben, werden diese Informationen automatisch mit den Informationen der veröffentlichen Einstellungsdatei eingegeben. **NOTE:** Veröffentlichungseinstellungen müssen pro Azure Konto nur einmal über die Core-UI definiert werden. Danach werden sie im Cache gespeichert. Wenn Sie eine zuvor hinzugefügte Veröffentlichungseinstellungsdatei verwenden möchten, verwenden Sie die Dropdown-Liste, um eine Datei auszuwählen. Wenn Sie eine Veröffentlichungseinstellungsdatei hinzufügen möchten, verwenden Sie die Schaltfläche + zum Öffnen des Fensters **Zertifikat laden** und navigieren Sie zu der Datei. Wenn Sie nach dieser Datei gefragt werden, melden Sie sich bei Ihrem Azure Konto an und laden Sie sie aus Ihrer VM unter https://manage.windowsazure.com/publishsettings/index?client=powershell herunter. Aus Sicherheitsgründen sollten Sie die Datei nach der Verwendung in diesem Verfahren an einem sicheren Ort speichern oder sie löschen.
Konto	Automatisch von der Abonnementdatei eingegeben. Dies ist das Azure Cloud-Konto, das mit Ihrem Core verknüpft wurde. **NOTE:** Sie müssen zuerst das Azure Cloud-Konto mit Ihrem Core verknüpfen, wie unter Hinzufügen eines Cloud-Kontos beschrieben.
Containername	Wählen Sie aus dem Dropdown-Menü den Namen eines entsprechenden Containers, der mit ihrem Azure Cloud-Konto verknüpft wurde, wenn ein Container bereits vorhanden ist. Oder geben Sie einen Namen für einen neuen Container ein. **NOTE:** Geben Sie einen Namen zwischen 3 und 63 Zeichen unter Verwendung von Kleinbuchstaben, Zahlen und Bindestrichen ein.
Ordnername	Geben Sie einen Namen für den Ordner innerhalb des Containers zum Speicher der exportierten virtuellen Maschine ein. **NOTE:** Ein Azure Ordner darf keines der folgenden Zeichen enthalten: / \ : * ? " < > E

7. Geben Sie auf der Seite **Bereitstellen** ein Ziel für die bereitgestellte VM ein, wie in der folgenden Tabelle beschrieben, und klicken Sie dann auf **Weiter**.

Tabelle 128. Optionen für die Bereitstellung zu Azure

Option	Description
Cloud-Dienstname	Der Azure Cloud-Dienst ist ein Container für virtuelle Maschinen unter Verwendung des klassischen Management-Modells. Wenn Sie bereits über einen Cloud-Dienst verfügen, wählen den entsprechenden Cloud-Dienstnamen aus dem Dropdown-Menü **Cloud Dienstname** aus. Oder geben Sie im Feld **Cloud-Dienstname** einen eindeutigen, aussagekräftigen Namen für den Cloud-Dienst ein. **NOTE:** Bei Microsoft Azure Abonnements gelten Standard-Limits in Bezug auf die Anzahl der Cloud-Dienste (in der Regel 25). Stellen Sie sicher, dass Sie Ihre Abonnement-Limits nicht überschreiten.
Bereitstellungsname	Wenn Sie einen Cloud-Dienst mit bestehenden virtuellen Maschinen ausgewählt haben, wird dieses Feld automatisch ausgefüllt. Wenn Sie einen Cloud-Dienst ausgewählt haben, der keine virtuellen Maschinen einschließt, geben Sie einen Namen für diese neue Bereitstellung ein. **NOTE:** Geben Sie einen Namen zwischen 3 und 63 Zeichen unter Verwendung von Kleinbuchstaben, Zahlen und Bindestrichen ein.
Zielcontainer	Geben Sie einen Namen für den Container zum Aufbewahren Ihrer VM ein. **NOTE:** Geben Sie einen Namen zwischen 3 und 63 Zeichen unter Verwendung von Kleinbuchstaben, Zahlen und Bindestrichen ein.

8. Geben Sie auf der Seite **Optionen für virtuelle Maschine** die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 129. Optionen für virtuelle Maschine

Option	Description
Name der virtuellen Maschine	Geben Sie einen Namen für die virtuelle Maschine ein. **NOTE:** Geben Sie einen Namen zwischen 3 und 15 Zeichen unter Verwendung von Kleinbuchstaben, Zahlen und Bindestrichen ein.
Größe der virtuellen Maschine	Wählen Sie aus dem Dropdown-Menü eine entsprechende VM-Größe aus. **NOTE:** Weitere Informationen zu den Konfigurationen und der Preisstruktur von Azure finden Sie auf der Seite Preisstruktur für virtuelle Maschinen der Azure Website. Links zu anderen hilfreichen Verweisen auf Microsoft Websites finden Sie unter .
Endpunkt (Remote Access-Einstellungen)	Im Folgenden sind VM-Optionen für Remote Access-Einstellungen aufgeführt.
Name	Wählen Sie **RemoteDesktop** oder **SSH**.
Protokoll	Wählen Sie **TCP** oder **UDP**
Anschlüsse	Öffentliche und private Ports verwenden standardmäßig 3389. Ändern Sie diesen Wert, falls nötig.

Option	Description
Serverports für Übertragungsdaten	Öffentliche und private Ports verwenden standardmäßig 8009. Ändern Sie diesen Wert, falls nötig.
Agent-Ports	Öffentliche und private Ports verwenden standardmäßig 8006. Ändern Sie diesen Wert, falls nötig.

9. Klicken Sie auf **Weiter**.
10. Wählen Sie auf der Seite **Volumens** die Volumes aus, die Sie exportieren möchten, und klicken Sie dann auf **Fertig stellen,** um den Assistenten zu schließen und die Bereitstellung zu starten.

> **NOTE:** Sie können Status und Fortschritt des Exports über die Anzeige der Exportwarteschlange auf der Seite **Virtual Standby** oder **Ereignisse** verfolgen.

Einrichten eines fortlaufenden Exports zu Azure

Bevor Sie einen fortlaufenden virtuellen Export zu Azure durchführen können, benötigen Sie Folgendes:

- Sie müssen über eine geschützte Maschine mit mindestens einem Wiederherstellungspunkt in einem Rapid Recovery Core verfügen, den Sie zu Azure exportieren möchten.
- Remote Access muss auf der geschützten Maschine aktiviert sein, damit die bereitgestellte VM erfolgreich starten kann.
- Sie müssen über Administratorrechte für ein Konto auf Azure verfügen.
- Um Ihr Azure Konto Ihrem Core zuzuordnen, müssen Sie zuerst eine Einstellungsdatei für Veröffentlichungen innerhalb von Azure herunterzuladen. Weitere Informationen hierzu finden Sie unter Abrufen der Veröffentlichungseinstellungendatei für Ihr Azure Konto.
- Optional können Sie vor dem Exportieren einen entsprechenden Container innerhalb Ihres Azure Kontos erstellen, in dem die exportierten Daten gespeichert werden. Denken Sie daran, dass die Speicheranforderungen wachsen, je mehr Daten Ihre geschützte Maschine schützt. In Ihrem Azure Konto muss der angegebene Container mit einem Speicherort verknüpft werden, der ausreichend Platz für die virtuelle Maschine bietet. Weitere Informationen dazu finden Sie unter Erstellen eines Containers in einem Azure Speicherkonto.

Führen Sie die Schritte in diesem Verfahren aus, um einen fortlaufenden virtuellen Export der ausgewählten Maschine in einen bestimmten Container in einem Azure Cloud-Konto über Rapid Recovery durchzuführen.

> **NOTE:** Dieser Vorgang schließt nicht das Bereitstellen der exportierten Dateien zum Erstellen einer startfähigen VM ein. Die Schritte zum Bereitstellen sind unter Bereitstellen einer virtuellen Maschine in Azure beschrieben.

1. Führen Sie in der Rapid Recovery Core Console eine der folgenden Maßnahmen aus:
   - Klicken Sie in der Core Console auf das Dropdown-Menü **Wiederherstellen** und dann auf **VM-Export**.
     1. Wählen Sie im Assistenten zum Exportieren von virtuellen Maschinen **Dauerhaft (virtueller Standby)**.

2. Klicken Sie auf **Weiter.**

- Klicken Sie in der Core Console in der Symbolleiste auf (Virtual Standby).
  - Klicken Sie auf der Registerkarte **Virtual Stanfdby** auf + **Hinzufügen**, um den Assistenten zum Exportieren von virtuellen Maschinen zu starten.

2. Wählen Sie auf der Seite **Maschinen** des Assistenten zum Exportieren von virtuellen Maschinen die geschützte Maschine, die Sie exportieren möchten.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Wiederherstellungspunkte** den Wiederherstellungspunkt aus, den Sie für den Export verwenden möchten.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Ziel** im Dropdown-Menü Export auf eine virtuelle Maschine die Option **Azure**. .
7. Geben Sie die Parameter für den Zugriff auf die virtuelle Maschine ein (siehe Beschreibung in der folgenden Tabelle), und klicken Sie auf **Weiter**.

Tabelle 130. Azure Anmeldeinformationen

Optionen	Description
Veröffentlichungseinstellungen	Diese Option wird nur angezeigt, wenn Sie Ihr Azure Abonnement noch nicht mit Ihrem Core verknüpft haben. Wenn Sie diese Option auswählen, laden Sie die Datei wie im Thema Abrufen der Veröffentlichungseinstellungendatei für Ihr Azure Konto beschrieben hoch und verknüpfen dann Ihr Abonnement mit dem Core. Diese Verknüpfung muss abgeschlossen sein, bevor Sie eine Verbindung zu Ihrem Azure Konto innerhalb des Core herstellen und einen virtuellen Export durchführen können. **NOTE:** Veröffentlichungseinstellungen müssen pro Azure Konto nur einmal über die Core-UI definiert werden. Danach werden sie im Cache gespeichert. Aus Sicherheitsgründen sollten Sie die Datei nach der Verwendung in diesem Verfahren an einem sicheren Ort speichern oder sie löschen.
Abonnement	Wenn Sie soeben eine Veröffentlichungseinstellungsdatei hinzugefügt haben, werden diese Informationen automatisch mit den Informationen der veröffentlichen Einstellungsdatei eingegeben. **NOTE:** Veröffentlichungseinstellungen müssen pro Azure Konto nur einmal über die Core-UI definiert werden. Danach werden sie im Cache gespeichert. Wenn Sie eine zuvor hinzugefügte Veröffentlichungseinstellungsdatei verwenden möchten, verwenden Sie die Dropdown-Liste, um eine Datei auszuwählen. Wenn Sie eine Veröffentlichungseinstellungsdatei hinzufügen möchten, verwenden Sie die Schaltfläche + zum Öffnen des Fensters **Zertifikat laden** und navigieren Sie zu der Datei.
Konto	Automatisch von der Abonnementdatei eingegeben. Dies ist das Azure Cloud-Konto, das mit Ihrem Core verknüpft wurde. **NOTE:** Sie müssen zuerst das Azure Cloud-Konto mit Ihrem Core verknüpfen, wie beschrieben unter Hinzufügen eines Cloud-Kontos
Containername	Wählen Sie aus dem Dropdown-Menü den Namen eines entsprechenden Containers, der mit ihrem Azure Cloud-Konto verknüpft wurde, wenn ein Container bereits vorhanden ist. Oder geben Sie einen Namen für einen neuen Container ein. **NOTE:** Geben Sie einen Namen zwischen 3 und 63 Zeichen unter Verwendung von Kleinbuchstaben, Zahlen und Bindestrichen ein.

Optionen	Description
Ordnername	Geben Sie einen Namen für den Ordner innerhalb des Containers zum Speicher der exportierten virtuellen Maschine ein. **NOTE:** Ein Azure Ordner darf keines der folgenden Zeichen enthalten: / \ : * ? " < > E
Ersten einmaligen Export durchführen	Beim Definieren von Virtual Standby: Wählen Sie diese Option, um den Exportjob sofort in die Warteschlange zu stellen. Deaktivieren Sie diese Option, wenn Sie möchten, dass der Core bis zum nächsten erzwungenen oder geplanten Sicherungs-Snapshot wartet.

8. Klicken Sie auf **Weiter**.
9. Wählen Sie auf der Seite **Volumes** die Volumes aus, die Sie exportieren möchten, und klicken Sie dann auf **Weiter**.
10. Klicken Sie auf der Seite **Zusammenfassung** auf **Fertigstellen**, um den Assistenten zu schließen und den Export zu starten.

NOTE: Sie können Status und Fortschritt des Exports über das Anzeigen der Seiten „Virtual Standby“ oder „Ereignisse“ anzeigen.

Der Virtual Standby-Parameter, den Sie in diesem Verfahren definieren, bewirkt den Export der Dateien, die zum Erstellen einer VM in Ihrem Azure Konto erforderlich sind. Nach jedem Snapshot (erzwungen oder geplant) werden diese Dateien in Azure mit allen neuen Sicherungsinformationen aktualisiert. Bevor Sie diese Dateien als eine virtuelle Maschine (VM) starten können, müssen Sie die VM auf Azure bereitstellen. Die Schritte zum Bereitstellen sind unter Bereitstellen einer virtuellen Maschine in Azure beschrieben.

Bereitstellen einer virtuellen Maschine in Azure

Bevor Sie eine VM in Azure bereitstellen können, müssen Sie über eine geschützte Maschine auf einem Rapid Recovery Core mit mindestens einem Wiederherstellungspunkt verfügen, und Sie müssen fortlaufenden Export (Virtual Standby) in der Core Console einrichten. Weitere Informationen zum Einrichten eines fortlaufenden Exports finden Sie unter Einrichten eines fortlaufenden Exports zu Azure. Dieser Prozess setzt ebenfalls voraus, dass Sie über ein Azure Konto mit ausreichend Speicherplatz verfügen, das mit dem Core verknüpft ist.

Wenn Sie Virtual Standby für eine geschützte Maschine auf Azure einrichten, werden nach jedem Sicherungs-Snapshot die letzten Sicherungsinformationen fortlaufend vom Core zu Ihrem Azure Konto exportiert. Durch diesen Prozess wird der vorherige Satz von Exportdateien mit aktualisierten Sicherungsinformationen überschrieben. Bevor Sie die virtuellen Exportdatei als eine virtuelle Maschine (VM) starten können (wenn beispielsweise Ihre ursprüngliche geschützte Maschine ausgefallen ist), müssen Sie diese zuerst in der Core Console bereitstellen. Dieser Prozess erzeugt eine startfähige VM in einem neuen Container.

Führen Sie die hier beschriebenen Schritte aus, um Ihre letzten Exportdateien für Virtual Standby in einer bootfähigen VM in Azure bereitzustellen.

1. Klicken Sie in der Rapid Recovery Core Console in der Symbolleiste auf (Virtual Standby).
2. Identifizieren Sie im Fensterbereich **Virtual Standby** die Maschine in Ihrem Rapid Recovery Core, die für fortlaufenden Export zu Azure eingerichtet ist.
3. Klicken Sie auf der Zeile für die Virtual Standby-Maschine, die Sie bereitstellen möchten, auf (Weitere Optionen) und wählen Sie **Virtuelle Maschine bereitstellen**.

Der Assistent **Deploy to Azure** wird angezeigt.

4. Wählen Sie auf der Seite **Ziel** im Drop-Down-Menü **Cloud-Dienstname** den entsprechenden Cloud-Dienstnamen aus den in Ihrem Azure Konto verfügbaren Optionen.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite „Wiederherstellungspunkte“ den Wiederherstellungspunkt aus, den Sie für den Export verwenden möchten.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Ziel** des Exportassistenten im Dropdown-Menü Export auf eine virtuelle Maschine**ESX(i)** aus.
9. Geben Sie die Parameter für den Zugriff auf die virtuelle Maschine ein (siehe Beschreibung in der folgenden Tabelle), und klicken Sie auf **Weiter**.

Tabelle 131. Parameter für virtuelle Maschine

Optionen	Description
Cloud-Dienstname	Wenn Sie bereits über einen Cloud-Dienst verfügen, wählen den entsprechenden Cloud-Dienstnamen aus dem Dropdown-Menü **Cloud Dienstname** aus. Oder geben Sie im Feld **Cloud-Dienstname** einen eindeutigen, aussagekräftigen Namen für den Cloud-Dienst ein. Der Cloud-Dienstname wird mit Ihrer Ressourcengruppe in Ihrem Azure Konto verknüpft. Wenn Sie über Administratorrechte in Azure verfügen, lesen Sie in der Azure Dokumentation nach, wie Sie das entsprechende Konto erstellen. Wenn Sie kein entsprechendes Cloud-Dienstkonto finden, fordern Sie Unterstützung von Ihrem Azure Administrator an. **NOTE:** Bei Microsoft Azure Abonnements gelten Standard-Limits in Bezug auf die Anzahl der Cloud-Dienste (in der Regel 25). Stellen Sie sicher, dass Sie Ihre Abonnement-Limits nicht überschreiten.
Bereitstellungsname	Wenn Sie einen Cloud-Dienst mit bestehenden virtuellen Maschinen ausgewählt haben, wird dieses Feld automatisch ausgefüllt. Wenn Sie einen Cloud-Dienst ausgewählt haben, der keine virtuellen Maschinen einschließt, geben Sie einen Namen für diese neue Bereitstellung ein. **NOTE:** Geben Sie einen Namen zwischen 3 und 63 Zeichen unter Verwendung von Kleinbuchstaben, Zahlen und Bindestrichen ein.
Zielcontainer	Geben Sie einen Namen für den Container zum Aufbewahren Ihrer VM ein. **NOTE:** Geben Sie einen Namen zwischen 3 und 63 Zeichen unter Verwendung von Kleinbuchstaben, Zahlen und Bindestrichen ein.

10. Geben Sie auf der Seite „Optionen für virtuelle Maschine“ die in der folgenden Tabelle beschriebenen Informationen ein und klicken Sie dann auf **Weiter**.

Tabelle 132. Optionen für virtuelle Maschine

Option	Description
Name der virtuellen Maschine	Geben Sie einen Namen für die virtuelle Maschine ein. **NOTE:** Geben Sie einen Namen zwischen 3 und 15 Zeichen unter Verwendung von Kleinbuchstaben, Zahlen und Bindestrichen ein.
Größe der virtuellen Maschine	Wählen Sie aus dem Dropdown-Menü eine entsprechende VM-Größe aus.

Option	Description
	NOTE: Weitere Informationen zu den Konfigurationen und der Preisstruktur von Azure finden Sie auf der Seite Preisstruktur für virtuelle Maschinen der Azure Website. Links zu anderen hilfreichen Verweisen auf Microsoft Websites finden Sie unter .
Endpunkt (Remote Access-Einstellungen)	
Name	Wählen Sie **RemoteDesktop** oder **SSH**.
Protokoll	Wählen Sie **TCP** oder **UDP**
Anschlüsse	Öffentliche und private Ports verwenden standardmäßig 3389. Ändern Sie diesen Wert, falls nötig.
Serverports für Übertragungsdaten	Öffentliche und private Ports verwenden standardmäßig 8009. Ändern Sie diesen Wert, falls nötig.
Agent-Ports	Öffentliche und private Ports verwenden standardmäßig 8006. Ändern Sie diesen Wert, falls nötig.

11. Wählen Sie auf der Seite **Datenträger** die Volumes aus, die Sie exportieren möchten, und klicken Sie dann auf **Fertig stellen,** um den Assistenten zu schließen und die Bereitstellung zu starten.

NOTE: Sie können den Fortschritt der Bereitstellung durch Anzeigen der Aufgaben auf der Seite **Ereignisse** überwachen.

Sobald die Bereitstellung abgeschlossen ist, können Sie in Ihrem Azure Konto die neue VM in der Azure Ansicht **Maschinen anzeigen (Klassisch)** anzeigen. Sobald die VM verfügbar ist, zahlen Sie auch Gebühren. Um fortlaufende Gebühren zu vermeiden, löschen Sie die bereitgestellte VM, wenn sie nicht mehr benötigt wird. Durch Wiederholung dieses Vorgangs können Sie jederzeit eine VM aus dem neuesten Satz von virtuellen Exportdateien bereitstellen.

Verwalten von Exporten

Wenn für Ihren Core fortlaufender Export eingerichtet ist, werden die Konfigurationsparameter für jeden virtuellen Export als eine Zeile auf der Seite **Virtual Standby** angezeigt. Von hier aus können Sie den Status von fortlaufenden Exporten anzeigen, die Sie derzeit eingerichtet haben, und Ihre virtuellen Standby-Maschinen verwalten. Sie können von Ihrer Core Console aus einen Virtual Standby hinzufügen, einen Export erzwingen, Virtual Standby vorübergehend deaktivieren oder wieder aktivieren oder die Anforderungen für den kontinuierlichen Export entfernen.

Wenn ein einmaliger Export stattfindet, wird der Job in der Export-Warteschlange auf der Seite **Virtual Standby** gelistet. Während dieser Zeit können Sie den einmaligen Exportvorgang vorübergehend deaktivieren, wieder aktivieren oder abbrechen.

NOTE: Rapid Recovery unterstützt Hyper-V-Export auf Windows 8, Windows 8.1, Windows 10, Windows Server 2012, Windows Server 2012 R2 und Windows Server 2016.

Virtueller Export auf eine virtuelle Standby-VM findet nicht statt, wenn die VM eingeschaltet ist.

Führen Sie die folgenden Schritte aus, um virtuelle Exporte zu verwalten.

1. Klicken Sie in der Core Console in der Symbolleiste auf (Virtual Standby).

Die Seite **Virtual Standby** wird angezeigt. Hier können Sie beiden Tabellen mit gespeicherten Exporteinstellungen anzeigen. Sie enthalten Informationen, die in der folgenden Tabelle beschrieben sind.

Tabelle 133. Informationen zu Virtual Standby

Spalte	Description
Element auswählen	Für jede Zeile in der Zusammenfassungstabelle können Sie das Kontrollkästchen zum Ausführen von Aktionen aus der Liste der Menüoptionen vor der Tabelle auswählen.
Statusanzeige	Farbige Kreise in der Status-Spalte zeigen den Status von Virtual Standby. Wenn Sie den Cursor über den farbigen Kreis bewegen, wird die Statusbedingung angezeigt. • **Grün**. Virtual Standby wurde erfolgreich konfiguriert, ist aktiv und wurde nicht vorübergehend deaktiviert. Der nächste Export wird sofort nach Abschluss des nächsten Snapshot durchgeführt. • **Gelb**. Virtual Standby hält an, aber die Parameter sind immer noch definiert und im Core gespeichert. Nach einer neuen Übertragung wird der Exportjob allerdings nicht automatisch gestartet, sodass keine neuen Exporte für die betreffende geschützte Maschine durchgeführt werden, bis sich der Status ändert.
Maschinenname	Der Name der Quellmaschine.
Exporttyp	Klicken Sie auf das , um den Exporttyp anzuzeigen. Dies zeigt den Typ der Plattform für virtuelle Maschinen für den Export, wie z. B. ESXi, VMware Workstation, Hyper-V, VirtualBox oder Azure.
Letzter Export	Klicken Sie auf das , um den Exporttyp anzuzeigen. Zeigt das Datum und die Uhrzeit des letzten Exportvorgangs. Wenn soeben ein Export hinzugefügt, aber nicht abgeschlossen wurde, wird eine Meldung mit dem Hinweis angezeigt, dass der Export noch nicht durchgeführt wurde. Wenn ein Export fehlgeschlagen ist oder abgebrochen wurde, wird ebenfalls eine entsprechende Meldung angezeigt.
Ziel	Die virtuelle Maschine und der Pfad, in den die Daten exportiert werden.
Einstellungen	Im Drop-Down-Menü (Weitere Optionen) können Sie folgende Aktionen durchführen: • **Bearbeiten**. Hiermit können Sie die Virtual Standby-Einstellungen bearbeiten. • **Erzwingen**. Erzwingt einen virtuellen Export. • **Vorübergehend deaktivieren**. Export wird vorübergehend deaktiviert. Nur verfügbar, wenn Status „Aktiv“ ist. • **Wieder aktivieren**. Export wird wieder aktiviert. Nur verfügbar, wenn Status vorübergehend deaktiviert wurde. • **Entfernen**. Entfernt die Anforderung für kontinuierlichen Export. Entfernt nicht die zuletzt aktualisierte VM. • **Virtuelle Maschine bereitstellen**. Nur für fortlaufenden Export zu Azure: dadurch werden die exportierten Dateien in Ihrem Azure Konto in eine startfähige VM konvertiert.

Tabelle 134. Informationen der Exportwarteschlange

Spalte	Description
Element auswählen	Für jede Zeile in der Zusammenfassungstabelle können Sie das Kontrollkästchen zum Ausführen von Aktionen aus der Liste der Menüoptionen vor der Tabelle auswählen. Mögliche Optionen sind: • **Abbrechen**. Bricht den aktuellen einmaligen virtuellen Export ab. • **Einstellungen**. Dient zum Aktualisieren der Einstellung für die maximale Anzahl gleichzeitiger Exporte.
Statusanzeige	Zeigt den Status des aktuellen Exports als Prozentsatz an. Wenn keine einmaligen Exporte in der Warteschlange stehen, besitzt diese Spalte keinen Wert.
Maschinenname	Der Name der Quellmaschine.
Exporttyp	Klicken Sie auf das , um den Exporttyp anzuzeigen. Dies zeigt den Typ der Plattform für virtuelle Maschinen für den Export, wie z. B. ESXi, VMware, Hyper-V, VirtualBox oder Azure.
Zeitplantyp	Klicken Sie auf das , um den Zeitplantyp anzuzeigen. Zeigt den Typ des Exports an („Einmalig“ oder „Kontinuierlich“).
Ziel	Die virtuelle Maschine und der Pfad, in den die Daten exportiert werden.

2. Wählen Sie einen Export aus, wenn Sie die gespeicherten Exporteinstellungen verwalten möchten, und klicken Sie dann auf eine der folgenden Optionen:
   - **Bearbeiten**. Öffnet den **Assistent zum Exportieren von virtuellen Maschinen** auf der Seite **VM-Optionen**. Hier können Sieden Speicherort des exportierten VM ändern, die Version des VM-Typs oder RAM oder Prozessoren für den Export angeben. Um sofort den VM-Export zu starten, wählen Sie **Anfänglichen einmaligen Export durchführen**.
   - **Erzwingen**. Erzwingt einen neuen Export. Diese Option kann hilfreich sein, wenn Virtual Standby vorübergehend deaktiviert und wieder aktiviert wurde, da der Exportjob erst nach einer neuen Übertragung wieder gestartet wird. Sie können dann einen Export erzwingen, wenn Sie nicht auf die neue Übertragung warten möchten.
   - **Vorübergehend deaktivieren**. Deaktiviert vorübergehend einen aktiven Export.
   - **Wieder aktivieren**. Aktiviert die Anforderung zum Fortsetzen des Exports zum nächsten geplanten oder erzwungen Snapshot wieder.
3. Um einen Export aus dem System zu entfernen, wählen Sie den Export aus und klicken dann auf **Entfernen**.

   Die Export-Konfiguration ist dauerhaft aus dem System entfernt. Das Entfernen der Konfiguration des virtuellen Standby entfernt keine virtuelle Maschine, die als Folge der Konfiguration exportiert wurde.
4. Um eine VM auf Azure bereitzustellen, wählen Sie **Virtuelle Maschinen bereitstellen** und geben die vollständige Einzelheiten im Assistenten „Deploy to Azure“ an.

Daten aus dem letzten virtuellen Export, die in Ihrem Konto Azure gespeichert wurden, werden innerhalb des zugeordneten Azure Kontos als startfähige VM bereitgestellt.

5. Gehen Sie folgendermaßen vor, um die Anzahl der Exportvorgänge zu verwalten, die gleichzeitig durchgeführt werden können:
   - Klicken Sie unter „Warteschlange exportieren“ auf **Einstellungen**.
   - Geben Sie im Dialogfeld **Maximale Anzahl gleichzeitiger Exporte** die Anzahl von Exporten ein, die gleichzeitig ausgeführt werden sollen. Die Standardnummer ist 5.
   - Klicken Sie auf **Speichern**.
6. Um einen einmaligen oder fortlaufender Export, der derzeit in der Warteschlange aufgeführt ist, abzubrechen, wählen Sie den Export und klicken dann auf **Abbrechen**.
7. Um einen neuen Virtual Standby-Export hinzuzufügen, können Sie auf **Hinzufügen** klicken, um den Exportassistenten zu starten. Das Abschließen der resultierenden Assistenten resultiert in einem fortlaufenden Export für die ausgewählte geschützte Maschine. Weitere Informationen zum Einrichten von Virtual Standby für eine bestimmte virtuelle Maschine finden Sie in den folgenden Abschnitten:
   - Einrichten eines fortlaufenden Exports zu ESXi
   - Einrichten eines fortlaufenden Exports zu VMware Workstation
   - Einrichten eines fortlaufenden Exports zu Hyper-V
   - Einrichten eines fortlaufenden Exports zu VirtualBox
   - Einrichten eines fortlaufenden Exports zu Azure

Wiederherstellen von Daten

In diesem Kapitel wird beschrieben, wie gesicherte Daten wiederhergestellt werden.

Informationen zur Wiederherstellung von Daten mit Rapid Recovery

Der Rapid Recovery Kern kann Daten sofort wiederherstellen oder ausgehend von den Wiederherstellungspunkten Computer als physische oder virtuelle Computer wiederherstellen. Die Wiederherstellungspunkte enthalten Snapshots der Agenten-Volumes, die auf Blockebene erfasst werden. Diese Snapshots sind anwendungskonsistent, d. h. dass alle offenen Transaktionen und laufenden Transaktionsprotokolle abgeschlossen und die Cache-Speicher auf der Festplatte abgelegt werden, bevor der Snapshot erstellt wird. Bei Verwendung anwendungskonsistenter Snapshots zusammen mit Verified Recovery kann der Core verschiedenartige Wiederherstellungen durchführen, z. B.:

- Wiederherstellung von Dateien und Ordnern
- Wiederherstellung von Daten-Volumes mithilfe von Live Recovery
- Wiederherstellung von Daten-Volumes für Microsoft Exchange Server und Microsoft SQL Server mithilfe von Live Recovery
- Bare Metal Restore mithilfe von Universal Recovery
- BMR-Wiederherstellung (Bare Metal Restore) auf anderer Hardware mithilfe von Universal Recovery
- Einmaliger On-Demand- und kontinuierlicher Export in virtuelle Maschinen

NOTE: Wenn Sie Daten wiederherstellen oder einen virtuellen Export durchführen, muss der verwendete Wiederherstellungspunkt Teil einer kompletten Wiederherstellungspunkt-Kette sein. Weitere Informationen über Wiederherstellungspunkt-Ketten finden Sie unter Wiederherstellungspunkt-Ketten und -Waisen.

Grundlegendes zu Live Recovery

Live Recovery ist eine Funktion der Wiederherstellung von Daten in Rapid Recovery Core. Wenn es in Ihrer geschützten Maschine zu Daten-Ausfall eines nicht System bedingten Windows Volume kommt, können Sie Daten von einem Wiederherstellungspunkt auf dem Rapid Recovery Core wiederherstellen. Die Auswahl von Live Recovery im Wiederherstellungsassistenten ermöglicht es Benutzern, mit einer gegen Null gehenden Ausfallzeit sofort mit Geschäftsvorgängen fortzufahren. Mit Live Recovery während der Wiederherstellung haben Sie sofort Zugriff auf Daten, selbst dann, wenn Rapid Recovery weiterhin das Wiederherstellen von Daten im Hintergrund fortsetzt. Diese Funktion ermöglicht eine gegen Null gehende Wiederherstellungszeit, selbst wenn der Wiederherstellungsvorgang Terabyte Daten umfasst.

Rapid Recovery Core verwendet eindeutige blockbasierte Sicherungs- und Wiederherstellungs-Technologie mit vollen Zugang auf die Zielserver während des Wiederherstellungsvorgangs. Angeforderte Blöcke werden für nahtlose Wiederherstellung On-Demand wiederhergestellt.

Live Recovery gilt für physische und virtuelle Maschinen, die durch Rapid Recovery Core geschützt sind, und zwar mit folgenden Ausnahmen:

- Live Recovery ist in nicht System bedingten Windows Volumes zugänglich. Das Laufwerk C:\ und die System reservierte Partition können nicht mithilfe von Live Recovery wiederhergestellt werden.
- Live Recovery ist zugänglich für Windows-basierte Volumes mithilfe des Rapid Recovery Agent. Agentenlose Volumes oder Linux-Volumes nutzen Live Recovery nicht.

Mit Live Recovery können Sie sofort physische oder virtuelle Server direkt aus der Sicherungsdatei wiederherstellen. Wenn ein nicht-System bedingtes Volume wiederhergestellt wird, präsentiert Rapid Recovery die Volume-Metadaten sofort dem Betriebssystem, wodurch diese Daten On-Demand erhältlich sind. Wenn zum Beispiel das Datenbank-Volume von Microsoft Exchange beschädigt ist, kann Live Recovery Volume, Datenbank und Exchange-Dienste innerhalb von Minuten wiederherstellen.

Diese Funktion bietet die schnellste Methode zum Wiederherstellen von großen Datenmengen bei minimaler Ausfallzeit. Benutzer können sofort mit Geschäftsprozessen fortfahren.

Sobald Live Recovery beginnt, stehen das wiederhergestellte Volume und dessen Inhalt sofort zur Verfügung. Rapid Recovery Core stellt weiterhin Daten im Hintergrund wieder her, obwohl das Volume, dessen Daten, Anwendungen und Dienste bereits wieder in einer Produktionsumgebung sind. Wenn bestimmte Daten angefordert werden, priorisiert der Hintergrundprozess die Wiederherstellung dieser Daten sofort. Diese leistungsstarke Funktionalität ermöglicht, dass auch die strengsten Vereinbarungen zum Servicelevel erfüllt werden.

Sobald Sie Live Recovery starten, werden Metadaten (Verzeichnisstruktur, Sicherheitsbeschreibungen, NTFS-Dateiattribute, freie Speicherplatzzuweisung usw.) des Zielvolumes rasch auf der geschützten Maschine wiederhergestellt. Im Anschluss daran werden das Volume und dessen Inhalt für das System verfügbar. Der Rapid Recovery Agent beginnt mit der Wiederherstellung von Datenblöcken aus dem Rapid Recovery Core-Server und schreibt die Blöcke auf das Ziel-Volume.

Anforderungen nach Daten, die noch nicht wiederhergestellt wurden, werden sofort beantwortet. Dabei erkennt das anfordernde Programm oder System nicht, dass die Blöcke gerade wiederhergestellt wurden.

Wiederherstellen von Daten aus Wiederherstellungspunkten

Rapid Recovery schützt Ihre Daten auf Windows- und Linux-Maschinen. Sicherungen von geschützten Maschinen werden im Repository von Rapid Recovery Core als Wiederherstellungspunkte gespeichert. Von diesen Wiederherstellungspunkten können Sie Ihre Daten mit einer von drei Methoden wiederherstellen.

- Aus Rapid Recovery Core Console können Sie ganze Volumes aus einem Wiederherstellungspunkt eines systemfremden Volumes wiederherstellen, wobei die Volumes auf der Zielmaschine ersetzt werden. Weitere Informationen hierzu finden Sie unter Informationen über das Wiederherstellen von Volumes aus Wiederherstellungspunkten.
- Sie können auch gesamte Volumes auf Linux-Maschinen von Wiederherstellungspunkten über die Befehlszeile des Linux-Agent wiederherstellen. Weitere Informationen zur Verwendung des Dienstprogramms „local_mount“ über die Befehlszeile finden Sie unter Wiederherstellen von Volumes einer Linux-Maschine über die Befehlszeile.

Sie können ein Volume, das das Betriebssystem enthält, nicht direkt aus einem Wiederherstellungspunkt wiederherstellen, da die Maschine, auf der die Wiederherstellung erfolgt, bei der Wiederherstellung das Betriebssystem und die Treiber benötigt. Wenn Sie ein System-Volume (z. B. das Laufwerk C: der geschützten Maschine) aus einem Wiederherstellungspunkt wiederherstellen möchten, müssen Sie eine BMR-Wiederherstellung (Bare Metal Restore) durchführen. Dies beinhaltet das Erstellen eines startbaren Images von dem Wiederherstellungspunkt, einschließlich Betriebssystem und Konfigurationsdateien sowie Daten. Starten Sie dann den Zielcomputer aus diesem startbaren Image, um die Wiederherstellung abzuschließen. Das Startimage hängt vom Betriebssystem der Maschine ab, die wiederhergestellt werden soll (Windows oder Linux).

Informationen zum Wiederherstellen eines Wiederherstellungspunkts für ein System-Volume auf einem Windows-Computer finden Sie unter Durchführen einer BMR-Wiederherstellung für Windows-Computer. Informationen zum Wiederherstellen eines Wiederherstellungspunkts für ein System-Volume auf einem Linux-Computer finden Sie unter Durchführen einer BMR-Wiederherstellung für Windows-Computer.

Wenn Sie ein Software-RAID auf einem Linux-Rechner haben, der durch Rapid Recovery Agent Version 6.2 geschützt ist, können Sie das Software-RAID aus einem Wiederherstellungspunkt wiederherstellen.

NOTE: Da diese Funktion in Version 6.2 eingeführt wurde, ist sie nicht kompatibel mit Snapshots, die auf früheren Versionen von Agent erstellt wurden. Wenn Sie Rapid Recovery Agent auf Version 6.2 oder höher aktualisieren und dann Snapshots in Rapid Recovery Coreerstellen, können Sie das Software-RAID aus den neuen Snapshots wiederherstellen.

Anstatt ganze Volumes wiederherzustellen, können Sie einen Wiederherstellungspunkt für eine Windows-Maschine bereitstellen sowie einzelne Ordner und Dateien durchsuchen, um nur bestimmte Dateien wiederherzustellen. Weitere Informationen hierzu finden Sie unter Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer. Informationen zum Beibehalten der ursprünglichen Dateiberechtigungen beim Wiederherstellen einzelner Dateien (z. B. beim Wiederherstellen eines Benutzerordners auf einem Dateiserver) finden Sie unter Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer und Beibehalten der Berechtigungen.

In diesem Abschnitt wird die Wiederherstellung von Daten auf physischen Maschinen behandelt. Weitere Information zum Exportieren geschützter Daten aus einem Wiederherstellungspunkt auf einen virtuellen Computer finden Sie unter VM-Export.

NOTE: Bei der Wiederherstellung von Daten auf Windows-Maschinen müssen Sie darauf achten, dass die Deduplizierung auch im Core-Server aktiviert ist, wenn für das wiederhergestellte Volume die Windows-Datendeduplizierung aktiviert ist. Rapid Recovery unterstützt Windows 8, Windows 8.1, Windows 10, Windows Server 2012, Windows Server 2012 R2 und Windows Server 2016 für normale Übertragungen (Basisimage und inkrementell) sowie für Datenwiederherstellung, BMR-Wiederherstellung und virtuelle Exporte. Weitere Informationen zu den Arten von Volumes, die für Sicherung und Wiederherstellung unterstützt werden, und solchen, die nicht unterstützt werden, finden Sie unter dem Thema „Einschränkungen der Unterstützung von dynamischen Volumes und Basisvolumes“ im *Rapid Recovery Systemanforderungen-Handbuch*.

Über die Dateisuch- und Wiederherstellungsfunktion

Über die Dateisuch- und Wiederherstellungsfunktion von Rapid Recovery können Sie eine oder mehrere Dateien in den Wiederherstellungspunkten der geschützten Maschine finden. Sie können dann ein oder mehrere der Ergebnisse auf einer lokalen Festplatte wiederherstellen.

Richtlinien für Suchvorgänge

Auf der Seite **Dateisuche** der Core Console können Sie nach einer Datei aus einem Satz von Wiederherstellungspunkten auf der ausgewählten Maschine suchen. Die Suchkriterien sind in zwei Gruppen unterteilt: Grundlegend und Erweitert.

Die grundlegende Gruppe umfasst die folgenden Parameter:

- Die geschützte Maschine mit Wiederherstellungspunkten, nach denen Sie suchen möchten.
- Ein Zeitraum, der die Suche auf die Wiederherstellungspunkte beschränkt, die zwischen der Start- und Endzeit erstellt wurden.
- Der Name oder die Maske der Datei, die Sie finden wollen. Sie können mit dem Platzhalter „?“ ein einzelnes Zeichen und mit dem Sternchen „*“ null oder mehrere Zeichen ersetzen; spezifischere Dateinamen erzeugen jedoch spezifischere Ergebnisse.
- Eine Liste der Pfade zu den Verzeichnissen, in denen gesucht werden soll.

NOTE: Alle grundlegenden Kriterien sind erforderlich. Wenn kein Verzeichnis angegeben ist, durchsucht Rapid Recovery alle Volumes der angegebenen geschützten Maschine.

Die Schaltfläche **Weitere Optionen** öffnet die erweiterte Gruppe. Diese umfasst die folgenden Parameter:

- Die Option für die rekursive Suche in Unterverzeichnissen des Speicherorts oder nur im angegebenen Speicherort.
- Die Möglichkeit zum Durchführen eines Algorithmus, der die Geschwindigkeit der Suchvorgänge auf NTFS-Volumes erhöht.
- Die Fähigkeit, die Anzahl der Suchergebnisse auf einen übersichtlicheren Wert zu begrenzen.

NOTE: Spezifische Suchkriterien produzieren schnellere und präzisere Suchergebnisse. Der Einschluss von Unterverzeichnissen (z. B. `C:\work\documents\accounting` anstelle von `C:`) reduziert die zum Durchführen des Suchvorgangs benötigte Zeit. Gleiches wird durch restriktivere Dateimasken erzielt (z. B. `invoice*.pdf` anstelle von `in*.*`).

Da die Funktion die Wiederherstellungspunkte und Speicherorte weiterhin durchsucht, selbst nachdem die angeforderte Datei gefunden wurde, können Sie eine Suche vor deren Abschluss anhalten oder beenden. Sie können mehrere Suchvorgänge gleichzeitig durchführen, Sie können sie jedoch nicht gleichzeitig beginnen. Beispiel: Um eine andere Datei zu finden, können Sie einen zweiten Suchvorgang starten, während die erste Suche noch nicht abgeschlossen ist. Sie können jedoch nur jeweils eine geschützte Maschine durchsuchen.

NOTE: Im vorherigen Beispiel wird durch Anhalten der ersten Suche mehr Arbeitsspeicher für den zweiten Suchvorgang verfügbar, wodurch der zweiten Suchvorgang schneller erfolgt. Das Ausführen mehrerer Suchvorgänge gleichzeitig ist speicherintensiv und erhöht die zum Abschließen eines Suchvorgangs erforderliche Zeit.

Jeder Suchvorgang erscheint als eine Registerkarte auf der Seite. Wenn Sie fertig sind, können Sie die Registerkarten einzeln oder alle gleichzeitig schließen.

Richtlinien zur Wiederherstellung

Nachdem Sie die Datei gefunden haben, können Sie sie direkt aus der Seite **Dateisuche** wiederherstellen.

Die Dateisuch- und Wiederherstellungsfunktion beschränkt die Wiederherstellungsmöglichkeiten auf Speicherorte auf dem Core. Sie können eine Datei nicht auf einer geschützten Maschine wiederherstellen.

Zugehörige Tasks

See also: Suchen und Wiederherstellen einer Datei

Suchen und Wiederherstellen einer Datei

Wenn Sie eine Datei anstelle eines Volumes wiederherstellen möchten, können Sie Rapid Recovery verwenden, um diese Datei unter den Wiederherstellungspunkten für Ihre geschützte Maschine zu finden. Durch Suchkriterien, wie z. B. Datumsbereich und Verzeichnis, können Sie die Suche auf eine kleine Gruppe relevanter Wiederherstellungspunkte beschränken.

NOTE: Spezifische Suchkriterien produzieren schnellere und präzisere Suchergebnisse und belegen weniger Speicher. Der Einschluss von Unterverzeichnissen (z. B. `C:\work\documents\accounting` anstelle von `C:`) reduziert die zum Durchführen des Suchvorgangs benötigte Zeit. Gleiches wird durch restriktivere Dateimasken erzielt (z. B. `invoice*.pdf` anstelle von `in*.*`).

Nachdem Sie die Datei gefunden haben, können Sie sie direkt aus der Liste der Suchergebnisse wiederherstellen.

1. Klicken Sie in der Rapid Recovery Core Console Symbolleiste auf das Drop-Down-Menü **Mehr** und wählen Sie **Dateisuche** aus.

   Die Seite **Dateisuche** wird geöffnet.
2. Um auf der Seite **Dateisuche** nach einer Datei innerhalb der Wiederherstellungspunkte einer bestimmten geschützten Maschine zu suchen, tragen Sie die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 135. Datei-Suchkriterien

Suchkriterien zum Suchen nach einer Datei innerhalb der Wiederherstellungspunkte der geschützten Maschine.

Textfeld	Description
Maschine	Wählen Sie die geschützte Maschine, nach der Sie suchen wollen, aus der Dropdown-Liste aus. **NOTE:** Sie können die Wiederherstellungspunkte von nur einer geschützten Maschine auf einmal durchsuchen.
Datumsbereich der Wiederherstellungspunkte	Geben Sie das Datum und die Uhrzeit des ältesten und des neuesten Wiederherstellungspunkts an, nach dem Sie suchen möchten. Nur die Wiederherstellungspunkte, die innerhalb dieses Zeitraums erstellt wurden, werden durchsucht. **NOTE:** Der Standardzeitraum ist der vorhergehende Monat. Beispiel: Wenn Sie eine Suche nach dem Dienstag, 22. August 2017 um 14:04 Uhr durchführen, so erstreckt sich der standardmäßige Datumsbereich vom 22.07.2017 14:04 Uhr bis 22.08.2017 14:04 Uhr.
Dateiname (die Platzhalter „*“ und „?“ können verwendet werden)	Geben Sie den Namen der Datei oder eine Dateimaske für die Datei ein, die Sie suchen und wiederherstellen möchten. Platzhalter können als Ersatz für unbekannte Zeichen verwendet werden. **NOTE:** Sie können mit dem Platzhalter „?“ ein einzelnes Zeichen und mit dem Sternchen „*“ null oder mehrere Zeichen ersetzen.
Zu durchsuchende Ordnern	Listen Sie ein oder mehrere Verzeichnisse auf der geschützten Maschine auf, um die Suche auf diese Speicherorte zu beschränken. **NOTE:** Wenn kein Verzeichnis angegeben ist, durchsucht Rapid Recovery alle Volumes der angegebenen geschützten Maschine.

3. Wählen Sie wahlweise **Weitere Optionen** und geben Sie dann die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 136. Weitere Dateisuchoptionen

Weitere Suchkriterien zum Suchen nach einer Datei innerhalb der Wiederherstellungspunkte der geschützten Maschine.

Textfeld	Description
Unterverzeichnisse einbeziehen	Durchsucht alle Unterverzeichnisse der in Schritt 3 aufgeführten Verzeichnisse. Ist standardmäßig aktiviert.
Schnellen Suchalgorithmus für NTFS-Volumes verwenden	Durchsucht NTFS-Volumes, ohne sie bereitzustellen, indem die Datenstrukturen des Dateisystems analysiert werden. Dies ist schneller und verbraucht weniger Speicherplatz beim Suchen. Ist standardmäßig aktiviert. **NOTE:** Wenn während einer Suche eines NTFS-Volumes ein Problem auftritt, versuchen die Suche erneut ohne diese Option.
Suchergebnisse beschränken auf	Geben Sie die maximale Anzahl der Ergebnisse an, die in den Ergebnissen angezeigt werden sollen. Die Standardeinstellung ist 1000.

4. Klicken Sie auf **Suche starten.**

   Der Suchvorgang wird gestartet. Jeder Suchvorgang erscheint als eine Registerkarte unter **Suchergebnisse**. Sie können die Schaltflächen für jede Registerkarte verwenden, um eines Suche zu unterbrechen oder zu beenden. Sie können aber auch auf das **X** auf der Registerkarte klicken, um die Suche zu löschen. Mehrere Suchvorgänge können gleichzeitig ausgeführt werden.
5. Wählen Sie aus der Liste der Suchergebnisse die Datei aus, die Sie wiederherstellen möchten.
6. Klicken Sie auf **Wiederherstellen**.

   Das Dialogfeld **Dateien wiederherstellen** wird geöffnet.
7. Geben Sie unter **Speicherort für** einen Zielpfad für die wiederhergestellte Datei der Maschine ein, auf der der Core installiert ist und ausgeführt wird.
8. Klicken Sie auf **Wiederherstellen**.

   Die ausgewählte Datei wird im angegebenen Zielpfad mit dem ursprünglichen Verzeichnisbaum, in dem die Datei auf der geschützten Maschine vorlag, wiederhergestellt.

Zugehörige Konzepte

See also: Über die Dateisuch- und Wiederherstellungsfunktion

Informationen über das Wiederherstellen von Volumes aus Wiederherstellungspunkten

Sie können die Volumes einer geschützten Maschine aus den Wiederherstellungspunkten in Rapid Recovery Core mithilfe des Assistenten zum Wiederherstellen einer Maschine wiederherstellen.

NOTE: In früheren Releases wurde dieser Prozess als Rollback bezeichnet.

NOTE: Rapid Recovery unterstützt Schutz und Wiederherstellung von Maschinen mit EISA-Partitionen. Die Unterstützung wurde auch auf Maschinen mit Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2 und Windows Server 2016 erweitert, die Windows RE (Windows Recovery Environment) verwenden.

Sie können eine Wiederherstellung an jeder Stelle in der Rapid Recovery Core Console starten, indem Sie auf das **Wiederherstellen**-Symbol in der Rapid Recovery Schaltflächenleiste klicken. Wenn Sie so eine Wiederherstellung starten, müssen Sie die geschützte Maschine im Core angeben, die wiederhergestellt werden soll, und dann das Volume auswählen, das wiederhergestellt werden soll.

Oder Sie können zu Seite **Wiederherstellungspunkte** für einen bestimmten Computer gehen, auf das Drop-Down -Menü für einen bestimmten Wiederherstellungspunkt klicken und **Restore** (Wiederherstellen) wählen. Führen Sie die nachstehend beschriebenen Schritte ab Schritt 5 im Thema Wiederherstellen von Volumes aus einem Wiederherstellungspunkt durch, wenn Sie so eine Wiederherstellung starten.

Sie können die Wiederherstellung aus einem Wiederherstellungspunkt auf einem Linux-Rechner auch über die Befehlszeile durchführen. Weitere Informationen dazu finden Sie unter Wiederherstellen von Volumes einer Linux-Maschine über die Befehlszeile.

Wenn Sie ein System-Volume aus einem Wiederherstellungspunkt oder Daten mithilfe einer Start-CD aus einem Wiederherstellungspunkt wiederherstellen möchten, müssen Sie eine BMR-Wiederherstellung (Bare Metal Restore) durchführen. Weitere Informationen über die BMR-Wiederherstellung finden Sie unter Bare-Metal-Wiederherstellung für Windows-Computer. Informationen zu den jeweils erforderlichen Komponenten für Windows- oder Linux-Betriebssysteme finden Sie unter Voraussetzungen für eine Bare-Metal-Wiederherstellung für einen Windows-Computer bzw. Voraussetzungen für eine BMR-Wiederherstellung für Linux-Maschinen. Sie können in der Core Console auf die BMR-Funktionen zugreifen (siehe Beschreibung in der Anleitung für das jeweilige Betriebssystem). Sie können auch mit dem Assistenten zum Wiederherstellen von Maschinen eine BMR-Wiederherstellung durchführen. Die folgende Vorgehensweise führt Sie zum entsprechenden Punkt im Assistenten, ab dem Sie die in Durchführen einer Bare-Metal-Wiederherstellung von Daten unter Verwendung des Assistenten zum Wiederherstellen eines Computers beschriebenen Schritte durchführen können.

Wiederherstellen von Volumes aus einem Wiederherstellungspunkt

Um Volumes aus einem Wiederherstellungspunkt wiederherzustellen, muss die Maschine auf dem Core auf Volume-Ebene geschützt sein und der Core muss Wiederherstellungspunkte enthalten, aus denen Sie die Wiederherstellung durchführen können.

Gehen Sie folgendermaßen vor, um Volumes aus einem Wiederherstellungspunkt wiederherzustellen.

1. Um ein Volume einer geschützten Maschine wiederherzustellen, navigieren Sie zur Core Console und klicken Sie auf **Wiederherstellen** in der Rapid Recovery Schaltflächenleiste.

   Der Assistent zum Wiederherstellen einer Maschine wird angezeigt.

2. Wählen Sie auf der Seite **Geschützte Maschinen** die geschützte Maschine aus, für die Sie Daten wiederherstellen möchten, und klicken Sie dann auf **Weiter**.

   Die Seite **Wiederherstellungspunkte** wird angezeigt.

3. Wählen Sie in der Liste der Wiederherstellungspunkte den Snapshot aus, der auf die geschützte Maschine wiederhergestellt werden soll.

   - Über die Navigationsschaltflächen am Ende der Seite können Sie bei Bedarf weitere Wiederherstellungspunkte anzeigen.
   - Um die Anzahl der Wiederherstellungspunkte zu begrenzen, die auf der Seite **Wiederherstellungspunkte** des Assistenten angezeigt werden, können Sie nach Volumes (falls definiert) oder nach Erstellungsdatum des Wiederherstellungspunkts filtern.

4. Klicken Sie auf einen Wiederherstellungspunkt, um ihn auszuwählen, und klicken Sie dann auf **Weiter**.

Die Seite **Ziel** wird angezeigt.

5. Wählen Sie auf der Seite **Ziel** die Maschine aus, auf die die Daten wiederhergestellt werden sollen. Gehen Sie dazu folgendermaßen vor:

   - Wählen Sie **Wiederherstellung auf eine geschützte Maschine (nur Nicht-System-Volumes)** aus, wenn Sie Daten aus dem ausgewählten Wiederherstellungspunkt auf dieselbe Agentenmaschine wiederherstellen möchten und die Volumes, auf die die Daten wiederhergestellt werden sollen, keine System-Volumes sind. Vergewissern Sie sich, dass die Zielmaschine ausgewählt ist, und klicken Sie dann auf **Weiter**.

     Die Seite **Volume-Zuordnung** wird angezeigt. Fahren Sie mit Schritt 9 fort.

   - Wählen Sie **Wiederherstellung auf eine geschützte Maschine (nur Nicht-System-Volumes)** aus, wenn Sie Daten aus dem ausgewählten Wiederherstellungspunkt auf eine andere geschützte Maschine wiederherstellen möchten (um beispielsweise den Inhalt von Maschine2 durch den von Maschine1 zu ersetzen). Wählen Sie die Zielmaschine in der Liste aus, und klicken Sie dann auf **Weiter**.

     Die Seite **Volume-Zuordnung** wird angezeigt. Fahren Sie mit Schritt 9 fort.

   - Wenn Sie Daten aus dem ausgewählten Wiederherstellungspunkt auf derselben Maschine oder mit einer Start-CD auf einer anderen Maschine wiederherstellen möchten, müssen Sie eine BMR-Wiederherstellung (Bare Metal Restore) durchführen. Informationen zur BMR-Wiederherstellung finden Sie unter Bare-Metal-Wiederherstellung.

     NOTE: Um eine BMR-Wiederherstellung durchführen zu können, müssen abhängig vom Betriebssystem der Maschine, die wiederhergestellt werden soll, bestimmte Voraussetzungen erfüllt sein. Grundlegende Informationen zu diesen Voraussetzungen finden Sie unter Voraussetzungen für eine Bare-Metal-Wiederherstellung für einen Windows-Computer bzw. Voraussetzungen für eine BMR-Wiederherstellung für Linux-Maschinen.

     NOTE: Wählen Sie **Wiederherstellung auf einen beliebigen Zielcomputer mit einer Start-CD** aus, wenn die Volumes, die wiederhergestellt werden sollen, nicht das System-Volume umfassen. Bei Auswahl dieser Option werden Sie aufgefordert, eine Start-CD zu erstellen.

     - Klicken Sie auf **Weiter**, um fortzufahren und mit dem Assistenten zum Wiederherstellen einer Maschine eine Start-CD mit den Daten des ausgewählten Wiederherstellungspunkts zu erstellen, und gehen Sie zu Durchführen einer BMR-Wiederherstellung für Windows-Computer.
     - Wenn die Start-CD bereits erstellt und der Zielcomputer bereits mit der Start-CD gestartet wurde, gehen Sie zu Schritt 8 im Abschnitt Durchführen einer BMR-Wiederherstellung für Windows-Computer.

   - Wenn Sie ein System-Volume (z. B. das Laufwerk C: der Agent-Maschine namens Maschine1) aus einem Wiederherstellungspunkt wiederherstellen möchten, handelt es sich ebenfalls um eine BMR-Wiederherstellung (Bare Metal Restore). Wählen Sie **Wiederherstellung auf einer beliebigen Zielmaschine mit einer Start-CD** aus. Bei Auswahl dieser Option werden Sie aufgefordert, eine Start-CD zu erstellen.

     - Klicken Sie auf **Weiter**, um fortzufahren und mit dem Assistenten zum Wiederherstellen einer Maschine eine Start-CD mit den Daten des ausgewählten Wiederherstellungspunkts zu erstellen, und gehen Sie zu Durchführen einer BMR-Wiederherstellung für Windows-Computer.
     - Gehen Sie zu Schritt 6, wenn Sie die Start-CD bereits erstellt haben.

6. Starten Sie die Maschine, die Sie wiederherstellen möchten, mit der Start-CD. Weitere Informationen zur BMR-Wiederherstellung auf einem Windows-Computer finden Sie unter Laden der Start-CD und Starten der Zielmaschine. Weitere Informationen zur BMR-Wiederherstellung auf einem Linux-Computer finden Sie unter Laden der Live DVD und Starten der Zielmaschine.
7. Wählen Sie auf dem Core-Server auf der Seite **Ziel** des Assistenten zum Wiederherstellen einer Maschine **Ich habe bereits eine Start-CD für die Zielmaschine** aus und geben Sie die Informationen zu der

Maschine ein, zu der eine Verbindung hergestellt werden soll (siehe Beschreibung in der folgenden Tabelle).

Tabelle 137. Maschineninformationen

Textfeld	Description
IP-Adresse	Die IP-Adresse der Maschine, die wiederhergestellt werden soll. Diese Adresse ist mit der IP-Adresse identisch, die im URC angezeigt wird.
Authentifizierungsschlüssel	Das jeweilige Kennwort für die Verbindung zum ausgewählten Server. Dieses Kennwort ist mit dem Authentifizierungsschlüssel identisch, der im URC angezeigt wird.

8. Klicken Sie auf **Weiter**.

   Wenn die eingegebenen Verbindungsinformationen mit den URC-Informationen übereinstimmen und Core und Zielserver sich gegenseitig einwandfrei im Netzwerk identifizieren können, werden die Volumes des ausgewählten Wiederherstellungspunkts geladen. Die Seite **Datenträgerzuordnung** wird angezeigt.

   Fahren Sie mit Schritt 9 im Abschnitt Durchführen einer BMR-Wiederherstellung für Windows-Computer fort, um die BMR-Wiederherstellung mit dem Assistenten zum Wiederherstellen eines Computers durchzuführen.

   NOTE: Rapid Recovery unterstützt FAT32- und ReFS-Partitionen. Nur vollständige Wiederherstellung und BMR werden unterstützt, da bei ReFS eine Treiberbeschränkung besteht. Wiederherstellung wird im Benutzermodus, VM-Export usw. implementiert. Wenn ein Core mindestens ein Agent-Volume schützt, das das Dateisystem ReFS enthält, muss die Installation auf einer Maschine mit Windows 8.1, Windows 10 (nur Enterprise oder Pro), Windows Server 2012, Windows Server 2012 R2 oder Windows Server 2016 erfolgen, die ReFS nativ unterstützen. Andernfalls ist die Funktionalität begrenzt und Vorgänge, bei denen beispielsweise ein Volume-Image bereitgestellt werden muss, funktionieren nicht. Die Rapid Recovery Core Console enthält zutreffende Fehlermeldungen in diesen Vorfällen. Eine BMR-Wiederherstellung (Bare Metal Restore) der Festplattenkonfiguration für Speicherplätze wird in dieser Version ebenfalls nicht unterstützt. Ausführliche Informationen hierzu finden Sie unter *Rapid Recovery-Installations- und Aktualisierungshandbuch*.

9. Wählen Sie auf der Seite **Volume-Zuordnung** für jedes Volume im Wiederherstellungspunkt, das wiederhergestellt werden soll, das gewünschte Ziel-Volume aus. Wählen Sie in der Spalte „Ziel-Volumes“ **Nicht wiederherstellen** aus, wenn ein Volume nicht wiederhergestellt werden soll.
10. Wählen Sie **Erweiterte Optionen anzeigen** aus und führen Sie die folgenden Aktionen aus:
    - Wählen Sie **Live Recovery** aus, um eine Wiederherstellung auf Windows-Maschinen mit Live Recovery durchzuführen.

      Mit der Live Recovery-Technologie für eine sofortige Wiederherstellung in Rapid Recovery können Sie Daten aus gespeicherten Wiederherstellungspunkten von Windows-Maschinen (einschließlich Microsoft Windows-Speicherplätzen) auf physischen oder virtuellen Maschinen wiederherstellen. Live Recovery ist für Linux-Computer oder VMs, die agentenlosen Schutz verwenden, nicht verfügbar.
    - Wenn Sie erzwingen möchten, dass die Bereitstellung der ausgewählten Volumes zur Beginn des Wiederherstellungsvorgangs aufgehoben wird, wählen Sie **Erzwungene Aufhebung der Bereitstellung**.

      CAUTION: Wenn Sie die Bereitstellung vor der Wiederherstellung von Daten nicht aufheben, kann die Wiederherstellung mit der Fehlermeldung fehlschlagen, dass ein Volume verwendet wird.
11. Klicken Sie auf **Weiter.**
12. Auf der Seite **Bereitstellung von Datenbanken aufheben**, wenn die Volumes, die Sie wiederherstellen möchten, Oracle-, SQL-, oder Microsoft Exchange-Datenbanken enthalten, werden Sie aufgefordert, die Bereitstellung aufzuheben. Wählen Sie ggf. **Alle Datenbanken nach der Wiederherstellung des Wiederherstellungspunkts wieder bereitstellen** aus, wenn diese Datenbanken nach der Wiederherstellung automatisch wieder bereitgestellt werden sollen. Löschen Sie andernfalls diese Option.

NOTE: Der entsprechenden VSS Writer erfasst die Snapshots der Datenbank im Backupmodus. Wenn Sie nicht alle Datenbanken automatisch wieder bereitstellen möchten (die Standardoption), müssen Sie nach der Wiederherstellung die Datenbanken manuell starten.

13. Klicken Sie auf **Weiter.**

    Möglicherweise erscheint die Warnungsseite mit einer Aufforderung, alle Programme auf den Volumes, die Sie wiederherstellen möchten, zu schließen. Klicken Sie in diesem Fall erneut auf Weiter.

14. Auf der Seite **Zusammenfassung** wählen Sie die Option **WICHTIG! Ich habe zur Kenntnis genommen, dass dieser Vorgang die ausgewählten Volumes durch die Daten aus dem ausgewählten Wiederherstellungspunkt überschreibt**, um zu bestätigen, dass Sie sich der Konsequenzen einer Volume-Wiederherstellung bewusst sind.

    WARNING: Diese Option betont noch einmal die Konsequenzen, dass sämtliche Daten, die nach dem Datum und der Uhrzeit des ausgewählten Wiederherstellungspunkts auf dem ausgewählten Volume gespeichert wurden, bei der Wiederherstellung verloren gehen.

15. Klicken Sie auf **Fertig stellen**.

Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer

Sie können Windows Explorer zum Kopieren und Einfügen von Verzeichnissen und Dateien von einem bereitgestellten Wiederherstellungspunkt auf einer beliebigen Windows-Maschine verwenden. Dies kann nützlich sein, wenn Sie nur einen Teil eines Wiederherstellungspunkts für Ihre Benutzer verteilen möchten.

Wenn Sie Verzeichnisse und Dateien kopieren, werden die Zugriffsberechtigungen des Benutzers, der den Kopiervorgang durchführt, verwendet und auf die eingefügten Verzeichnisse und Dateien angewendet. Informationen zum Beibehalten der ursprünglichen Dateiberechtigungen beim Wiederherstellen von Verzeichnissen und Dateien für Benutzer (z. B. beim Wiederherstellen eines Benutzerordners auf einem Dateiserver) finden Sie unter Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer und Beibehalten der Berechtigungen.

1. Stellen Sie den Wiederherstellungspunkt mit den Daten bereit, die Sie wiederherstellen möchten. Entsprechende Details finden Sie unter Bereitstellen eines Wiederherstellungspunkts.
2. Navigieren Sie in Windows Explorer zu dem bereitgestellten Wiederherstellungspunkt und wählen Sie die Verzeichnisse und Dateien aus, die Sie wiederherstellen möchten. Klicken Sie mit der rechten Maustaste und wählen Sie **Kopieren**.
3. Navigieren Sie in Windows Explorer zu dem Speicherort, an dem Sie die Daten wiederherstellen möchten. Klicken Sie mit der rechten Maustaste und wählen Sie **Einfügen**.

Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer und Beibehalten der Berechtigungen

Sie können Windows Explorer zum Kopieren und Einfügen von Verzeichnissen und Dateien von einem bereitgestellten Wiederherstellungspunkt auf eine beliebige Windows-Maschine verwenden und gleichzeitig die Dateizugriffsberechtigungen bewahren.

Wenn Sie beispielsweise einen Ordner wiederherstellen müssen, auf den nur von bestimmten Benutzern auf einem Dateiserver zugegriffen wird, können Sie die Befehle zum Kopieren und Einfügen mit Berechtigungen verwenden, um sicherzustellen, dass die wiederhergestellten Dateien die Berechtigungen behalten, die

den Zugriff einschränken. Auf diese Weise können Sie verhindern, dass manuell Berechtigungen auf die wiederhergestellten Verzeichnisse und Dateien angewendet werden müssen.

Für einige Dateien gelten Dateizugriffsbeschränkungen, die Administratorrechte erfordern. Speziell für Windows Server 2012 und neuere Betriebssysteme muss der Benutzer, der die Wiederherstellung versucht, über die richtigen NTFS-Berechtigungen verfügen, damit das Wiederherstellen mit Berechtigungen erfolgreich ist. Um zum Beispiel vollständige NTFS-Berechtigungen von einem Bereitstellungspunkt zu kopieren, muss der Benutzer über Administratorrechte verfügen (mit vollen NTFS-Berechtigungen).

NOTE: Der Befehl „Einfügen mit Berechtigungen“ wird mit der Rapid Recovery Core- und Agent-Software installiert. Er ist nicht im Local Mount Utility verfügbar.

1. Stellen Sie den Wiederherstellungspunkt mit den Daten bereit, die Sie wiederherstellen möchten. Entsprechende Details finden Sie unter Bereitstellen eines Wiederherstellungspunkts.
2. Navigieren Sie in Windows Explorer zu dem bereitgestellten Wiederherstellungspunkt und wählen Sie die Verzeichnisse und Dateien aus, die Sie wiederherstellen möchten. Klicken Sie mit der rechten Maustaste und wählen Sie **Kopieren**.
3. Navigieren Sie in Windows Explorer zu dem Speicherort, an dem Sie die Daten wiederherstellen möchten. Klicken Sie mit der rechten Maustaste und wählen Sie **Mit Berechtigungen einfügen**.

   NOTE: Wenn in diesem Schritt der Befehl „Mit Berechtigungen einfügen“ auf dem Rechtsklick-Menü deaktiviert ist, hat Windows Explorer keine Kenntnis der Dateien, die Sie kopieren möchten. Wiederholen Sie Schritt 2, um den Befehl „Einfügen mit Berechtigungen“ im Kontextmenü zu aktivieren.

Wiederherstellen von Clustern und Cluster-Knoten

Bei einer Wiederherstellung werden die Volumes auf einer Maschine aus Wiederherstellungspunkten wiederhergestellt. Bei einem Server-Cluster wird die Wiederherstellung auf Knoten- oder Maschinenebene durchgeführt. Dieser Abschnitt enthält Richtlinien zum Durchführen einer Wiederherstellung für Cluster-Volumes.

Durchführen einer Wiederherstellung für CCR- und DAG-Cluster (Exchange)

Führen Sie die folgenden Schritte aus, um eine Wiederherstellung für CCR- und DAG-Cluster (Exchange) durchzuführen.

1. Schalten Sie alle Knoten bis auf einen aus.
2. Führen Sie eine Wiederherstellung mit dem Standardverfahren von Rapid Recovery für die Maschine durch (Informationen über das Wiederherstellen von Volumes aus Wiederherstellungspunkten und Wiederherstellen von Volumes einer Linux-Maschine über die Befehlszeile).
3. Stellen Sie nach der Wiederherstellung Sie alle Datenbanken für die Cluster-Volumes bereit.
4. Schalten Sie alle anderen Knoten ein.
5. Navigieren Sie zur Central Management Console und führen Sie für jede Datenbank den Vorgang „Datenbankkopie“ aktualisieren aus.

Durchführen einer Wiederherstellung für SCC-Cluster (Exchange, SQL)

Führen Sie die folgenden Schritte aus, um eine Wiederherstellung für CCR-Cluster (Exchange, SQL) durchzuführen.

1. Schalten Sie alle Knoten bis auf einen aus.
2. Führen Sie eine Wiederherstellung mit dem Standardverfahren von Rapid Recovery für die Maschine durch (Informationen über das Wiederherstellen von Volumes aus Wiederherstellungspunkten und Wiederherstellen von Volumes einer Linux-Maschine über die Befehlszeile).
3. Stellen Sie nach der Wiederherstellung Sie alle Datenbanken der Cluster-Volumes bereit.

4. Schalten Sie alle anderen Knoten einzeln nacheinander ein.

NOTE: Sie brauchen kein Rollback, um den Quorumdatenträger durchzuführen. Er kann automatisch oder mithilfe der Cluster-Dienstfunktionalität neu erstellt werden.

Wiederherstellen von einem angehängten Archiv

Es gibt zwei Möglichkeiten, Daten aus einem Archiv wiederherzustellen: Sie können ein Archiv als Quelle für eine Bare-Metal-Wiederherstellung (Bare Metal Restore, BMR) verwenden; oder Sie können ein Archiv anhängen, einen Wiederherstellungspunkt aus dem Archiv bereitstellen und anschließend die archivierten Daten wieder bereitstellen.

Wenn Sie ein Archiv anhängen, wird dieses unter „Angehängte Archive“ auf der Seite „Archive“ der Core Console angezeigt, und die Inhalte des Archivs werden aus dem linken Navigationsbereich zugänglich gemacht. Der Inhalt wird unter dem Namen des Archivs angezeigt. Maschinen, die archiviert wurden erscheinen als Nur-Wiederherstellungspunkte-Maschinen, sodass Sie auf die Wiederherstellungspunkte auf die gleiche Art und Weise zugreifen können, wie Sie es bei einer zurzeit geschützten Maschine tun würden: durch Bereitstellen eines Wiederherstellungspunktes, der das Element ausfindig macht, das Sie wiederherstellen möchten und das Element unter Verwendung von Windows Explorer zu Ihrem Ziel zu kopiert und einfügt.

Es gibt Vorteile, von einem angehängten Archiv wieder herzustellen, anstatt ein Archiv in ein Repository zu importieren.

- Wiederherstellen von einem angehängten Archiv spart Zeit, die Sie möglicherweise zum Importieren eines gesamten Archivs in ein Repository aufwenden.
- Auch wenn Sie ein Archiv importieren, werden die archivierten Wiederherstellungspunkte zum Repository hinzugefügt.

  Da diese archivierten Wiederherstellungspunkte wahrscheinlich die ältesten Positionen im Repository sind, werden sie evtl. entsprechend Ihrer Aufbewahrungsrichtlinie während der nächsten nächtlichen Aufgabe aufgerollt. (Obwohl diese Aktion sie nicht aus dem Archiv löschen; könnten Sie Sie sie am nächsten Tage erneut importieren.)
- Zuletzt erinnert sich der Core an die Anhang-Zuordnung zu den Archiven, auch nach dem Trennen eines Archivs, wodurch es einfacher und schneller ist, das Archiv später erneut anzuhängen.

  Sie können die Zuordnung durch Löschen des Anhangs entfernen.

Zum Wiederherstellen von Daten von einem angeschlossenen Archiv führen Sie die folgenden Schritte unter Verwendung der zugehörigen Verknüpfungen aus:

NOTE: Das Verfahren für die Wiederherstellung von einem angehängten Archiv setzt voraus, dass Sie bereits ein Archiv der aufgerollten Wiederherstellungspunkte haben.

1. Hängen Sie das Archiv an.
2. Stellen Sie den Wiederherstellungspunkt mit den Daten bereit, die wiederhergestellt werden sollen.
3. Stellen Sie Daten anhand einer der folgenden Methoden wieder her:
   - Wiederherstellen von Daten, wie z. B. Datei oder Ordner, aus dem Wiederherstellungspunkt.
   - Wiederherstellen des gesamten Wiederherstellungspunkts.
   - Exportieren des Wiederherstellungspunkts in eine virtuelle Maschine.

See also: Grundlegende Informationen zu Archiven
See also: Anfügen eines Archivs
See also: Importieren eines Archivs
See also: Bereitstellen eines Wiederherstellungspunkts
See also: Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer

See also: Wiederherstellen von Volumes aus einem Wiederherstellungspunkt
See also: Exportieren auf virtuelle Maschinen mit Rapid Recovery
See also: Eine BMR aus einem Archiv durchführen

E-Mail-Wiederherstellung in Rapid Recovery

Anhand der E-Mail-Wiederherstellungsfunktion inRapid Recovery können Sie eine Mailbox, einen Ordner oder ein Element, wie etwa eine Nachricht, einen Kalendertermin oder einen Kontakt, vom Datenspeicher einer geschützten Exchange Server-Maschine wiederherstellen. Sie können Ihre Auswahl auf einem Recovery Ordner, an der ursprünglichen Quelle oder in einer oder mehreren PST-Dateien wiederherstellen.

Der Zugriff auf die Seite „E-Mail wiederherstellen“ erfolgt über das Menü **Mehr** (...) Menü derRapid Recovery Core Console. Von dort aus können Sie die folgenden Aktionen durchführen:

- Eine Exchange-Datenbank öffnen
- Ein Element aus der offenen Datenbank wiederherstellen
- Die Datenbank schließen
- In der offenen Datenbank nach einem Element suchen

Weitere Informationen hierzu finden Sie unterÖffnen einer Exchange-Datenbank in Rapid Recovery und Wiederherstellen eines E-Mail-Elements in Rapid Recovery.

Voraussetzungen der E-Mail-Wiederherstellung

Bevor Sie E-Mail-Einstellungen zurücksetzen können, müssen Sie die folgenden Voraussetzungen erfüllen:

- Outlook 2007 oder höher ist auf der Core-Maschine installiert.
- Es ist mindestens ein Profil in Microsoft Outlook konfiguriert.
- Das Outlook-Profil verfügt über die Berechtigung „Vollständige Kontrolle“, einschließlich „Senden als“, und „Empfangen als“.Weitere Informationen hierzu finden Sie unter.
- Die Option „Outlook Cached Exchange Mode“ unter dem mit Rapid Recovery verknüpften Outlook-Profil ist deaktiviert.
- Die Core-Maschine befindet sich in der gleichen Domain wie die Exchange-Datenbank.
- Die erforderliche Exchange-Datenbank ist geöffnet und Sie befinden sich auf der Seite **E-Mail wiederherstellen** derRapid Recovery Core Console.Weitere Informationen hierzu finden Sie unterÖffnen einer Exchange-Datenbank in Rapid Recovery.

Ohne die richtigen Berechtigungen und eine Instanz von Outlook, die auf der Core-Maschine installiert ist, kann keine Wiederherstellung eines Exchange-Elements durchgeführt wird, selbst wenn der Exchange Server durch einen Rapid Recovery Core geschützt ist.

Öffnen einer Exchange-Datenbank in Rapid Recovery

Bevor Sie diese Aufgabe beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Outlook 2007 oder höher ist auf der Core-Maschine installiert.
- Die Core-Maschine befindet sich in der gleichen Domain wie die Exchange-Datenbank.
- Die entsprechenden Berechtigungen sind in Exchange eingestellt. Weitere Informationen hierzu finden Sie unter .

Rapid Recovery ermöglicht die Wiederherstellung von E-Mail-Elementen, ohne die Schnittstelle zu verlassen. Die E-Mail-Elemente liegen in der Exchange-Datenbank innerhalb des Wiederherstellungspunkts einer geschützten Exchange Server-Maschine vor, die Sie mit dem Assistent zum Öffnen von Exchange-Datenbanken öffnen können.

1. Aus Rapid Recovery Core Console klicken Sie auf das Menü „Mehr“ (**...**) und anschließend auf **Wiederherstellen**.
2. Klicken Sie auf der Seite **E-Mail wiederherstellen** zum Zugriff auf die Exchange-Datenbank, in der das E-Mail-Element gespeichert ist, auf **Datenbank öffnen**.

   Der Assistent zum Öffnen von Exchange-Datenbanken wird geöffnet.
3. Auf der Seite **Speicherort** des Assistenten können Sie eine Datenbank von einer geschützten Maschine oder von einem lokalen Pfad wie z. B. Ihrer aktuellen Maschine oder einer Dateifreigabe öffnen:
   - **Von geschützter Maschine öffnen**: Klicken Sie auf **Weiter** und fahren Sie dann mit dem nächsten Schritt in dieser Aufgabe fort.
   - **Von lokalem Pfad öffnen**: Geben Sie die folgenden Informationen für den Speicherort ein und klicken Sie dann auf **Fertig stellen**:
     - Datenbankdateipfad
     - Protokollpfad
     - Systempfad
4. Wählen Sie auf der Seite **Maschinen** die geschützte Maschine aus, auf der sich die Exchange-Datenbank befindet, und klicken Sie dann auf **Weiter**.
5. Auf der Seite **Wiederherstellungspunkte** wählen Sie den Wiederherstellungspunkt für den Zeitpunkt aus, zu dem Sie die Datenbank öffnen möchten, und klicken Sie dann auf **Weiter**.
6. Wählen Sie auf der Seite **Datenbanken** die Exchange-Datenbank aus, die Sie öffnen möchten, und klicken Sie dann auf **Weiter**.

   Rapid Recovery öffnet die ausgewählte Datenbank und zeigt diese auf der Seite **E-Mail wiederherstellen** an, wobei die Mailboxen und Ordner auf der linken Seite in einer erweiterbaren Navigationsstruktur angezeigt werden. Elemente in Ordnern werden auf der rechten Seite angezeigt.

   NOTE: Die Zeit, die Rapid Recovery zum Öffnen der Exchange-Datenbank benötigt, hängt von der Größe der Datenbank ab.

Informationen zum Wiederherstellen eines Elements aus der Datenbank finden Sie unter Wiederherstellen eines E-Mail-Elements in Rapid Recovery.

Wiederherstellen eines E-Mail-Elements in Rapid Recovery

Bevor Sie diese Aufgabe beginnen, stellen Sie sicher, dass Sie die Voraussetzungen zum Durchführen einer E-Mail-Wiederherstellung erfüllen.Weitere Informationen hierzu finden Sie unterVoraussetzungen der E-Mail-Wiederherstellung.

Anhand der E-Mail-Wiederherstellungsfunktion inRapid Recovery können Sie eine Mailbox, einen Ordner oder ein Element, wie etwa eine Nachricht, einen Kalendertermin oder einen Kontakt, vom Datenspeicher einer geschützten Exchange Server-Maschine wiederherstellen. Sie können Ihre Auswahl auf einem Recovery Ordner, an der ursprünglichen Quelle oder in einer oder mehreren PST-Dateien wiederherstellen. Zum Wiederherstellen eines E-Mail-Element aus der Rapid Recovery Core Console führen Sie die folgenden Schritte aus.

1. Wählen Sie das Element, das Sie wiederherstellen möchten, in der Open Exchange-Datenbank auf der Seite **E-Mail wiederherstellen** aus und klicken Sie dann auf der Aktionsleiste **E-Mail wiederherstellen** auf **Wiederherstellen**.

   Der **E-Mail-Wiederherstellungsassistent** wird geöffnet.
2. Führen Sie auf der Seite **Sitzung wiederherstellen** eine der folgenden Optionen aus und klicken Sie dann auf **Weiter**.
   - Wenn Sie E-Mail-Elemente zum ersten Mal wiederherstellen, geben Sie einen Anzeigenamen und Ihre Outlook-Anmeldeinformationen für die Wiederherstellungssitzung ein. Sie können dann diese Sitzung für eine zukünftige Wiederherstellung auswählen.
   - Wenn Sie zuvor erstellte Wiederherstellungssitzungen haben, wählen Sie eine der folgenden Optionen aus:
     - Wählen Sie **Vorhandene Wiederherstellungssitzung verwenden** aus, und wählen Sie dann eine Sitzung aus der Dropdown-Liste aus.
     - Wählen Sie **Neue Wiederherstellungssitzung erstellen** und geben Sie dann einen Anzeigenamen und Ihre Outlook-Anmeldeinformationen für die Wiederherstellungssitzung ein.
3. Auf der Seite **Ziel** wählen Sie den Zielort des wiederhergestellten Elements aus den folgenden Optionen und klicken Sie dann auf **Weiter**:

Tabelle 138. E-Mail-Wiederherstellungsziele

Option	Description
In den Wiederherstellungsordner wiederherstellen	Stellt die ausgewählten Elemente (einschließlich Ordnerhierarchie) in einen Wiederherstellungsordner in einem beliebigen Onlinepostfach wieder her. Fahren Sie mit Schritt 4 fort.
Am ursprünglichen Speicherort wiederherstellen	Leitet das ausgewählte Element (einschließlich Ordnerhierarchie) an das E-Mail-Postfach im Onlinedatenspeicher um, in dem sich das Element ursprünglich befunden hat. Fahren Sie mit Schritt 5 fort.
In die PST-Datei wiederherstellen	Speichert die ausgewählten Elemente (einschließlich der Ordnerhierarchie) durch Erstellen einer Personal Storage Table (PST)-Datei oder Schreiben in eine bestehende PST-Datei. Fahren Sie mit Schritt 6 fort.
In die PST-Datei(en) wiederherstellen	Speichert jedes Postfach als Personal Storage Table (PST)-Datei. Fahren Sie mit Schritt 6 fort.

Option	Description
(separate Datei für jedes Postfach)	

4. Falls Sie **In den Wiederherstellungsordner wiederherstellen** auf der **Konfigurationsseite** ausgewählt haben, wählen Sie ein **Profil** aus der Dropown-Liste und das Outlook-Adressbuch aus, und gehen Sie dann zu Schritt 7.

   Wählen Sie optional **Erweiterte Optionen anzeigen**, um die Wiederherstellung mit den folgenden Optionen weiter anzupassen:

Tabelle 139. Erweiterte E-Mail-Wiederherstellungsoptionen

Option	Description
Fehlerbehandlung	Bestimmt die Art und Weise, wie mit Fehlern, die während der Wiederherstellung auftreten, verfahren wird und wie diese verwaltet werden. Wählen Sie eine der folgenden Optionen aus: • **Protokollieren und fortfahren**. Sammelt Fehlermeldungen in einem Protokoll und fährt mit dem Wiederherstellungsvorgang fort. • **Benutzer benachrichtigen**. Hält die Wiederherstellung an und zeigt eine Meldung im Dialog „Aktive Aufgabe überwachen“ an, wenn ein Fehler auftritt, und gibt Ihnen die Möglichkeit, mit der Wiederherstellung fortzufahren oder diese abzubrechen. • **Wiederherstellung abbrechen**. Beendet den Wiederherstellungsvorgang, wenn ein Fehler auftritt.
Gelöschte Objekte wiederherstellen	Bei Exchange 2010-, 2013- und 2016-Datenbanken werden permanent gelöschte Elemente wiederhergestellt. Bei Exchange 2007-Datenbanken werden „Strikethrough“-Elemente aus dem aktuellen Ordner wiederhergestellt.
E-Mail-Regeln wiederherstellen	Stellt alle Regeln, die der Benutzer zum Zeitpunkt der Sicherung der Daten eingerichtet hatte, wieder her.

5. Wenn Sie **Am ursprünglichen Speicherort wiederherstellen** auf der Seite **Konfiguration** ausgewählt haben, wählen Sie das Ziel-Outlook-**Profil** sowie einen **Wiederherstellungstyp** aus den folgenden Optionen und gehen Sie dann zu Schritt 7:

   - **Nur Unterschiede wiederherstellen**. Ermittelt, ob das wiederhergestellte Element bereits im Zielordner vorhanden ist. Die Wiederherstellung wird nur dann durchgeführt, wenn kein Duplikat des Elements vorhanden ist. Auch als differentielles Wiederherstellen bezeichnet.
   - **Doppelte Einträge erstellen**. Stellt jedes ausgewählte Element wieder her, ohne vorhandene Elemente zu überschreiben, sodass Duplikate der zuvor vorhandenen Elemente entstehen.
   - **Überschreiben, wenn neuer**. Stellt nur neuere Elemente wieder her, die nicht im Onlinedatenspeicher vorhanden sind. Es werden auch Elemente wiederhergestellt, die im Onlinedatenspeicher vorhanden, aber älter sind als die Elemente in die Kopie der Exchange-Datenbank.

   Wählen Sie optional **Erweiterte Optionen anzeigen**, um die Wiederherstellung mit den folgenden Optionen weiter anzupassen:

Tabelle 140. Erweiterte E-Mail-Wiederherstellungsoptionen

Option	Description
Fehlerbehandlung	Bestimmt die Art und Weise, wie mit Fehlern, die während der Wiederherstellung auftreten, verfahren wird und wie diese verwaltet werden. Wählen Sie eine der folgenden Optionen aus: • **Protokollieren und fortfahren**. Sammelt Fehlermeldungen in einem Protokoll und fährt mit dem Wiederherstellungsvorgang fort. • **Benutzer benachrichtigen**. Hält die Wiederherstellung an und zeigt eine Meldung im Dialog „Aktive Aufgabe überwachen“ an, wenn ein Fehler auftritt, und gibt Ihnen die Möglichkeit, mit der Wiederherstellung fortzufahren oder diese abzubrechen. • **Wiederherstellung abbrechen**. Beendet den Wiederherstellungsvorgang, wenn ein Fehler auftritt.
Gelöschte Objekte wiederherstellen	Bei Exchange 2010-, 2013- und 2016-Datenbanken werden permanent gelöschte Elemente wiederhergestellt. Bei Exchange 2007-Datenbanken werden „Strikethrough“-Elemente aus dem aktuellen Ordner wiederhergestellt.
E-Mail-Regeln wiederherstellen	Stellt alle Regeln, die der Benutzer zum Zeitpunkt der Sicherung der Daten eingerichtet hatte, wieder her.
Benutzerberechtigungen wiederherstellen	Stellt die benutzerdefinierten Berechtigungen, die für einen öffentlichen Ordner eingerichtet sind, wieder her. **NOTE:** Diese Option ist nur verfügbar, wenn Sie einen öffentlichen Ordner an seinem ursprünglichen Speicherort wiederherstellen. Wenn Sie die Option zur Wiederherstellung der Berechtigungen nicht wählen, werden die Standard-Ordnerberechtigungen mit dem Inhalt wiederhergestellt.

6. Wenn Sie **In die PST-Datei wiederherstellen** oder **In die PST-Datei(en) wiederherstellen (separate Datei für jedes Postfach)** auf der Seite **Konfiguration** ausgewählt haben, führen Sie die folgenden Auswahlen aus und gehen Sie dann zu Schritt 7:
   a. **Profil**. Wählen Sie ein Outlook-Profil aus der Dropdown-Liste aus.
   b. **Primärer PST-Speicher**. Um den anfänglichen Zielordner für die PST-Datei zu suchen und auszuwählen, geben Sie den Pfad ein oder wählen Sie eine vorhandene Date aus.
   c. **PST-Überlaufspeicher (optional)**. Hat das primäre Ziel nicht genügend Speicherplatz für die PST-Datei, so wählen Sie für diese ein sekundäres Ziel.

   NOTE: Weisen Sie den Überlaufspeicherort nicht demselben Datenträger zu wie dem primären Speicherort.

   Wählen Sie optional **Erweiterte Optionen anzeigen**, um die Wiederherstellung mit den folgenden Optionen weiter anzupassen:

Tabelle 141. Erweiterte E-Mail-Wiederherstellungsoptionen

Option	Description
Fehlerbehandlung	Bestimmt die Art und Weise, wie mit Fehlern, die während der Wiederherstellung auftreten, verfahren wird und wie diese verwaltet werden. Wählen Sie eine der folgenden Optionen aus: • **Protokollieren und fortfahren**. Sammelt Fehlermeldungen in einem Protokoll und fährt mit dem Wiederherstellungsvorgang fort. • **Benutzer benachrichtigen**. Hält die Wiederherstellung an und zeigt eine Meldung im Dialog „Aktive Aufgabe überwachen“ an, wenn ein Fehler auftritt, und gibt Ihnen die Möglichkeit, mit der Wiederherstellung fortzufahren oder diese abzubrechen. • **Wiederherstellung abbrechen**. Beendet den Wiederherstellungsvorgang, wenn ein Fehler auftritt.
Gelöschte Objekte wiederherstellen	Bei Exchange 2010-, 2013- und 2016-Datenbanken werden permanent gelöschte Elemente wiederhergestellt. Bei Exchange 2007-Datenbanken werden „Strikethrough“-Elemente aus dem aktuellen Ordner wiederhergestellt.

7. Klicken Sie auf **Fertig stellen**.

   Die Elemente werden am ausgewählten Ziel wiederhergestellt. Sie können den Fortschritt des Jobs auf der Seite „Ereignisse“ überwachen.

Bare-Metal-Wiederherstellung

In diesem Kapitel wird beschrieben, wie eine BMR-Wiederherstellung (Bare Metal Restore) für einen geschützten Windows-Computer mit ähnlicher oder nicht ähnlicher Hardware durchgeführt wird.

Bare-Metal-Wiederherstellung für Windows-Computer

Wenn Server wie erwartet funktionieren, führen sie ihre Aufgaben gemäß ihrer Konfiguration aus. Nur bei Serverfehlern kommt es zu Änderungen. Wenn ein Server durch eine Notfallsituation oder durch eine Störung ausfällt, müssen unverzüglich entsprechende Maßnahme durchgeführt werden, um die volle Funktionsfähigkeit der Maschine wiederherzustellen.

Rapid Recovery bietet die Möglichkeit, eine BMR-Wiederherstellung (Bare Metal Restore) für Windows- oder Linux-Maschinen durchzuführen. Bei einer BMR-Wiederherstellung wird die vollständige Softwarekonfiguration eines bestimmten Systems wiederhergestellt. Der Begriff „Bare Metal“ soll verdeutlichen, dass bei der Wiederherstellung nicht nur die Daten des Servers wiederhergestellt werden, sondern auch Festplattenlaufwerke neu formatiert sowie Betriebssystem und alle Softwareanwendungen neu installiert werden. Um eine BMR-Wiederherstellung durchzuführen, geben Sie einen Wiederherstellungspunkt einer geschützten Maschine an und führen Sie ein Rollback (Durchführung einer Wiederherstellung) auf die angegebene physische oder virtuelle Maschine durch. Bei der Durchführung einer Wiederherstellung auf ein System-Volume handelt es sich um eine BMR-Wiederherstellung. Wenn bei der Durchführung einer Wiederherstellung eine Start-CD erforderlich ist, handelt es sich ebenfalls um eine BMR-Wiederherstellung. Zu anderen Situationen, in denen Sie u. U. eine BMR-Wiederherstellung durchführen möchten, zählen Hardware-Upgrades oder der Austausch eines Servers. In beiden Fällen wird eine Wiederherstellung aus einem Wiederherstellungspunkt auf die aktualisierte oder ersetzte Hardware durchgeführt.

Rapid Recovery unterstützt den Schutz und die Wiederherstellung der Betriebssysteme Windows 8, 8.1 und Windows Server 2012, 2012 R2, wenn diese von FAT32-EFI-Partitionen gestartet werden, sowie von ReFS-Volumes (Resilient File System).

NOTE: Eine BMR-Wiederherstellung (Bare Metal Restore) der Festplattenkonfiguration für Speicherplätze (eine Funktion von Windows 8.1) wird in diesem Release ebenfalls nicht unterstützt. Zurzeit werden lediglich vollständige Wiederherstellung und BMR-Wiederherstellung unterstützt, da es bei ReFS Treibereinschränkungen gibt, sodass Wiederherstellung, VM-Export usw. im Benutzermodus implementiert sind. Wenn ein Core mindestens ein Agent-Volume schützt, das das Dateisystem ReFS enthält, muss die Installation auf einer Maschine mit Windows 8, Windows 8.1, Windows Server 2012 oder Windows Server 2012 R2 erfolgen, da diese Betriebssysteme ReFS nativ unterstützen. Andernfalls ist die Funktionalität begrenzt und Vorgänge, bei denen beispielsweise ein Volume-Image bereitgestellt werden muss, funktionieren nicht. Die Rapid Recovery Core Console zeigt bei diesen Vorkommnissen entsprechende Fehlermeldungen an.

Nur unterstützte Linux-Betriebssysteme können geschützt und wiederhergestellt werden. Dazu gehören Ubuntu, Red Hat Enterprise Linux, CentOS und SUSE Linux Enterprise Server (SLES). Ausführliche Informationen hierzu finden Sie unter *Rapid Recovery-Installations- und Aktualisierungshandbuch*.

eine BMR-Wiederherstellung kann für physische oder virtuelle Maschinen durchgeführt werden. Ein weiterer Vorteil besteht darin, dass Sie mit Rapid Recovery eine BMR-Wiederherstellung unabhängig davon durchführen können, ob die Hardware vergleichbar oder unterschiedlich ist. Bei der Durchführung einer BMR-

Wiederherstellung in Rapid Recovery wird das Betriebssystem von einer bestimmten Plattform getrennt, sodass das System portabel wird.

Beispiele für eine BMR-Wiederherstellung für vergleichbare Hardware sind u. a. der Austausch der Festplatte eines vorhandenen Systems oder der Ersatz eines ausgefallenen Servers durch eine identische Maschine.

Beispiele für eine BMR-Wiederherstellung für andere Hardware sind u. a. die Wiederherstellung eines ausgefallenen Systems durch einen Server eines anderen Herstellers oder mit einer anderen Konfiguration. Dieser Vorgang umfasst das Erstellen eines Start-CD-Image, das Brennen des Image auf einen Datenträger, das Starten des Zielservers vom Start-Image, das Herstellen einer Verbindung zur Recovery Console-Instanz, das Zuordnen von Volumes, die Initiierung der Wiederherstellung und anschließend die Überwachung des Vorgangs. Nachdem die BMR-Wiederherstellung durchgeführt wurde, können Sie das Betriebssystem und die Softwareanwendungen auf den wiederhergestellten Server laden sowie die erforderlichen Einstellungen für die jeweilige Konfiguration vornehmen.

Die BMR-Wiederherstellung wird nicht nur in Notfallwiederherstellungsszenarien verwendet, sondern auch bei der Migration von Daten beim Upgrade oder Austausch von Servern.

Wiederherstellen virtueller Maschinen

Obwohl eine BMR-Wiederherstellung für virtuelle Maschinen (VMs) unterstützt wird, muss darauf hingewiesen werden, dass die Durchführung eines virtuellen Exports für eine VM einfacher ist als eine BMR-Wiederherstellung auf einer physischen Maschine. Weitere Informationen zum Durchführen eines VM-Exports für virtuelle Maschinen finden Sie unter Exportieren auf virtuelle Maschinen mit Rapid Recovery.

Informationen zum Durchführen einer BMR auf einer Windows-Maschine finden Sie in der betreffenden Windows-Anleitung. Dort werden auch die Voraussetzungen beschrieben. Weitere Informationen finden Sie unter Durchführen einer BMR-Wiederherstellung für Windows-Computer.

Sie können auch mit dem Assistenten zum Wiederherstellen einer Maschine eine BMR-Wiederherstellung durchführen. Führen Sie dazu zunächst die in Informationen über das Wiederherstellen von Volumes aus Wiederherstellungspunkten beschriebenen Schritte durch und wechseln Sie an der dort genannten Stelle zu Durchführen einer BMR-Wiederherstellung für Windows-Computer.

Informationen zur Durchführung einer BMR (Bare-Metal-Wiederherstellung) auf einer Linux-Maschine finden Sie unter Durchführen einer BMR-Wiederherstellung für Linux-Maschinen. Neben einer BMR-Wiederherstellung mit dem Befehlszeilenprogramm „local_mount“ können Sie eine BMR-Wiederherstellung jetzt auch in der Benutzeroberfläche der Core Console durchführen. In der Anleitung werden beide Verfahren behandelt.

Durchführen einer BMR-Wiederherstellung für Windows-Computer

Um eine BMR-Wiederherstellung für Windows-Maschinen durchzuführen, müssen Sie die folgenden Aufgaben durchführen.

- Erstellen eines Windows-Startimage. Das ISO-Image der Start-CD wird zum Starten des Ziellaufwerks verwendet. Von dort aus können Sie auf die Universal Recovery Console zugreifen, um Sicherungen auf dem Core zu übertragen. Informationen dazu finden Sie unter Grundlegendes zum Erstellen einer Start-CD für Windows-Computer.
    - Wenn zum Starten des Zielcomputers ein physischer Datenträger erforderlich ist, müssen Sie das ISO-Image für die Start-CD auf ein Medium übertragen. Informationen dazu finden Sie unter Übertragen des ISO-Image der Start-CD auf Datenträger.
    - In allen Fällen müssen Sie das Startimage im Zielserver laden und den Server vom Startimage starten. Informationen dazu finden Sie unter Laden der Start-CD und Starten der Zielmaschine.

NOTE: In diesem Prozess wird beschrieben, wie ein Start-CD-Image im Dialogfeld „Start-CD erstellen“ verwaltet wird. Sie können diese Schritte auch im Assistenten zum Wiederherstellen einer Maschine durchführen (ab der Start-CD-Seite des Assistenten). Diese Seite wird angezeigt, wenn Sie auf der Seite „Ziel“ des Assistenten Wiederherstellung auf einer beliebigen Zielmaschine mit einer Start-CD auswählen.

- Starten einer BMR-Wiederherstellung für Windows. Nachdem der Zielcomputer von der Start-CD gestartet wurde, können Sie die BMR-Wiederherstellung starten. Informationen dazu finden Sie unter Verwendung der Universal Recovery Console für eine BMR. Inbegriffen sind die folgenden Aufgaben:
  - Einleiten einer Wiederherstellung aus einem Wiederherstellungspunkt im Core. Informationen dazu finden Sie unter Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung.
  - Weisen Sie die Volumes zu. Informationen dazu finden Sie unter Informationen über die Zuweisung der Laufwerke für eine Bare-Metal-Wiederherstellung (BMR).
  - Wenn bei einer Wiederherstellung auf einer unterschiedlichen Hardware die erforderlichen Speicher- und Netzwerktreiber nicht auf der Start-CD vorhanden sind, müssen Sie die Treiber u. U. von einem Wechselmedium laden. Weitere Informationen finden Sie unter Laden von Treibern mit der Universal Recovery Console.
- BMR-Wiederherstellung mit dem Assistenten zum Wiederherstellen einer Maschine durchführen. Die Schritte zum Verwalten eines Windows-Start-Image und zum Starten der BMR-Wiederherstellung (mit allen untergeordneten Aufgaben) können mit dem Assistenten zum Wiederherstellen einer Maschine durchgeführt werden. Informationen zum Starten des Assistenten finden Sie in den Schritten 1 bis 5 von Informationen über das Wiederherstellen von Volumes aus Wiederherstellungspunkten.
- Überprüfen einer BMR-Wiederherstellung. Nachdem die BMR-Wiederherstellung (Bare Metal Restore) gestartet wurde, können Sie den Fortschritt überprüfen und überwachen. Informationen dazu finden Sie unter Überprüfen einer BMR-Wiederherstellung.
  - Sie können den Fortschritt der Wiederherstellung überwachen. Informationen dazu finden Sie unter Anzeigen des Wiederherstellungsfortschritts.
  - Danach können Sie den wiederhergestellten Server starten. Siehe . Starten eines wiederhergestellten Zielservers
  - Beheben von Fehlern beim BMR. Siehe Beheben von Universal Recovery Console-Verbindungsproblemen und Beheben von Problemen beim Starten.

Voraussetzungen für eine Bare-Metal-Wiederherstellung für einen Windows-Computer

Damit Sie eine BMR-Wiederherstellung (Bare Metal Restore) für eine Windows-Maschine durchführen können, müssen die folgenden Bedingungen und Kriterien erfüllt sein:

- Eine 64-Bit-CPU (Central Processing Unit). Die Rapid Recovery Start-CD enthält das Betriebssystem Win PE 5.1. Rapid Recovery BMR-Wiederherstellungen sind nicht kompatibel mit x86-basierten CPUs. Sie können eine BMR-Wiederherstellung nur auf einer 64-Bit-CPU durchführen.

NOTE: Diese Anforderung ist neu ab Version 6.0.

- Vorhandensein von Sicherungen der Maschine, die wiederhergestellt werden soll. Es muss ein funktionierender Rapid Recovery Kern mit Wiederherstellungspunkten des geschützten Servers vorhanden sein, der wiederhergestellt werden soll.
- Hardware für die Wiederherstellung (neu oder alt, vergleichbar oder unterschiedlich) Der Zielcomputer muss die Installationsanforderungen für einen Agenten erfüllen. Entsprechende Details finden Sie im Installations- und Aktualisierungshandbuch für Rapid Recovery.
- Image-Datenträger und -Software. Sie müssen über eine leere CD oder DVD sowie über eine Software zum Brennen von Datenträgern oder eine Software zum Erstellen eines ISO-Image verfügen. Wenn Sie Maschinen remote mit einer virtuellen Vernetzungssoftware wie UltraVNC verwalten, benötigen Sie einen VNC-Viewer.
- Kompatible Speichertreiber und Netzwerkadaptertreiber. Bei der Wiederherstellung auf abweichender Hardware müssen ggf. kompatible Speichertreiber und Netzwerkadaptertreiber (z. B. RAID, AHCI) sowie Chipsatztreiber für den Zielcomputer vorhanden sein.
- Speicherplatz und Partitionen je nach Bedarf. Auf der Zielfestplatte muss genügend Speicherplatz zum Erstellen der Zielpartitionen auf der Zielmaschine für die Quell-Volumes vorhanden sein. Jede Zielpartition muss mindestens so groß sein wie die ursprüngliche Quellpartition.
- Kompatible Partitionen. Die Betriebssysteme Windows 8, Windows 8.1, Windows Server 2012 und Windows Server 2012 R2, die von FAT32-EFI-Partitionen gestartet werden, sowie ReFS-Volumes (Resilient File System) können geschützt und wiederhergestellt werden. UEFI-Partitionen werden als einfache FAT32-Volumes behandelt. Inkrementelle Übertragungen werden vollständig unterstützt und geschützt. Rapid Recovery unterstützt UEFI-Systeme für BMR-Wiederherstellung, einschließlich der automatischen Partitionierung von GPT-Datenträgern.

Durchführen einer Bare-Metal-Wiederherstellung von Daten unter Verwendung des Assistenten zum Wiederherstellen eines Computers

Sie können den Assistenten zum Wiederherstellen eines Computers zum Erstellen einer startfähigen CD sowie dem Durchführen einer Bare-Metal-Wiederherstellung (BMR) verwenden.

Lesen Sie vor einer BMR-Wiederherstellung Voraussetzungen für eine Bare-Metal-Wiederherstellung für einen Windows-Computer bzw. Voraussetzungen für eine BMR-Wiederherstellung für Linux-Maschinen durch. Wenn Sie die BMR für einen Windows-Computer aus der Core Console heraus starten, finden Sie weitere Informationen unter Durchführen einer BMR-Wiederherstellung für Windows-Computer.

Auf dem geschützten Computer muss die Agent-Software installiert sein. Außerdem müssen Wiederherstellungspunkte vorhanden sein, aus denen Daten wiederhergestellt werden können.

Das Verwalten eines Windows-Startimage über der Assistent umfasst die folgenden Aktionen:

- Einleiten der Erstellung der Start-CD
- Definition des Pfads für das Image auf dem Core-Computer
- Die Auswahl der Wiederherstellungsumgebung entsprechend den Hardwarekomponenten, die Sie wiederherstellen möchten
- Optional das Definieren der Verbindungsparameter für die Verwendung des Netzwerks oder von UltraVNC durch den wiederhergestellten Agenten
- Optional eine Treiberinjektion für die Hardware, auf der die Wiederherstellung erfolgen soll
- Optional das Übertragen des Startimage auf physische Datenträger
- Starten des Agenten-Computer, auf dem Sie Daten über die Start-CD wiederherstellen möchten
- Herstellen einer Verbindung zur Universal Recovery Console
- Zuweisen von Volumes
- Einleiten der Bare-Metal-Wiederherstellung vom ausgewählten Wiederherstellungspunkt im Core

NOTE: Dieser Prozess beschreibt, wie ein Start-CD-Image im Assistenten zum Wiederherstellen einer Maschine bei der Durchführung einer BMR-Wiederherstellung mit dem Assistenten verwaltet wird. Sie können ein Start-Image auch im Dialogfeld „Start-CD erstellen“ verwalten. Informationen zum Verwalten eines Start-CD-Image außerhalb des Assistenten zum Wiederherstellen einer Maschine finden Sie unter Grundlegendes zum Erstellen einer Start-CD für Windows-Computer.

1. Um ein Volume einer geschützten Maschine wiederherzustellen, navigieren Sie zur Core Console und klicken Sie auf **Wiederherstellen** in der Rapid Recovery Schaltflächenleiste.

   Der Assistent zum Wiederherstellen einer Maschine wird angezeigt.
2. Wählen Sie auf der Seite „Computer“ den geschützten Computer aus, den Sie wiederherstellen möchten, und klicken Sie auf **Weiter**.

   Die Seite „Wiederherstellungspunkte“ wird angezeigt.
3. Wählen Sie den Wiederherstellungspunkt aus, den Sie zum Wiederherstellen des Computers verwenden möchten.

   - Optional können Sie, um die Anzahl der Wiederherstellungspunkte, die angezeigt werden, zu begrenzen, nach Volumes (falls definiert) oder nach Erstellungsdatum des Wiederherstellungspunkts filtern. Sie können auch eine Suche nach einem bestimmten Wiederherstellungspunkt ausführen.
4. Klicken Sie auf **Weiter**.
5. Wählen Sie auf der Ziel-Seite **Wiederherstellung auf einem beliebigen Zielcomputer mit einer Start-CD** aus.

   - Wenn Sie noch keine Start-CD auf dem Computer, den Sie wiederherstellen möchten, geladen haben, klicken Sie auf **Weiter** und fahren Sie mit Schritt 6 fort.
   - Wenn Sie bereits eine Start-CD auf dem Zielcomputer der BMR-Wiederherstellung geladen haben, wählen Sie **Ich habe bereits eine Start-CD auf dem Zielcomputer ausgeführt**, klicken Sie auf **Weiter** und fahren Sie mit Schritt 16 fort.
6. Geben Sie auf der Seite "Start-CD" im Feld "Ausgabepfad" den Pfad ein, in dem das ISO-Image der Start-CD gespeichert werden soll.

   NOTE: Wenn auf dem freigegebenen Laufwerk, auf dem das Image gespeichert werden soll, nicht genügend Speicherplatz vorhanden ist, können Sie den Pfad nach Bedarf anpassen, z. B. "F:\Dateiname.iso".

NOTE: Die Dateierweiterung muss .iso sein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche, umgekehrte Schrägstriche (nur als Pfadtrennzeichen) und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.

7. Wahlweise können Sie zum Einrichten der Netzwerkparameter für den Ziel-Computer oder für die Verwendung von UltraVNC-Funktionen die Option **Erweiterte Optionen anzeigen** auswählen und einen der folgenden Schritte ausführen:
   - Wählen Sie **Folgende IP-Adresse verwenden** aus, um eine Netzwerkverbindung zum Ziel-Computer der BMR-Wiederherstellung einzurichten, und geben Sie die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 142. Optionen für die Netzwerkverbindung

Option	Description
IP-Adresse	Die IP-Adresse für den wiederhergestellten Computer.
Subnetzmaske	Die Subnetzmaske für den wiederhergestellten Computer.
Standard-Gateway	Geben Sie das Standardgateway für die wiederhergestellte Maschine ein.
DNS-Server	Geben Sie den DNS-Server für die wiederhergestellte Maschine ein.

   - Wenn Sie über eine UltraVNC-Konto verfügen und es zum Ausfüllen der BMR verwenden möchten, wählen Sie **UltraVNC hinzufügen** und geben Sie die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 143. Anmeldeinformationen für UltraVNC-Verbindung

Option	Description
Kennwort	Das Kennwort für Ihr UltraVNC-Konto.
Port	Den Port, den Sie verwenden möchten, um eine Verbindung zum Ziel der BMR herzustellen. Die Standardportnummer ist 5900.

8. Klicken Sie auf **Weiter**.
9.
   - Wählen Sie **Folgende IP-Adresse verwenden** aus, um eine Netzwerkverbindung zur wiederhergestellten Maschine einzurichten, und geben Sie die in der folgenden Tabelle beschriebenen Informationen ein.
   - Wählen Sie **UltraVNC hinzufügen** aus, um UltraVNC-Informationen festzulegen, und geben Sie die in der folgenden Tabelle beschriebenen Informationen ein.

     Verwenden Sie diese Option, wenn ein Remote-Zugriff auf die Wiederherstellungskonsole erforderlich ist. Sie können sich nicht über Microsoft-Terminaldienste anmelden, wenn Sie die Start-CD verwenden.

Tabelle 144. UltraVNC-Verbindung

Option	Description
Kennwort	Geben Sie ein Kennwort für die UltraVNC-Verbindung ein.

Option	Description
Port	Geben Sie einen Port für die UltraVNC-Verbindung ein. Die Standardportnummer ist 5900.

10. Wenn Sie die gewünschten Optionen auf der Seite „Start-CD“ festgelegt haben, klicken Sie auf **Weiter**.
11. Optional können Sie, wenn Sie eine Wiederherstellung auf abweichender Hardware planen, auf der Seite "Treiberinjektion" die entsprechenden Speichercontroller und andere Treiber für das Zielsystem anhand der folgenden Schritte injizieren:
    a. Laden Sie die Treiber von der Website des Serverherstellers herunter und entpacken Sie sie.
    b. Komprimieren Sie jeden Treiber mit einem entsprechenden Programm (z. B. WinZip) in eine .zip-Datei.
    c. Klicken Sie auf der Seite "Treiberinjektion" des Assistenten zum Wiederherstellen eines Computers auf **Treiber-Archiv hinzufügen**.
    d. Navigieren Sie im Dateisystem zur komprimierten Treiberdatei, wählen Sie die Datei aus, und klicken Sie auf **Öffnen**.
    e. Wiederholen Sie Schritt c und Schritt d, je nach Bedarf, bis Sie alle erforderlichen Treiber injiziert haben.

    Weitere Informationen zur Treiberinjektion finden Sie unter Grundlegendes zur Treiberinjektion in eine Start-CD.

    NOTE: Nicht alle Versionen von Windows sind mit der automatischen Treiber-Injektion kompatibel. Wenn Ihr Betriebssystem nicht kompatibel ist, speichern Sie die Treiber manuell in das Verzeichnis `C:\Program Files\AppRecovery\Core\BootCdKit\Drivers\`.

    Rapid Recovery erstellt das ISO-Image der Start-CD.
12. Klicken Sie auf **Weiter**.
13. Starten Sie den Zielcomputer der BMR und führen Sie dann eine der folgenden Optionen vollständig aus:
    - Wenn Sie den Agent-Computer vom ISO-Image der Start-CD starten können, starten Sie den Computer jetzt.
    - Wenn Sie den Zielcomputer nicht starten können, kopieren Sie das ISO-Image auf physische Datenträger (CD oder DVD), laden Sie den Datenträger in den Zielcomputer, konfigurieren Sie den Computer zum Laden von der Start-CD und führen Sie einen Neustart von der Start-CD aus.

      NOTE: Sie müssen u. U. die BIOS-Einstellungen des Zielcomputers ändern, damit die Start-CD als erstes Volume geladen wird.

      Beim Start von der Start-CD wird auf dem Zielcomputer die Benutzeroberfläche der Universal Recovery Console (URC) angezeigt. Diese Umgebung wird verwendet, um das Systemlaufwerk bzw. die ausgewählten Volumes direkt vom Rapid Recovery Core wiederherzustellen. Die IP-Adresse und der Authentifizierungsschlüssel für die Anmeldung werden bei jedem Start mit der Start-CD in der URC geändert.
14. Geben Sie auf der Seite "Verbindung" des Assistenten zum Wiederherstellen eines Computers die Authentifizierungsinformationen der URC-Instanz des Computers, den wiederhergestellt werden soll, wie folgt ein:

Tabelle 145. Authentifizierungsoptionen

Option	Description
IP-Adresse	Die angegebene IP-Adresse in der URC auf dem Zielcomputer.

Option	Description
Authentifizierungsschlüssel	Den Authentifizierungsschlüssel in der URC auf dem Zielcomputer.

15. Klicken Sie auf **Weiter**.
16. Wenn Sie Volumes manuell zuordnen möchten, fahren Sie auf der Seite Datenträger-Mapping mit Schritt 10 fort. Wenn Volumes automatisch zugeordnet werden sollen, gehen Sie wie folgt vor:
    a. Wählen Sie im Dropdown-Menü „Volume-Mapping“ **Automatisch** aus.
    b. Vergewissern Sie sich, dass in der Liste der Volumes die Volumes, die Sie wiederherstellen möchten, ausgewählt sind. Alle Volumes sind per Standardeinstellung ausgewählt.

    Deaktivieren Sie die Option, wenn Sie ein aufgelistetes Volume nicht wiederherstellen möchten.

    NOTE: Zum Durchführen der Wiederherstellung muss mindestens ein Volume ausgewählt werden.

    c. Wählen Sie auf der rechten Seite den Zieldatenträger für die Wiederherstellung aus.
    d. Klicken Sie auf **Weiter**.
    e. Überprüfen Sie auf der Seite „Datenträgerzuordnung - Vorschau“ die Parameter der ausgewählten Wiederherstellungsaktionen.
    f. Fahren Sie mit Schritt 18 fort.
17. Um Volumes manuell zuzuordnen, führen Sie auf der Seite Datenträger-Mapping die folgenden Schritte aus:
    a. Wählen Sie im Dropdown-Menü „Volume-Mapping“ **Manuell** aus.
    b. Wählen Sie in der Spalte Ziel ein Ziel Volume aus, das Sie wiederherstellen möchten. Deaktivieren Sie die Option, wenn Sie ein aufgelistetes Volume nicht wiederherstellen möchten.

    NOTE: Zum Durchführen der Wiederherstellung muss mindestens ein Volume ausgewählt werden.
18. Klicken Sie auf **Fertig stellen**.

    CAUTION: Es werden alle bestehenden Partitionen und Daten auf dem Zieldatenträger dauerhaft entfernt und mit dem Inhalt des ausgewählten Wiederherstellungspunkts, einschließlich des Betriebssystems und aller Daten, ersetzt.
19. Wenn die wiederherzustellenden Volumes Oracle-, SQL-, Server- oder Microsoft Exchange-Datenbanken enthalten und Sie eine Live-Wiederherstellung durchführen, werden Sie auf der Seite „Datenbankbereitstellungen aufheben“ aufgefordert, die Volumes zu unmounten. Wählen Sie ggf. **Alle Datenbanken nach der Wiederherstellung des Wiederherstellungspunkts wieder bereitstellen** aus, wenn die Datenbanken nach der Wiederherstellung wieder bereitgestellt werden sollen.
20. Klicken Sie auf **Wiederherstellen**.
21. Klicken Sie in der Statusmeldung auf **OK** um zu bestätigen, dass der Wiederherstellungsprozess gestartet wurde.

    Die Wiederherstellung beginnt. Sie können den Fortschritt auf der Seite „Ereignisse“ verfolgen. Weitere Informationen hierzu finden Sie unter Anzeigen von Ereignissen mithilfe von Aufgaben, Warnungen und Journalseiten.

Grundlegendes zum Erstellen einer Start-CD für Windows-Computer

Für eine BMR-Wiederherstellung (Bare Metal Restore) für Windows ist ein Startimage (Start-CD genannt) erforderlich, das Sie durch Festlegen der entsprechenden Parameter in der Rapid Recovery Core erstellen können. Dieses Image wird an die jeweiligen Anforderungen angepasst. Mit dem Image wird die Windows-Zielmaschine gestartet. Abhängig von den jeweiligen Eigenschaften der Umgebung müssen Sie dieses Image

u. U. auf ein physisches Medium übertragen (z. B. CD oder DVD). Anschließend müssen Sie das Start-Image virtuell oder physisch laden und den Windows-Server mit dem Start-Image starten.

Bei der Durchführung einer BMR-Wiederherstellung (Bare Metal Restore) für eine Windows-Maschine muss zuerst die Start-CD-Datei in der Rapid Recovery Core Console erstellt werden. Dabei handelt es sich um ein startfähiges ISO-Image, das die Rapid Recovery Universelle Wiederherstellungskonsole (URC) enthält, eine Umgebung, mit der das Systemlaufwerk oder ein ganzer Server direkt vom Rapid Recovery Core aus wiederhergestellt werden kann.

Das erstellte ISO-Image für die Start-CD wird an die Maschine angepasst, die wiederhergestellt wird, und muss daher die richtigen Netzwerk- und Massenspeichertreiber enthalten. Wenn vorhersehbar ist, dass die Wiederherstellung auf einer anderen Hardware als der Maschine erfolgt, von der der Wiederherstellungspunkt stammt, müssen Sie Speichercontroller- und andere Treiber in die Start-CD aufnehmen. Informationen zur Treiberinjektion in die Start-CD finden Sie unter Grundlegendes zur Treiberinjektion in eine Start-CD.

Grundlegendes zur Treiberinjektion in eine Start-CD

Im Start-CD-Image müssen Speichertreiber vorhanden sein, damit die Laufwerke des Servers erkannt werden, sowie Netzwerkadaptertreiber, damit eine Kommunikation mit dem Rapid Recovery Core über das Netzwerk möglich ist.

Beim Erstellen einer Start-CD für Windows wird automatisch ein Standardsatz von Windows 8.1 64-Bit-Speichercontroller- und -Netzwerkadaptertreibern hinzugefügt. Dadurch werden die Anforderungen neuerer Systeme erfüllt. Bei Systemen anderer Hersteller oder älteren Systemen müssen Sie beim Erstellen der Start-CD u. U. Speichercontroller- oder Netzwerkadaptertreiber hinzufügen. Wenn Sie feststellen, dass die erstellte Start-CD nicht die erforderlichen Treiber für die Wiederherstellung enthält, können Sie die Treiber auch mit der URC auf die Zielmaschine laden. Weitere Informationen hierzu finden Sie unter Laden von Treibern mit der Universal Recovery Console.

Beim Erstellen der Start-CD wird die Treiberinjektion verwendet, um die Interoperabilität zwischen Recovery Console, Netzwerkadapter und Speicher auf dem Zielserver zu ermöglichen.

Die aus dem Wiederherstellungspunkt wiederhergestellten Daten enthalten die Treiber der zuvor verwendeten Hardware. Bei der Durchführung einer BMR-Wiederherstellung (Bare Metal Restore) auf eine unterschiedliche Hardware müssen Sie mit der URC auch Speichercontrollertreiber in das wiederhergestellte Betriebssystem injizieren, nachdem die Daten auf dem Laufwerk wiederhergestellt wurden, damit das wiederhergestellte Betriebssystem mit der neuen Hardware gestartet werden kann. Nachdem das Betriebssystem nach der Wiederherstellung neu gestartet wurde, können Sie alle weiteren Treiber herunterladen und installieren, die vom Betriebssystem für die Interaktion mit der neuen Hardware benötigt werden.

Erstellen eines ISO-Image für die Start-CD

„Start-CD" ist der Begriff, den Rapid Recovery für den tragbaren Speicherort des ISO-Images verwendet, das für die Durchführung einer BMR-Wiederherstellung (Bare Metal Restore) reserviert ist. Das Image umfasst die Rapid Recovery Universal Recovery Console (URC).

Um eine BMR-Wiederherstellung auf einem Computer durchzuführen, müssen Sie den Computer von der Start-CD starten, mit der die URC ausgeführt wird. Die URC ermöglicht es, den Ziel-Computer der BMR-Wiederherstellung mit dem Speicherort des Wiederherstellungspunkt zu verbinden, den Sie verwenden möchten, um die Wiederherstellung abzuschließen.

1. Klicken Sie in der Rapid Recovery Core Console, mit der der Server geschützt ist, den Sie wiederherstellen möchten, in der Symbolleiste auf das Menü „Mehr“ und klicken Sie dann auf **Start-CDs**.
2. Klicken Sie auf der Seite "Start-CDs" auf **Start-CD erstellen**.

Das Dialogfeld „Start-CD erstellen“ wird angezeigt.

3. Geben Sie im Dialogfeld „Start-CD erstellen“ im Textfeld **Ausgabepfad** den Speicherort ein, an dem das ISO-Image der Start-CD gespeichert werden soll.

   NOTE: Die Dateierweiterung muss .iso sein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche, umgekehrte Schrägstriche (nur als Pfadtrennzeichen) und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung nicht unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.

4. Führen Sie unter „Verbindungsoptionen“ eine der folgenden Aktionen aus:

   - Wählen Sie **IP-Adresse automatisch beziehen** aus, um die IP-Adresse dynamisch von DHCP (Dynamic Host Configuration Protocol) zu beziehen.
   - Zur Konfiguration einer statischen IP-Adresse für die URC wählen Sie **Folgende IP-Adresse verwenden** und geben Sie die folgenden Informationen ein:
     - IP-Adresse
     - Subnetzmaske
     - Standard-Gateway
     - DNS-Server

   NOTE: Sie müssen alle vier Felder ausfüllen.

5. Wenn Sie Remote-Zugriff auf die Wiederherstellungskonsole benötigen und UltraVNC installiert haben, führen Sie unter UltraVNC-Optionen die folgenden Schritte aus:

   NOTE: UltraVNC ermöglicht Ihnen die Verwaltung der URC über Fernzugriff, während sie verwendet wird. Sie können sich nicht über Microsoft-Terminaldienste anmelden, wenn Sie die Start-CD verwenden.

   a. Wählen Sie **Hinzufügen von UltraVNC**.
   b. Geben Sie Ihr **UltraVNC-Kennwort** ein.
   c. Geben Sie den **UltraVNC-Port** ein. Die Standardportnummer ist 5900.

   NOTE: Die UltraVNC-Optionen sind nur verfügbar, wenn Sie UltraVNC bereits installiert haben. Um diese Optionen verfügbar zu machen, gehen Sie zu http://www.uvnc.com/downloads/ultravnc/ zum Herunterladen von UltraVNC Version 1.0.9.1 oder höher für x64-Architektur. Führen Sie die Installation durch und speichern Sie die Datei "winvnc.exe" in das Verzeichnis C:\Program Files \AppRecovery\Core\BootCdKit\UltraVnc_x64\.

6. Wenn Sie eine Wiederherstellung auf abweichender Hardware planen, injizieren Sie die entsprechenden Speichercontroller und andere Treiber für das Zielsystem anhand der folgenden Schritte:

   NOTE: Nicht alle Versionen von Windows sind mit der automatischen Treiber-Injektion kompatibel. Wenn Ihr Betriebssystem nicht kompatibel ist, speichern Sie die Treiber manuell in das Verzeichnis C: \Program Files\AppRecovery\Core\BootCdKit\Drivers\.

   a. Laden Sie die Treiber von der Website des Serverherstellers herunter und entpacken Sie sie.
   b. Komprimieren Sie jeden Treiber mit einem entsprechenden Programm (z. B. WinZip) in eine .zip-Datei.
   c. Klicken Sie im Dialogfeld "Start-CD erstellen" im Fenster "Treiber", auf **Treiber hinzufügen**.
   d. Navigieren Sie im Dateisystem zur komprimierten Treiberdatei, wählen Sie die Datei aus, und klicken Sie auf **Öffnen**.

   Die Treiberdatei wird im Fensterbereich „Treiber“ des Dialogfelds „Start-CD erstellen“ angezeigt.

   e. Wiederholen Sie Schritt c und Schritt d, je nach Bedarf, bis Sie alle erforderlichen Treiber hinzugefügt haben.
   f. Wählen Sie im Fensterbereich „Treiber“ die Treiber aus, die Sie injizieren möchten.

Weitere Informationen zur Treiberinjektion finden Sie unter Grundlegendes zur Treiberinjektion in eine Start-CD.

7. Klicken Sie auf **Start-CD erstellen**.

   Rapid Recovery erstellt die Start-CD und speichert sie mit dem Dateinamen ab, den Sie eingegeben haben.

8. Gehen Sie zur Überwachung des Fortschritts dieser Aufgabe zur Symbolleiste und klicken Sie auf das Ereignis-Symbol.

   Weitere Informationen zur Überwachung von Rapid Recovery Ereignissen finden Sie unter Anzeigen von Ereignissen mithilfe von Aufgaben, Warnungen und Journalseiten.

   Wenn das Erstellen des ISO-Images abgeschlossen ist, wird auf der Seite "Start-CD" ein Datensatz des Images angezeigt, auf die Sie aus dem Menü "Weitere" in der Symbolleiste zugreifen können.

Um auf das ISO-Image zuzugreifen, navigieren Sie zum angegebenen Ausgabepfad. Sie können auch auf den Link auf der Seite "Start-CD" klicken, um das Image an einem Speicherort abzulegen, von dem aus Sie es in das neue System laden können, z. B. ein Netzlaufwerk.

Übertragen des ISO-Image der Start-CD auf Datenträger

Beim Erstellen der Start-CD-Datei wird diese als ISO-Image im angegebenen Pfad gespeichert. Sie müssen in der Lage sein, dieses Image als ein Laufwerk auf dem Server bereitzustellen, auf dem Sie eine Bare-Metal-Wiederherstellung durchführen möchten.

Sie können das ISO-Image der Start-CD auf CD- oder DVD-Datenträger brennen, die beim Systemstart zugänglich sind.

Wenn Sie die Maschine von der Start-CD starten, startet die Universal Recovery Console automatisch.

Beim Durchführen einer BMR auf einer virtuellen Maschine ist dieser Schritt nicht erforderlich. Laden Sie das ISO-Image einfach in ein Laufwerk und bearbeiten Sie die Einstellungen der VM so, dass sie von diesem Laufwerk aus gestartet wird.

Laden der Start-CD und Starten der Zielmaschine

Nachdem Sie das Start-CD-Image erstellt haben, müssen Sie den Zielserver mit der neu erstellten Start-CD starten.

Um eine Verbindung mit der Rapid Recovery Core Console herzustellen oder für die Verwendung von Chromium zum Herunterladen von zusätzlichen Treibern, müssen Sie zuerst einen Ethernet-Controller und einen Netzwerkadapter laden. Weitere Informationen hierzu finden Sie unter Laden von Treibern mit der Universal Recovery Console.

NOTE: Falls Sie die Start-CD mit DHCP erstellt haben notieren Sie sich die IP-Adresse und das Kennwort.

1. Laden Sie auf dem neuen Server das Start-CD-Image vom entsprechenden Speicherort und starten Sie anschließend den Server aus dem Start-CD-Image zum Laden der Rapid Recovery Agenten-Software und Win PE 5.1.

   Auf der Zielmaschine wird ein blauer Quest Bildschirm mit drei Symbolschaltflächen am oberen Rand des Bildschirms angezeigt.

2. Um die Rapid Recovery Universal Recovery Console (URC)-Benutzerschnittstelle zu öffnen, klicken Sie auf das Quest Symbol am oberen Rand des Bildschirms.

Die IP-Adresse und das Kennwort für die Maschine werden unter „Authentifizierung“ angezeigt.

NOTE: Bei jedem Starten der Maschine mit der Start-CD wird ein neues temporäres Kennwort generiert. Notieren Sie sich die im Einstellungsbereich des Netzwerkadapters angezeigte IP-Adresse und das im Authentifizierungsbereich angezeigte Authentifizierungskennwort. Sie benötigen diese Information später während des Datenwiederherstellungsvorgangs, um sich wieder bei der Konsole anzumelden.

NOTE: Wenn keine IP-Adresse angegeben ist, laden Sie den Ethernet-Controller und den Netzwerkadapter.

3. Wenn Sie die IP-Adresse ändern möchten, wählen Sie sie aus und klicken Sie auf **Ändern**.

NOTE: Wenn Sie eine IP-Adresse im Dialogfeld „Start-CD erstellen“ angegeben haben, wird diese Adresse von der Universal Recovery Console verwendet und in der Anzeige „Einstellungen für Netzwerkadapter“ angezeigt.

Die Maschine bereit, eine Verbindung mit dem Core herzustellen. Wählen Sie einen Wiederherstellungspunkt und fahren Sie mit dem Bare-Metal-Wiederherstellungsprozess fort.

Verwendung der Universal Recovery Console für eine BMR

Um eine BMR-Wiederherstellung für Windows-Computer durchzuführen, müssen die folgenden Bedingungen erfüllt sein:

- Um einen Wiederherstellungspunkt im Core wiederherzustellen, muss eine geeignete Hardware vorhanden sein. Weitere Informationen finden Sie unter Voraussetzungen für eine Bare-Metal-Wiederherstellung für einen Windows-Computer.
- Die Windows-Zielmaschine für die BMR-Wiederherstellung muss mit dem Start-CD-Image gestartet werden. Weitere Informationen finden Sie unter Grundlegendes zum Erstellen einer Start-CD für Windows-Computer.

Eine BMR-Wiederherstellung initiiert einen Computer über einen Wiederherstellungspunkt, den Sie auswählen. Der Wiederherstellungspunkt enthält die Treiber für die vorherige Hardware. Bei der Durchführung einer Wiederherstellung auf eine nicht ähnlichen Hardware müssen Sie mit der URC Speichercontroller-Treiber in das wiederherzustellende Betriebssystem injizieren, nachdem die Daten auf dem Laufwerk wiederhergestellt wurden, damit das wiederhergestellte Betriebssystem mit der neuen Hardware gestartet werden kann. Nachdem das BS gestartet wurde, können Sie zusätzliche Treiber herunterladen und installieren, die das Betriebssystem zur Interaktion mit der neuen Hardware benötigt.

Führen Sie die folgenden Aufgaben durch, um eine BMR-Wiederherstellung über die Rapid Recovery Core Console zu starten.

- Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung
- Informationen über die Zuweisung der Laufwerke für eine Bare-Metal-Wiederherstellung (BMR)
- Laden von Treibern mit der Universal Recovery Console

Dieser Prozess ist ein Schritt von Durchführen einer BMR-Wiederherstellung für Windows-Computer.

Die Universal Recovery Console-Tools

Die Universal Recovery Console (URC) umfasst den Zugriff auf Tools, die Ihnen bei der Durchführung einer Bare-Metal-Wiederherstellung (Bare Metal Restore, BMR) helfen könnten.

Sie finden die folgenden Tools durch Klicken auf das mittlere Symbol am oberen Rand des Quest Begrüßungsbildschirms auf einem BMR-Ziel, das im URC gestartet wird:

- **Far Manager.** Dieses Tool ist ähnlich dem Windows Explorer. Es bietet eine Methode zum Suchen nach Dateien auf dem Server bis zum Abschluss des BMR und Installieren eines Betriebssystems mit eigener Browsing-Funktion, wie Windows Explorer.
- **Chromium.** Mit diesem Open-Source-Browser erhalten Sie Zugang zum Internet auf einem Server mit einem über die URC geladenen Netzwerkcontroller.
- **PuTTY.** Dieses Tool ist eine Open-Source-Terminalemulation. Im Kontext einer Rapid Recovery BMR ermöglicht es Ihnen die Verbindung mit einem NAS-Speichergerät, das nicht eine Benutzerschnittstelle beinhaltet. Diese Funktion ist möglicherweise erforderlich, wenn Sie aus einem Archiv wiederherstellen möchten und das Archiv auf einem NAS ist.
- **Notepad.** Wie bei einem Windows Betriebssystem, können Sie mit diesem Tool unformatierte Anmerkungen eingeben und Protokolldateien anzeigen.
- **Task-Manager.** Wie bei einem Windows Betriebssystem ermöglicht Ihnen dieses Tool die Verwaltung von Prozessen und das Überwachen der Leistung des Servers, während die Wiederherstellung durchgeführt wird.
- **Registrierungs-Editor.** Wie bei einem Windows Betriebssystem ermöglicht dieses Tool das Ändern der Systemregistrierung des BMR-Ziels.
- **Eingabeaufforderung.** Dieses Tool ermöglicht Ihnen das Ausführen von Befehlen auf dem BMR-Ziel außerhalb der URC, bis Sie eine Benutzerschnittstelle installieren.

Laden von Treibern mit der Universal Recovery Console

Mithilfe dieser Funktion können Sie Treiber hinzufügen, die nicht im ISO-Image enthalten, aber für eine BMR-Wiederherstellung erforderlich sind.

Diese Aufgabe ist ein Schritt in Durchführen einer BMR-Wiederherstellung für Windows-Computer. Dieser ist Bestandteil des Prozesses zum Verwendung der Universal Recovery Console für eine BMR.

Beim Erstellen einer Start-CD können Sie die erforderlichen Treiber zum ISO-Image hinzufügen. Nach dem Starten der Zielmaschine können Sie Speicher- oder Netzwerktreiber auch in der Universal Recovery Console (URC) laden.

Bei der Wiederherstellung auf einer anderen Hardware müssen Sie Speichercontroller-, RAID-, AHCI-, Chipsatz- und andere Treiber injizieren, wenn diese noch nicht auf der Start-CD vorhanden sind. Diese Treiber ermöglichen einen einwandfreien Betrieb aller Geräte des Zielservers im Betriebssystem, sobald das System nach der Wiederherstellung neu gestartet wurde.

Führen Sie die Schritte eines der folgenden Verfahren aus, um Treiber mit der URC zu laden:

- Laden von Treibern in der Universellen Wiederherstellungskonsole unter Verwendung tragbarer Medien
- Laden eines Treibers mit URC Chromium

Laden von Treibern in der Universellen Wiederherstellungskonsole unter Verwendung tragbarer Medien

Die folgenden Aufgaben sind Voraussetzung für dieses Verfahren.

- Erstellen eines ISO-Image für die Start-CD
- Übertragen des ISO-Image der Start-CD auf Datenträger
- Laden der Start-CD und Starten der Zielmaschine

Führen Sie die folgenden Verfahren für die Verwendung eines tragbaren Mediengerätes zum Laden von Treibern in der Universellen Wiederherstellungskonsole (URC) aus.

1. Laden Sie die Treiber auf einem mit dem Internet verbundenen Computer von der Webseite des Server-Herstellers herunter und entpacken Sie sie.
2. Komprimieren Sie jeden Treiber mit einem entsprechenden Programm (z. B. WinZip) in eine .zip-Datei.
3. Kopieren und speichern Sie die .zip-Datei der Treiber auf ein tragbares Mediengerät, wie z. B. ein USB-Laufwerk.
4. Entnehmen Sie den Datenträger aus der Maschine und schließen Sie ihn an den Zielserver an, der gestartet werden soll.
5. Navigieren Sie zum Zielserver, laden Sie die Start-CD und starten Sie den Computer.

   Der Begrüßungsbildschirm von Quest wird angezeigt.
6. Klicken Sie zum Starten der URC auf das **Quest-Symbol**.

   Die URC öffnet sich in der Registerkarte "Treibermanager" der Start-CD.
7. Erweitern Sie die liste **andere Geräte**.

   Diese Liste zeigt die Treiber an, die notwendig für die Hardware, aber nicht in der Start-CD enthalten sind.
8. Klicken Sie mit der rechten Maustaste ein Gerät in der Liste an und klicken Sie auf **Treiber laden**.
9. Wählen Sie im Fenster "Treiberlast-Modus wählen" eine der folgenden Optionen:
   - Einzelnes Treiberpaket laden (Treiber werden ohne Überprüfung der Geräteunterstützung geladen)
   - Ordner nach Treiberpaketen durchsuchen (Treiber für ausgewählte Gerät werden in den ausgewählten Ordnern gesucht)
10. Erweitern Sie das Laufwerk für das tragbare Mediengerät wählen Sie den Treiber (mit der Dateierweiterung .inf), und klicken Sie auf **OK**.

    Der Treiber wird in das aktuelle Betriebssystem geladen.
11. Klicken Sie im Fenster "Information" auf **OK**, um zu bestätigen, dass der Treiber erfolgreich geladen wurde.
12. Wiederholen Sie die obigen Schritte nach Bedarf für jeden Treiber, den Sie laden möchten.

Laden eines Treibers mit URC Chromium

Die folgenden Aufgaben sind Voraussetzung für dieses Verfahren.

- Erstellen eines ISO-Image für die Start-CD
- Übertragen des ISO-Image der Start-CD auf Datenträger
- Laden der Start-CD und Starten der Zielmaschine

Führen Sie das folgende Verfahren zur Verwendung des Chromium-Browsers durch, der auf der Start-CD zum Laden von Treibern in der URC installiert ist.

1. Navigieren Sie zum Zielserver, laden Sie die Start-CD und starten Sie den Computer.

Der Begrüßungsbildschirm von Quest wird angezeigt.

2. Klicken Sie zum Starten der URC auf das **Quest-Symbol**.

   Die URC öffnet sich in der Registerkarte "Treibermanager" der Start-CD.
3. Klicken Sie im BMR-Ziel auf die Tools (mittleres Symbol) am oberen Rand des Bildschirms und klicken Sie dann auf **Chromium**.
4. Im Chromium-Browser navigieren Sie zu einer Website, wo Sie die erforderlichen Treiber laden können.
5. Laden Sie den/die Treiber für den Standort Ihrer Wahl, wie z. B. einen lokalen Ordner oder eine Netzwerkdateifreigabe.
6. Erweitern Sie die liste **andere Geräte**.

   Diese Liste zeigt die Treiber an, die notwendig für die Hardware, aber nicht in der Start-CD enthalten sind.
7. Klicken Sie mit der rechten Maustaste ein Gerät in der Liste an und klicken Sie auf **Treiber laden**.
8. Wählen Sie im Fenster "Treiberlast-Modus wählen" eine der folgenden Optionen:
   - Einzelnes Treiberpaket laden (Treiber werden ohne Überprüfung der Geräteunterstützung geladen)
   - Ordner nach Treiberpaketen durchsuchen (Treiber für ausgewähltes Gerät werden in den ausgewählten Ordnern gesucht)
9. Navigieren Sie zum Speicherort der Treiber, wählen Sie den Treiber und klicken Sie dann auf **OK**.

   Der Treiber wird in das aktuelle Betriebssystem geladen.
10. Klicken Sie im Fenster "Information" auf **OK**, um zu bestätigen, dass der Treiber erfolgreich geladen wurde.
11. Wiederholen Sie die obigen Schritte nach Bedarf für jeden Treiber, den Sie laden möchten.

Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung

Nachdem die Universal Recovery Console (URC) auf der Bare-Metal-Wiederherstellung (BMR) Zielmaschine zugänglich ist, müssen Sie den Wiederherstellungspunkt wählen, den Sie wiederherstellen möchten.

Navigieren Sie zur Core Console, um den Wiederherstellungspunkt auszuwählen, der geladen werden soll, und geben Sie die Wiederherstellungskonsole als Ziel für die wiederhergestellten Daten an.

NOTE: Dieser Schritt ist erforderlich, um die BMR auf allen Windows-Maschinen und optional auf Linux-Maschinen durchzuführen.

Diese Aufgabe ist ein Schritt in Durchführen einer BMR-Wiederherstellung für Windows-Computer. Dieser ist Bestandteil des Prozesses zum Verwendung der Universal Recovery Console für eine BMR.

Bei der Durchführung einer BMR-Wiederherstellung für eine Linux-Maschine in der Core Console ist diese Aufgabe auch ein Schritt in Durchführen einer BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Starten einer BMR-Wiederherstellung für Linux-Maschinen über die Befehlszeile.

1. Klicken Sie in der Rapid Recovery Core Console aus der Liste der geschützten Maschinen auf den Namen der geschützten Maschine, die Sie wiederherstellen möchten.

   Die Registerkarte Zusammenfassung für die ausgewählte Maschine wird angezeigt.
2. Klicken Sie auf **Wiederherstellungspunkte**.
3. Klicken Sie im Dropdown-Menü neben dem Wiederherstellungspunkt, den Sie für die BMR verwenden möchten, auf **Wiederherstellung**.

   Der Assistent zum Wiederherstellen einer Maschine wird angezeigt.
4. Wählen Sie **Wiederherstellung auf einer beliebigen Zielmaschine mit einer Start-CD** aus.
5. Wählen Sie **Ich habe bereits eine Start-CD für die Zielmaschine**.

Die Authentifizierungs-Textfelder werden angezeigt.

6. Geben Sie wie in der folgenden Tabelle beschrieben die Verbindungsinformationen für die Maschine ein.

Tabelle 146. Informationen zur Zielmaschine

Textfeld	Description
IP-Adresse	Die IP-Adresse der Maschine, die wiederhergestellt werden soll. Diese Adresse ist mit der IP-Adresse identisch, die im URC angezeigt wird.
Authentifizierungsschlüssel	Das jeweilige Kennwort für die Verbindung zum ausgewählten Server. Dieses Kennwort ist mit dem Authentifizierungsschlüssel identisch, der im URC angezeigt wird.

7. Klicken Sie auf **Weiter**.

   Wenn die eingegebenen Verbindungsinformationen mit den URC-Informationen übereinstimmen und Core und Zielserver sich gegenseitig einwandfrei im Netzwerk finden, werden die Volumes des ausgewählten Wiederherstellungspunkt geladen und die Seite „Datenträgerzuordnung“ geladen. In diesem Fall ist der nächste Schritt Volumes zuzuordnen.

8. Fahren Sie fort mit Informationen über die Zuweisung der Laufwerke für eine Bare-Metal-Wiederherstellung (BMR), um Näheres über Ihr über Laufwerk-Zuweisungsoptionen zu erfahren.

Informationen über die Zuweisung der Laufwerke für eine Bare-Metal-Wiederherstellung (BMR)

Nachdem die Verbindung zur Universal Recovery Console hergestellt wurde, müssen Sie die im Wiederherstellungspunkt aufgeführten Volumes und die Volumes der Zielhardware zuordnen.

Rapid Recovery versucht, Volumes automatisch zuzuordnen. Wenn Sie die Standardzuordnung übernehmen, wird die Festplatte in der Zielmaschine bereinigt und neu partitioniert, sodass alle bereits vorhandenen Daten gelöscht werden. Die Zuordnung erfolgt in der Reihenfolge, in der die Volumes im Wiederherstellungspunkt aufgelistet sind, und die Volumes werden den Datenträgern entsprechend der Größe usw. zugewiesen. Ausgehend davon, dass genügend Speicherplatz auf dem Ziellaufwerk ist, ist keine Partitionierung erforderlich, wenn die automatische Datenträgerzuordnung verwendet wird. Ein Datenträger kann von mehreren Volumes genutzt werden. Wenn Sie die Laufwerke manuell zuordnen, müssen Sie beachten, dass Sie einen Datenträger nicht zweimal verwenden können.

Bei einer manuellen Zuordnung muss die neue Maschine vor der Wiederherstellung bereits richtig formatiert sein. Die Zielmaschine muss über eine separate Partition für jedes Volume im Wiederherstellungspunkt verfügen (einschließlich dem für das System reservierten Volume). Weitere Informationen hierzu finden Sie unter Verwendung der Universal Recovery Console für eine BMR.

Befolgen Sie die Prozedur für eine der folgenden Laufwerkszuordnungsoptionen:

- Automatisches Datenträgermapping für eine BMR-Wiederherstellung
- Manuelles Datenträgermapping für eine BMR-Wiederherstellung

CAUTION: Obwohl Rapid Recovery FAT32- und ReFS-Partitionen unterstützt, werden zurzeit lediglich vollständige Wiederherstellungen und BMR-Wiederherstellungen unterstützt, da es bei ReFS Treibereinschränkungen gibt, sodass Wiederherstellung, VM-Export usw. im Benutzermodus implementiert sind. Wenn ein Core mindestens ein Agent-Volume schützt, das das Dateisystem ReFS enthält, muss die Installation auf einer Maschine mit Windows 8.1, Windows 10 (nur Enterprise oder Pro), Windows Server 2012, Windows Server 2012 R2 oder Windows Server 2016 erfolgen, die ReFS nativ unterstützen. Andernfalls ist die Funktionalität begrenzt und Vorgänge, bei denen beispielsweise ein Volume-Image bereitgestellt werden muss, funktionieren nicht. Die Rapid Recovery **Core Console enthält zutreffende Fehlermeldungen in diesen Vorfällen.**

CAUTION: Eine BMR-Wiederherstellung (Bare Metal Restore) der Festplattenkonfiguration für Speicherplätze wird nicht unterstützt. Ausführliche Informationen hierzu finden Sie unter *Rapid Recovery-Installations- und Aktualisierungshandbuch*

Diese Aufgabe ist ein Schritt in Durchführen einer BMR-Wiederherstellung für Windows-Computer. Dieser ist Bestandteil des Prozesses zum Verwendung der Universal Recovery Console für eine BMR.

Bei der Durchführung einer BMR-Wiederherstellung für eine Linux-Maschine in der Core Console ist diese Aufgabe auch ein Schritt in Durchführen einer BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Starten einer BMR-Wiederherstellung für Linux.

Automatisches Datenträgermapping für eine BMR-Wiederherstellung

Mit dieser Prozedur können Sie automatisch Laufwerke während einer Bare-Metal-Wiederherstellung (Bare Metal Restore, BMR) unter Verwendung des Assistenten zum Wiederherstellen zuordnen.

Führen Sie die hier beschriebenen Schritte aus, um automatisch die Volumes auszuwählen, die Sie wiederherstellen möchten, und wo diese wiederhergestellt werden sollen.

1. Wählen Sie auf der Seite „Datenträgerzuordnung“ des Assistenten zum Wiederherstellen einer Maschine neben „Volume-Zuordnung“ **Automatisch** im Drop-Down-Menü.
2. Überprüfen Sie in der linken Tabelle, ob die entsprechenden Volumes aufgelistet und ausgewählt sind.

   NOTE: Bei einer BMR-Wiederherstellung sollte zumindest das Volume „System-reserviert“ und das System-Volume (normalerweise, aber nicht immer das Volume C:\) wiederhergestellt werden. Sie müssen mindestens ein Volume zur Durchführung einer BMR auswählen.
3. Wählen Sie in der rechten Tabelle den/die Datenträger, auf dem/denen Sie Volumes auf der Zielmaschine zuordnen möchten.
4. Klicken Sie auf **Weiter**.
5. Prüfen Sie auf der Seite „Datenträgerzuordnung - Vorschau“ die Zuordnung der Wiederherstellungspunktvolumes und das Ziel-Volume für die Wiederherstellung.
6. Klicken Sie auf **Fertigstellen**, um zu starten.

   CAUTION: Wenn Sie Wiederherstellung beginnen auswählen, werden alle bestehenden Partitionen und Daten auf dem Ziellaufwerk dauerhaft entfernt und mit dem Inhalt des ausgewählten Wiederherstellungspunkts, einschließlich des Betriebssystems und aller Daten, ersetzt.

Manuelles Datenträgermapping für eine BMR-Wiederherstellung

Dieses Verfahren beschreibt, wie Sie bestimmen, welche Datenträger an welchen Standorten auf dem wiederhergestellten Computer gespeichert werden sollen.

Für das manuelle Datenträgermapping müssen Sie zuerst DiskPart in der Befehlszeile des Zielcomputers für die BMR-Wiederherstellung zum Erstellen und Formatieren der Ziel-Volumes verwenden. Weitere Informationen finden Sie unter Befehlszeilenoptionen für DiskPart (Standard 7 SP1) im MSDN.

Führen Sie die hier beschriebenen Schritte aus, um manuell die Volumes auszuwählen, die Sie wiederherstellen möchten, und wo diese wiederhergestellt werden sollen.

1. Wählen Sie auf der Seite "Datenträgermapping" des Assistenten zum Wiederherstellen eines Computers neben "Volume-Mapping" **manuell** im Drop-Down-Menü.

   NOTE: Wenn keine Volumes auf dem Laufwerk des Computers vorhanden sind, auf dem eine BMR-Wiederherstellung durchgeführt wird, können Sie diese Option nicht anzeigen oder keine Volumes manuell zuordnen.

2. Überprüfen Sie im Bereich „Volume-Zuordnung“ unter „Quell-Volume“, ob das Quell-Volume ausgewählt ist und die entsprechenden Volumes darunter aufgelistet werden sowie ausgewählt sind.
3. Wählen Sie im Dropdown-Menü unter „Ziel“ das gewünschte Ziel für das Ziel-Volume aus, um die BMR-Wiederherstellung des ausgewählten Wiederherstellungspunkts durchzuführen, und klicken Sie dann auf **Wiederherstellen**.
4. Überprüfen Sie im Bestätigungsdialogfeld die Zuordnung des Quell-Volumes im Wiederherstellungspunkt und den Ziel-Volumes für die Wiederherstellung.
5. Klicken Sie auf **Wiederherstellung starten**, um die Wiederherstellung durchzuführen.

   CAUTION: Wenn Sie auf Wiederherstellung starten klicken, werden alle vorhandenen Partitionen und Daten auf dem Ziellaufwerk permanent gelöscht und durch den Inhalt des ausgewählten Wiederherstellungspunkts ersetzt (einschließlich Betriebssystem und allen Daten).

Eine BMR aus einem Archiv durchführen

Mit Rapid Recovery können Sie eine Maschine von Bare-Metal unter Verwendung eines archivierten Wiederherstellungspunkts wiederherstellen.

Die folgenden Aufgaben sind Voraussetzung für dieses Verfahren.

- Erstellen eines ISO-Image für die Start-CD
- Laden der Start-CD und Starten der Zielmaschine

Von der Universal Recovery Console (URC) können Sie auf Rapid Recovery Core zugreifen und einen Wiederherstellungspunkt für eine Wiederherstellung abrufen. Sie können jedoch auch jederzeit Wiederherstellen Ihrer Bare-Metal-Maschine von einem Wiederherstellungspunkt, der in einem Archiv gespeichert ist, wählen. Mit der URC können Sie auf dieses Archiv unabhängig davon, ob es sich um auf ein lokales Laufwerk, eine Netzwerkfreigabe oder ein Cloud-Konto handelt zugreifen.

1. Klicken Sie in der URC auf die Registerkarte **Wiederherstellung aus Archiv**.
2. Wählen Sie in der Drop-Down-Liste **Typ des Speicherorts** den Speicherort Ihres Archivs aus. Sie können zwischen folgenden Optionen wählen.
   - Lokal
   - Netzwerk
   - Cloud
3. Geben Sie die Anmeldeinformationen in der folgenden Tabelle entsprechend Ihrer Standort-Type-Auswahl ein.

Tabelle 147. Optionen für Anmeldeinformationen nach Typ des Speicherorts

Typ des Speicherorts	Option	Description
Lokal	Lokaler Pfad	Die derzeitige Position des Archivs.
Netzwerk	Netzwerkpfad	Die derzeitige Position des Archivs.
	Benutzer	Den Benutzernamen für Zugriff auf die Netzwerkfreigabe.
	Kennwort	Das Kennwort für Zugriff auf die Netzwerkfreigabe.
Cloud	Cloud-Typ	Den Provider für Ihren Cloud-Speicherort. Wählen Sie aus folgenden Optionen aus: • Microsoft Azure • Amazon S3 • Powered by OpenStack • Rackspace Cloud-Dateien • Google Cloud

4. Wenn Sie einen Cloud-Typ gewählt haben, füllen Sie die Anmeldeinformationen, die zu Ihrem Cloud-Anbieter gehören, aus.
   - Für Microsoft Azure, führen Sie die folgenden Schritte aus:
     1. Geben Sie die folgenden Anmeldeinformationen ein:
        - Speicherkontoname
        - Zugriffsschlüssel
     2. Für den Container Namen wählen Sie aus der Drop-Down-Liste einen Container aus.
     3. Für den Cloud Pfad wählen Sie aus der Drop-Down-Liste den Pfad in das Archiv aus.
   - Für Amazon S3 führen Sie die folgenden Schritte aus
     1. Geben Sie die folgenden Anmeldeinformationen ein:
        - Zugriffsschlüssel
        - Geheimer Schlüssel
     2. Für den Container Namen wählen Sie aus der Drop-Down-Liste einen Container aus.
     3. Für den Cloud Pfad wählen Sie aus der Drop-Down-Liste den Pfad in das Archiv aus.
   - Für Powered by OpenStack- oder Rackspace Cloud Files-Konten führen Sie die folgenden Schritte aus:
     1. Geben Sie die folgenden Informationen ein:
        - Region
        - Benutzer
     2. Wählen Sie eine der folgenden Optionen aus:
        - Kennwort
        - API-Schlüssel
     3. Geben Sie in das Textfeld die Informationen basierend auf Ihrer Auswahl in Schritt c ein.

4. Geben Sie die folgenden Informationen ein:
   - Tenant-ID
   - Authentifizierungs-URL
   - Containername
   - Cloud-Pfad

◦ Für Google Cloud-Konten führen Sie die folgenden Schritte aus:

1. Geben Sie die folgenden Anmeldeinformationen ein:
   - Zertifikatsdatei
   - Privater Schlüssel
2. Geben Sie die folgenden Informationen ein:
   - Projekt-ID
   - E-Mail-Adresse des Service-Kontos
3. Wählen Sie im Feld mit dem Containernamen aus der Drop-Down-Liste den entsprechenden Container aus.

   Als Cloud-Pfad wählen Sie aus der Drop-Down-Liste den Pfad zum Archiv aus.

5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Maschinen** die geschützte Maschine aus, die Sie wiederherstellen möchten, und klicken Sie auf **Weiter**.
7. Wählen Sie auf der Seite **Wiederherstellungspunkte** den Wiederherstellungspunkt aus, den Sie verwenden möchten, um die Maschine wiederherzustellen und klicken Sie dann auf **Weiter**.
8. Wählen Sie auf der Seite **Zuordnung** eine der folgenden Optionen, und dann führen Sie die entsprechenden Schritte aus:

   • Wählen Sie im Dropdown-Menü **Volume-ZuordnungAutomatisch** aus.

   1. Überprüfen Sie in der linken Tabelle, ob die entsprechenden Volumes aufgelistet und ausgewählt sind.

      NOTE: Bei einer BMR-Wiederherstellung sollte zumindest das Volume „System-reserviert“ und das System-Volume (normalerweise, aber nicht immer das Volume `C:\`) wiederhergestellt werden. Sie müssen mindestens ein Volume zur Durchführung einer BMR auswählen.
   2. Wählen Sie in der rechten Tabelle den/die Datenträger, auf dem/denen Sie Volumes auf der Zielmaschine zuordnen möchten.

   • Wählen Sie im Dropdown-Menü **Volume-ZuordnungManuell** aus.

   NOTE: Für das manuelle Datenträgermapping müssen Sie zuerst DiskPart in der Befehlszeile zum Erstellen und Formatieren der Ziel-Volumes verwenden. Weitere Informationen finden Sie unter Befehlszeilenoptionen für DiskPart (Standard 7 SP1) im MSDN.

   NOTE: Wenn keine Volumes auf dem Laufwerk des Computers vorhanden sind, auf dem eine BMR-Wiederherstellung durchgeführt wird, können Sie diese Option nicht anzeigen oder keine Volumes manuell zuordnen.

   - Wählen Sie unter **Ziel-Volumes** aus dem Drop-Down-Menü das entsprechende Volume für jedes Volume im Wiederherstellungspunkt.

9. Geben Sie im Textfeld **Bereitstellungszuordnungspfad** ein Ziel für die temporäre Speicherung der Zuordnungsdateien ein.

   Der Standardspeicherort ist: `X:\ProgramData\AppRecovery\IndexEntriesMaps`.

NOTE: Um sicherzustellen, dass Ihr Ziel über ausreichend freien Speicherplatz verfügt, teilen Sie die Gesamt-Volume-Kapazität durch 1.024. Beispiel: Wenn Sie die Formel `(Mount volume total capacity) / 1024 = Free space` verwenden, dann `1 TB / 1024 = 1 GB`.

10. Klicken Sie auf **Wiederherstellen**.

    Die URC ordnet die Volumes dem Datenträger/den Datenträgern zu.

11. Klicken Sie auf **Wiederherstellen**.

    Die URC stellt die Daten auf der Zielmaschine wieder her. Sie können den Fortschritt auf der Registerkarte **Wiederherstellungsfortschritt** verfolgen.

12. Nach Abschluss der Wiederherstellung entfernen Sie die Start-CD.
13. Zum Starten der BMR-Zielmaschine in Windows, den Computer neu starten.

Laden von Treibern in das Betriebssystem

In diesem Verfahren wird beschrieben, wie Sie Treiber in das Betriebssystem eines Zielcomputers für eine BMR-Wiederherstellung laden.

Um dem Betriebssystem Treiber zu injizieren, haben Sie bereits die folgenden Aufgaben abgeschlossen:

- Erstellen einer Start-CD mit dem Start-CD-Generator in der Rapid Recovery Core Console. Weitere Informationen hierzu finden Sie unter Erstellen eines ISO-Image für die Start-CD.
- Laden der Start-CD in den Zielcomputer der BMR-Wiederherstellung. Weitere Informationen hierzu finden Sie unter Laden der Start-CD und Starten der Zielmaschine.
- Laden aller erforderlichen Treiber oder Controller für Server, Speicher und Netzwerke. Weitere Informationen hierzu finden Sie unter Laden von Treibern mit der Universal Recovery Console.
- Durchführen einer Wiederherstellung mittels entweder dem Assistenten zum Wiederherstellen einer Maschine in der Rapid Recovery Core Console oder einem Archiv aus der Universellen Wiederherstellungskonsole (URC). Weitere Informationen finden Sie unter Durchführen einer Bare-Metal-Wiederherstellung von Daten unter Verwendung des Assistenten zum Wiederherstellen eines Computers und Eine BMR aus einem Archiv durchführen.

Nachdem Sie führen Sie eine Wiederherstellung durchgeführt haben, ist der Vorgang nicht beendet, bis Sie die Treiber für das Betriebssystem des Ziel-Computers der BMR-Wiederherstellung injizieren. Diese Aufgabe erfolgt zusätzlich zum Laden von Treibern in die URC.

1. Nach dem Klicken auf Wiederherstellung im BMR-Verfahren Ihrer Wahl (lesen Sie den Abschnitt Voraussetzungen), klicken Sie auf die Registerkarte **Verwaltung vorhandener Windows-Treiber**.
2. Wählen Sie aus der Dropdown-Liste das Betriebssystem aus.

   Die URC sucht nach verfügbaren Treiber.

3. Um zusätzliche Treiber zu laden, klicken Sie auf **Laden erzwingen**.
4. Navigieren Sie im Dateisystem zur komprimierten Treiberdatei und wählen Sie die Datei aus.
5. Klicken Sie auf **OK**.

   Die URC lädt die Treiber, die Sie ausgewählt haben, in das Betriebssystem.

6. Wiederholen Sie Schritt 3 bis Schritt 5 für jeden zusätzlichen Treiber, den Sie laden möchten.
7. Starten Sie den Zielcomputer der BMR-Wiederherstellung neu.

   Die BMR-Wiederherstellung wurde abgeschlossen. Wenn ein Problem nach dem Neustart auftritt, lesen Sie Beheben von Problemen beim Starten.

Durchführen einer BMR-Wiederherstellung für Linux-Maschinen

In Rapid Recovery können Sie eine BMR-Wiederherstellung (Bare Metal Restore) für eine Linux-Maschine durchführen (einschließlich der Wiederherstellung der System-Volumes). Die BMR-Wiederherstellung kann mit dem Befehlszeilenprogramm `local_mount` sowie in der Benutzeroberfläche der Core Console durchgeführt werden.

CAUTION: Rapid Recovery **unterstützt Ext2-Partition nur, wenn der Kernel 3.10 und höher ist. Wenn Sie einen früheren Kernel verwenden, konvertieren Sie alle ext2-Partitionen in ext3, ext4 oder XFS, bevor Sie beginnen die Maschine zu schützen und zu sichern.**

CAUTION: Beim ersten Start einer wiederhergestellten Linux-Maschine nach einer BMR-Wiederherstellung erstellt Rapid Recovery **ein Basisimage der wiederhergestellten Maschine. Je nach Datenmenge auf der Maschine kann dieser Vorgang länger als ein inkrementeller Snapshot dauern. Weitere Informationen für Basisimages und inkrementelle Snapshots finden Sie unter Grundlegende Informationen zu Schutzzeitplänen.**

Um eine BMR-Wiederherstellung für Linux-Maschinen durchzuführen, müssen Sie die folgenden Aufgaben ausführen.

- Verwalten eines Linux-Startimage. Das Linux Live DVD-ISO-Image wird zum Starten des Ziellaufwerks verwendet. Von dort aus können Sie auf die Universal Recovery Console zugreifen, um Sicherungen auf dem Core zu übertragen. Informationen dazu finden Sie unter Verwalten eines Linux-Startimage.
  - Um das Start-Image für die BMR zu verwenden, stellen Sie sicher, dass die LiveDVD-Version der Core-Version entspricht. Weitere Informationen finden Sie unter Informationen über das ISO-Startimage für Linux gefolgt von Herunterladen eines ISO-Start-Image für Linux.
  - Wenn zum Starten der Linux-Zielmaschine ein physischer Datenträger erforderlich ist, müssen Sie das ISO-Image für die Start-CD auf ein Medium übertragen. Informationen dazu finden Sie unter Speichern des Live DVD ISO-Image auf Datenträger.
  - In allen Fällen müssen Sie das Startimage im Zielserver laden und den Server vom Start-Image starten. Informationen dazu finden Sie unter Laden der Live DVD und Starten der Zielmaschine.
  - Nachdem Sie das Material geladen haben, müssen Sie eine Verbindung zwischen der Linux-Maschine und dem Rapid Recovery Core herstellen. Informationen dazu finden Sie unter Herstellen einer Verbindung mit dem Ziel der BMR-Wiederherstellung vom Rapid Recovery Core aus.
- Partitionen verwalten. Möglicherweise müssen Sie Partitionen erstellen oder bereitstellen, bevor Sie eine BMR für eine Linux-Maschine durchführen. Informationen dazu finden Sie unter Verwalten von Linux-Partitionen.
  - Das Linux-System, auf dem Sie eine BMR durchführen, muss die gleichen Partitionen wie die Quell-Volumes im Wiederherstellungspunkt aufweisen. Möglicherweise müssen Sie zusätzliche Partitionen auf dem Zielsystem erstellen, falls erforderlich. Informationen dazu finden Sie unter Erstellen von Partitionen auf dem Ziellaufwerk.
  - Wenn Sie eine manuelle BMR durchführen, müssen Sie die Partitionen zuerst bereitstellen. Informationen dazu finden Sie unter Breitstellen von Partitionen über die Befehlszeile. Schritte zum Bereitstellen der Partitionen sind im Prozess der BMR von der Befehlszeile aus bereits eingeschlossen. Informationen dazu finden Sie unter Starten einer BMR-Wiederherstellung für Linux-Maschinen über die Befehlszeile.

Wenn Sie die automatische Partitionierung für die BMR in der Core Console verwenden, müssen Sie keine Partitionen bereitstellen. Rapid Recovery stellt die gleichen Partitionen wieder her, die auch in den Wiederherstellungspunkten vorlagen, die Sie wiederherstellen.

- Eine BMR-Wiederherstellung für Linux starten. Nachdem die Zielmaschine vom Live-DVD-Image gestartet wurde, können Sie die BMR-Wiederherstellung starten. Die jeweils erforderlichen Aufgaben hängen davon ab, ob die Wiederherstellung in der Rapid Recovery Benutzeroberfläche oder über die Befehlszeile mit dem Dienstprogramm „local_mount“ erfolgt. Informationen dazu finden Sie unter Starten einer BMR-Wiederherstellung für Linux.
  - Wenn Sie die Core Console verwenden, müssen Sie eine Wiederherstellung aus einem Wiederherstellungspunkt auf dem Core einleiten. Informationen dazu finden Sie unter Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung.
  - Bei Verwendung der Core Console müssen Sie die Volumes über die Benutzeroberfläche zuweisen. Informationen dazu finden Sie unter Informationen über die Zuweisung der Laufwerke für eine Bare-Metal-Wiederherstellung (BMR).
  - Bei der Wiederherstellung über die Befehlszeile können Sie ggf. das Dienstprogramm „Screen“ verwenden, damit die Befehle in der Terminalkonsole übersichtlicher angezeigt werden und die Bedienung erleichtert wird. Dieses Dienstprogramm wird standardmäßig geöffnet. Wenn Sie es schließen, können Sie sie erneut starten. Weitere Informationen finden Sie unter Starten des Dienstprogramms „Screen“.
  - Wenn Sie „local_mount“ verwenden, werden alle Aufgaben über die Befehlszeile ausgeführt. Weitere Informationen finden Sie unter Starten einer BMR-Wiederherstellung für Linux-Maschinen über die Befehlszeile.
- Überprüfen einer BMR-Wiederherstellung. Nachdem die BMR-Wiederherstellung (Bare Metal Restore) gestartet wurde, können Sie den Fortschritt überprüfen und überwachen. Informationen dazu finden Sie unter Überprüfen der BMR-Wiederherstellung über die Befehlszeile.
  - Sie können den Fortschritt der Wiederherstellung überwachen. Informationen dazu finden Sie unter Anzeigen des Wiederherstellungsfortschritts.
  - Danach können Sie den wiederhergestellten Server starten. Informationen dazu finden Sie unter Starten eines wiederhergestellten Zielservers.
  - Beheben von Fehlern beim BMR. Siehe Beheben von Universal Recovery Console-Verbindungsproblemen und Beheben von Problemen beim Starten.

Voraussetzungen für eine BMR-Wiederherstellung für Linux-Maschinen

Damit Sie eine BMR-Wiederherstellung (Bare Metal Restore) für eine Linux-Maschine durchführen können, müssen die folgenden Bedingungen und Kriterien erfüllt sein:

- Vorhandensein von Sicherungen der Maschine, die wiederhergestellt werden soll. Es muss ein funktionierender Rapid Recovery Core mit Wiederherstellungspunkten des geschützten Servers vorhanden sein, der wiederhergestellt werden soll.
- Hardware für die Wiederherstellung (neu oder alt, vergleichbar oder unterschiedlich) Die Zielmaschine muss die Installationsanforderungen für einen Agenten erfüllen. Entsprechende Details finden Sie im *Rapid Recovery-Installations- und Aktualisierungshandbuch*.
- Live DVD-Start-Image. Besorgen Sie sich das Linux Live DVD-ISO-Image, das eine startfähige Linux-Version umfasst. Laden Sie es vom Rapid Recovery Lizenzportal unterhttps://licenseportal.com herunter.

Wenden Sie sich an den Quest Datenschutz-Support, wenn Probleme beim Herunterladen der Live DVD auftreten.

- Image-Datenträger und -Software. Wenn Sie physische Medien verwenden, müssen Sie über eine leere CD oder DVD sowie über eine Software zum Brennen von Datenträgern oder eine Software zum Erstellen eines ISO-Image verfügen.
- Kompatible Speichertreiber und Netzwerkadaptertreiber. Bei der Wiederherstellung auf unterschiedlicher Hardware müssen ggf. kompatible Speichertreiber und Netzwerkadaptertreiber (z. B. RAID, AHCI) für die Zielmaschine sowie Chipsatztreiber für das Zielbetriebssystem vorhanden sein.
- Speicherplatz und Partitionen je nach Bedarf. Auf der Zielfestplatte muss genügend Speicherplatz zum Erstellen der Zielpartitionen auf der Zielmaschine für die Quell-Volumes vorhanden sein. Jede Zielpartition muss mindestens so groß sein wie die ursprüngliche Quellpartition.
- Wiederherstellungspfad. Geben Sie den Pfad für die Wiederherstellung an (Pfad zum Deskriptor der Gerätedatei). Geben Sie in einem Terminalfenster den Befehl `fdisk` ein, um den Pfad für den Gerätedateideskriptor zu ermitteln.

Verwalten eines Linux-Startimage

Für eine BMR-Wiederherstellung (Bare Metal Restore) unter Linux ist ein Live DVD-Startimage erforderlich, das Sie vom Rapid Recovery Lizenzportal herunterladen können. Mit diesem Image wird die Linux-Zielmaschine gestartet. Abhängig von den jeweiligen Eigenschaften der Umgebung müssen Sie dieses Image u. U. auf ein physisches Medium übertragen (z. B. CD oder DVD). Anschließend müssen Sie das Start-Image virtuell oder physisch laden und den Linux-Server mit dem Start-Image starten.

NOTE: Die Live DVD wurde zuvor Live CD genannt.

Das Verwalten eines Linux-Startimage ist ein Schritt von Durchführen einer BMR-Wiederherstellung für Linux-Maschinen.

Sie können die folgenden Aufgaben durchführen:

- Informationen über das ISO-Startimage für Linux
- Speichern des Live DVD ISO-Image auf Datenträger
- Laden der Live DVD und Starten der Zielmaschine
- Herstellen einer Verbindung mit dem Ziel der BMR-Wiederherstellung vom Rapid Recovery Core aus

Informationen über das ISO-Startimage für Linux

Bei der Durchführung einer BMR-Wiederherstellung (Bare Metal Restore) für eine Linux-Maschine muss zunächst das ISO-Image für die Linux Live DVD vom Rapid Recovery Lizenzportal heruntergeladen werden. Die Live DVD funktioniert mit allen Linux-Dateisystemen, die Rapid Recovery unterstützt. Sie enthält eine startfähige Linux-Version, ein Bildschirm-Dienstprogramm sowie die Benutzeroberfläche der Universellen Wiederherstellungskonsole für Rapid Recovery. Bei der Universellen Wiederherstellungskonsole für Rapid Recovery handelt es sich um eine Umgebung, mit der das Systemlaufwerk oder ein ganzer Server direkt vom Rapid Recovery Core aus wiederhergestellt werden kann.

NOTE: Die ISO (International Organization for Standardization) ist eine internationale Organisation von Vertretern aus verschiedenen nationalen Organisationen, die Normen für Dateisysteme festlegt. ISO 9660 ist eine Norm für Dateisysteme, die für optische Datenträger zum Austausch von Daten verwendet wird und mehrere Betriebssysteme unterstützt. Ein ISO-Image ist die Archivdatei oder das Datenträger-Image, das die Daten der einzelnen Sektoren sowie das Dateisystem des Datenträgers enthält.

Herunterladen eines ISO-Start-Image für Linux

Zum Abschließen einer Bare-Metal-Wiederherstellung für eine Linux-Maschine benötigen Sie ein Live-DVD ISO-Image, das Ihrer Version von Rapid Recovery entspricht. Die aktuelle Version von Live-DVD ist vom Rapid Recovery Lizenzportal unter https://licenseportal.com erhältlich. Wenn Sie eine andere Version benötigen, wenden Sie sich an Quest Datenschutz-Support.

NOTE: Weitere Informationen zu Rapid Recovery Lizenzportal finden Sie im *Rapid Recovery Lizenzportal - Benutzerhandbuch.*

Diese Aufgabe ist ein Schritt in Durchführen einer BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Verwalten eines Linux-Startimage.

Zum Herunterladen des Live-DVD ISO-Image führen Sie die Schritte in diesem Verfahren aus.

1. Melden Sie sich bei der Rapid Recovery Lizenzportal unter https://licenseportal.com an.
2. Klicken Sie im linken Navigationsmenü auf **Downloads**.

   Die Seite **Downloads** wird angezeigt.
3. Blättern Sie nach unten zu Linux-basierten Anwendungen und klicken Sie im Linux Live DVD-Abschnitt auf **Herunterladen**.
4. Speichern Sie das Live DVD ISO-Image.

   NOTE: Wenn Sie eine virtuelle Maschine wiederherstellen, speichern Sie das Image an einem Speicherort im Netzwerk und legen anschließend fest, dass die VM von einem CD- oder DVD-Laufwerk mit dem Image startet.
5. Wenn Sie von einer physischen Maschine wiederherstellen, brennen Sie das ISO-Image für die Start-CD auf eine CD (Compact Disc) oder Digital Video Disk (DVD), von der die Zielmaschine gestartet werden kann. Weitere Informationen hierzu finden Sie unter Speichern des Live DVD ISO-Image auf Datenträger.

Speichern des Live DVD ISO-Image auf Datenträger

Beim Herunterladen der Linux Live DVD-Datei wird diese als ISO-Image im angegebenen Pfad gespeichert. Sie müssen in der Lage sein, die Linux Ziel-Maschine aus dem Live DVD-Image zu starten.

Diese Aufgabe ist ein Schritt in Durchführen einer BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Verwalten eines Linux-Startimage.

1. Das ISO-Image der Start-CD auf CD- oder DVD-Datenträger brennen.

   Beim Durchführen einer BMR auf einer virtuellen Maschine ist dieser Schritt nicht erforderlich. Laden Sie das ISO-Image einfach in ein Laufwerk und bearbeiten Sie die Einstellungen der VM so, dass sie von diesem Laufwerk aus gestartet wird. Sie können auch virtuellen Export zum Wiederherstellen einer Linux-VM verwenden. Weitere Informationen hierzu finden Sie unter VM-Export.

Laden der Live DVD und Starten der Zielmaschine

Nachdem Sie das Live-DVD ISO-Image erhalten haben, starten Sie die Linux-Maschine von der neu erstellten Live-DVD.

Diese Aufgabe ist ein Schritt in Durchführen einer BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Verwalten eines Linux-Startimage.

1. Navigieren Sie zum neuen Server und laden Sie das Live-DVD-Image vom entsprechenden Speicherort herunter. Geben Sie an, dass der Server vom Live DVD-Image starten soll.
2. Starten Sie die Maschine.

   Daraufhin werden eine Rapid Recovery Begrüßungsanzeige angezeigt und ein Terminalfenster wird geöffnet, in dem die IP-Adresse sowie das Authentifizierungskennwort für die Maschine angezeigt werden.

NOTE: Bei jedem Starten der Maschine mit dem Live DVD-Image wird ein neues temporäres Kennwort generiert.

3. Notieren Sie sich die auf dem Einführungsbildschirm angezeigte IP-Adresse und das Authentifizierungskennwort. Sie benötigen diese Information später während des Datenwiederherstellungsvorgangs, um sich wieder bei der Konsole anzumelden.

Herstellen einer Verbindung mit dem Ziel der BMR-Wiederherstellung vom Rapid Recovery Core aus

Nachdem der Linux-Zielcomputer mit der Live DVD gestartet wurde, kann vom Kern aus eine Verbindung zu diesem Computer hergestellt und der BMR-Wiederherstellungsvorgang gestartet werden. Sie haben dazu zwei Möglichkeiten:

- Starten eines Wiederherstellungsvorgangs vomRapid Recovery Core Console aus. Weitere Informationen finden Sie unter Starten einer BMR-Wiederherstellung für Linux.
- Starten einer Wiederherstellung über die Befehlszeile mit dem Dienstprogramm „local_mount“. Weitere Informationen finden Sie unter Starten einer BMR-Wiederherstellung für Linux-Maschinen über die Befehlszeile.

Verwalten von Linux-Partitionen

Beim Durchführen einer BMR muss das Ziel-Laufwerk, auf dem Sie Daten wiederherstellen werden, die gleichen Partitionen aufweisen wie im Wiederherstellungspunkt, den Sie wiederherstellen. Möglicherweise müssen Sie Partitionen erstellen, um diese Anforderung zu erfüllen.

Sie können die Wiederherstellung in der Befehlszeile mit dem Dienstprogramm „local_mount“ oder über die Rapid Recovery Core Console starten. Bei der Wiederherstellung über die Benutzeroberfläche müssen Sie die Partitionen zuerst bereitstellen.

Das Verwalten der Linux-Partitionen ist ein Schritt in Durchführen einer BMR-Wiederherstellung für Linux-Maschinen.

Sie können die folgenden Aufgaben durchführen:

Zugehörige Tasks

See also: Erstellen von Partitionen auf dem Ziellaufwerk
See also: Formatieren von Partitionen auf dem Ziellaufwerk
See also: Breitstellen von Partitionen über die Befehlszeile

Erstellen von Partitionen auf dem Ziellaufwerk

Häufig ist beim Durchführen einer BMR das Ziellaufwerk ein neues Volume, das aus einer einzelnen Partition besteht. Das Laufwerk auf der Zielmaschine muss die gleiche Partitionstabelle wie im Wiederherstellungspunkt aufweisen, einschließlich der Größe der Volumes. Wenn das Ziellaufwerk nicht die gleichen Partitionen enthält, müssen Sie diese erstellen, bevor Sie die Bare-Metal-Wiederherstellung durchführen. Verwenden Sie das Dienstprogramm fdisk zum Erstellen von Partitionen auf dem Ziellaufwerk entsprechend den Partitionen auf dem Quelllaufwerk.

CAUTION: Das folgende Verfahren dient nur als Beispiel. Kundenumgebungen können unterschiedlich sein. Sie sollten die Befehle ändern, die Sie für die Anpassung der Einzelheiten an Ihre Umgebung verwenden.

Diese Aufgabe ist ein Schritt in Durchführen einer BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Verwalten von Linux-Partitionen.

1. Optional können Sie das Dienstprogramm „Screen“ verwenden. Dieses Dienstprogramm startet standardmäßig und bleibt aktiv, bis Sie die Maschine neu starten.

NOTE: Falls Sie explizit schließen und es erneut öffnen möchten, siehe Starten des Dienstprogramms „Screen“.

2. Geben Sie von der Befehlszeile aus den folgenden Befehl ein und drücken Sie dann die **Eingabetaste,**, um Berechtigungen zum Ausführen als Administrator zu ändern, und zeigen Sie dann die Liste vorhandener Laufwerkspartitionen an:

   ```
   sudo fdisk -l
   ```

   Eine Liste aller Volumes wird angezeigt.

   In diesem Beispiel wird davon ausgegangen, dass das Volume, das Sie partitionieren möchten, /dev/sda ist. Wenn sich Ihr Volume davon unterscheidet (z. B. für ältere Laufwerke, sehen Sie möglicherweise /dev/hda), ändern Sie die Befehle entsprechend.

3. Geben Sie den folgenden Befehl ein, um eine neue Startpartition zu erstellen, und drücken Sie die **Eingabetaste**:

   ```
   sudo fdisk /dev/sda
   ```

4. Geben Sie den folgenden Befehl ein, um eine neue Startpartition zu erstellen, und drücken Sie die **Eingabetaste**:

   ```
   n
   ```

5. Geben Sie den folgenden Befehl ein, um eine neue primäre Partition zu erstellen, und drücken Sie die **Eingabetaste**:

   ```
   p
   ```

6. Zum Festlegen der Partitionsnummer geben Sie die Nummer der Partition ein und drücken die **Eingabetaste**. Geben Sie zum Beispiel Partition 1, Typ 1 an und drücken Sie die **Eingabetaste**.
7. Um den ersten Sektor, 2048, zu verwenden, drücken Sie die **Eingabetaste**.
8. Weisen Sie der Startpartition eine entsprechende Menge an Speicherplatz zu, indem Sie auf das Pluszeichen drücken und die zugewiesene Menge eingeben. Drücken Sie dann die **Eingabetaste**.

   Beispiel: Um der Startpartition 500 M zuzuweisen, geben Sie die Folgendes ein und drücken dann die **Eingabetaste**:

   ```
   +512000K
   ```

9. Um der Startpartition eine startfähige Markierung hinzuzufügen (damit die Partition startfähig wird), geben Sie den folgenden Befehl ein und drücken die **Eingabetaste**:

   ```
   a
   ```

10. Um einer bestimmten Partition eine startfähige Markierung zuzuweisen, geben Sie die Nummer der Partition ein und drücken die **Eingabetaste**. Um beispielsweise Partition 1 eine startfähige Markierung zuzuweisen, geben Sie 1 ein und drücken die **Eingabetaste**.
11. Partitionieren der Festplatte nach Bedarf fortsetzen.
12. Um alle Änderungen im Dienstprogramm fdisk zu speichern, geben Sie den folgenden Befehl ein und drücken die **Eingabetaste**:

    w

Formatieren von Partitionen auf dem Ziellaufwerk

Nach dem Erstellen von Partitionen auf einem neuen Volume auf dem Ziellaufwerk, müssen Sie, um Bare-Metal-Wiederherstellung durchzuführen, wenn Sie nicht die automatische Partition verwenden, die Partitionen formatieren, bevor sie geladen werden können. Wenn diese Situation auf Sie zutrifft, folgen Sie diesem Verfahren, um die Partitionen im ext3-, ext4- oder XFS-Format zu formatieren.

In allen anderen Szenarien brauchen Sie gemäß der Beschreibung in diesem Thema keine Partitionen zu formatieren.

Diese Aufgabe ist ein Schritt in Durchführen einer BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Verwalten von Linux-Partitionen.

1. Optional können Sie das Dienstprogramm „Screen“ verwenden. Dieses Dienstprogramm startet standardmäßig und bleibt aktiv, bis Sie die Maschine neu starten.

   NOTE: Falls Sie explizit schließen und es erneut öffnen möchten, siehe Starten des Dienstprogramms „Screen“.

2. Geben Sie von der Befehlszeile aus den folgenden Befehl ein und drücken Sie dann die **Eingabetaste**,, um Berechtigungen zum Ausführen als Administrator zu ändern, und zeigen Sie dann die Liste vorhandener Laufwerkspartitionen an:

   ```
   sudo fdisk -l
   ```

   Eine Liste aller Volumes wird angezeigt.

   In diesem Beispiel wird davon ausgegangen, dass Sie die Partition, die Sie partitionieren möchten, /dev/sda1 ist. Wenn sich Ihr Volume davon unterscheidet (z. B. für ältere Laufwerke, sehen Sie möglicherweise /dev/hda), ändern Sie die Befehle entsprechend.

3. Wählen Sie einen der folgenden Befehle, basierend auf dem Format, das Sie für die Ziel-Partition verwenden möchten:

   - Geben Sie den folgenden Befehl ein, um eine Partition im ext3-Format zu formatieren, und drücken Sie die **Eingabetaste**:

     ```
     sudo mkfs.ext3 /dev/sda1
     ```

   - Geben Sie den folgenden Befehl ein, um eine Partition im ext4-Format zu formatieren und drücken Sie die **Eingabetaste**:

     ```
     sudo mkfs.ext4 /dev/sda1
     ```

   - Geben Sie den folgenden Befehl ein, um eine Partition im XFS-Format zu formatieren und drücken Sie die **Eingabetaste**:

     ```
     sudo mkfs.xfs /dev/sda1
     ```

     Die ausgewählte Partition wird entsprechend formatiert.

4. Wenn Sie andere Partitionen formatieren müssen, wiederholen Sie dieses Verfahren.

Breitstellen von Partitionen über die Befehlszeile

Bei der Durchführung einer BMR-Wiederherstellung mit der Rapid Recovery Core Console müssen Sie zuerst die entsprechenden Partitionen auf der Zielmaschine bereitstellen. Führen Sie diesen Vorgang über die Befehlszeile in der Universal Recovery Console aus.

Diese Aufgabe ist ein Schritt in Durchführen einer BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Verwalten von Linux-Partitionen.

Führen Sie die Schritte in diesem Verfahren zum Bereitstellen von Partitionen auf der Linux-Maschine aus, bevor Sie eine Wiederherstellung ausführen.

1. Geben Sie von der Befehlszeile aus den folgenden Befehl ein und drücken Sie dann die **Eingabetaste**,, um Berechtigungen zum Ausführen als Administrator zu ändern, und zeigen Sie dann die Liste vorhandener Laufwerkspartitionen an:

   ```
   sudo fdisk -l
   ```

   Eine Liste aller Volumes wird angezeigt.

2. Formatieren Sie alle Partitionen, auf denen Sie die BMR ausführen müssen, um das Verzeichnis bereitzustellen. Diese müssen mit den Volumes im Wiederherstellungspunkt übereinstimmen. Wenn das Volume, das Sie bereitstellen möchten, mit sda1 bezeichnet ist und das Bereitstellungsverzeichnis „/mnt“ ist, geben Sie den folgenden Befehl ein und drücken die **Eingabetaste**:
3. Stellen Sie alle Partitionen bereit, auf denen Sie die BMR ausführen müssen, um das Verzeichnis bereitzustellen. Diese müssen mit den Volumes im Wiederherstellungspunkt übereinstimmen. Wenn das

Volume, das Sie bereitstellen möchten, mit sda1 bezeichnet ist und das Bereitstellungsverzeichnis „/mnt“ ist, geben Sie den folgenden Befehl ein und drücken die **Eingabetaste**:

```
mount /dev/sda1 /mnt
```

4. Wiederholen Sie Schritt 3, bis alle erforderlichen Volumes bereitgestellt wurden.

   Nachdem die Volumes bereitgestellt wurden, können Sie in der Rapid Recovery Core Console eine Wiederherstellung auf die Linux-Zielmaschine durchführen. Siehe Starten einer BMR-Wiederherstellung für Linux.

Starten einer BMR-Wiederherstellung für Linux

Um eine BMR-Wiederherstellung für Linux-Computer durchzuführen, müssen die folgenden Bedingungen erfüllt sein:

- Um einen Wiederherstellungspunkt im Core wiederherzustellen, muss eine geeignete Hardware vorhanden sein. Weitere Informationen finden Sie unter Voraussetzungen für eine BMR-Wiederherstellung für Linux-Maschinen.
- Die Linux-Zielmaschine für die BMR-Wiederherstellung muss mit dem Live DVD-Start-Image gestartet werden. Weitere Informationen finden Sie unter Verwalten eines Linux-Startimage.
- Die Anzahl der Volumes auf der Linux-Maschine, die wiederhergestellt werden soll, muss mit der Anzahl der Volumes im Wiederherstellungspunkt übereinstimmen. Sie müssen außerdem entscheiden, ob die Wiederherstellung von der Rapid Recovery Core Console aus oder über die Befehlszeile mit „local_mount“ durchgeführt werden soll. Weitere Informationen finden Sie unter Verwalten von Linux-Partitionen.
- Bei einer Wiederherstellung über die Benutzeroberfläche der Core Console muss zunächst der entsprechende Wiederherstellungspunkt ausgewählt werden, um eine BMR-Wiederherstellung zu starten. Anschließend müssen die Wiederherstellung auf der Hardware eingeleitet und IP-Adresse und temporäres Kennwort, das von der Universal Recovery Console ermittelt wurde, angegeben werden. Anschließend müssen Sie die Laufwerke zuordnen und die Wiederherstellung starten.

Dieser Prozess ist ein Schritt von Durchführen einer BMR-Wiederherstellung für Linux-Maschinen.

Führen Sie die folgenden Aufgaben durch, um eine BMR-Wiederherstellung über die Rapid Recovery Core Console zu starten.

- Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung
- Informationen über die Zuweisung der Laufwerke für eine Bare-Metal-Wiederherstellung (BMR)

Bei einer Wiederherstellung über die Befehlszeile mit dem Dienstprogramm „local_mount“ müssen Sie zuerst die entsprechenden Berechtigungen aktivieren, Volumes bereitstellen, „local_mount“ ausführen, Informationen zum Kern aus der Liste der Computer abrufen, eine Verbindung zum Kern herstellen, eine Liste der Wiederherstellungspunkte abrufen, den Wiederherstellungspunkt auswählen, der für die BMR-Wiederherstellung verwendet werden soll, und die Wiederherstellung starten.

Optional können Sie das Dienstprogramm „Screen“ starten.

Führen Sie die folgenden Aufgaben durch, um eine BMR-Wiederherstellung über die Befehlszeile zu starten.

- Starten des Dienstprogramms „Screen“
- Starten einer BMR-Wiederherstellung für Linux-Maschinen über die Befehlszeile

Starten des Dienstprogramms „Screen“

Auf dem Live-DVD-Bildschirm ist ein Dienstprogramm verfügbar, wenn Sie aus der Live-DVD in die Universal Recovery Console starten. Screen ermöglicht Benutzern die Verwaltung mehrerer Shells gleichzeitig über eine einzige SecureShell (SSH)-Sitzung oder ein Konsolenfenster. Sie können damit eine Aufgabe in einem Terminalfenster durchführen (z. B. gemountete Volumes überprüfen) und parallel dazu eine weitere Shell-Instanz

öffnen oder verwenden, um eine andere Aufgabe durchzuführen (z. B. das Dienstprogramm „local_mount“ ausführen).

Das Screen-Dienstprogramm verfügt über einen eigenen Bildlaufleiste-zurück-Puffer, mit dem Sie den Bildschirm scrollen können, um größere Datenmengen, wie etwa eine Liste der Wiederherstellungspunkte, anzeigen zu können.

NOTE: Dieses Dienstprogramm dient ausschließlich Informationszwecken; die Verwendung des Dienstprogramms „Screen“ ist optional.

Das Dienstprogramm „Screen“ wird auf der Maschine mit der Live DVD als Standardeinstellung gestartet. Wenn Sie diese Anwendung jedoch geschlossen haben, müssen Sie das Dienstprogramm „Screen“ von der Live DVD mithilfe des nachstehenden Verfahrens starten.

1. Geben Sie im Terminalfenster „screen“ ein, wenn die Maschine von der Live DVD gestartet wurde und drücken Sie die **Eingabetaste**.

   Das Dienstprogramm „Screen“ wird gestartet.

Starten einer BMR-Wiederherstellung für Linux-Maschinen über die Befehlszeile

Wenn das Live DVD ISO-Image auf der Maschine, auf der die BMR-Wiederherstellung durchgeführt werden soll, verfügbar ist sowie Anzahl und Größe der Volumes von Zielmaschine und Wiederherstellungspunkt, der für die BMR-Wiederherstellung verwendet werden soll, übereinstimmen, können Sie die Wiederherstellung in der Befehlszeile mit dem Dienstprogramm local_mount starten.

NOTE: Diese Komponente wurde früher als `aamount` bezeichnet.

Informationen zum Durchführen einer BMR-Wiederherstellung in der Rapid Recovery Core Console-Benutzeroberfläche finden Sie unter Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung.

NOTE: Versuchen Sie beim Ausführen dieses Verfahrens nicht, Wiederherstellungspunkte im Ordner „/tmp“ bereitzustellen, da dieser die rapidrecovery-vdisk-Dateien (ehemals aavdisk) enthält.

Diese Aufgabe ist ein Schritt in Durchführen einer BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Starten einer BMR-Wiederherstellung für Linux-Maschinen über die Befehlszeile.

Führen Sie die Schritte in diesem Verfahren durch, um einen Wiederherstellungspunkt im Core auszuwählen, auf den für die physische oder virtuelle BMR Zielmaschine ein Rollback durchgeführt werden soll.

1. Geben Sie den folgenden Befehl ein, um das Rapid Recovery-Dienstprogramm local_mount als „root“ auszuführen, und drücken Sie die **Eingabetaste**:

   ```
   sudo local_mount
   ```

2. Geben Sie den folgenden Befehl ein, um die geschützten Maschinen aufzulisten, und drücken Sie die **Eingabetaste**:

   ```
   lm
   ```

3. Geben Sie die Verbindungsinformationen für den Rapid Recovery Core ein (siehe Beschreibung in der folgenden Tabelle), wenn Sie dazu aufgefordert werden. Drücken Sie nach jeder Eingabe die **Eingabetaste**:

Tabelle 148. Rapid Recovery Core **Verbindungsinformationen**

Textfeld	Description	Erforderlich
Rapid Recovery Core IP-Adresse oder Hostname	Die IP-Adresse bzw. der Hostname des Rapid Recovery Core.	Ja

Textfeld	Description	Erforderlich
Domain	Die Domain des Rapid Recovery Core. Dies ist optional.	Nein
Benutzer	Der Benutzername eines Benutzers mit Administratorrechten im Core	Ja
Kennwort	Das Passwort, mit dem der Benutzer mit Administratorrechten eine Verbindung zum Core hergestellt hat.	Ja

Es wird eine Liste der vom Rapid Recovery Core geschützten Maschinen angezeigt. Enthalten ist eine Auflistung der gefundenen Maschinen mit deren laufender Zeilennummer, Host-Anzeigename oder IP-Adresse und einer ID-Nummer für die Maschine.

4. Um die Wiederherstellungspunkte für die Maschine aufzulisten, die Sie wiederherstellen möchten, geben Sie den Befehl zum Auflisten der Wiederherstellungspunkte mit der folgenden Syntax ein und drücken die **Eingabetaste**:

   ```
   lr <machine_line_item_number>
   ```

   NOTE: Sie können in diesem Befehl auch die ID-Nummer der Maschine anstelle der laufenden Zeilennummer angeben.

   Daraufhin werden die Basiswiederherstellungspunkte und die inkrementellen Wiederherstellungspunkte für die betreffende Maschine angezeigt. Diese Liste umfasst:

   - Eine Zeilennummer
   - Datums- und Zeitstempel
   - Ein alphabetische Liste von Volumes innerhalb des Wiederherstellungspunkts
   - Speicherort des Volumes
   - Größe des Wiederherstellungspunkts
   - Die ID-Nummer des Volume, einschließlich einer Folgenummer am Ende, die den Wiederherstellungspunkt identifiziert

5. Um den Wiederherstellungspunkt für die Wiederherstellung auszuwählen, geben Sie den folgenden Befehl ein und drücken die **Eingabetaste**:

   ```
   r <recovery_point_ID_number> <path>
   ```

   CAUTION: Sie müssen sicherstellen, dass das Systemvolume nicht bereitgestellt ist.

   NOTE: Wenn Sie die Maschine von der Live-DVD gestartet haben, ist das Systemvolume nicht bereitgestellt.

   Dieser Befehl führt ein Rollback des Volume-Image mit der angegebenen ID vom Core im angegebenen Pfad durch. Der Pfad für die Wiederherstellung ist der Pfad für den Deskriptor der Gerätedatei und nicht das Bereitstellungsverzeichnis.

NOTE: Sie können im Befehl auch die Zeilennummer anstelle der ID-Nummer für den Wiederherstellungspunkt angeben, um den Wiederherstellungspunkt anzugeben. In diesem Fall müssen Sie die Zeilennummer für Agent/Maschine (in der `lm`-Ausgabe), gefolgt von der Zeilennummer des Wiederherstellungspunkts und dem Volume-Buchstaben (aus der alphabetischen Liste der Volumes im Wiederherstellungspunkt) und dahinter den Pfad angeben. Beispiel:

```
r <machine_line_item_number> <base_image_recovery_point_line_number>
<volume_letter> <path>
```

Beispiel: `r 1 24 a /dev/sda1`

In diesem Befehl ist `<Pfad>` der Dateideskriptor für das eigentliche Volume.

6. Geben Sie y für Ja ein, wenn Sie aufgefordert werden, den Vorgang fortzusetzen und drücken Sie die **Eingabetaste**.

   Sobald die Wiederherstellung fortgesetzt wird, werden entsprechende Meldungen angezeigt, die Sie über den Status der Wiederherstellung informieren.

   NOTE: Falls eine Ausnahmemeldung angezeigt wird, finden Sie die zugehörigen Details für die Ausnahme in der Datei „local_mount“. Die Datei „local_mount.log“ befindet sich in `/var/log/apprecovery`.

7. Beenden Sie local_mount, wenn die Wiederherstellung erfolgreich durchgeführt wurde, indem Sie `exit` eingeben und dann die **Eingabetaste** drücken.
8. Ihr nächster Schritt ist die Überprüfung der Wiederherstellung. Weitere Informationen hierzu finden Sie unter Überprüfen der BMR-Wiederherstellung über die Befehlszeile.

Wiederherstellen von Volumes einer Linux-Maschine über die Befehlszeile

Vor der Wiederherstellung aus einem Wiederherstellungspunkt über die Befehlszeile müssen Sie die Bereitstellung des Datenträgers aufheben, auf dem Sie Daten wiederherstellen werden.

In Rapid Recovery können Sie Volumes von geschützten Linux-Maschinen mit dem Befehlszeilenprogramm `local_mount` wiederherstellen.

NOTE: Dieser Prozess wurde früher als Rollback bezeichnet. Versuchen Sie beim Ausführen dieses Verfahrens nicht, Wiederherstellungspunkte im Ordner „/tmp“ bereitzustellen, da dieser die rapidrecovery-vdisk-Dateien (ehemals aavdisk) enthält. Die Wiederherstellung von Volumes für geschützte Maschinen ist auch in der Rapid Recovery Core Console möglich. Weitere Informationen finden Sie unter Informationen über das Wiederherstellen von Volumes aus Wiederherstellungspunkten.

CAUTION: Informationen zum Wiederherstellen der System- oder Root-Partition (/) bzw. des gesamten Betriebssystems finden Sie unter Durchführen einer BMR-Wiederherstellung für Linux-Maschinen.

1. Führen Sie das Dienstprogramm Rapid Recovery`local_mount` als Root aus, z. B.:

   ```
   sudo local_mount
   ```

2. Geben Sie den folgenden Befehl in die Rapid Recovery Bereitstellungsaufforderung ein, um die geschützten Maschinen aufzulisten.

   ```
   lm
   ```

3. Wenn Sie dazu aufgefordert werden, geben Sie die IP-Adresse oder den Hostnamen Ihres Rapid Recovery Core Core-Servers an.
4. Geben Sie die Anmeldeinformationen (Benutzername und Kennwort) für den Server ein.

   Es wird eine Liste der vom jeweiligen Rapid Recovery Core-Server geschützten Maschinen angezeigt. Enthalten ist eine Auflistung der gefundenen geschützten Maschinen mit deren

laufender Zeilennummer, Host/IP-Adresse und einer ID-Nummer für die Maschine. (Beispiel: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2).

5. Geben Sie den folgenden Befehl ein, um die derzeit bereitgestellten Wiederherstellungspunkte für die angegebene Maschine anzuzeigen:

   ```
   lr <machine_line_item_number>
   ```

   NOTE: Sie können in diesem Befehl auch die ID-Nummer der Maschine anstelle der laufenden Zeilennummer angeben.

   Daraufhin werden die Basiswiederherstellungspunkte und die inkrementellen Wiederherstellungspunkte für die betreffende Maschine angezeigt. Diese Liste umfasst eine laufende Zeilennummer, Datum/Zeitstempel, Speicherort des Volumes, Größe des Wiederherstellungspunkts und eine ID-Nummer für das Volume mit einer laufenden Nummer am Ende (beispielsweise ”293cc667-44b4-48ab-91d8-44bc74252a4f:2”), die den Wiederherstellungspunkt kennzeichnet.

6. Geben Sie den folgenden Befehl ein, um einen Wiederherstellungspunkt für die Wiederherstellung auszuwählen:

   ```
   r <volume_recovery_point_ID_number> <device path>
   ```

   Dieser Befehl stellt das Volume-Image mit der angegebenen ID vom Core im angegebenen Pfad wieder her. Der Pfad für die Wiederherstellung ist der Pfad für den Deskriptor der Gerätedatei und nicht das Bereitstellungsverzeichnis.

   - Sie können im Befehl auch die Zeilennummer anstelle der ID-Nummer für den Wiederherstellungspunkt angeben, um den Wiederherstellungspunkt anzugeben. In diesem Fall müssen Sie die Zeilennummer des Computer (in der lm-Ausgabe) gefolgt von der Zeilennummer des Wiederherstellungspunkts und dem Volume-Buchstaben und dahinter den Pfad angeben, z. B. „r <Zeilennummer_für_Computer> <Zeilennummer_für_Wiederherstellungspunkt> <Volume-Buchstabe> <Pfad>“. In diesem Befehl ist <Pfad> der Dateideskriptor für das eigentliche Volume.

     Wenn zum Beispiel die `lm` Ausgabe drei geschützte Maschinen aufführt, Sie den Befehl `lr` für die geschützte Maschine Nummer `2` eingeben und die `23` Wiederherstellungspunktvolume `b` auf das Volume wiederherstellen möchten, das im Verzeichnis `/dev/sda5`, bereitgestellt wurde, würde der Befehl wie folgt lauten:

     ```
     r2 23 b /dev/sda5
     ```

     NOTE: Es ist möglich, eine Wiederherstellung auf / bei Bedarf durchzuführen. Wenn die Durchführung einer BMR-Wiederherstellung mit einer Live DVD erfolgt, wird angenommen, dass Sie auf einem anderen Computer wiederherstellen möchten. Weitere Informationen hierzu finden Sie unter Starten einer BMR-Wiederherstellung für Linux.

7. Geben Sie `y` für „Ja“ ein, wenn Sie aufgefordert werden, den Vorgang fortzusetzen.

   Sobald die Wiederherstellung fortgesetzt wird, werden entsprechende Meldungen angezeigt, die Sie über den Status informieren.

8. Bei einer erfolgreichen Wiederherstellung stellt das Dienstprogramm `local_mount` automatisch wieder das Kernel-Modul im wiederhergestellten Volume bereit, wenn das Ziel vorher geschützt und bereitgestellt war. Andernfalls müssen Sie das wiederhergestellte Volume auf der lokalen Festplatte bereitstellen (z. B. mit dem Befehl `sudo mount`) und anschließend überprüfen, ob die Dateien wiederhergestellt wurden (z. B. mit dem Befehl `ls`).

Überprüfen einer BMR-Wiederherstellung

Nachdem Sie eine BMR-Wiederherstellung (Bare Metal Restore) durchgeführt haben, können Sie den Fortschritt der Wiederherstellung überprüfen. Wenn der Vorgang erfolgreich durchgeführt wurde, können Sie den wiederhergestellten Server starten. Auch einige Informationen zur Fehlerbehebung sind vorhanden, wenn beim

Herstellen der Verbindung zur Universellen Wiederherstellungskonsole zum Durchführen der Wiederherstellung oder beim Neustart des wiederhergestellten Computers Probleme auftreten.

Sie können die folgenden Aufgaben durchführen:

- Anzeigen des Wiederherstellungsfortschritts
- Starten eines wiederhergestellten Zielservers
- Beheben von Universal Recovery Console-Verbindungsproblemen
- Beheben von Problemen beim Starten

Anzeigen des Wiederherstellungsfortschritts

Führen Sie die Schritte in diesem Verfahren durch, um den Fortschritt der Datenwiederherstellung aus einem Wiederherstellungspunkt anzuzeigen, die in der Rapid Recovery Core Console eingeleitet wurde (einschließlich BMR-Wiederherstellung).

1. Nachdem die Wiederherstellung aus einem Wiederherstellungspunkt gestartet wurde, können Sie den Fortschritt über das Dropdown-Menü **Aktive Aufgaben** in der Core Console anzeigen, während die Aufgabe durchgeführt wird.
2. Optional können Sie detaillierte Informationen auf der Seite **Ereignisse** anzeigen. Weitere Informationen zur Überwachung von Rapid Recovery Ereignissen finden Sie unter Anzeigen von Ereignissen mithilfe von Aufgaben, Warnungen und Journalseiten.

Starten eines wiederhergestellten Zielservers

Führen Sie die nachstehend beschriebenen Schritte aus, um den wiederhergestellten Zielserver zu starten.

NOTE: Bevor Sie den wiederhergestellten Zielserver starten, sollten Sie überprüfen, ob die Wiederherstellung erfolgreich durchgeführt wurde. Weitere Informationen hierzu finden Sie unter Anzeigen des Wiederherstellungsfortschritts.

Diese Aufgabe ist ein Schritt in Durchführen einer BMR-Wiederherstellung für Windows-Computer. Dieser ist Bestandteil des Prozesses zum Überprüfen einer BMR-Wiederherstellung.

1. Überprüfen Sie auf dem Zielserver, dass die Rapid Recovery Universelle Wiederherstellungskonsole aktiv ist.
2. Entnehmen Sie die Start-CD aus dem wiederhergestellten Server (oder trennen Sie den physischen Datenträger mit dem Start-CD-Image).
3. Klicken Sie in der Universellen Wiederherstellungskonsole auf das Einschalt-Menüsymbol am oberen Rand des Bildschirms und klicken Sie dann auf **Neu starten**.
4. Geben Sie an, dass das Betriebssystem normal gestartet werden soll.
5. Melden Sie sich bei der Maschine an. Das wiederhergestellte System sollte auf den im Wiederherstellungspunkt erfassten Zustand gesetzt worden sein.

Beheben von Universal Recovery Console-Verbindungsproblemen

Nachstehend finden Sie einige Informationen zum Beheben von Problemen beim Herstellen einer Verbindung zum Start-CD-Image als Teil des Prozesses für Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung.

Wenn eine Fehlermeldung angezeigt wird, die angibt, dass der Core keine Verbindung mit dem Remote-Server herstellen konnte, kann es dafür mehrere mögliche Ursachen geben.

- Vergewissern Sie sich, dass die in der URC angezeigte IP-Adresse und das aktuelle Kennwort mit den Informationen übereinstimmen, die Sie im Dialogfeld „Recovery Console-Instanz“ eingegeben haben.
- Um den Server erreichen zu können, auf dem die Daten wiederhergestellt sollen, muss der Core in der Lage sein, den Server im Netzwerk zu identifizieren. Um festzustellen, ob Server-Identifikation möglich ist, können Sie auf dem Core eine Eingabeaufforderung öffnen und einen Ping-Befehl an die IP-Adresse des BMR-Zielservers absetzen. Sie können auch auf dem Zielserver eine Eingabeaufforderung öffnen und die IP-Adresse des Rapid Recovery Core anpingen.
- Vergewissern Sie sich, dass die Netzwerkadaptereinstellungen zwischen Core und Ziel-BMR-Server kompatibel sind.

Beheben von Problemen beim Starten

Die folgenden Aufgaben sind Voraussetzung für dieses Verfahren.

- Erstellen eines ISO-Image für die Start-CD
- Laden der Start-CD und Starten der Zielmaschine
- Laden von Treibern mit der Universal Recovery Console

Führen Sie die folgenden Schritte aus, um Startprobleme zu beheben. Denken Sie daran, dass Sie bei der Wiederherstellung auf einer anderen Hardware Speichercontroller-, RAID-, AHCI-, Chipsatz- und andere Treiber injizieren müssen, wenn diese noch nicht auf der Start-CD vorhanden sind. Diese Treiber ermöglichen es dem Betriebssystem, alle Geräte auf Ihrem Zielserver erfolgreich zu betreiben. Weitere Informationen finden Sie unter Laden von Treibern mit der Universal Recovery Console. Führen Sie die folgenden Verfahren zum Reparieren von Startproblemen auf Ihrem Zielserver aus.

1. Klicken Sie von der Universal Recovery Console auf die Registerkarte **Vorhandener Windows-Treiber-Manager**.
2. Klicken Sie auf **Startprobleme reparieren**.

   Die Startparameter im Boot Record des Zielservers werden automatisch repariert.

Überprüfen der BMR-Wiederherstellung über die Befehlszeile

Quest empfiehlt, die folgenden Schritte durchzuführen, um eine BMR-Wiederherstellung zu überprüfen, die über die Befehlszeile durchgeführt wurde.

Diese Aufgabe ist ein Schritt in Durchführen einer BMR-Wiederherstellung für Linux-Maschinen.

- Durchführen einer Dateisystemprüfung für das wiederhergestellte Volume
- Startbarmachen einer wiederhergestellten Linux-Maschine über die Befehlszeile

Durchführen einer Dateisystemprüfung für das wiederhergestellte Volume

Sobald Sie eine Bare-Metal-Wiederherstellung von der Befehlszeile ausgeführt haben, sollten Sie eine Dateisystemprüfung für das wiederhergestellte Volume durchführen, um sicherzustellen dass die vom Wiederherstellungspunkt wiederhergestellten Daten nicht beschädigt wurden.

Diese Aufgabe ist ein Schritt in Durchführen einer BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Überprüfen der BMR-Wiederherstellung über die Befehlszeile.

Führen Sie zum Durchführen einer Dateisystemprüfung für das wiederhergestellte Volume die Aufgabe unten aus.

1. Geben Sie auf der Befehlszeile in der Universal Recovery Console der Linux-Maschine, die Sie wiederhergestellt haben, den folgenden Befehl ein und drücken Sie die **Eingabetaste**, um zu prüfen, ob die entsprechenden Partitionen gemountet sind:

   ```
   df
   ```

2. Wechseln Sie zu Schritt 3, wenn das wiederhergestellte Volume nicht gemountet ist. Wenn das wiederhergestellte Volume gemountet ist, unmounten Sie es, indem Sie den folgenden Befehl eingeben und dann die **Eingabetaste** drücken:

   ```
   umount <Bereitstellungspunkt>
   ```

3. Führen Sie eine Dateisystemprüfung der wiederhergestellten Volumes durch, indem Sie den folgenden Befehl eingeben und die **Eingabetaste** drücken :

   ```
   fsck -f <Volume>
   ```

   Wenn fsck ohne Fehler abgeschlossen wird, ist das Dateisystem verifiziert.

4. Mounten Sie die entsprechenden Volumes erneut. Geben Sie dazu den folgenden Befehl im Format `mount <Volume> <Ordner>` ein und drücken Sie die **Eingabetaste**.

   Wenn der Pfad beispielsweise „prod/sda1“ lautet und der Ordner, den Sie mounten möchten, „mnt“ ist, und geben Sie Folgendes ein und drücken die **Eingabetaste**:

   ```
   mount /dev/sda1 /mnt
   ```

Startbarmachen einer wiederhergestellten Linux-Maschine über die Befehlszeile

Sobald Sie eine saubere Dateisystemprüfung des wiederhergestellten Volumes durchgeführt haben, müssen Sie startbare Partitionen erstellen.

GNU Grand Unified Bootloader (GRUB) ist ein Bootloader, anhand dessen Administratoren konfigurieren können, welches Betriebssystem oder welche bestimmte Kernel-Konfiguration verwendet wird, um das System zu starten. Nach einer BMR muss die Konfigurationsdatei für GRUB so angepasst werden, dass die Maschine den entsprechenden Universally Unique Identifier (UUID) für das Stamm-Volume verwendet. Vor diesem Schritt müssen Sie die Stamm- und Startvolumes bereitstellen und die UUIDs für jedes überprüfen. Damit wird sichergestellt, dass Sie von der Partition starten können.

NOTE: Dieses Verfahren gilt für Linux-Maschinen mit GRUB1 oder GRUB2. Bei der Verwendung dieses Verfahrens ist sicherzustellen, dass die Startpartition in gutem Funktionszustand und geschützt ist.

GRUB oder GRUB2 wird in der Regel mit Linux-Betriebssystemen installiert. Sie können diesen Vorgang mithilfe der Version, die im Lieferumfang Ihrer Linux-Distribution enthalten ist ausführen. Wenn eine Version von GRUB nicht installiert ist, müssen Sie die Standardversion entsprechenden für Ihre Linux-Distribution neu installieren.

CAUTION: Beim ersten Start einer wiederhergestellten Linux-Maschine nach einer BMR-Wiederherstellung erstellt Rapid Recovery **ein Basisimage der wiederhergestellten Maschine. Je nach Datenmenge auf der Maschine kann dieser Vorgang länger als ein inkrementeller Snapshot dauern. Weitere Informationen für Basisimages und inkrementelle Snapshots finden Sie unter Grundlegende Informationen zu Schutzzeitplänen.**

Diese Aufgabe ist ein Schritt in Durchführen einer BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Überprüfen der BMR-Wiederherstellung über die Befehlszeile.

Führen Sie die Aufgabe zum Erstellen startfähiger Partitionen mithilfe der Befehlszeile durch.

1. Sie müssen zuerst das Stamm-Volume und anschließend das Startvolume bereitstellen. Stellen Sie jedes wiederhergestelltes Volume unter Verwendung der folgenden Befehle bereit:

a. Geben Sie den folgenden Befehl ein, um das Stamm-Volume bereitzustellen, und drücken Sie die **Eingabetaste**:

```
mount /<restored volume[root]> /mnt
```

Wenn beispielsweise /dev/sda2 das Stamm-Volume ist, geben Sie mount /dev/sda2 /mnt ein und drücken die **Eingabetaste**.

b. Geben Sie den folgenden Befehl ein, um das Startvolume bereitzustellen, und drücken Sie die **Eingabetaste**:

```
mount /<restored volume[boot]> /mnt/boot
```

Wenn beispielsweise /dev/sda1 das Startvolume ist, geben Sie mount /dev/sda1 /mnt ein und drücken die **Eingabetaste**.

NOTE: Einige Systemkonfigurationen können das Startverzeichnis als Teil des Stamm-Volume einschließen.

2. Wenn die Größe des Volume ansteigt, also wenn das Ziel-Volume auf der neuen Linux-Maschine größer als das Volume im Wiederherstellungspunkt ist, müssen Sie alle vorhandenen Bitmap-Dateien löschen.
3. Ermitteln Sie den UUID (Universally Unique Identifier) der neuen Volumes mit dem Befehl `blkid`. Geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
blkid [volume]
```

NOTE: Sie können auch den Befehl `ls -l /dev/disk/by-uuid-` verwenden.

4. Wenn Sie eine BMR auf einer brandneuen Festplatte auf der Zielmaschine durchführen, kommentieren Sie die Swap-Partition in fstab in Ihrem Stamm-Volume aus.
5. Das Ändern der fstab- und mtab-Pfade sollten im wiederhergestellten Volume, nicht der Live-DVD stattfinden. Es ist nicht erforderlich, Pfade auf der Live-DVD zu ändern. Bereiten Sie die Installation von Grand Unified Bootloader (GRUB) durch Eingabe der folgenden Befehle vor. Drücken Sie nach jedem Befehl die **Eingabetaste**:

```
mount --bind /dev /mnt/dev
mount --bind /proc /mnt/proc
mount --bind /sys /mnt/sys
```

6. Geben Sie den folgenden Befehl ein, um das Stammverzeichnis zu ändern, und drücken Sie die **Eingabetaste**:

```
chroot /mnt /bin/bash
```

7. Ermitteln Sie die UUID der Partitionen anhand der Datei der gemounteten Wiederherstellungspunkte `/etc/fstab` und vergleichen Sie sie mit den UUIDs für das Stamm-Volume (Ubuntu und CentOS) sowie für das Start-Volume (CentOS und RHEL) und die Datenpartitionen, indem Sie den folgenden Befehl eingeben und dann die **Eingabetaste** drücken:

```
less /mnt/etc/fstab
```

8. Ermitteln Sie die UUID der Partitionen anhand der Datei der gemounteten Wiederherstellungspunkte `/etc/mtab` und vergleichen Sie sie mit den UUIDs für das Stamm-Volume (Ubuntu und CentOS) sowie für das Start-Volume (CentOS und RHEL) und die Datenpartitionen, indem Sie den folgenden Befehl eingeben und dann die **Eingabetaste** drücken:

```
less /mnt/etc/mtab
```

9. Installieren Sie GRUB bei Verwendung von SLES 11, indem Sie die folgenden Befehle eingeben und nach jedem Befehl die **Eingabetaste** drücken:

```
grub-install --recheck /dev/sda
grub-install /dev/sda
```

10. Bei Verwendung von Ubuntu, CentOS 6.x, RHEL 6.x oder Oracle Linux 6.x, installieren Sie GRUB durch Eingabe des folgenden Befehls und drücken anschließend die **Eingabetaste**:

```
grub-install /dev/sda
```

11. Bei der Verwendung von SLES 12, CentOS 7, RHEL 7 oder Oracle 7, installieren Sie GRUB2 durch Eingabe des folgenden Befehls und drücken anschließend die **Eingabetaste**:

```
grub2-install /dev/sda
```

12. Nach Abschluss der Installation führen Sie eines der folgenden Updates aus:
    - Für SLES:

      ```
      grub-install.unsupported --recheck /dev/sda
      grub-install.unsupported /dev/sda
      update-grub
      ```

      NOTE: Ignorieren Sie den Befehl, wenn der Befehl `update-grub` nicht in Ihrer Linux-Distribution vorhanden ist.

    - Für andere Distributionen:

      ```
      grub-install /dev/sda
      update-grub
      ```

      NOTE: Ignorieren Sie den Befehl, wenn der Befehl `update-grub` nicht in Ihrer Linux-Distribution vorhanden ist.
13. Entfernen Sie die Live-DVD aus dem CD-ROM- oder DVD-Laufwerk und starten Sie die Linux-Maschine neu.

Verwalten der Alterung von Daten

Dieser Abschnitt beschreibt, wie Sie alternde Snapshot-Daten, die in Ihrem Repository gespeichert sind, verwalten. Er enthält Informationen über die Aufbewahrung von Wiederherstellungspunkten in Ihrem Repository, Aufbewahrungsrichtlinien und den resultierenden Prozess des „Rollup“ von Wiederherstellungspunkten, um Platz zu sparen. Er beschreibt die neue Fähigkeit, Wiederherstellungspunkte von Ihrem Repository in eine Quest DR Sicherungs- und Deduplizierungs-Appliance zu verlegen.

In diesem Abschnitt wird außerdem beschrieben, wie Sie Aufbewahrungsrichtlinien verwalten, die Rollup steuern, und wie Sie Rollup auf Abruf erzwingen.

Datenaufbewahrung, Verknüpfen mit einem sekundären Speicher und Archivierung

Jedes Mal, wenn der Core einen Snapshot erfasst, werden die Daten als ein Wiederherstellungspunkt für Ihr Repository gespeichert. Wiederherstellungspunkte sammeln sich mit der Zeit an. Der Core verwendet eine Aufbewahrungsrichtlinie, um festzustellen, wie lange Snapshot-Daten im Repository aufbewahrt werden. Beim Ausführen nächtlicher Jobs (insbesondere während des Roll-ups) erzwingt der Core die Aufbewahrungsrichtlinie zur Reduzierung des verbrauchten Speicherplatzes. Dabei wird das Datum der einzelnen Wiederherstellungspunkte mit dem Datum des aktuellsten Wiederherstellungspunkts verglichen. Der Core kombiniert ältere Wiederherstellungspunkte, mit anderen Worten, er führt ein „Roll-up“ durch. Ältere Wiederherstellungspunkte im Repository werden fortlaufend durch neuere ersetzt, wenn die ältesten Wiederherstellungspunkte ihr in der Aufbewahrungszeit definiertes maximales Alter erreichen.

Ab Rapid Recovery Version 6.1.1 können Sie außerdem Wiederherstellungspunkte vom primären DVM-Repository auf ein Tiering-Repository auf eine Quest DR Sicherungs- und Deduplizierungs-Appliance verlagern. Dadurch wird Speicherplatz in Ihrem primären Repository freigegeben.

Um Wiederherstellungspunkte auf diese Weise mit einem sekundären Speicher zu verknüpfen, müssen Sie zunächst die DR-Appliance als Repository auf Ihrem Rapid Recovery Core hinzufügen. Weitere Informationen zum Erstellen eines neuen sekundären Tiering-Repository auf einer DR finden Sie unter Erstellen eines Tiering-Repositorys.Geben Sie dann auf der Ebene der geschützten Maschine in den Aufbewahrungsrichtlinien das Alter an, in dem Wiederherstellungspunkte vom primären auf das sekundäre Repository verlagert werden sollen. Weitere Informationen finden Sie unter Anpassen der Aufbewahrungsrichtlinieneinstellungen für eine geschützte Maschine (insbesondere Schritte 7 und 10).

NOTE: Unabhängig davon, wo sich die Wiederherstellungspunkte befinden (lokales primäres DVM Repository oder sekundäres Tiering-Repository auf einer DR-Backup-Appliance), unterliegen sie stets den Aufbewahrungsrichtlinien und werden weiterhin kombiniert. Wenn Sie ältere Wiederherstellungspunkte beibehalten müssen, steht Ihnen als eine Möglichkeit die Archivierung zur Verfügung. Der andere Ansatz besteht darin, Rollup zu deaktivieren oder die Aufbewahrungsdauer für die relevanten geschützten Maschinen zu erweitern.

Um Wiederherstellungspunkte, die ansonsten kombiniert und schließlich gelöscht werden, aufzubewahren, können Sie in der Core Console ein Archiv erstellen. Ein Archiv ist eine Datei, die eine Kopie des vollen Satzes der Wiederherstellungspunkte für Maschinen, die auf Ihrem Core zum Zeitpunkt seiner Erstellung geschützt sind, enthält. Sie können zu einem späteren Zeitpunkt über die Core Console auf archivierte Informationen zugreifen.

Im Gegensatz zu Wiederherstellungspunkten im Repository, findet für Wiederherstellungspunkte in einem Archiv kein Rollup statt.

Archive sind nützlich zur Aufbewahrung von Compliance-Daten, zum Sichern des Core, zum Seeding von Replikationsdaten auf einem Remote-Replikat-Core und zum Einsparen von Speicherplatz auf Ihrem Core, sodass Sie dort aktuelle geschäftskritische Transaktionen halten und gleichzeitig Sicherungskopien für einen längeren Zeitraum aufbewahren könnten.

Weitere Informationen zu Archiven finden Sie unter Archivierung.

Verwalten von Aufbewahrungsrichtlinien

Eine Aufbewahrungsrichtlinie ist ein Satz von Regeln, der den Zeitraum für den Core vorgibt, Wiederherstellungspunkte vor Beginn des Rollup beizubehalten. Aufbewahrungsrichtlinien können so eingestellt werden, dass der Rollup basierend auf Stunden und Tagen sowie Wochen, Monaten und Jahren ausgeführt wird. Sie können bis zu sechs Regeln einrichten (die Standardrichtlinie stellt fünf Regeln ein).

Da Sie so häufig wie alle 5 Minuten sichern können (einmal pro Stunde beim DL1000), legt die erste Regel in der Aufbewahrungsrichtlinie fest, wie lange alle Wiederherstellungspunkte beibehalten werden. Wenn Sie beispielsweise eine Maschine pro Viertelstunde sichern, werden 96 Wiederherstellungspunkte im Repository für diese Maschine pro Tag gespeichert, bis der Rollup beginnt. Ohne das Verwalten Ihrer Aufbewahrungsrichtlinie, kann die Menge an Daten schnell ein Repository füllen.

NOTE: Administratoren sollten beachten, dass regelmäßige Sicherungskopien sich Auswirkungen auf den Netzwerkverkehr haben können. Andere Faktoren, die den Netzwerkdatenverkehr beeinträchtigen sind beispielsweise Übertragungen (z. B. Replikation), die Änderungsrate der Daten, und Ihre Netzwerk-Hardware, Kabel und Switches.

Der Core ist vorab bereits mit einer standardmäßigen Aufbewahrungsrichtlinie eingestellt. Die Standardrichtlinie behält bei:

- Alle Wiederherstellungspunkte für 3 Tage
- Einen Wiederherstellungspunkt pro Stunde für zwei Tage
- Einen Wiederherstellungspunkt pro Tag für vier Tage
- Einen Wiederherstellungspunkt pro Woche für drei Wochen
- Einen Wiederherstellungspunkt pro Monat für zwei Monate
- Einen Wiederherstellungspunkt pro Jahr für X Jahre (deaktiviert in Standardrichtlinie).

Nach dieser Standardrichtlinie, ist der älteste Wiederherstellungspunkt in der Regel 92 Tage alt. Daten nach dem Ursprungsdatum für eine Standardrichtlinie werden gelöscht.

Einstellung der Aufbewahrungsrichtlinie auf die Core-Ebene gilt automatisch für alle Maschinen, die vom Core geschützt werden. Sie können die Standardrichtlinie gemäß Ihren Bedürfnissen ändern.

Für jede Maschine können Sie auch eine benutzerdefinierte Aufbewahrungsrichtlinie erstellen. Einstellen der Richtlinie auf Maschinenebene ermöglicht die Angabe einer anderen Aufbewahrungsrichtlinie als die Standard-Core-Richtlinie. Weitere Informationen zum Konfigurieren von Aufbewahrungsrichtlinien finden Sie unter Konfigurieren der Standardeinstellungen für die Aufbewahrungsrichtlinie des Core und Anpassen der Aufbewahrungsrichtlinieneinstellungen für eine geschützte Maschine.

Konfigurieren der Standardeinstellungen für die Aufbewahrungsrichtlinie des Core

Die Aufbewahrungsrichtlinie für den Core gibt an, wie lange die Wiederherstellungspunkte für eine geschützte Maschine im Repository gespeichert werden.

Diese Aufbewahrungsrichtlinie wird von einem Rollup-Prozess durchgesetzt, der im Rahmen der Ausführung der nächtlichen Jobs durchgeführt wird. Wiederherstellungspunkte, die älter sind als das in der Aufbewahrungsrichtlinie angegebene Alter, werden in weniger Wiederherstellungspunkte zusammengefasst (Rollup), die einen größeren Zeitraum abdecken. Durch die nächtliche Anwendung der Aufbewahrungsrichtlinie erfolgt ein laufender Rollup älterer Sicherungen. Die ältesten Wiederherstellungspunkte werden abhängig von der jeweiligen Aufbewahrungsrichtlinie schließlich gelöscht.

Für Quell- und Ziel-Core können unterschiedliche Aufbewahrungseinstellungen konfiguriert werden.

NOTE: In diesem Abschnitt wird die Anpassung der Einstellungen für die Aufbewahrungsrichtlinie auf dem Rapid Recovery Core behandelt. Wenn Sie die angepassten Einstellungen der Aufbewahrungsrichtlinie im Core speichern, werden die Standardeinstellungen für Aufbewahrungsrichtlinien festgelegt, die auf alle Maschinen angewendet werden können, die durch den jeweiligen Core geschützt werden. Weitere Informationen zum Anpassen der Aufbewahrungsrichtlinieneinstellungen für einzelne geschützte Maschinen finden Sie unter Anpassen der Aufbewahrungsrichtlinieneinstellungen für eine geschützte Maschine.

1. Navigieren Sie zu dem Rapid Recovery Core Console.
2. Klicken Sie auf der Symbolleiste auf (Einstellungen) und führen Sie dann einen der folgenden Schritte aus:
   - Klicken Sie in der Liste der Core-Einstellungen auf der linken Seite der Seite „Einstellungen“ auf **Nächtliche Jobs**.
   - Scrollen Sie auf der rechten Seite der Seite „Einstellungen“ nach unten, bis sie die Überschrift **Nächtliche Jobs** sehen können.

   Die Core-Einstellungen für nächtliche Jobs werden angezeigt.
3. Klicken Sie unter **Nächtliche Jobs** auf **Ändern**.

   Das Dialogfeld **Nächtliche Jobs** wird angezeigt.
4. Wählen Sie die Option **Rollup** im Bereich „Nächtliche Jobs“ aus, um die gewünschten Zeitintervalle für die Aufbewahrung von Sicherungsdaten anzugeben, und klicken Sie dann auf **Einstellungen**.

   Das Dialogfeld **Konfiguration** für die Standard-Aufbewahrungsrichtlinie von Core wird angezeigt.
5. Sie können die standardmäßigen Core-Aufbewahrungsrichtlinieneinstellungen jederzeit wiederherstellen, indem Sie im unteren Bereich des Dialogfelds „Konfiguration“ auf **Standardeinstellungen wiederherstellen** und anschließend auf **Ja** klicken, um den Vorgang zu bestätigen.

   Alle Einstellungen werden auf die in der Tabelle in Schritt 6 beschriebenen Standardwerte zurückgesetzt.
6. Geben Sie den Standard-Aufbewahrungszeitplan für Wiederherstellungspunkte an (siehe Beschreibung in der folgenden Tabelle). Die erste Einstellung gibt die primäre Aufbewahrungsfrist für alle im Repository gespeicherten Wiederherstellungspunkte an. Jede zusätzliche Einstellung, wenn aktiviert, bietet eine detailliertere Ebene der Aufbewahrung, indem die Intervalle definiert werden, in denen ein Rollup von Wiederherstellungspunkten erfolgen soll. Diese Einstellungen definieren die Dauer, für die Wiederherstellungspunkte beibehalten werden.

   Die Optionen für die Aufbewahrungsrichtlinie werden in der folgenden Tabelle beschrieben.

Tabelle 149. Zeitplanoptionen für standardmäßige Aufbewahrungsrichtlinie

Textfeld	Description
Alle Wiederherstellungspunkte beibehalten für n [Aufbewahrungsdauer]	Gibt die primäre Aufbewahrungsfrist für alle im Repository gespeicherten Wiederherstellungspunkte an. Geben Sie eine Zahl für die Aufbewahrungsdauer an und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist 3 Tage. Sie haben folgende Auswahlmöglichkeiten: Tage, Wochen, Monate und Jahre
...and then keep one recovery point per hour for n [retention time period] (...und dann einen Wiederherstellungspunkt pro Stunde beibehalten für n [Aufbewahrungsdauer])	Wenn diese Einstellung ausgewählt ist, wird ein Wiederherstellungspunkt pro Stunde für einen von Ihnen angegebenen Zeitraum beibehalten. Die Standardeinstellung ist 2 Tage. Sie können aus folgenden Optionen wählen: Tage, Wochen, Monate und Jahre Wenn Sie nicht mindestens ein Wiederherstellungspunkt pro Stunde speichern möchten, deaktivieren Sie diese Option.
...and then keep one recovery point per day for n [retention time period] (...und dann einen Wiederherstellungspunkt pro Tag beibehalten für n [Aufbewahrungsdauer])	Wenn diese Einstellung ausgewählt ist, wird ein Wiederherstellungspunkt pro Tag für einen von Ihnen angegebenen Zeitraum beibehalten. Die Standardeinstellung ist 4 Tage. Sie können aus folgenden Optionen wählen: Tage, Wochen, Monate und Jahre Wenn Sie nicht mindestens ein Wiederherstellungspunkt pro Tag speichern möchten, deaktivieren Sie diese Option.
...and then keep one recovery point per week for n [retention time period] (...und dann einen Wiederherstellungspunkt pro Woche beibehalten für n [Aufbewahrungsdauer])	Wenn diese Einstellung ausgewählt ist, wird ein Wiederherstellungspunkt pro Woche für einen von Ihnen angegebenen Zeitraum beibehalten. Die Standardeinstellung ist 3 Wochen. Sie können aus folgenden Optionen wählen: Wochen, Monate und Jahre Wenn Sie nicht mindestens ein Wiederherstellungspunkt pro Woche speichern möchten, deaktivieren Sie diese Option.
...and then keep one recovery point per month for n [retention time period] (...und dann einen Wiederherstellungspunkt pro Monat beibehalten für n [Aufbewahrungsdauer])	Wenn diese Einstellung ausgewählt ist, wird ein Wiederherstellungspunkt pro Monat für einen von Ihnen angegebenen Zeitraum beibehalten. Die Standardeinstellung ist 2 Monate. Sie können aus folgenden Optionen wählen: Monate und Jahre. Wenn Sie nicht mindestens einen Wiederherstellungspunkt pro Monat speichern möchten, deaktivieren Sie diese Option.
...and then keep one recovery point per year for n [retention time period] (...und dann einen Wiederherstellungspunkt pro Jahr beibehalten für n [Aufbewahrungsdauer])	Wenn diese Einstellung ausgewählt ist, wird ein Wiederherstellungspunkt pro Jahr für eine von Ihnen angegebene Anzahl von Jahren beibehalten. Der Standardwert (1 Jahr) ist standardmäßig deaktiviert. Wenn Sie mindestens einen Wiederherstellungspunkt pro Jahr speichern möchten, aktivieren Sie diese Option und geben Sie eine Anzahl von Jahren an. Wenn Sie nicht mindestens einen Wiederherstellungspunkt pro Jahr speichern möchten, deaktivieren Sie diese Option.

Der älteste Wiederherstellungspunkt wird durch die Aufbewahrungsrichtlinieneinstellungen bestimmt.

Im folgenden Beispiel wird die Berechnung der Aufbewahrungsdauer veranschaulicht.

Alle Wiederherstellungspunkte beibehalten für drei Tage.

...und dann einen Wiederherstellungspunkt pro Stunde beibehalten für drei Tage

...und dann einen Wiederherstellungspunkt pro Tag beibehalten für vier Tage

...und anschließend einen Wiederherstellungspunkt pro Woche beibehalten für drei Wochen

...und anschließend einen Wiederherstellungspunkt pro Monat beibehalten für zwei Monate

...und anschließend einen Wiederherstellungspunkt pro Monat beibehalten für ein Jahr

In diesem Beispiel wäre der älteste Wiederherstellungspunkt demzufolge ein Jahr und drei Monate alt.

7. Wenn Sie mit Ihren Aufbewahrungsrichtlinieneinstellungen zufrieden sind, klicken Sie auf **Save** (Speichern).

   Das Dialogfeld **Configuration** (Konfiguration) wird geschlossen.

8. Klicken Sie im Dialogfeld **Nightly Jobs** (Nächtliche Jobs) auf **OK**.

   Das Dialogfeld **Nightly Jobs** (Nächtliche Jobs) wird geschlossen. Die von Ihnen definierte Aufbewahrungsrichtlinie wird im Rahmen des nächtlichen Rollups verwendet.

   Sie können diese Einstellungen auch verwenden, wenn Sie die Aufbewahrungsrichtlinie für eine einzelne geschützte Maschine angeben. Weitere Informationen zum Festlegen von Aufbewahrungsrichtlinien für eine geschützte Maschine finden Sie unter Anpassen der Aufbewahrungsrichtlinieneinstellungen für eine geschützte Maschine.

Anpassen der Aufbewahrungsrichtlinieneinstellungen für eine geschützte Maschine

Wenn Sie die Wiederherstellungspunkte für eine bestimmte geschützte Maschine von einem primären DVM-Repository auf ein Tiering-Repository verlagern möchten, muss das Tiering-Repository bereits vorhanden sein. Informationen zum Definieren eines Tiering-Repository finden Sie unter dem Thema Erstellen eines Tiering-Repositorys.

Die Aufbewahrungsrichtlinie für eine geschützte Maschine gibt an, wie lange die Wiederherstellungspunkte im Repository gespeichert werden. Sofern Sie keine benutzerdefinierte Aufbewahrungsrichtlinie angeben (siehe folgende Beschreibung), verwendet jede geschützte Maschine standardmäßig die Standardaufbewahrungsrichtlinie, die für den Core festgelegt wurde.

Ab AppAssure Version 5.4.1 bietet Rapid Recovery die Möglichkeit, unterschiedliche Aufbewahrungsrichtlinien für geschützte Maschinen im Quell-Core und die entsprechenden replizierten Maschinen im Ziel-Core festzulegen.

Wenden Sie dieses Verfahren an, um eine benutzerdefinierte Aufbewahrungsrichtlinie für eine geschützte Maschine bzw. eine replizierte Maschine festzulegen.

NOTE: Folgendes gilt für Umgebungen, die von AppAssure Version 5.3.x auf Version 5.4.1 oder eine beliebige Version von Rapid Recovery Core aktualisiert werden. Wenn Sie eine Aufbewahrungsrichtlinie für eine beliebige replizierte Maschine anpassen möchten, aktualisieren Sie zuerst die Quell- und Ziel-Cores auf AppAssure Core Version 5.4.1 und führen Sie anschließend den Repository-Prüfjob auf jedem Repository in diesem Ziel-Core aus. Die Durchführung dieses Jobs kann abhängig von der Größe des Repositorys und vom zugrunde liegenden Speichersystem erhebliche Zeit in Anspruch nehmen. Weitere Informationen zu diesem Job finden Sie unter Informationen über das Überprüfen der Integrität der DVM Repositorys. Informationen zur Durchführung dieses Jobs finden Sie unter Ausführen einer Integritätsprüfung auf einem DVM-Repository.

1. Klicken Sie im Menü „Maschinen“ der Rapid Recovery Core Console auf den Namen der Maschine, die Sie ändern möchten.

   Die Registerkarte **Zusammenfassung** für die ausgewählte Maschine wird angezeigt.

2. Klicken Sie auf das Menü **Einstellungen**.

   Die Seite **Einstellungen** wird angezeigt. Sie enthält Konfigurationseinstellungen für die ausgewählte Maschine.

3. Optional können Sie auf den Link **Nächtliche Jobs** klicken, um einen Bildlauf nach unten auf die Seite „Einstellungen“ durchführen, um die Einstellungen für nächtliche Jobs anzuzeigen.

4. Unter der Überschrift „Nächtliche Jobs“ klicken Sie auf **Ändern**.

   Das Dialogfeld **Nächtliche Jobs** wird angezeigt.

5. Wählen Sie die Option **Rollup** aus, um die gewünschten Zeitintervalle für die Aufbewahrung von Sicherungsdaten anzugeben und klicken Sie dann auf **Settings** (Einstellungen).

   Das Dialogfeld **Konfiguration** für die Aufbewahrungsrichtlinie wird angezeigt.

6. Führen Sie den entsprechenden Schritt durch, wenn bei der Anpassung der Aufbewahrungsrichtlinieneinstellungen für eine replizierte Maschine eine Warnung mit dem Hinweis angezeigt wird, dass für das Repository eine Integritätsprüfung durchgeführt werden sollte. Andernfalls fahren Sie mit Schritt 7 fort.

   a. Klicken Sie auf **Integrität prüfen**, wenn der Job durchgeführt werden kann.
   b. Klicken Sie auf **Ja**, um den Integritätsprüfjob durchzuführen.

   NOTE: Die Ausführung dieses Jobs kann abhängig von der Größe des Repositorys erhebliche Zeit in Anspruch nehmen. In dieser Zeit können Sie keine anderen Aktionen (Snapshot-Erstellung, Replikation, virtueller Export usw.) im Repository durchführen. Informationen zu diesem Job finden Sie unter Informationen über das Überprüfen der Integrität der DVM Repositorys.

   - Kehren Sie hierher zurück, nachdem alle untergeordneten Repository-Prüfjobs erfolgreich durchgeführt wurden, und fahren Sie mit dem nächsten Schritt fort.

7. Führen Sie im Dialogfeld **Configuration** (Konfiguration) eine der folgenden Aktionen aus:

   - Wählen Sie die Option **Use Core default retention policy** (Standard-Aufbewahrungsrichtlinie von Core verwenden) aus, wenn die Standard-Aufbewahrungsrichtlinie für diese geschützte Maschine verwendet werden soll, und klicken Sie dann auf **Save** (Speichern). Die Standardrichtlinie wird auf diese geschützte Maschine angewendet.
   - Wählen Sie die Option **Use custom retention policy** (Benutzerdefinierte Aufbewahrungsrichtlinie verwenden) aus, wenn Sie eine benutzerdefinierte Aufbewahrungsrichtlinie für diesen Agenten festlegen möchten, und fahren Sie mit dem nächsten Schritt fort.

   Das Dialogfeld **Configuration** (Konfiguration) wird erweitert, um Informationen zur benutzerdefinierten Aufbewahrungsrichtlinie anzuzeigen.

8. Geben Sie den benutzerdefinierten Aufbewahrungszeitplan für Wiederherstellungspunkte an (siehe Beschreibung in der folgenden Tabelle). Die erste Einstellung gibt die primäre Aufbewahrungsfrist für alle im Repository gespeicherten Wiederherstellungspunkte an. Jede zusätzliche Einstellung, wenn aktiviert, bietet eine detailliertere Ebene der Aufbewahrung, indem die Intervalle definiert werden, in denen ein

Rollup von Wiederherstellungspunkten erfolgen soll. Diese Einstellungen definieren die Dauer, für die Wiederherstellungspunkte beibehalten werden.

Tabelle 150. Zeitplanoptionen für benutzerdefinierte Aufbewahrungsrichtlinie

Textfeld	Description
Alle Wiederherstellungspunkte beibehalten für n [Aufbewahrungsdauer]	Gibt die primäre Aufbewahrungsfrist für alle im Repository gespeicherten Wiederherstellungspunkte an. Geben Sie eine Zahl für die Aufbewahrungsdauer an und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist 3 Tage. Sie haben folgende Auswahlmöglichkeiten: Tage, Wochen, Monate und Jahre
...and then keep one recovery point per hour for n [retention time period] (...und dann einen Wiederherstellungspunkt pro Stunde beibehalten für n [Aufbewahrungsdauer])	Wenn diese Einstellung ausgewählt ist, wird ein Wiederherstellungspunkt pro Stunde für einen von Ihnen angegebenen Zeitraum beibehalten. Die Standardeinstellung ist 2 Tage. Sie können aus folgenden Optionen wählen: Tage, Wochen, Monate und Jahre Wenn Sie nicht mindestens ein Wiederherstellungspunkt pro Stunde speichern möchten, deaktivieren Sie diese Option.
...and then keep one recovery point per day for n [retention time period] (...und dann einen Wiederherstellungspunkt pro Tag beibehalten für n [Aufbewahrungsdauer])	Wenn diese Einstellung ausgewählt ist, wird ein Wiederherstellungspunkt pro Tag für einen von Ihnen angegebenen Zeitraum beibehalten. Die Standardeinstellung ist 4 Tage. Sie können aus folgenden Optionen wählen: Tage, Wochen, Monate und Jahre Wenn Sie nicht mindestens ein Wiederherstellungspunkt pro Tag speichern möchten, deaktivieren Sie diese Option.
...and then keep one recovery point per week for n [retention time period] (...und dann einen Wiederherstellungspunkt pro Woche beibehalten für n [Aufbewahrungsdauer])	Wenn diese Einstellung ausgewählt ist, wird ein Wiederherstellungspunkt pro Woche für einen von Ihnen angegebenen Zeitraum beibehalten. Die Standardeinstellung ist 3 Wochen. Sie können aus folgenden Optionen wählen: Wochen, Monate und Jahre Wenn Sie nicht mindestens ein Wiederherstellungspunkt pro Woche speichern möchten, deaktivieren Sie diese Option.
...and then keep one recovery point per month for n [retention time period] (...und dann einen Wiederherstellungspunkt pro Monat beibehalten für n [Aufbewahrungsdauer])	Wenn diese Einstellung ausgewählt ist, wird ein Wiederherstellungspunkt pro Monat für einen von Ihnen angegebenen Zeitraum beibehalten. Die Standardeinstellung ist 2 Monate. Sie können aus folgenden Optionen wählen: Monate und Jahre. Wenn Sie nicht mindestens einen Wiederherstellungspunkt pro Monat speichern möchten, deaktivieren Sie diese Option.
...and then keep one recovery point per year for n [retention time period] (...und dann einen Wiederherstellungspunkt	Wenn diese Einstellung ausgewählt ist, wird ein Wiederherstellungspunkt pro Jahr für eine von Ihnen angegebene Anzahl von Jahren beibehalten. Der Standardwert (1 Jahr) ist standardmäßig deaktiviert. Wenn Sie mindestens einen Wiederherstellungspunkt pro Jahr speichern möchten, aktivieren Sie diese Option und geben Sie eine Anzahl von Jahren an.

Textfeld	Description
pro Jahr beibehalten für n [Aufbewahrungsdauer])	Wenn Sie nicht mindestens einen Wiederherstellungspunkt pro Jahr speichern möchten, deaktivieren Sie diese Option.

Im folgenden Beispiel wird die Berechnung der Aufbewahrungsdauer veranschaulicht.

Alle Wiederherstellungspunkte beibehalten für drei Tage.

...und dann einen Wiederherstellungspunkt pro Stunde beibehalten für drei Tage

...und dann einen Wiederherstellungspunkt pro Tag beibehalten für vier Tage

...und anschließend einen Wiederherstellungspunkt pro Woche beibehalten für drei Wochen

...und anschließend einen Wiederherstellungspunkt pro Monat beibehalten für zwei Monate

...und anschließend einen Wiederherstellungspunkt pro Monat beibehalten für ein Jahr

In diesem Beispiel wäre der älteste Wiederherstellungspunkt demzufolge ein Jahr und 3 Monate alt.

9. Wenn SieWiederherstellungspunkte in Ihrem primären DVM-Repository erhalten möchten, fahren Sie mit Schritt 11 fort.
10. Wenn Sie Wiederherstellungspunkte von Ihrem primären DVM-Repository auf ein sekundäres Tiering-Repository verlagern möchten, dasauf einer Quest DR-Sicherungs-Appliance gespeichert ist, führen Sie folgende Schritte aus:
    a. Wählen Sie die Option **Veraltete Wiederherstellungspunkte auf ein Tiering-Repository verlagern**.
    b. Geben Sie das Alter an, ab dem Sie Wiederherstellungspunkte vom primären Repository auf das Tiering-Repository verlagern möchten.

    Sie können das Alter in Wochen, Monaten oder Jahren angeben. Die kürzeste Periode, die Sie festlegen können, ist 1 Woche.

    c. Wählen Sie aus dem Drop-Down-Menü **Ein Repository auswählen** das Tiering-Repository, auf das Sie alle Wiederherstellungspunkte für die angegebene Maschine verlagern möchten.

> **NOTE:** Unabhängig davon, wo sich die Wiederherstellungspunkte befinden (lokales primäres DVM Repository oder sekundäres Tiering-Repository auf einer DR-Backup-Appliance), unterliegen sie stets den Aufbewahrungsrichtlinien und werden weiterhin kombiniert. Wenn Sie ältere Wiederherstellungspunkte beibehalten müssen, steht Ihnen als eine Möglichkeit die Archivierung zur Verfügung. Der andere Ansatz besteht darin, Rollup zu deaktivieren oder die Aufbewahrungsdauer für die relevanten geschützten Maschinen zu erweitern.

11. Klicken Sie auf **Speichern**.

Erzwingen eines Rollup für alle geschützten Maschinen

Sie können Ihre geplante Aufbewahrungsrichtlinie umgehen, indem Sie einen Rollup der Wiederherstellungspunkte auf Ebene der geschützten Maschine erzwingen.

1. Klicken Sie im Menü „Geschützte Maschinen“ der Rapid Recovery Core Console auf den Namen einer bestimmten geschützten Maschine.

   Die Seite **Summary** (Zusammenfassung) für die ausgewählte Maschine wird angezeigt.

2. Klicken Sie auf das Drop-Down-Menü **Mehr** oben auf der Ansicht der geschützte Maschine und wählen Sie dann **Aufbewahrungsrichtlinie** aus.

   Die Seite **Aufbewahrungsrichtlinie** für die angegebene Maschine wird angezeigt.
3. Klicken Sie auf **Rollup erzwingen**.
4. Klicken Sie im Dialogfeld **Ja**, um den Vorgang zu bestätigen.

Rapid Recovery initiiert den Rollup für diese Maschine, und zwar unabhängig vom Zeitplan der Aufbewahrungsrichtlinie.

Archivierung

Dieser Abschnitt enthält konzeptionelle Informationen über Rapid Recovery Archive, einschließlich Geschäftsfälle für ihre Erstellung, Speicherung und Verwendung. Außerdem wird beschrieben, wie Sie ein einmaliges Archiv oder ein Archiv erstellen, das nach einem Zeitplan fortlaufend aktualisiert wird. Sie finden Themen, die beschreiben, wie Sie geplante Archive anhalten oder bearbeiten, wie Sie ein Archiv erzwingen oder prüfen, anhängen oder importieren.

Grundlegende Informationen zu Archiven

Der Rapid Recovery Core speichert Snapshot-Daten im Repository. Wenngleich ein Repository auf verschiedenen Speichertechnologien (wie SAN, DAS oder NAS) vorliegen kann, ist der kritischste Leistungsfaktor die Geschwindigkeit. Repositorys verwenden (schnelle und teure) Kurzzeitmedien. Um zu verhindern, dass sich ein Repository schnell füllt, erzwingt der Core eine Aufbewahrungsrichtlinie, die Wiederherstellungspunkte im Laufe der Zeit aufrollt und sie schließlich durch neuere Sicherungsdaten ersetzt.

Wenn Sie Wiederherstellungspunkte beibehalten müssen, sei es aufgrund ihrer historischen Bedeutung, zur Einhaltung gesetzlicher Vorschriften, zur Erfüllung von Offsite-Datenspeicherrichtlinien oder aus anderen Gründen, können Sie ein Archiv erstellen. Ein Archiv ist eine Kopie der Wiederherstellungspunkte von Ihrem Repository für die angegebenen Maschinen über einen von Ihnen festgelegten Datumsbereich. Durch die Archivierung eines Satzes von Wiederherstellungspunkten werden die ursprünglichen Wiederherstellungspunkte in Ihrem Repository nicht gelöscht. Vielmehr friert das Archiv die Sammlung der Wiederherstellungspunkte zu dem Zeitpunkt, in dem das Archiv erstellt wurde, als eine separate Kopie an einem von Ihnen angegebenen Speicherort ein. Im Gegensatz zu Wiederherstellungspunkte in Ihrem Repository, unterliegen die Daten in einem Archiv nicht dem Rollup.

Sie können Archive mit der Option  **Archive** auf der Schaltflächenleiste oder über die Seite **Archive**, die über das Symbol (Mehr) auf der Core Console zugänglich ist, erstellen, importieren und anhängen.

See also: Erstellen eines Archivs und Speicheroptionen
See also: Amazon Speicheroptionen und Archivierung
See also: Wiederherstellungspunktkettenoptionen für Archive
See also: Methoden für den Zugriff auf ein Archiv
See also: Verwendungen für Archive
See also: Erstellen eines Archivs

Erstellen eines Archivs und Speicheroptionen

Sie können ein einmaliges Archiv jederzeit bei Bedarf erstellen.

Sie können auch die Anforderungen für die kontinuierliche planmäßige Archivierung definieren. Mit dieser Aktion wird ein Archiv der Wiederherstellungspunkte für die von Ihnen ausgewählten Maschinen an dem von Ihnen bestimmten Speicherort erstellt. Zusätzliche Wiederherstellungspunkte für diese Maschinen werden dann kontinuierlich nach einem von Ihnen festgelegten Zeitplan (täglich, wöchentlich oder monatlich) an das Archiv angehängt.

Legen Sie beim Erstellen eines Archivs fest, wo Sie es speichern möchten. Sie können ein Archiv in einem Dateisystem (lokal oder in einem Netzwerk) oder auf einem Speicherkonto in der Cloud speichern.

NOTE: Vor dem Archivieren in einem Cloud-Konto müssen Sie zunächst die Anmeldeinformationen für das Speicherkonto auf Ihrem Rapid Recovery Core hinzufügen. Weitere Informationen zum Definieren eines Cloud-Kontos im Core finden Sie unter Hinzufügen eines Cloud-Kontos.

Wenn Sie Ihr Archiv in einem Amazon Cloud-Speicherkonto speichern, müssen Sie die Speicherklasse bei der Erstellung des Kontos definieren. Um direkt nach Amazon Glacier zu archivieren, können Sie Glacier Speicher beim Festlegen des Speicherorts im Archivierungsassistenten festlegen. Weitere Informationen zu Amazon Speicherklassen finden Sie unter Amazon Speicheroptionen und Archivierung.

- Einmalige Archive sind schreibgeschützt. Beim Erstellen eines einmaligen Archivs muss der Zielspeicherort, den Sie angeben, leer sein.
- Bei Verwendung einer geplanten Archivierung hängt der Core zusätzliche Wiederherstellungspunkte an das vorhandene Archiv an.
- Wenn auf einem Speichermedium, das Sie ausgewählt haben, der Speicherplatz ausgeht, hält Rapid Recovery den Archivierungsauftrag an, damit Sie einen anderen Speicherort angeben können. Das Archiv wird dann in Segmente aufgeteilt, die sich an verschiedenen Orten befinden können (sofern Platz vorhanden ist).

See also: Hinzufügen eines Cloud-Kontos

Amazon Speicheroptionen und Archivierung

Wenn Sie die Daten in einem Amazon Simple Storage Service (S3)-Konto archivieren, können Sie zwischen verschiedenen Speicherklassen wählen. Jede hat unterschiedliche Kosten, Vorteile und Einschränkungen. Preise variieren je nach Region. Rapid RecoveryVersion 6.2 erweitert die Unterstützung von Amazon Konten für alle Speicherklassen. Dies ist hilfreich bei der Planung zum Speichern von Rapid Recovery Archiven in der Amazon Cloud.

Ein Verständnis der verfügbaren Speicherklassen und der Unterschied in den Lieferzeiten für den Zugriff auf diese Klassen ist entscheidend für eine wirksame Kontrolle der Speicherkosten, während Sie gleichzeitig innerhalb akzeptabler Zeitrahmen auf Ihre Archive zugreifen können.

NOTE: Quest stellt diese Informationen seinen Rapid Recovery Kunden gratis zur Verfügung, um ihnen die Faktoren, die den Preis von Speicher beeinflussen, näher zu bringen. Diese Konzepte können Ihnen bei der Planung und Ihrem Budget helfen. Sie sind verantwortlich für alle Speicherkosten auf Amazon ebenso wie allen anderen Cloud-Serviceanbietern. Da Amazon die Voraussetzungen, Anforderungen, Kosten, Speicherebenendefinitionen usw. ändern kann, sollten Sie die Amazon Website als primäre und maßgebliche Quelle für diese Informationen verwenden.

Generell bietet Amazon derzeit die folgenden Klassen.

Standard. Diese Speicherklasse ist für Daten gedacht, auf die Sie häufig zugreifen werden oder für die Sie schnellen Zugriff benötigen. Diese Klasse ist die Standard-Specheroption bei allen Rapid Recovery Assistenten, Fenstern und Dialogfeldern. Es werden keine separaten Gebühren zum Abrufen von Informationen in der Standard-Speicherklasse erhoben.

Standard Infrequent Access (IA). Diese Speicherklasse ist günstiger als Standard und für Daten gedacht, auf die Sie nicht häufig zugreifen werden. Für den Zugriff auf Daten in dieser Speicherklasse wird eine Abrufgebühr erhoben. Allerdings sind sie sofort verfügbar. Amazon erhebt Gebühren für Objekte, die früher als 30 Tage aus dem Infrequent Access-Speicher gelöscht werden.

Glacier. Diese Speicherklasse ist für die langfristige Aufbewahrung von Daten gedacht, die nicht in Echtzeit zur Verfügung stehen müssen. Es ist die günstigste Option für die langfristige Speicherung von Daten, die selten abgerufen werden. Für den Zugriff auf Daten in dieser Speicherklasse wird eine Abrufgebühr erhoben. Amazon erhebt Gebühren für Objekte, die früher als 90 Tage aus Glacier gelöscht werden. Der Abruf von in Glacier gespeicherten Daten erfolgt nicht sofort. Standard-Abrufzeiten können 3 bis 5 Stunden betragen; der Bulk-Abruf für große Datenmengen kann bis zu 12 Stunden betragen. Beschleunigte Abrufvorgänge können bis zu 5 Minuten dauern. Es werden Gebühren für jede Abrufoption erhoben.

NOTE: Im Gegensatz zu den anderen Amazon Speicherklassen,unterstützt Rapid Recovery nicht die Erstellung eines spezifischen Glazier Cloud-Kontos. Zum Archivieren von Daten in Glacier wählen Sie ein Amazon Cloud-Konto aus und aktivieren die Option **Glacier Speicher verwenden** auf der Seite **Speicherort** des Archivierungs-Assistenten.

Reduced Redundancy Storage (RRS). Diese Kategorie ist eine kostengünstigere Speicherklasse und für nicht kritische reproduzierbare Daten mit weniger Redundanz als die Standard-Speicherklasse gedacht. Für den Zugriff auf Daten in dieser Speicherklasse wird eine geringfügige Abrufgebühr erhoben. Ein Bruchteil (laut Amazon bis zu 0,01 %) der Objekte in dieser Klasse wird voraussichtlich nicht wiederherstellbar sein.

Für die neuesten Informationen sollten Sie stets die Angaben auf der Amazon-Website prüfen.

Im Allgemeinen gelten die folgenden Richtlinien:

- Wenn Sie erwarten, dass Sie regelmäßig Daten von einem Rapid Recovery Archiv wiederherstellen werden, ist Standard wahrscheinlich die beste Option.
- Aus Kostengründen sollten Sie die Option „Standard Infrequent Access“ erwägen, wenn Sie vorhaben, Daten nur gelegentlich wiederherzustellen.
- Glacier ist ausschließlich für die langfristige Speicherung von archivierten Wiederherstellungspunkte gedacht, die Sie voraussichtlich nur selten wiederherstellen werden. Ein gutes Beispiel für die Verwendung von Glacier Speicher ist die Aufbewahrung von Daten für die Einhaltung behördlicher Auflagen. Glacier ist im Archivierungsassistenten als Archivierungsoption verfügbar.
- Für die Aufbewahrung nicht kritischer, reproduzierbarer Daten sollten Sie RRS erwägen.

Wiederherstellungspunktkettenoptionen für Archive

Vor der Einrichtung Ihres Archivs müssen Sie den ordnungsgemäßen Ansatz für Wiederherstellungspunktketten festlegen. Führen Sie die folgenden Schritte aus, um festzulegen, welche Option Sie auf der Seite **Optionen** des Archiv-Assistenten auswählen werden.

- **Vollständige Wiederherstellungspunktketten, einschließlich referenzierter Basisabbilder außerhalb des Datumsbereichs, erstellen.** Wenn Sie die Option zum Erstellen vollständiger Wiederherstellungsketten auswählen, können Sie den vollen Umfang der Wiederherstellungsaktionen für einen beliebigen Wiederherstellungspunkt im Archiv durchführen. Diese umfassen Wiederherstellung auf Dateiebene, Wiederherstellung auf Volume-Ebene und Bare-Metal-Wiederherstellung. Wenn Sie diese Option wählen, werden vollständige Wiederherstellungspunktketten mit Ihrem Archiv gespeichert. Sie können Daten wiederherstellen, selbst wenn das Basisabbild, das dem ausgewählten Wiederherstellungspunkt entspricht, älter als der Datumsbereich Ihres Archivs ist. Die Dateigröße dieses Archiv ist jedoch größer, um sicherzustellen, dass Sie auf die Daten in der vollständigen Wiederherstellungspunktkette zugreifen können.
- **Nur die Wiederherstellungspunkte im Datumsbereich einschließen. Dies spart Speicherplatz, aber Sie sind verantwortlich für die Archivierung aller erforderlichen Basisabbilder.** Wenn Sie nur die Wiederherstellungspunkte im angegebenen Datumsbereich in das Archiv einschließen, ist die Dateigröße des Archivs kleiner. Für die Daten, bei denen das Basisabbild in den angegebenen Datumsbereich fällt, haben Sie Zugriff auf die gesamte Palette der Wiederherstellungsoptionen. Wenn Sie jedoch Daten wiederherstellen möchten, die in einem Basisabbild mit einem Datum erfasst wurden, das vor dem angegebenen Datumsbereich liegt, sind Sie möglicherweise auf die Wiederherstellung auf Dateiebene beschränkt. Daten außerhalb des Bereichs des Archivs sind verwaist.

Weitere Informationen über Wiederherstellungspunktketten finden Sie im Abschnitt Wiederherstellungspunkt-Ketten und -Waisen.

Zugehörige Konzepte

See also: Wiederherstellungspunkt-Ketten und -Waisen

Zugehörige Tasks

See also: Erstellen eines Archivs

See also: Bearbeiten einer geplanten Archivierung

Methoden für den Zugriff auf ein Archiv

Wenn Sie auf die Daten in einem archivierten Wiederherstellungspunkt zugreifen müssen, haben Sie zwei Optionen.

- Für Archive, die mit Rapid Recovery Version 6.0.1 und höher erstellt wurden, können Sie das Archiv anhängen. Das angehängte Archiv wird im linken Navigationsmenü der Core Console angezeigt. Sie können die Wiederherstellungspunkte im Archiv durchsuchen und die gleichen Aktionen mit den Daten ausführen wie bei allen anderen Wiederherstellungspunkten in Ihrem Repository, ohne diese Daten in das Repository importieren zu müssen.
- Sie können ein Archiv importieren, wodurch diese Wiederherstellungspunkte in Ihrem Repository wiederhergestellt werden. Anschließend können Sie die gleichen Aktionen mit den Daten ausführen, wie bei allen anderen Wiederherstellungspunkten, die sich aktuell in Ihrem Core befinden. Rapid Recovery Core ist abwärtskompatibel und unterstützt den Import von Archiven von allen Versionen von AppAssure undRapid Recovery.

CAUTION: Da der Core die ursprünglichen Daten der Wiederherstellungspunkte in einem Archiv erkennt, können Wiederherstellungspunkte, die von einem Archiv importiert wurden, erneut aufgerollt oder bei der nächsten nächtlichen Aufgabe gelöscht werden, wenn ihr Alter die Aufbewahrungsdauer überschreitet. Wenn Sie ältere Wiederherstellungspunkte beibehalten möchten, die von einem Archiv importiert wurden, können Sie Rollup deaktivieren oder die Aufbewahrungsdauer für die relevanten geschützten Maschinen erweitern.

Wenn Sie auf die Daten in einem Wiederherstellungspunkt zugreifen müssen, können Sie das Archiv später anhängen (für Rapid Recovery 6.x und höher) oder importieren und so diese Wiederherstellungspunkte in Ihrem Repository wiederherstellen.

Zugehörige Tasks

See also: Anfügen eines Archivs
See also: Importieren eines Archivs

Verwendungen für Archive

Sobald ein Archiv erstellt wurde, kann es in einer der folgenden Arten verwendet werden:

- Ein Archiv kann zum Verschieben von Daten zwischen Repositorys verwendet werden.
- Ein Archiv kann an die Core Console angehängt und als Dateisystem für einfache Datei- oder Ordner-Wiederherstellung bereitgestellt werden. Es gelten einige Einschränkungen.
- Ein Archiv kann in ein Repository importiert werden. Wenn alle Wiederherstellungspunkte im Archiv bereits aufgerollt oder aus dem Repository gelöscht wurden, werden sie durch diesen Vorgang wiederhergestellt.
- Ein Archiv kann als Quelle für eine Bare-Metal-Wiederherstellung oder Export in eine virtuelle Maschine verwendet werden.

Erstellen eines Archivs

Sie können dieses Verfahren verwenden, um ein einmaliges oder geplantes Archiv zu erstellen.

Wenn Sie vorhaben, ein Archiv an einem Cloud-Speicherort zu erstellen, fügen Sie zunächst Ihr Cloud-Konto zur Rapid Recovery Core Console hinzu. Weitere Informationen hierzu finden Sie unter Hinzufügen eines Cloud-Kontos.

Ein einmaliges Archiv ist ein Archiv, das bedarfsorientiert für eine bestimmte Maschine erstellt wird. Ein geplantes Archiv ist ein Archiv, das automatisch an dem im Assistenten festgelegten Datum und zu der festgelegten Uhrzeit erstellt wird. Wenn Sie eine wiederkehrende Archivierung planen, erfüllen Sie die Anforderungen für die Archivierung von Daten aus den geschützten Maschinen häufig, ohne dass Sie jedes Mal ein einmaliges Archiv definieren müssen.

Wenn Sie ein Archiv erstellen, müssen Sie entscheiden, ob eine vollständige Wiederherstellungspunktkette in das Archiv eingeschlossen werden soll. Weitere Informationen finden Sie unter Wiederherstellungspunktkettenoptionen für Archive.

1. Klicken Sie auf der Schaltflächenleiste der Rapid Recovery Core Console auf **Archiv**.

   Der Archivierungsassistent wird geöffnet.
2. Wählen Sie auf der Seite **Archivtyp** des Assistenten eine der folgenden Optionen aus:
   - Einmaliges Archiv
   - Fortlaufende Archivierung (nach Zeitplan)
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Speicherort** eine Option aus der Drop-Down-Liste **Speicherorttyp** und geben Sie die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 151. Optionen zum Speicherorttyp des Archivs

Option	Textfeld	Description
Lokal	Speicherort	Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. `d:\work\archive`.
Netzwerk	Speicherort	Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. `\\servername\sharename`.
	Benutzername	Geben Sie den Benutzernamen für den Benutzer mit Zugriff auf die Netzwerkfreigabe ein.
	Kennwort	Geben Sie das Kennwort für den Benutzer mit Zugriff auf die Netzwerkfreigabe ein.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **NOTE:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen hierzu finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.
	Ordnername	Geben Sie einen Namen für den Ordner ein, in dem die archivierten Daten gespeichert sind.
	Glacier Speicher verwenden	Wählen Sie diese Option zum Speichern Ihres Archivs im Amazon Glacier Speicher. Diese Option ist für die langfristige Speicherung von Archiven

Option	Textfeld	Description
		vorgesehen. Weitere Informationen finden Sie unter Amazon Speicheroptionen und Archivierung.

5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Maschinen** des Assistenten aus, welche geschützten Maschinen Sie archivieren möchten, und klicken Sie dann auf **Weiter**.
7. Führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie sich dafür entschieden haben, ein einmaliges Archiv zu erstellen, fahren Sie mit Schritt 14 fort.
   - Wenn Sie sich dafür entschieden haben, eine geplante Archivierung zu erstellen, fahren Sie mit Schritt 8 fort.
8. Wählen Sie auf der Seite **Zeitplan** eine der folgenden Optionen aus der Drop-Down-Liste **Daten senden** aus:
   - Täglich
   - Wöchentlich
   - Monatlich
9. Geben Sie abhängig von Ihrer Auswahl in Schritt 8 die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 152. Optionen zum Senden von Daten

Option	Textfeld	Description
Täglich	Uhrzeit	Wählen Sie die Uhrzeit aus, zu der täglich ein Archiv erstellt werden soll.
Wöchentlich	Wochentag	Wählen Sie einen Wochentag aus, an dem das Archiv automatisch erstellt werden soll.
	Uhrzeit	Wählen Sie die Uhrzeit aus, zu der ein Archiv erstellt werden soll.
Monatlich	Tag im Monat	Wählen Sie den Tag im Monat aus, an dem das Archiv automatisch erstellt werden soll.
	Uhrzeit	Wählen Sie die Uhrzeit aus, zu der ein Archiv erstellt werden soll.

10. Wenn Sie nach Abschluss des Assistenten nicht möchten, dass der Archivierungsauftrag zum nächsten geplanten Zeitpunkt beginnt, können Sie optional **Anfängliche Archivierung vorübergehend anhalten** auswählen.

    NOTE: Sie können die geplante Archivierung beispielsweise zunächst deaktivieren, wenn Sie den Zielspeicherort vorbereiten müssen, bevor die Archivierung stattfindet. Wenn Sie diese Option nicht auswählen, beginnt die Archivierung zum angegebenen geplanten Zeitpunkt.
11. Klicken Sie auf **Weiter**.
12. Wählen Sie auf der Seite **Optionen** für eine fortlaufende Archivierung, eine der in der folgenden Tabelle beschriebenen Recycling-Aktionen ein.

Tabelle 153. Optionen zum Recycling bei fortlaufender Archivierung

Textfeld	Description
Diesen Core ersetzen	Alle bereits vorhandenen archivierten Daten auf dem Core werden überschrieben. Die Daten anderer Cores bleiben aber unverändert.

Textfeld	Description
Vollständig löschen	Alle archivierten Daten werden aus dem Verzeichnis gelöscht, bevor das neue Archiv geschrieben wird.
Inkrementell	Bietet die Möglichkeit, Wiederherstellungspunkte zu einem vorhandenen Archiv hinzuzufügen. Die Wiederherstellungspunkte werden verglichen, um eine Duplizierung von bereits im Archiv vorhandenen Daten zu vermeiden.

13. Legen Sie auf der Seite **Optionen** für eine fortlaufende Archivierung fest, ob volle Wiederherstellungspunktketten in das Archiv eingeschlossen werden sollen. Weitere Informationen zu den Optionen für Wiederherstellungspunktketten finden Sie unter Wiederherstellungspunktkettenoptionen für Archive. Führen Sie eine der folgenden Aktionen aus:
    - Wählen Sie **Vollständige Wiederherstellungsketten, einschließlich referenzierter Basisabbilder außerhalb des Datumsbereichs, erstellen** und gehen Sie dann zu Schritt 17.
    - **Nur die Wiederherstellungspunkte im Datumsbereich einschließen. Diese Option spart Speicherplatz, aber Sie sind verantwortlich für die Archivierung alle erforderlichen Basisabbilder** und gehen Sie dann zu Schritt 17.
14. Geben Sie auf der Seite **Optionen** (Optionen) die in der folgenden Tabelle beschriebenen Informationen ein:

Tabelle 154. Optionen für einmaliges Archiv

Textfeld	Description
Maximale Größe	Umfangreiche Datenarchive können in mehrere Segmente aufgeteilt werden. Wählen Sie den maximalen Speicherplatz aus, der zum Erstellen des Archivs reserviert werden soll. Führen Sie dazu einen der folgenden Schritte aus: • Wählen Sie **Gesamtes Ziel** aus, um den gesamten verfügbaren Speicherplatz im Pfad, der in Schritt 4 für das Ziel angegeben wurde, zu reservieren. (Wenn beispielsweise `D:\work\archive`, als Speicherort angegeben wurde, wird der gesamte verfügbare Speicherplatz auf dem Laufwerk D: reserviert.) • Geben Sie in das Textfeld die Menge an Speicherplatz ein und wählen Sie dann eine Maßeinheit in der Dropdown-Liste aus, um den maximal reservierten Speicherplatz festzulegen. **NOTE:** Archive in der Amazon-Cloud werden automatisch in 50-GB-Segmente aufgeteilt. Archive in der Microsoft Azure-Cloud werden automatisch in 200-GB-Segmente aufgeteilt.
Recyclingaktion	Wählen Sie eine der folgenden Optionen als Recyclingaktion aus: • **Nicht wiederverwenden.** Vorhandene archivierte Daten am Speicherort werden nicht überschrieben oder gelöscht. Wenn der Speicherort nicht leer ist, gestattet Ihnen Rapid Recovery, einen anderen Speicherort auszuwählen. • **Diesen Core ersetzen.** Alle bereits vorhandenen archivierten Daten auf dem Core werden überschrieben. Die Daten anderer Cores bleiben aber unverändert. • **Vollständig löschen.** Alle archivierten Daten werden aus dem Verzeichnis gelöscht, bevor das neue Archiv geschrieben wird. • **Inkrementell.** Bietet die Möglichkeit, Wiederherstellungspunkte zu einem vorhandenen Archiv hinzuzufügen. Die Wiederherstellungspunkte werden verglichen, um eine Duplizierung von bereits im Archiv vorhandenen Daten zu vermeiden.

Textfeld	Description
Anmerkung	Geben Sie alle zusätzlich erforderlichen Informationen für die Erfassung des Archivs ein. Der Kommentar wird angezeigt, wenn Sie das Archiv später importieren.
Vollständige Wiederherstellungspunkte einschließlich referenzierter Basisabbilder außerhalb des Datumsbereichs, erstellen.	Wählen Sie diese Option aus, um die gesamte Wiederherstellungspunkt-Kette zu archivieren. Diese Option ist standardmäßig ausgewählt.
Nur die Wiederherstellungspunkte im Datumsbereich einschließen. Dies spart Speicherplatz, aber Sie sind verantwortlich für die Archivierung aller erforderlichen Basisabbilder.	Wählen Sie diese Option aus, um nur die inkrementellen Wiederherstellungspunkte und keine Basisabbilder zu archivieren. **NOTE:** Diese Option führt zu einem Archiv verwaister Wiederherstellungspunkte. Sie können diese nicht für die Wiederherstellung verwenden, bis Sie auch die zugehörigen Basisabbilder archivieren. Weitere Informationen zu den Optionen für Wiederherstellungspunktketten finden Sie unter Wiederherstellungspunktkettenoptionen für Archive.

15. Wenn Sie die Option gewählt haben, dass nur Wiederherstellungspunkte in dem Datumsbereich eingeschlossen werden sollen, klicken Sie auf **Weiter**. Andernfalls klicken Sie auf **Fertigstellen**.
16. Geben Sie auf der Seite **Datumsbereich** entweder manuell das Start- und Enddatum der zu archivierenden Wiederherstellungspunkte ein oder wählen Sie Datum/Uhrzeit aus, indem Sie auf das Kalendersymbol und dann auf das Uhrsymbol unter dem Kalenderfenster klicken.
17. Klicken Sie auf **Fertig stellen**.

    Der Assistent wird geschlossen.

Archivieren in einer Cloud

Wenn die Daten das Ende eines Aufbewahrungszeitraums erreichen, können Sie die Aufbewahrung verlängern, indem Sie ein Archiv der alten Daten erstellen. Beim Archivieren von Daten, ist stets zu überlegen, wo Sie sie speichern sollten. Rapid Recovery ermöglicht das Hochladen Ihres Archivs auf eine Vielzahl von Cloud-Anbietern direkt über die Core Console. Kompatible Clouds sind Microsoft Azure, Amazon S3, jeder OpenStack-basierte Anbieter, Rackspace-Cloud-Dateien und Google Cloud.

Der Export eines Archivs in eine Cloud mit Rapid Recovery umfasst die folgenden Verfahren:

- Hinzufügen Ihres Cloud-Kontos zum Rapid Recovery Core Console. Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos.
- Daten archivieren und in das Cloud-Konto exportieren. Weitere Informationen finden Sie unter Erstellen eines Archivs.
- Abrufen archivierter Daten durch Anhängen eines Archivs oder Importieren vom Cloud-Speicherort. Weitere Informationen finden Sie unter Anfügen eines Archivs bzw. Importieren eines Archivs.

Bearbeiten einer geplanten Archivierung

Sie können in Rapid Recovery die Details einer geplanten Archivierung ändern. Führen Sie die nachstehend beschriebenen Schritte aus, um eine geplante Archivierung zu bearbeiten.

1. Klicken Sie in der Rapid Recovery Core Console auf das Drop-Downmenü **More** (Mehr) in der Symbolleiste und wählen Sie dann **Archivierungen** aus.
2. Klicken Sie auf der Seite **Archivierungen** auf das Drop-Down-Menü unter „geplanten Archivierungen“ neben der zu ändernden Archivierung und klicken Sie dann auf **Bearbeiten**.

   Der **Archivierungsassistent** wird geöffnet.
3. Wählen Sie auf der Seite **Location** (Speicherort) des Assistenten zum Hinzufügen von Archiven eine der folgenden Optionen aus der Dropdownliste **Location Type** (Speicherorttyp) aus:
   - Lokal
   - Netzwerk
   - Cloud
4. Geben Sie die in der folgenden Tabelle beschriebenen Details für das Archiv auf Basis der Position, die Sie in Schritt 3 ausgewählt haben, ein.

Tabelle 155. Archivierungsdetails

Option	Textfeld	Description
Lokal	Speicherort	Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. `d:\work\archive`.
Netzwerk	Speicherort	Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. `\\servername\sharename`.
	Benutzername	Geben Sie den Benutzernamen für den Benutzer mit Zugriff auf die Netzwerkfreigabe ein.
	Kennwort	Geben Sie das Kennwort für den Benutzer mit Zugriff auf die Netzwerkfreigabe ein.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **NOTE:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen hierzu finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.
	Ordnername	Geben Sie einen Namen für den Ordner ein, in dem die archivierten Daten gespeichert sind.
	Glacier Speicher verwenden	Wählen Sie diese Option zum Speichern Ihres Archivs im Amazon Glacier Speicher. Diese Option ist für die langfristige Speicherung von Archiven

Option	Textfeld	Description
		vorgesehen. Weitere Informationen finden Sie unter Amazon Speicheroptionen und Archivierung/

5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Machines** (Maschinen) des Assistenten die geschützte/n Maschine/n aus, die Wiederherstellungspunkte enthält/enthalten, die Sie archivieren möchten. Löschen Sie die Maschinen, die Sie nicht archivieren möchten.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Zeitplan** eine der folgenden Optionen aus der Drop-Down-Liste **Daten senden** aus:
   - Täglich
   - Wöchentlich
   - Monatlich
9. Geben Sie abhängig von Ihrer Auswahl in Schritt 8 die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 156. Optionen zum Senden von Daten

Option	Textfeld	Description
Täglich	Uhrzeit	Wählen Sie die Uhrzeit aus, zu der täglich ein Archiv erstellt werden soll.
Wöchentlich	Wochentag	Wählen Sie einen Wochentag aus, an dem das Archiv automatisch erstellt werden soll.
	Uhrzeit	Wählen Sie die Uhrzeit aus, zu der täglich ein Archiv erstellt werden soll.
Monatlich	Tag im Monat	Wählen Sie den Tag im Monat aus, an dem das Archiv automatisch erstellt werden soll.
	Uhrzeit	Wählen Sie die Uhrzeit aus, zu der täglich ein Archiv erstellt werden soll.

10. Wahlweise können Sie **Pause initial archiving** (Anfängliche Archivierung anhalten) auswählen, um die Archivierung anzuhalten und zu einem späteren Zeitpunkt wieder aufzunehmen.

> **NOTE:** Sie können die geplante Archivierung beispielsweise zunächst deaktivieren, wenn Sie den Zielspeicherort vorbereiten müssen, bevor die Archivierung stattfindet. Wenn Sie diese Option nicht auswählen, beginnt die Archivierung zum angegebenen geplanten Zeitpunkt.

11. Klicken Sie auf **Weiter**.
12. Wählen Sie auf der Seite **Options** (Optionen) in der Dropdownliste **Recycle action** (Maßnahme wiederverwenden) eine der in der folgenden Tabelle beschriebenen Optionen aus:

Tabelle 157. Optionen zur Wiederverwendung von Maßnahmen

Textfeld	Description
Inkrementell	Bietet die Möglichkeit, Wiederherstellungspunkte zu einem vorhandenen Archiv hinzuzufügen. Die Wiederherstellungspunkte werden verglichen, um eine Duplizierung von bereits im Archiv vorhandenen Daten zu vermeiden.
Diesen Core ersetzen	Alle bereits vorhandenen archivierten Daten auf dem Core werden überschrieben. Die Daten anderer Cores bleiben aber unverändert.

Textfeld	Description
Vollständig löschen	Alle archivierten Daten werden aus dem Verzeichnis gelöscht, bevor das neue Archiv geschrieben wird.

13. Legen Sie auf der Seite **Optionen** des Assistenten, fest, ob volle Wiederherstellungspunktketten in das Archiv eingeschlossen werden sollen. Weitere Informationen zu den Optionen für Wiederherstellungspunktketten finden Sie unter Wiederherstellungspunktkettenoptionen für Archive. Führen Sie eine der folgenden Aktionen aus:
    - Wählen Sie**Vollständige Wiederherstellungsketten, einschließlich referenzierter Basisabbilder außerhalb des Datumsbereichs, erstellen**.
    - **Nur die Wiederherstellungspunkte im Datumsbereich einschließen. Dies spart Speicherplatz, aber Sie sind verantwortlich für die Archivierung aller erforderlichen Basisabbilder.**
14. Klicken Sie auf **Fertig stellen**.

    Rapid Recovery nimmt die gewünschten Änderungen am Archiv vor.

Deaktivieren oder Aktivieren einer geplanten Archivierung

Wenn Sie einen Archivierungsjob als wiederholt geplant haben, können Sie diese Maßnahme nach Bedarf anhalten oder wiederaufnehmen.

Bisweilen kann es vorkommen, dass Sie einen geplanten Archivierungsjob vorübergehend deaktivieren müssen, z. B. wenn der Zielspeicherort für das Archiv geändert werden muss. Wenn die Archivierung bei der Durchführung der in Erstellen eines Archivs beschriebenen Schritte vorübergehend deaktiviert wurde, soll die geplante Archivierung vermutlich zu einem späteren Zeitpunkt wieder aktiviert werden. Führen Sie die folgenden Schritte aus, um eine geplante Archivierung vorübergehend zu deaktivieren und wieder zu aktivieren.

1. Klicken Sie in der Rapid Recovery Core Console auf das Menü **Mehr** in der Symbolleiste und wählen Sie dann **Archive** aus.
2. Wählen Sie auf der Seite **Archive** unter „Geplante Archive“ eine der folgenden Optionen aus:
    - Wählen Sie das gewünschte Archiv aus und klicken Sie dann auf eine der folgenden Aktionen:
        - Vorübergehend deaktivieren
        - Fortsetzen
    - Klicken Sie neben dem gewünschten Archiv im Dropdown-Menü auf eine der folgenden Aktionen:
        - Vorübergehend deaktivieren
        - Fortsetzen

    Der Status des Archivs wird in der Spalte „Zeitplan“ angezeigt.

Erzwingen eines Archivierungs-Jobs

Mithilfe dieses Verfahrens können Sie Rapid Recovery zwingen, den Archivierungs-Job zu einem beliebigen Zeitpunkt an einer geplanten Archivierung durchzuführen.

Um einen Archivierungs-Job zu erzwingen, müssen Sie eine Archivierung auf dem Kern geplant haben.

1. Klicken Sie in der Rapid Recovery Core Console auf das Menü **Mehr** in der Symbolleiste und klicken Sie dann auf **Archive**.
2. Klicken Sie auf der Seite „Archive“ unter „Geplante Archivierung“ auf das Dropdown-Menü neben der Archivierung, die erzwungen werden soll, und klicken Sie dann auf **Erzwingen**.

   Rapid Recovery archiviert die Wiederherstellungspunkte entsprechend den gewählten Einstellungen für diese Archivierung, und zwar unabhängig von der Zeit, die für die geplante Archivierung eingestellt wurde.

Überprüfen eines Archivs

Durch Überprüfen eines Archivs lässt sich feststellen, ob sich ein Archiv und sein Inhalt in einem Zustand befinden, der eine Wiederherstellung zulässt.

Sie können ein Archiv auf die Integrität seiner Struktur, Datensegmente, und Indexdateien scannen, indem Sie eine Archivprüfung durchführen. Die Archivprüfung ermittelt, ob alle erforderlichen Dateien im Archiv vorliegen und ob die Dateien funktionsfähig sind. Führen Sie die nachstehend beschriebenen Schritte aus, um eine Archivprüfung durchzuführen.

1. Klicken Sie in der Rapid Recovery Core Console auf das Menü **Mehr** in der Symbolleiste und klicken Sie dann auf **Archive**.
2. Klicken Sie auf der Seite **Archive** auf **Überprüfen**.

   Das Dialogfeld **Archiv überprüfen** wird angezeigt.
3. Wählen Sie für **Location Type** (Speicherorttyp) eine der folgenden Optionen aus der Drop-Down-Liste aus:
   - Lokal
   - Netzwerk
   - Cloud
4. Basierend auf dem Positionstyp, den Sie in Schritt 3 ausgewählt haben, geben Sie die Details für das Archiv ein, wie in der folgenden Tabelle beschrieben.

Tabelle 158. Archivierungsdetails

Option	Textfeld	Description
Lokal	Speicherort	Geben Sie den lokalen Pfad für das Archiv ein.
Netzwerk	Speicherort	Geben Sie den Netzwerkpfad für das Archiv ein.
	Benutzername	Geben Sie den Benutzernamen ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
	Kennwort	Geben Sie das Kennwort für den Netzwerkpfad ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **NOTE:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen hierzu finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.

Option	Textfeld	Description
	Ordnername	Wählen Sie den Ordner aus, in dem die archivierten Daten gespeichert sind, z. B. „Rapid Recovery-7-Archive-[ERSTELLUNGSDATUM]-[ERSTELLUNGSZEIT]“.

5. Wählen Sie eine der in der folgenden Tabelle beschriebenen Optionen aus bzw. löschen Sie die Auswahl. Alle sind standardmäßig ausgewählt.

   NOTE: Löschen Sie nicht alle Prüfungen. Sie müssen mindestens eine Option auswählen.

Option	Description
Index files mapping offsets (Zuordnungsoffsets von Indexdateien)	Diese Option überprüft, ob sich alle Daten in der internen Struktur des Archivs an der korrekten Position befinden.
Structure integrity (Strukturelle Integrität)	Diese Option überprüft, ob bestimmte interne Dateien vorliegen und ob die Ordnerstruktur des Archivs korrekt ist. Wenn irgendwelche Dateien oder Ordner fehlen, schlägt die Prüfung fehl.
Prüfsummenintegrität	Diese Option prüft die Integrität der Datensegmente im Archiv, um sicherzustellen, dass die Segmente funktionsfähig sind.

6. Klicken Sie auf **Datei überprüfen**.

   Rapid Recovery überprüft das Archiv entsprechend Ihrer Auswahl.

Anfügen eines Archivs

Durch Anfügen eines Archivs sind Sie in der Lage, Wiederherstellungspunkte aus dem Archiv anzuzeigen.

Sie müssen über ein bereits vorhandenes Archiv verfügen, das in Rapid Recovery Core Version 6.0.1 oder höher erstellt wurde, um dieses Verfahren durchführen zu können. Weitere Informationen hierzu finden Sie unter Erstellen eines Archivs.

Wenn Sie ein Archiv anfügen, wird der von Ihnen angegebene Archivname als ein Archivmenü im linken Navigationsmenü der Core Console angezeigt. Jede geschützte Maschine mit Wiederherstellungspunkten im Archiv wird separat unter dem Archivmenü aufgeführt. Sie können auf einen beliebigen Maschinennamen im Archiv klicken und durch seine Wiederherstellungspunkte blättern. Sie können dann dieselben Aktionen wie mit jedem anderen Wiederherstellungspunkt, der derzeit in Ihrem Core sichtbar ist, durchführen.

Durch Anfügen des Archivs werden auch die Anmeldeinformationen für den Zugriff auf die Informationen zwischengespeichert. Bis Sie die angefügte Archivdefinition löschen, können Sie das Archiv nach Belieben einfach neu anfügen und trennen, wodurch Sie einfachen Zugriff auf die Wiederherstellungspunkte erhalten.

Gehen Sie folgendermaßen vor, um ein Archiv anzufügen.

1. Klicken Sie auf der Rapid Recovery Core Console auf das Drop-Down-Menü **Archiv** und wählen Sie dann **Archiv anfügen**.

   Das Dialogfeld **Archiv anfügen** wird angezeigt.
2. Geben Sie im Textfeld **Name** einen Namen für dieses angefügte Archiv ein.

   Der in diesem Feld eingegebene Wert wird im linken Navigationsmenü als der Archiv-Menüname angezeigt.

Gemäß bewährten Verfahren zum Anzeigen von Namen sollte der Archivname zwischen 1 und 64 alphanumerische Zeichen einschließlich Leerzeichen enthalten. Verwenden Sie keine unzulässigen Zeichen oder unzulässigen Phrasen.

3. Wählen Sie in der Drop-Down-Liste**Speicherorttyp** den Speicherorttyp Ihres Archiv aus den folgenden Optionen aus:
   - Lokal
   - Netzwerk
   - Cloud
4. Geben Sie die in der folgenden Tabelle beschriebenen Details für das Archiv auf Basis der Position, die Sie in Schritt 3 ausgewählt haben, ein.

Tabelle 159. Details zum Speicherorttyp

Option	Textfeld	Description
Lokal	Speicherort	Geben Sie den Pfad zum Archiv ein, z. B. `D:\Arbeit\Archiv`.
Netzwerk	Speicherort	Geben Sie den Pfad zum Archiv ein, z. B. `\\Servername\Freigabename`.
	Benutzername	Geben Sie den Benutzername für die Anmeldung bei der Netzwerkfreigabe ein.
	Kennwort	Geben Sie das Kennwort für die Anmeldung bei der Netzwerkfreigabe ein.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **NOTE:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen hierzu finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Drop-Down-Menü den Container für das mit dem Konto verknüpfte Archiv aus.
	Ordnername	Geben Sie den Namen des Ordners ein, in dem die archivierten Daten gespeichert sind, z. B. „Rapid-Recovery-Archive-[ERSTELLUNGSDATUM]-[ERSTELLUNGSZEIT]“.

5. Klicken Sie auf **Attach** (Verknüpfen).

   Das Archiv wird an diesen Core angefügt und mountet den Inhalt als ein Dateisystem.

Importieren eines Archivs

Sie können dieses Verfahren anwenden um ein Archiv einmalig zu importieren oder um den wiederholten Import eines Archivs zu planen.

Wenn Sie archivierte Daten wiederherstellen möchten, können Sie das gesamte Archiv an einen angegebenen Speicherort importieren.

CAUTION: Führen Sie diesen Schritt nur nach sorgfältiger Prüfung durch. Durch den Import eines Archivs wird das Repository mit den Inhalten des Archivs neu gefüllt, wobei alle neuen Daten im Repository seit Erfassung des Archivs ersetzt werden.

Führen Sie die nachstehend beschriebenen Schritte aus, um ein Archiv zu importieren.

1. Klicken Sie in der Menüleiste der Rapid Recovery Core Console auf das Drop-Down-Menü **Archiv** und wählen Sie dann **Archiv importieren** aus.

   Der **Import Archive Wizard** (Assistent zum Hinzufügen eines Archivs) wird geöffnet.
2. Wählen Sie auf der Seite **Import Type** (Importtyp) des Assistenten eine der folgenden Optionen aus:
   - Einmaliger Import
   - Wiederholter Import (nach Zeitplan)
3. Klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite **Location** (Speicherort) in der Dropdownliste den Speicherort des Archivs aus, das Sie importieren möchten und geben Sie dann die in der folgenden Tabelle beschriebenen Informationen ein:

Tabelle 160. Speicherort-Optionen für importierte Archive

Option	Textfeld	Description
Lokal	Speicherort	Geben Sie den lokalen Pfad an, in dem das Archiv gespeichert werden soll, z. B. `d:\work\archive`.
Netzwerk	Speicherort	Geben Sie den Netzwerkpfad an, in dem das Archiv gespeichert werden soll, z. B. `\\servername\sharename`.
	Benutzername	Geben Sie den Benutzernamen für den Benutzer mit Zugriff auf die Netzwerkfreigabe ein.
	Kennwort	Geben Sie das Kennwort für den Benutzer mit Zugriff auf die Netzwerkfreigabe ein.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **NOTE:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen hierzu finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.
	Ordnername	Geben Sie einen Namen für den Ordner ein, in dem die archivierten Daten gespeichert sind.

5. Klicken Sie auf **Weiter**.
6. Wenn Sie alle im Archiv enthaltenen Maschinen importieren möchten, wählen Sie auf der Seite **Archive Information** (Archivinformationen) des Assistenten die Option **Import all machines** (Alle Maschinen importieren) aus.
7. Schließen Sie basierend auf Ihrer Auswahl eine der folgenden Optionen ab:
   - Wenn Sie **Einmaliger Import** in Schritt 2 und **Alle Maschinen importieren** in Schritt 6 ausgewählt haben und alle Maschinen als geschützte, replizierte oder reine Wiederherstellungspunkt-Maschinen im Core vorhanden sind, fahren Sie fort mit Schritt 12.
   - Wenn Sie **Wiederholter Import (nach Zeitplan)** in Schritt 2 und **Alle Maschinen importieren** in Schritt 6 ausgewählt haben und mindestens eine Maschine nicht als geschützte, replizierte oder reine

Wiederherstellungspunkt-Maschine im Core vorhanden ist, klicken Sie auf **Weiter** und fahren Sie mit Schritt 9 fort.

- Falls Sie in Schritt 6 nicht alle Maschinen importiert haben, klicken Sie auf **Weiter** und fahren Sie mit Schritt 8 fort.

8. Wählen Sie auf der Seite **Machines** (Maschinen) die Maschinen aus, die aus dem Archiv importiert werden sollen.
   - Wenn Sie **Einmaliger Import** in Schritt 2 ausgewählt haben und mindestens eine Maschine nicht als geschützte, replizierte oder reine Wiederherstellungspunkt-Maschine im Core vorhanden ist, verwenden Sie die Drop-Down-Listen, um ein Repository für jede Maschine auszuwählen, die Sie importieren möchten, und fahren Sie dann mit Schritt 12 fort.
   - Wenn alle Maschinen bereits als geschützte, replizierte oder reine Wiederherstellungspunkt-Maschinen im Core vorhanden sind, fahren Sie mit Schritt 12 fort.
9. Klicken Sie auf **Weiter**.
10. Schließen Sie auf der Seite **Repository** eine der folgenden Optionen ab:
    - Wenn ein Repository mit dem Core verknüpft ist, wählen Sie eine der Optionen der folgenden Tabelle aus:

Tabelle 161. Repository-Optionen

Option	Description
Use an existing Repository (Vorhandenes Repository verwenden)	Wählen Sie ein Repository, das derzeit mit diesem Core verknüpft ist, aus der Dropdownliste aus.
Create a Repository (Neues Repository erstellen)	Geben Sie im Server-Textfeld den Namen des Servers ein, auf dem Sie das neue Repository speichern möchten, zum Beispiel: Servername oder lokaler Host, und befolgen Sie anschließend die Anweisungen unter. Erstellen eines DVM-Repository.

    - Wenn kein Repository mit dem Core verknüpft ist, geben Sie den Namen des Servers ein, auf dem Sie das neue Repository speichern möchten, zum Beispiel: Servername oder Localhost, und befolgen Sie anschließend die Anweisungen unter Erstellen eines DVM-Repository.
11. Wenn Sie **Wiederholter Import (nach Zeitplan)** in Schritt 2 ausgewählt haben, wählen Sie auf der Seite **Zeitplan** die in der folgenden Tabelle beschriebenen Optionen aus:

Tabelle 162. Zeitplan-Importoptionen

Option	Description
Täglich	Klicken Sie auf das Uhrsymbol und verwenden Sie die Auf- und Abwärtspfeile, um auszuwählen, zu welchem Zeitpunkt der Archivierungsjob beginnen soll. Wenn Sie ein System mit 12-Stunden-Zeitformat verwenden, klicken Sie zur Angabe der Tageszeit auf die AM- oder PM-Schaltfläche.
Wöchentlich	Wählen Sie den Wochentag und die gewünschte Startzeit des Archivierungsjobs aus. Wenn Sie ein System mit 12-Stunden-Zeitformat verwenden, klicken Sie zur Angabe der Tageszeit auf die AM- oder PM-Schaltfläche.
Monatlich	Wählen Sie den Tag des Monats und die Uhrzeit, zu der der Archivierungsjob beginnen soll.

Option	Description
	Wenn Sie ein System mit 12-Stunden-Zeitformat verwenden, klicken Sie zur Angabe der Tageszeit auf die AM- oder PM-Schaltfläche.
Pause initial importing (Anfängiche Import anhalten)	Wählen Sie diese Option aus, wenn Sie nicht möchten, dass der Importjob zum nächsten geplanten Zeitpunkt nach Abschluss des Assistenten ausgeführt wird. **NOTE:** Sie können den geplanten Import beispielsweise zunächst deaktivieren, wenn Sie den Zielspeicherort vorbereiten müssen, bevor der Import stattfindet. Wenn Sie diese Option nicht auswählen, beginnt der Import zum geplanten Zeitpunkt.

12. Klicken Sie auf **Fertig stellen**.

Cloud-Konten

Rapid Recovery ermöglicht das Definieren von Verbindungen zwischen bestehenden Cloud-Speicher- oder Cloud-Dienstanbietern und Ihrer Rapid Recovery Core. Kompatible Cloud-Dienste sind Microsoft Azure, Amazon Web Services (AWS), jeder OpenStack-basierte Anbieter (einschließlich Rackspace) und Google Cloud. US-Regierungsspezifische Plattformen umfassen AWS GovCloud (US) und Azure Government. Sie können eine beliebige Anzahl von Cloud-Konten zur Core Console hinzufügen, einschließlich mehrerer Konten für den gleichen Anbieter.

Sie fügen Cloud-Konten zu Ihrer Core Console hinzu, damit Sie mit ihnen zusammenarbeiten können, wie im Abschnitt Informationen zu Cloud-Konten beschrieben.

Sobald diese Konten hinzugefügt wurde, können Sie die Verbindung zwischen dem Core und den Cloud-Konten verwalten. Insbesondere können Sie den Anzeigenamen oder die Anmeldedaten bearbeiten, die Kontoverbindungsoptionen konfigurieren oder das Konto aus Rapid Recovery entfernen. Wenn Sie Cloud-Konten in der Core Console bearbeiten oder entfernen, ändern Sie nicht die Cloud-Konten selbst, sondern nur die Verknüpfung zwischen diesen Konten und Ihre Fähigkeit, über die Core Console darauf zuzugreifen.

In diesem Abschnitt wird beschrieben, wie Sie Verknüpfungen zwischen vorhandenen Cloud-Speicheranbieter- oder Cloud-Dienstanbieter-Konten und der Rapid Recovery Core Console definieren. Außerdem wird beschrieben, wie Sie diese Cloud-Konten in Rapid Recovery verwalten.

Folgende Themen werden behandelt:

- Informationen zu Cloud-Konten
- Überlegungen zu Cloud-Speicheroptionen
- Hinzufügen eines Cloud-Kontos
- Bearbeiten eines Cloud-Kontos
- Entfernen eines Cloud-Kontos

Informationen zu Cloud-Konten

Rapid Recovery kann mit Cloud-Konten auf die folgenden Weisen eingesetzt werden:

- **Archiv**. Sie können ein einmaliges Archiv oder ein fortwährend geplantes Archiv in der Cloud speichern. Diese Funktion wird für alle Cloud-Kontotypen unterstützt. Wenn Sie in die Cloud archivieren, können Sie später auf die Informationen in den archivierten Wiederherstellungspunkten zugreifen, indem Sie die Archive anhängen (gilt für Archive, die in Version 6.0.1 oder höher erstellt wurden). Für alle Archive gilt, dass Sie diese auch importieren können. Sie können auch eine Bare-Metal-Wiederherstellung aus einem Archiv durchführen.
- **Virtueller Export.** Sie können einen virtuellen Export zu einem Azure Cloud-Konto einleiten. Dies beinhaltet einen einmaligen Export einer virtuellen Maschine oder den fortwährenden Export einer virtuellen Standby-VM.

Konzeptionelle Informationen zu verschiedenen Cloud-Konten finden Sie unter Überlegungen zu Cloud-Speicheroptionen.

Informationen zum Konfigurieren von Timeout-Einstellungen zwischen dem Core und Cloud-Konten finden Sie unter Konfigurieren von Verbindungseinstellungen des Cloud-Kontos.

Informationen zum Durchführen eines virtuellen Exports zur Azure Cloud finden Sie unter Exportieren von Daten in eine virtuelle Azure Maschine.

Überlegungen zu Cloud-Speicheroptionen

In diesem Abschnitt wird die Unterstützung für Cloud-Speicherkonten von US-Behörden erläutert. Er beschreibt auch Kompromisse zwischen Kosten und andere Faktoren bei der Auswahl der Cloud-Konten für die Archivierung.

Sichere Cloud-Konten für die US-Regierung

Staatliche, Bundes-, und lokale US-Regierungsbehörden und ihre Partner haben Zugang zur erweiterten Cloud-Kontooptionen.Rapid Recovery unterstützt die folgenden Angebote für Regierungs- und Cloud-Konten:

- **AWS GovCloud (US).**Amazon Web Services bietet einen Dienst namens AWS GovCloud (US). Dabei handelt es sich um eine isolierte AWS-Region zur Erfüllung bestimmter behördlicher Auflagen und Complianceanforderungen. Mit diesem Dienst können US-Regierungsbehörden und Kunden gemeinsam mit privaten Unternehmen Cloud-Konten nutzen.Rapid Recovery Unterstützt die Archivierung in Amazon S3-Speicherkonten in der AWS GovCloud.
- **Azure Government.** Azure Government ist eine der US-Regierung vorbehaltene Cloud-Plattform, die ausschließlich staatlichen, Bundes-, lokalen und stammeszugehörigen Regierungsbehörden und deren Partnern zur Verfügung steht. Rapid Recovery unterstützt Azure Government auf die gleiche Weise, wie wir auch standardmäßigen Azure Support bieten. Beispiel:
  - Rapid Recovery unterstützt die Archivierung in Azure Government und standardmäßigen Azure Speicherkonten.
  - Rapid Recovery unterstützt den virtuellen Export auf eine virtuelle Azure Maschine (einmalig oder virtueller Standby) auf öffentlichen und Azure Government Plattformen.
  - Rapid Recovery unterstützt die Replikation firmeninterner Cores auf ein Replikationsziel in der öffentlichen und Azure Government Cloud-Plattform. Für beide Plattformen können Sie bei Anmeldung bei Azure Marketplace die Option „Rapid Recovery Replication Target“ im Azure Government Marketplace auswählen. Auf dieser VM berechnet Azure Dienste und Speicher, die Sie zur VM für Ihr Repository hinzufügen, sodass Benutzer schnell und einfach einen Ziel-Core einrichten können, der Ihre firmeninternen Sicherungsdaten in der Azure Government-Cloud repliziert.

Ausgleich von Zugriffszeit, Kosten und Komfort für die Archivierung in Cloud-Konten

Um unseren Nutzern kostengünstige Cloud-Archivierung und virtuelle Exportoptionen bereitzustellen, erweitertRapid Recovery weiterhin den Support von Cloud-Speicher-Anbietern (und Speicherklassen für führende Anbieter, die diese anbieten). Erfahrene Anwender können durch Anwendung von Richtlinien einen Kompromiss zwischen Einfachheit der Datenarchivierung, Datenzugriffszeit und Kosten erzielen.

Beim Abwägen der Strategien für die Archivierung oder Export in die Cloud sind Rapid Recovery Anwender angehalten, sich über die Kompromisse zwischen den anfänglichen Speicherkosten von Daten, wie häufig die Daten erwartungsgemäß verwendet werden, die Notwendigkeit, innerhalb einer vorgeschriebenen Zeit Zugriff auf die Daten zu erhalten und die Kosten im Zusammenhang mit dem Abruf der Daten zu informieren.

Einige Anbieter (z. B. Amazon S3) bieten verschiedene Speicherklassen an. Die Auswahl der richtigen Speicherklasse kann Ihnen Geld sparen, sofern Ihre Annahmen bezüglich dieser Faktoren korrekt sind. Quest empfiehlt Rapid Recovery Benutzern, Datenspeicherungsrichtlinien mindestens einmal jährlich zu prüfen, um sicherzustellen, dass Sie Ihre Ressourcen effektiv nutzen. Ebenso wird Administratoren nahegelegt, die in Cloud-Konten archivierten oder exportierten Daten zu prüfen , damit Sie Ihre Annahmen bezüglich der Planung und Migration der Daten entsprechend anpassen können.

Die Speicherung von Daten ist bei einigen Anbietern mit sehr niedrigen Kosten verbunden oder in einigen Fällen kostenlos. Jedoch können Cloud-Dienstanbieter oft Gebühren auferlegen, wenn Sie auf die entsprechenden Daten zugreifen oder sie abrufen. Es gibt oft unterschiedliche Gebühren, je nachdem wie schnell Sie auf die Daten zugreifen müssen. In einigen Fällen kann sich die Nutzung der teureren Speicheroptionen (z. B.

Amazon S3-Standard) als kostengünstiger erweisen, wenn Sie vorhaben, von Wiederherstellungspunkten wiederherzustellen, als wenn Sie in Glacier gespeicherte Daten wiederherstellen müssen.

Bei Amazon können Sie Lebenszyklus-Richtlinien für Daten definieren, damit Daten im Laufe der Zeit zwischen Amazon S3-Klassen verschoben werden. Zum Beispiel könnten Sie kürzlich hochgeladene Daten mit der Standard-Speicherklasse speichern, sie 30 Tage später in die Standard – Infrequent Access-Klasse verschieben und dann nach weiteren 60 Tagen in die Reduced Redundancy Storage-Klasse. Sie können Daten auch ausdrücklich mit dem Archivierungsassistenten für jeden Typ von Amazon S3-Cloud-Konto in Glacier archivieren. Dies wird empfohlen, wenn erwartungsgemäß sehr selten eine Datenwiederherstellung erforderlich sein wird. Bevor Sie diese Option auswählen, sollten Sie sich über die Gebühren im Zusammenhang mit Zugriff, Speicherungsalter usw. informieren. Lesen Sie dazu das Thema Amazon Speicheroptionen und Archivierung.

Einige Rapid Recovery Funktionen sind speziell für die Cloud vorgesehen. Wenn Sie einen virtuellen Export in die Cloud mit Azure durchführen, sollten Sie Virtual Standby erwägen. Dieser Vorgang ermöglicht Ihnen, eine voll startfähige virtuelle Maschine in der Azure Cloud zu erstellen. Die VM-Dateien werden fortlaufend mit neu erfassten Wiederherstellungspunkten aktualisiert. Im Gegensatz zu einem firmenintern durchgeführten Virtual Standby werden die VM-Dateien nicht in einer startfähigen VM bereitgestellt, oder erst dann, wenn Sie sie benötigen. Die anfänglichen Kosten für Virtual Standby in Azure umfassen nur die Speicherkosten. Berechnungskosten (die bei Azure langfristig gesehen beträchtlich sein können) entstehen nur dann, wenn die VM bereitgestellt wird, was zum Starten einer VM und dem Durchführen einer Wiederherstellung erforderlich ist.

Sie können auch einen firmeneigenen Core in der Azure Cloud mitRapid Recovery „Replikationsziel“ replizieren. Sie können durch Auswahl von „Rapid Recovery Replikationsziel“ in Azure Marketplace schnell und einfach einen Ziel-Core einrichten. Die Berechnungskosten werden dem Ziel-Core zugeschrieben. Sie müssen auch für Repository-Speicher in Azure planen. Wenn Sie mit Version 6.2 noch nicht vertraut sind, können Sie „Replikationsziel“ auch in der Government-Cloud verwenden. Informationen zum Replizieren in Azure finden Sie im *Rapid Recovery Replication Target for Microsoft Azure - Setup-Handbuch*

Rapid Recovery Benutzer, die solche Cloud-Speicheroptionen nutzen, werden aufgefordert, sich über die Kompromisse zwischen den anfänglichen Speicherkosten von Daten, der Notwendigkeit, innerhalb einer vorgeschriebenen Zeit Zugriff auf die Daten zu erhalten, und die Kosten im Zusammenhang mit dem Abruf der Daten zu informieren.

Die Speicherung von Daten ist bei einigen Anbietern mit sehr niedrigen Kosten verbunden oder in einigen Fällen kostenlos. Jedoch können Cloud-Dienstanbieter oft Gebühren auferlegen, wenn Sie auf die entsprechenden Daten zugreifen oder sie abrufen. Es gibt oft unterschiedliche Gebühren, je nachdem wie schnell Sie auf die Daten zugreifen müssen. In einigen Fällen kann sich die Nutzung der teureren Speicheroptionen (z. B. Amazon S3-Standard) als kostengünstiger erweisen, wenn Sie vorhaben, von Wiederherstellungspunkten wiederherzustellen, als wenn Sie in Glacier gespeicherte Daten wiederherstellen müssen.

Bei Amazon können Sie Lebenszyklus-Richtlinien für Daten definieren, damit Daten im Laufe der Zeit zwischen Amazon S3-Klassen verschoben werden. Zum Beispiel könnten Sie kürzlich hochgeladene Daten mit der Standard-Speicherklasse speichern, sie 30 Tage später in die Standard – IA-Klasse verschieben und dann nach weiteren 60 Tagen nach Amazon Glacier.

Hinzufügen eines Cloud-Kontos

Bevor Sie Daten in beide Richtungen zwischen einem Cloud-Konto und Ihrem Core verschieben können, müssen Sie die Kontoinformationen des Cloud-Anbieters auf der Rapid Recovery Core Console hinzufügen. Diese Informationen identifizieren das Cloud-Konto in der Core Console, während die Verbindungsinformationen auf sichere Weise gecacht werden. Dieser Prozess ermöglicht dann dem Rapid Recovery Core, eine Verbindung zum Cloud-Konto herzustellen, um die angegebenen Vorgänge durchzuführen.

Führen Sie die nachstehend beschriebenen Schritte aus, um ein Cloud-Konto hinzuzufügen.

1. Klicken Sie auf der Rapid Recovery Core Console Symbolleiste auf das Symbol **Mehr** und wählen Sie dann **Cloud-Konten**.

   Die Seite **Cloud-Konten** wird angezeigt.
2. Klicken Sie auf der Seite **Clouds** auf **Neues Konto hinzufügen**.

Daraufhin wird das Dialogfeld **Add New Account** (Neues Konto hinzufügen) geöffnet.

3. Wählen Sie in der Drop-Down-Liste „Cloud-Typ“ einen kompatiblen Cloud-Anbieter aus.
4. Geben Sie die in der folgenden Tabelle beschriebenen Informationen auf der Grundlage des Cloud-Typs ein, den Sie in Schritt 3 ausgewählt haben.

Tabelle 163. Cloud-Kontodetails

Cloud-Typ	Textfeld	Description
Microsoft Azure	Anzeigename	Geben Sie einen Anzeigenamen für dieses Cloud-Konto für die Anzeige auf der Rapid Recovery Core Console ein, z. B. Azure Cloud-Konto 1.
	Speicherkontoname	Geben Sie den Namen Ihres Microsoft Azure-Speicherkontos ein. **NOTE:** Der Name muss mit dem Speicherkontonamen in Azure genau übereinstimmen. Er darf nur Kleinbuchstaben und Zahlen enthalten und muss zwischen 3 und 24 Zeichen lang sein.
	Zugriffsschlüssel	Geben Sie den Zugriffsschlüssel für Ihr Konto ein. **NOTE:** Sie können den primären oder sekundären Schlüssel eingeben. Um den Zugriffsschlüssel von Ihrem Azure Konto abzurufen, aktivieren Sie **Schlüssel** unter **Einstellungen**.
	HTTPS-Protokoll verwenden	Wählen Sie diese Option aus, um das sichere https-Protokoll anstelle des standardmäßigen http-Protokolls zu verwenden.
Amazon S3	Anzeigename	Geben Sie einen Anzeigenamen für dieses Cloud-Konto für die Anzeige auf der Rapid Recovery Core Console ein, z. B. Amazon S3 Cloud-Konto 1.
	Zugriffsschlüssel	Geben Sie den Zugriffsschlüssel für Ihr Amazon Cloud-Konto ein.
	Geheimer Schlüssel	Geben Sie den geheimen Schlüssel für dieses Konto ein.
	Dienst-Endpunkt	Wenn ein anderes S3-kompatibles Speicherkonto als das standardmäßige Amazon S3-Konto verwenden, geben Sie die vollständig qualifizierten Http- oder Https-URL für den Speicher ein.
	Speicherklasse	Wählen Sie eine Speicherklasse für das S3-Konto. Sie haben folgende Auswahlmöglichkeiten: • Standard • Standard – Unregelmäßiger Zugriff • Weniger Redundanzspeicher Wenn Sie auf Glacier archivieren möchten, können Sie Ihr Amazon Cloud-Konto mit jeder aufgeführten Speicherklasse definieren. Die Option zur Auswahl des Glacier Speichers ist über den Archivierungsassistenten verfügbar.

Cloud-Typ	Textfeld	Description
		NOTE: Weitere Informationen zu Speicherklassen finden Sie im Thema Überlegungen zu Cloud-Speicheroptionen.
Powered by OpenStack	Anzeigename	Geben Sie einen Anzeigenamen für dieses Cloud-Konto für die Anzeige auf der Rapid Recovery Core Console ein, z. B. OpenStack Cloud-Konto 1.
	Region	Geben Sie die Region für Ihr Cloud-Konto ein.
	Benutzername	Geben Sie den Benutzernamen für Ihr OpenStack-basiertes Cloud-Konto ein.
	Kennwort oder API-Schlüssel	Wählen Sie aus, ob Sie ein Kennwort verwenden oder einen API-Schlüssel und geben Sie dann Ihre Auswahl für dieses Konto ein.
	Tenant-ID	Geben Sie Ihre Tenant-ID für dieses Konto ein.
	Authentifizierungs-URL	Geben Sie die Authentifizierungs-URL für dieses Konto ein. Dies ist die Basis-URL für die Cloud-Instanz. Sofern nicht bereitgestellt, verwendet Rapid Recovery Core die Standard-URL https://identity.api.rackspacecloud.com.
Rackspace Cloud-Dateien	Anzeigename	Geben Sie einen Anzeigenamen für dieses Cloud-Konto für die Anzeige auf der Rapid Recovery Core Console ein, z. B. Rackspace Cloud-Konto 1.
	Region	Verwenden Sie die Drop-Down-Liste, um die Region für Ihr Konto auszuwählen.
	Benutzername	Geben Sie den Benutzernamen für Ihr Rackspace-Cloud-Konto ein.
	Kennwort oder API-Schlüssel	Wählen Sie aus, ob Sie ein Kennwort verwenden oder einen API-Schlüssel und geben Sie dann Ihre Auswahl für dieses Konto ein.
	Tenant-ID	Geben Sie Ihre Tenant-ID für dieses Konto ein.
	Authentifizierungs-URL	Geben Sie die Authentifizierungs-URL für dieses Konto ein. Dies ist die Basis-URL für die Cloud-Instanz. Sofern nicht bereitgestellt, verwendet Rapid Recovery Core die Standard-URL https://identity.api.rackspacecloud.com.
Google Cloud	Anzeigename	Geben Sie einen Anzeigenamen für dieses Cloud-Konto für die Anzeige auf der Rapid Recovery Core Console ein, z. B. Google Cloud-Konto 1.
	Zertifikatsdatei	Suchen Sie Ihre Google Zertifikat-Datei für die Authentifizierung dieses Cloud-Kontos und wählen Sie sie aus.
	Privater Schlüssel	Geben Sie Ihren geheimen Schlüssel für dieses Konto ein.

Cloud-Typ	Textfeld	Description
	Projekt-ID	Geben Sie die Projekt-ID für dieses Konto ein.
	E-Mail-Adresse des Service-Kontos	Geben Sie die E-Mail-Adresse ein, die bei Google Cloud als Eigentümer dieses Cloud-Dienstkontos registriert ist.

5. Klicken Sie auf **Speichern**.

   Das Dialogfeld wird geschlossen und das Konto wird auf der Seite **Cloud-Konten** der Core Console angezeigt.

Bearbeiten eines Cloud-Kontos

Wenn Sie die Informationen für die Verbindung zu Ihrem Cloud-Konto ändern müssen, z. B. um das Kennwort oder den Anzeigenamen zu ändern, können Sie dies auf der Seite **Cloud-Konten** der Rapid Recovery Core Console durchführen. Führen Sie die folgenden Schritte aus, um ein Cloud-Konto zu bearbeiten.

1. Klicken Sie auf der Rapid Recovery Core Console Symbolleiste auf das Symbol **Mehr** und wählen Sie dann **Cloud-Konten**.

   Die Seite **Cloud-Konten** wird angezeigt.

2. Klicken Sie im Drop-Down-Menü neben dem Cloud-Konto, das Sie bearbeiten möchten, auf **Bearbeiten**.

   Das Fenster **Konto bearbeiten** wird geöffnet.

3. Bearbeiten Sie die Details nach Bedarf und geben Sie dann das Kennwort (oder den API-Schlüssel, geheimen Schlüssel, privaten Schlüssel usw.) ein, das erforderlich ist, um sich mit dem Cloud-Konto zu verbinden. Klicken Sie dann auf **Speichern**.

   NOTE: Sie können den Cloud-Typ nicht bearbeiten.

Entfernen eines Cloud-Kontos

Wenn Sie den Cloud-Dienst nicht mehr weiter nutzen oder für einen bestimmten Core nicht mehr nutzen möchten, können Sie das Cloud-Konto aus der Core Console entfernen. Führen Sie die folgenden Schritte aus, um ein Cloud-Konto zu entfernen.

1. Klicken Sie auf der Rapid Recovery Core Console Symbolleiste auf das Symbol **Mehr** und wählen Sie dann **Cloud-Konten**.

   Die Seite **Cloud-Konten** wird angezeigt.

2. Klicken Sie im Drop-Down-Menü neben dem Cloud-Konto, das Sie bearbeiten möchten, auf das Drop-Down-Konto und wählen Sie dann **Entfernen** aus.
3. Klicken Sie im Dialogfeld **Konto löschen** auf **Ja**, um zu bestätigen, dass das Konto gelöscht werden soll.
4. Wenn das Cloud-Konto derzeit verwendet wird, werden Sie in einem zweiten Dialogfeld gefragt, ob das Konto dennoch entfernt werden soll. Klicken Sie zur Bestätigung auf **Ja**.

   NOTE: Wenn Sie ein Konto entfernen, das derzeit verwendet wird, schlagen alle für das betreffende Konto geplanten Archivierungsjobs fehl.

Das Dialogfeld wird geschlossen und die Anmeldeinformationen für den Zugriff auf das angegebene Cloud-Konto werden aus dem Core entfernt.

Das Local Mount Utility

In diesem Abschnitt wird das Herunterladen, Installieren und Verwenden des Windows-basierten Rapid Recovery Local Mount Utility (LMU) beschrieben, das zum Laden von Wiederherstellungspunkten und Durchsuchen der Inhalte auf Dateiebene mithilfe eines Computers, der keinen Rapid Recovery Core hostet, dient.

Informationen zum Local Mount Utility

LMU (Local Mount Utility) ist eine herunterladbare Windows-basierte Anwendung, mit der Sie einen Rapid Recovery-Wiederherstellungspunkt in jedem der drei verfügbaren Modi auf einem beliebigen kompatiblen Windows-Computer laden können. Das schlanke Programm kann auf demselben 32-Bit und 64-Bit Windows-Betriebssystem wie die Rapid Recovery Agent-Software installiert werden, muss aber nicht auf dem gleichen Computer wie der Agent installiert werden. Die LMU umfasst die Treiber rapidrecovery-vdisk (ehemals aavdisk) und aavstor, wird aber nicht als Dienst ausgeführt. Wenn Sie das Programm installieren, wird es standardmäßig im Verzeichnis `C:\Program Files\AppRecovery\Local Mount Utility` installiert und es wird eine Verknüpfung auf dem Desktop des Computers erstellt.

Das Dienstprogramm wurde zwar für den Remote-Zugriff auf einen Computer mit Rapid Recovery Kern konzipiert, Sie können das LMU aber auch auf demselben Computer als Rapid RecoveryKern installieren. Wenn es in einem Kern ausgeführt wird, erkennt es alle Bereitstellungen dieses Kerns und zeigt sie an, einschließlich der Bereitstellungen durch die Rapid Recovery Kern-Konsole. Genauso werden auch Bereitstellungen, die durch das LMU durchgeführt wurden, in der Kern-Konsole angezeigt.

Wenn das LMU auf dem gleichen Computer wie Mailbox Restore installiert ist, führt das LMU automatisch Mailbox Restore aus, wenn Sie es zum Öffnen einer Exchange-Datenbank verwenden. Mailbox Restore ist die Rapid Recovery Anwendung, die von Quest verwendet wird, um Microsoft Exchange Datenspeicher und Elemente wiederherzustellen. Sie können es bei der Installation des LMU oder des Rapid Recovery Kerns installieren. Weitere Informationen zu Mailbox Restore finden Sie in *Mailbox Restore for Exchange - Benutzerhandbuch.*

NOTE: Linux-Computer verwenden das Befehlszeilendienstprogramm local_mount für die Abfrage des Kerns geschützter Computer und deren entsprechenden Wiederherstellungspunkten. In gleicher Weise ermöglicht es dieses Dienstprogramm dem Benutzer einen Wiederherstellungspunktvolume im Remote-Zugriff zu laden, den Inhalt des Volume auf Dateiebene zu durchsuchen und einzelne Dateien oder ein ganzes Volume aus dem Wiederherstellungspunkt wiederherzustellen, einschließlich einer BMR-Wiederherstellung des System-Volumes. Weitere Informationen finden Sie unter *Rapid Recovery Benutzerhandbuch.*

Arbeiten mit Rapid Recovery Kern-Computern im Local Mount Utility

Das Local Mount Utility (LMU) ermöglicht Ihnen das Arbeiten mit einer unbegrenzten Anzahl von Kern-Computern lokal oder im Fernzugriff. Wenn Sie das LMU auf einem Rapid Recovery Core Server installieren, wird diese Maschine automatisch im LMU als Localhost angezeigt. Alle weiteren Remote-Kerne werden mit ihren Computernamen oder IP-Adressen je nach den eingegebenen Informationen beim Hinzufügen angezeigt. Mit

dem LMU können Sie Kerncomputer hinzufügen, bearbeiten und entfernen. Weitere Informationen finden Sie in den folgenden Abschnitten:

- Hinzufügen einer Core-Maschine zum Local Mount Utility
- Verändern der Optionen des Local Mount Utility
- Bearbeiten von Core-Verbindungseinstellungen im Local Mount Utility
- Erneut verbinden mit einem Core
- Verschieben einer Rapid Recovery Core-Maschine zum Local Mount Utility

Zugehörige Tasks

See also: Hinzufügen einer Core-Maschine zum Local Mount Utility
See also: Verändern der Optionen des Local Mount Utility
See also: Bearbeiten von Core-Verbindungseinstellungen im Local Mount Utility
See also: Erneut verbinden mit einem Core
See also: Verschieben einer Rapid Recovery Core-Maschine zum Local Mount Utility

Hinzufügen einer Core-Maschine zum Local Mount Utility

Zum Bereitstellen eines Wiederherstellungspunkts müssen Sie eine Core-Maschine zum LMU hinzufügen. Es gibt keine Beschränkung, wie viele Cores Sie hinzufügen können.

Führen Sie die folgenden Schritte aus, um das Local Mount Utility durch Hinzufügen eines Core einzurichten.

1. Auf der Maschine, auf der das LMU installiert ist, starten Sie das LMU durch Doppelklicken auf das Desktop-Symbol.
2. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie aus dem Local Mount Utility-Menü in der oberen linken Eck auf **Core hinzufügen**.
   - Klicken Sie mit der rechten Maustaste auf den freien Platz im linken Bereich und klicken Sie dann auf **Core hinzufügen**.

   Das Dialogfeld **Core hinzufügen** wird angezeigt.
3. Geben Sie im Dialogfeld **Core hinzufügen** die erforderlichen Anmeldeinformationen ein (siehe folgende Tabelle).

Tabelle 164. Rapid Recovery **Core-Anmeldeinformationen**

Option	Description
Hostname	Der Name oder die IP-Adresse des Core, von dem aus Sie Wiederherstellungspunkte bereitstellen möchten. **NOTE:** Wenn Sie das Local Mount Utility in einem Rapid Recovery Core installieren, fügt das Programm automatisch die lokale Maschine (localhost) hinzu.
Port	Die zur Kommunikation mit dem Core verwendete Portnummer. Die Standardportnummer ist 8006.
Meine Windows-Benutzeranmeldeinformationen verwenden	Wählen Sie diese Option aus, wenn die Anmeldeinformationen, die Sie für den Zugriff auf den Core verwenden, die gleichen wie Ihre Windows-Anmeldeinformationen sind.

Option	Description
Bestimmte Anmeldeinformationen verwenden	Wählen Sie diese Option aus, wenn die Anmeldeinformationen, mit denen Sie auf den Core zugreifen, sich von Ihren Windows-Anmeldeinformationen unterscheiden.
Benutzername	Der Benutzername, der zum Zugriff auf die Core-Maschine verwendet wird. **NOTE:** Diese Option ist nur verfügbar, wenn Sie bestimmte Anmeldeinformationen verwenden.
Kennwort	Das Kennwort, das für den Zugriff auf die Core-Maschine verwendet wird. **NOTE:** Diese Option ist nur verfügbar, wenn Sie bestimmte Anmeldeinformationen verwenden.

4. Klicken Sie auf **Verbinden**.
5. Wenn Sie mehrere Cores hinzufügen möchten, wiederholen Sie die Schritte wie erforderlich.

Verändern der Optionen des Local Mount Utility

Führen Sie das folgende Verfahren zum Ändern der Optionen für alle Rapid Recovery Core aus, die mit dem LMU verbunden sind.

1. Klicken Sie in der Benutzeroberfläche der Local Mount Utility Benutzeroberfläche auf **Optionen**.
2. Im Dialogfeld **Optionen** können Sie die Einstellungen ändern, wie in der folgenden Tabelle beschrieben.

Tabelle 165. Core-Einstellungen

Option	Description
Speicherort	Verwenden Sie die Schaltfläche **Durchsuchen** oder geben Sie den Pfad zum Ordner ein, den Sie für die Bereitstellung von Wiederherstellungspunkten verwenden möchten.
Bereitstellungstyp	Geben Sie an, wie der Datenzugriff für den bereitgestellten Wiederherstellungspunkt erfolgen soll: • Nur-Lesen • Schreibgeschützt mit vorherigen Schreibvorgängen • Beschreibbar

Option	Description
Sprache	Wählen Sie die Sprache aus, in der Sie möchten, dass das LMU angezeigt wird. Sie können zwischen folgenden Optionen wählen: • Englisch • Französisch • Deutsch • Portugiesisch • Spanisch • Chinesisch (vereinfacht) • Japanisch • Koreanisch
Autom. aktualisieren	Wählen Sie aus (bzw. geben Sie ein), in welchem Zeitraum das LMU seine Verbindung zu einem Core aktualisieren sollte, um die neuesten Informationen zu erhalten.
Lokalen Core anzeigen	Wenn das LMU auf einem Core-Rechner installiert ist, zeigen Sie den Core durch Aktivieren dieser Option an.
Popup-Benachrichtigungen anzeigen	Gestatten Sie dem LMU, Sie anhand von Popups auf Ihrem Desktop über Ereignisse und Warnungen zu informieren.
Bereitstellungsordner in Windows Explorer öffnen, wenn die Bereitstellung erfolgreich war	Wählen Sie diese Option, um den Inhalt eines bereitgestellten Wiederherstellungspunkts durchsuchen zu können.

3. Klicken Sie auf **Speichern**.

Bearbeiten von Core-Verbindungseinstellungen im Local Mount Utility

Zum Bearbeiten der Einstellungen, die Sie beim Hinzufügen eines Core zum LMU hergestellt haben, gehen Sie wie folgt vor.

NOTE: Dieses Verfahren gilt nicht für den localhost-Core. Es gilt nur für Remote Core-Maschinen.

1. Klicken Sie aus der Local Mount Utility-Benutzeroberfläche mit der rechten Maustaste auf den Core, dessen Einstellungen Sie bearbeiten möchten und klicken Sie dann auf **Core bearbeiten**.
2. Im Dialogfeld **Core bearbeiten** können Sie die Einstellungen ändern, wie in der folgenden Tabelle beschrieben.

Tabelle 166. Core-Einstellungen

Option	Description
Hostname	Der Name des Core, von dem aus Sie Wiederherstellungspunkte bereitstellen möchten. **NOTE:** Wenn Sie das Local Mount Utility in einem Rapid Recovery Core installieren, fügt das Programm automatisch die lokale Maschine (localhost) hinzu.
Port	Die zur Kommunikation mit dem Core verwendete Portnummer. Die Standardportnummer ist 8006.
Meine Windows-Benutzeranmeldeinformationen verwenden	Wählen Sie diese Option aus, wenn die Anmeldeinformationen, die Sie für den Zugriff auf den Core verwenden, die gleichen wie Ihre Windows-Anmeldeinformationen sind.
Bestimmte Anmeldeinformationen verwenden	Wählen Sie diese Option aus, wenn die Anmeldeinformationen, mit denen Sie auf den Core zugreifen, sich von Ihren Windows-Anmeldeinformationen unterscheiden.
Benutzername	Der Benutzername, der zum Zugriff auf die Core-Maschine verwendet wird. **NOTE:** Diese Option ist nur verfügbar, wenn Sie bestimmte Anmeldeinformationen verwenden.
Kennwort	Das Kennwort, das für den Zugriff auf die Core-Maschine verwendet wird. **NOTE:** Diese Option ist nur verfügbar, wenn Sie bestimmte Anmeldeinformationen verwenden.

3. Nachdem Sie Ihre Änderungen vorgenommen haben, klicken Sie auf **OK**.

Erneut verbinden mit einem Core

Wenn Sie die Verbindung zu einerRapid Recovery Core Maschine verlieren, können Sie die Verbindung wiederherstellen, indem Sie auf der LMU-Startseite auf **Aktualisieren** klicken.

Verschieben einer Rapid Recovery Core-Maschine zum Local Mount Utility

Führen Sie die folgenden Verfahren aus, um einen Core aus dem LMU zu entfernen.

NOTE: Diese Option ist nicht verfügbar für einen Rapid Recovery Core, der sich auf dem „localhost“ befindet und so benannt ist.

1. Klicken Sie aus der Local Mount Utility-Benutzeroberfläche mit der rechten Maustaste auf den Core, Sie entfernen möchten und klicken Sie dann auf **Core entfernen**.
2. Um den Befehl zu bestätigen, klicken Sie im Dialogfeld auf **Ja**.

   Das LMU entfernt den Core und seine geschützte Maschinen aus der Navigationsstruktur.

Arbeiten mit geschützten Maschine im Local Mount Utility

Mit dem Local Mount Utility (LMU) können Sie Wiederherstellungspunkte von geschützten Maschinen laden und durchsuchen, ohne mit der Rapid Recovery Core Console im Zusammenhang mit dieser Maschine angemeldet zu sein. Weitere Informationen finden Sie in den folgenden Abschnitten:

- Bereitstellen eines Wiederherstellungspunkts mit dem Local Mount Utility
- Untersuchen eines bereitgestellten Wiederherstellungspunktes mit dem Local Mount Utility
- Aktualisieren von Wiederherstellungspunkten
- Aufheben der Bereitstellung von Wiederherstellungspunkten in der Local Mount Utility

Bereitstellen eines Wiederherstellungspunkts mit dem Local Mount Utility

Mit dem LMU können Sie einen beliebigen Wiederherstellungspunkt im Zusammenhang mit einer verbundenen Core-Maschine bereitstellen, einschließlich der geschützten Maschinen, replizierten Maschinen und Nur-Wiederherstellungspunkte-Maschinen.

Vor dem Bereitstellen eines Wiederherstellungspunktes muss das Local Mount Utility (LMU) eine Verbindung mit dem Core herstellen, auf dem der Wiederherstellungspunkt gespeichert ist. Wie in der Vorgehensweise Hinzufügen einer Core-Maschine zum Local Mount Utility beschrieben, ist die Anzahl der Cores, die zum LMU hinzugefügt werden können, unbegrenzt.

1. Wählen Sie in der LMU die Maschine aus, von der ein Wiederherstellungspunkt bereitgestellt werden soll.
2. Wählen Sie den Wiederherstellungspunkt, den Sie bereitstellen möchten, und wählen Sie dann eine der folgenden Optionen aus:

Option	Description
Bereitstellen	Mit dieser Option können Sie den Wiederherstellungspunkt mit der Standardauswahl aus den LMU-Optionen bereitstellen. Weitere Informationen hierzu finden Sie unter. Verändern der Optionen des Local Mount Utility.
Erweiterte Bereitstellung...	Diese Option öffnet das Dialogfeld **Erweiterte Bereitstellung**.

3. Wenn Sie die Option **Erweiterte Bereitstellung** gewählt haben, führen Sie die in der folgenden Tabelle beschriebenen Optionen aus.

Tabelle 167. Erweiterte Bereitstellungsoptionen

Option	Description
Pfad für Bereitstellungspunkt	Geben Sie den Speicherort für die Bereitstellung der Wiederherstellungspunkte an oder navigieren Sie zu diesem Speicherort.

Option	Description
Bereitstellungstyp	Wählen Sie eine der folgenden Optionen aus: • Schreibgeschützt bereitstellen • Mit Schreibzugriff bereitstellen • Schreibgeschützt bereitstellen mit vorherigen Schreibvorgängen Beschreibungen zu jeder Option finden Sie in Schritt 4.

- Klicken Sie auf **Bereitstellen**.

Das LMU öffnet automatisch den Ordner, in dem sich der bereitgestellte Wiederherstellungspunkt befindet. In der Spalte der lokalen Bereitstellungen auf der Seite „Wiederherstellungspunkte“ der LMU ist angegeben, wie der Wiederherstellungspunkt bereitgestellt wurde.

Untersuchen eines bereitgestellten Wiederherstellungspunktes mit dem Local Mount Utility

Das Untersuchen eines Wiederherstellungspunkts öffnet die gesicherten Daten in einem Windows Explorer-Fenster. Sie haben die Möglichkeit zum Durchsuchen von Volumes und Ordnern für das Element oder die Elemente, das/die Sie wiederherstellen möchten.

Sie können dann Elemente durch Kopieren an Ihren bevorzugten Standort mithilfe eines Datei Managers, wie z. B. Windows Explorer (oder programmatisch mit Windows-APIs) wiederherstellen. Führen Sie das folgende Verfahren aus, um einen aktuell geladenen Wiederherstellungspunkt zu untersuchen.

NOTE: Das Verfahren ist nicht erforderlich, wenn Sie einen Wiederherstellungspunkt direkt nach seiner Bereitstellung untersuchen, da sich der Ordner, in dem sich der Wiederherstellungspunkt befindet, nach Abschluss des Bereitstellungsvorgangs automatisch öffnet.

1. Klicken Sie in der Benutzeroberfläche des Local Mount Utility auf **Aktive Bereitstellungen**.

   Das Fenster Aktive Bereitstellungen wird geöffnet. Darin werden alle bereitgestellten Wiederherstellungspunkte angezeigt.
2. Erweitern Sie die Navigationsstruktur, um die für jede Maschine und deren Volumes bereitgestellt Wiederherstellungspunkte anzuzeigen.
3. Klicken Sie auf **Untersuchen** neben dem Volume, das Sie untersuchen möchten.

Aktualisieren von Wiederherstellungspunkten

Wenn die Option aktiviert ist, erhält das Local Mount Utility (LMU) Updates in Echtzeit vom Core und von geschützten Maschinen. Wenn diese Option deaktiviert ist, müssen Sie auf der LMU-Startseite regelmäßig auf **Aktualisieren** klicken, um die neuesten Wiederherstellungspunkte für eine Maschine zu erhalten.

Aufheben der Bereitstellung von Wiederherstellungspunkten in der Local Mount Utility

Führen Sie die folgenden Schritte aus, um eine Bereitstellung von Wiederherstellungspunkten aufzuheben, die in der Local Mount Utility (LMU) bereitgestellt sind.

1. Klicken Sie in der LMU-Benutzeroberfläche auf den Core oder die geschützte Maschine in Zusammenhang mit dem Wiederherstellungspunkt oder den Wiederherstellungspunkten.
2. Führen Sie eine der folgenden Aktionen aus:
   - Um die Bereitstellung aller bereitgestellten Wiederherstellungspunkte in dem ausgewählten Core oder der ausgewählten geschützten Maschine gleichzeitig aufzuheben, klicken Sie auf **Bereitstellung aller aufheben.** und klicken Sie dann im Dialogfeld auf **Ja**.
   - Um einen einzelnen Wiederherstellungspunkt aufzuheben, wählen Sie den Wiederherstellungspunkt aus der Liste aus und klicken Sie anschließend auf **Bereitstellung aufheben**.

   Der Wiederherstellungspunkt bzw. die Wiederherstellungspunkte werden aufgehoben.

Core Console-Referenzen

Dieser Anhang enthält außerdem Referenztabellen, die viele der Funktionen und Symbole in der Rapid Recovery Core Console beschreiben. Er dient als Ergänzung für das Kapitel Core Console des *Rapid Recovery Benutzerhandbuch*.

Anzeigen der Benutzeroberfläche der Core Console

Die Core Console ist die Hauptbenutzeroberfläche, über die Benutzer Rapid Recovery bedienen. Wenn Sie sich bei der Rapid Recovery Core Console anmelden, werden die folgenden Elemente angezeigt.

Tabelle 168. UI-Elemente der Core Console

Beschreibungen zu den Menüs und Informationen, die in der Core Console erscheinen.

UI-Element	Description
Brandingbereich	Bei typischen Umgebungen ist der rechte obere Bereich der Core Console mit dem vollen Produktname gekennzeichnet, einschließlich Quest Logo. Klicken im Bereich Branding führt dazu, dass eine neue Registerkarte in einem Web-Browser geöffnet wird, die Produktdokumentation auf der Support-Website anzeigt.
Schaltflächenleiste	Die Schaltflächenleiste, die rechts neben dem Branding-Bereich angezeigt wird, enthält Schaltflächen, die überall auf der Core Console zugänglich sind. Diese Tasten starten Assistenten, die häufige Aufgaben, wie Schutz einer Maschine, Durchführen einer Wiederherstellung von einem Wiederherstellungspunkt, Erstellen, Verbinden oder Importieren eines Archivs oder Replikation von diesem Quell-Core auf einen Ziel-Core, erledigen. Jede Schaltfläche in der Schaltflächenleiste ist in der Tabelle Tabelle 169 näher beschrieben.
Anzahl aktiver Aufgaben	Zeigt die Anzahl der Jobs an, die derzeit ausgeführt werden. Dieser dynamische Wert hängt vom Systemzustand ab. Wenn Sie auf das Dropdown-Menü klicken, wird eine Statusübersicht für alle derzeit aktiven Jobs angezeigt. Durch Klicken auf das **X** für einen Job können Sie den betreffenden Job abbrechen.
Dropdown-Menü „Hilfe“	Das Menü **Hilfe** enthält folgende Optionen: • **Hilfe**. Links zur Produkthilfe, die sich in einem separaten Browserfenster öffnet. • **Dokumentation**. Ruft die Rapid Recovery technische Dokumentation auf der Quest Website auf. • **Support**. Ruft die Quest Datenschutz-Support Website auf, die Zugriff auf Live-Chats, Videolernprogramme, Rapid Recovery Knowledge Base-Artikel, häufig gestellte Fragen usw. ermöglicht. • **Schnellstarthandbuch**. Beim Schnellstarthandbuch handelt es sich um eine Folge der vorgeschlagenen Aufgaben zum Konfigurieren und Verwenden von Rapid Recovery. Die Anleitung wird automatisch geöffnet, wenn Sie sich bei der Core Console anmelden (sofern diese Funktion nicht deaktiviert wurde). Sie können die Kurzanleitung auch

UI-Element	Description
	jederzeit im Hilfemenü öffnen. Weitere Informationen zu dieser Funktion finden Sie unter Grundlegende Informationen zur Kurzanleitung. • **Eine Idee einsenden**. Wenn Sie Vorschläge zu Funktionen oder Verbesserungen haben, wählen Sie diese Option zum Öffnen des Quest Ideen-Portals, in dem Sie schnell und einfach ihre Ideen beschreiben und von Produktmanagern für die potenzielle Aufnahme in eine zukünftigen Version von Rapid Recovery prüfen lassen können. • **Info**. Öffnet das Dialogfeld „Informationen über Rapid Recovery“. Die hier angezeigten Informationen umfassen die Rapid Recovery Komponente, Versionsinformationen, die Core-ID, einen Hyperlink für Drittanbieter-Beiträge und eine Beschreibung der Software.
Serverdatum und -uhrzeit	Oben rechts in der Core Console wird die aktuelle Uhrzeit der Maschine angezeigt, auf der der Rapid Recovery Core Dienst ausgeführt wird. Wenn Sie mit der Maus auf den Zeitraum zeigen, wird auch das Server-Datum angezeigt. Diese Zeitangabe wird vom System für Ereignisse bei Protokollierung, Planung und Berichterstellung verwendet. Bei der Anwendung von Schutzzeitplänen wird beispielsweise die in der Core Console angezeigte Uhrzeit verwendet. Dies gilt auch, wenn die Zeitzone auf dem Datenbankserver oder auf der Clientmaschine, auf der der Browser ausgeführt wird, unterschiedlich ist.
Symbolleiste	Die Symbolleiste enthält eine grafische Darstellung für Hauptfunktionen in der Core Console. Es wird auf der linken Seite der Benutzeroberfläche (UI), direkt unter dem Branding-Bereich angezeigt. Durch Klicken auf das entsprechende Element in der Symbolleiste gelangen Sie zum entsprechenden Abschnitt der Benutzeroberfläche, in dem Sie die jeweilige Funktion verwalten können. Jedes der Symbole in der Symbolleiste ist in der Tabelle Tabelle 170 näher beschrieben.
Linker Navigationsbereich	Der linke Navigationsbereich wird auf der linken Seite der Benutzeroberfläche, unterhalb der Symbolleiste angezeigt. • Der linke Navigationsbereich enthält den Textfilter und das Menü „Maschinen“. • Wenn die Replikationsfunktion für diesen Core aktiviert wurde, enthält dieser Bereich das Menü „Replizierte Maschinen“. • Wenn Maschinen vorhanden sind, die aus der Schutzfunktion entfernt wurden, für die aber Wiederherstellungspunkte gespeichert wurden, enthält dieser Bereich das Menü „Nur Wiederherstellungspunkte“. • Wenn benutzerdefinierte Gruppen hinzugefügt wurden, enthält dieser Bereich ein Menü für benutzerdefinierte Gruppen. • Wenn Sie ein Archiv eingebunden haben dann enthält dieser Bereich ein angefügtes Archiv-Menü. Sie können den linken Navigationsbereich ein- und ausblenden. Dies ist von Nutzen, wenn im Hauptnavigationsbereich der Benutzeroberfläche mehr Inhalt angezeigt werden soll. Klicken Sie auf den grauen Rand zwischen dem linken Navigationsbereich und dem Hauptnavigationsbereich, um diesen Abschnitt auszublenden. Klicken Sie erneut auf diesen grauen Rand, um dieses UI-Element wieder anzuzeigen. Jedes Element im linken Navigationsbereich ist in der Tabelle Tabelle 172 näher beschrieben.
Kontextsensit Hilfe	Wenn Sie in der Rapid Recovery Core Console auf das Hilfe-Symbol (blaues Fragezeichen) klicken, wird ein Browserfenster veränderlicher Größe mit zwei Bereichen geöffnet. Der linke Frame enthält eine Navigationsstruktur mit Themen aus der *Rapid Recovery Benutzerhandbuch*. Im rechten Bereich wird

UI-Element	Description
?	der Inhalt des ausgewählten Hilfethemas angezeigt. In der Navigationsstruktur der Hilfe wird immer die Position des ausgewählten Themas in der Hierarchie angezeigt. Mit dieser kontextsensitiven Hilfefunktion können Sie alle Themen des *Benutzerhandbuchs* durchsuchen. Schließen Sie den Browser, wenn Sie die Hilfethemen nicht mehr benötigen. Sie können die Hilfe auch über die Option **Hilfe** im Menü **Hilfe** öffnen.

Schaltflächenleiste

Einzelheiten über die Schaltflächenleiste werden in der folgenden Tabelle angezeigt.

Tabelle 169. Schaltflächenleisten-Schaltflächen und -Menüs

Beschreibungen der verfügbaren Aktionen für jedes Menü und der Schaltfläche auf der Schaltflächenleiste der Core Console.

UI-Element	Description
Schaltflächen Schaltfläche und Menüoption „Schützen“	Über die Schaltfläche **Schützen** wird der Assistent zum Schützen einer Maschine gestartet, mit dem Sie eine einzelne Maschine im Rapid Recovery Core schützen können. Weitere Schutzoptionen bietet außerdem das Dropdown-Menü neben dieser Schaltfläche, die folgende Optionen enthält. • Über die Option **Maschine schützen** wird ebenfalls der Assistent zum Schützen einer Maschine aufgerufen. • Über die Option **Cluster schützen** können Sie eine Verbindung zu einem Server-Cluster herstellen. • Über die Option **Schutz mehrerer Maschinen** wird der Assistent zum Schützen mehrerer Maschinen geöffnet, mit dem Sie zwei oder mehr Maschinen gleichzeitig schützen können. • Mit der Option **Bereitstellung der Agentensoftware** haben Sie die Möglichkeit, die Rapid Recovery Agentensoftware auf eine oder mehrere Maschinen gleichzeitig zu installieren. Diese Funktion verwendet den Bereitstellungsassistenten für die Agentensoftware.
Schaltflächen Schaltfläche und Menü „Wiederherstellen“	Über die Schaltfläche **Wiederherstellen** wird der Assistent zum Wiederherstellen einer Maschine geöffnet, mit dem Sie Daten aus Wiederherstellungspunkten wiederherstellen können, die von einer geschützten Maschine gespeichert wurden. Weitere Wiederherstellungs- oder Export-Optionen bietet außerdem das Dropdown-Menü neben dieser Schaltfläche mit dem Sie zwei oder mehr Maschinen gleichzeitig schützen können. • Die Option **Maschine wiederherstellen** ist eine weitere Methode, den Assistenten zum Wiederherstellen einer Maschine zu starten, um Daten wiederherzustellen. • Die Option **Wiederherstellungspunkt bereitstellen** startet den Bereitstellungs-Assistenten, der es Ihnen ermöglicht, Wiederherstellungspunkte von einer geschützten Maschine bereitzustellen. • Über die Option **VM-Export** wird der Exportassistent geöffnet. Mit diesem Assistenten können Sie eine virtuelle Maschine aus Wiederherstellungspunkten erstellen, die im Rapid Recovery Core gespeichert sind. Sie können einen einmaligen Export erstellen oder Parameter für eine VM definieren, die nach jedem Snapshot für eine geschützte Maschine kontinuierlich aktualisiert wird.

UI-Element	Description
Schaltflächen Schaltfläche und Menü „Archiv“ 	Über die Schaltfläche **Archiv** wird der Archivassistent geöffnet. Mithilfe dieses Assistenten können Sie ein einmaliges Archiv von ausgewählten Wiederherstellungspunkten erstellen oder Sie können ein Archiv erstellen und kontinuierlich dieses Archiv basierend auf einem von Ihnen festgelegten Zeitplan archivieren und kontinuierlich speichern. Weitere Archivoptionen bietet außerdem das Dropdown-Menü neben dieser Schaltfläche, die folgende Optionen enthält. • Die ODER **Archiv erstellen** ist eine andere Methode zum Starten des Assistenten zum Erstellen eines Archivs zum Erstellen, um ein einmaligen Archiv zu erstellen oder kontinuierlich zu archivieren. • Die Option **Archiv importieren** startet den Assistenten zum Importieren von Archiven, der es Ihnen ermöglicht, ein Archiv zu importieren. • Die Option **Archiv verbinden** stellt ein Archiv bereit, sodass Sie die Inhalte wie ein Dateisystem lesen können.
Schaltflächen Schaltfläche „Replikation“ 	Über die Schaltfläche **Replikation** wird der Replikationsassistent geöffnet. Mithilfe dieses Assistenten können Sie einen Ziel-Core bestimmen, auf Ihrem Quell-Core geschützte Maschinen wählen und Wiederherstellungspunkte von ausgewählten Maschinen auf dem Ziel-Core, in dem Repository, das Sie angeben, replizieren. Sie können die Replikation vorübergehend deaktivieren oder Sie können die Replikation sofort beginnen. Zusätzlich können Sie festlegen, ob ein Seed-Laufwerk dazu verwendet wird, Daten für die vorhandenen Wiederherstellungspunkte auf den Ziel-Core zu kopieren.

Symbolleiste

Einzelheiten über die Symbolleiste werden in der folgenden Tabelle angezeigt.

Tabelle 170. Symbolleiste

Beschreibungen der verfügbaren Aktionen für jedes Menü auf der Symbolleiste der Core Console.

UI-Element	Description
Symbolleiste	Die Symbolleiste enthält eine grafische Darstellung für Hauptfunktionen in der Core Console. Durch Klicken auf das entsprechende Symbol gelangen Sie zum entsprechenden Abschnitt der Benutzeroberfläche, in dem Sie die jeweilige Funktion verwalten können. Die Symbolleiste umfasst folgende Symbole:
Symbolleiste: Symbol „Startseite“ 	**Startseite**. Klicken Sie auf das Symbol „Startseite“, um zur Core-Startseite zu navigieren.
Symbolleiste: Symbol „Replikation“ 	**Replikation**. Klicken Sie auf das Symbol „Replikation“, um die ein- oder ausgehende Replikation anzuzeigen oder zu verwalten.
Symbolleiste: Symbol „Virtual Standby“ 	**Virtual Standby**. Klicken Sie auf das Symbol „Virtual Standby“, um Informationen aus einem Wiederherstellungspunkt exportieren, um eine startbare virtuelle Maschine zu erstellen.

UI-Element	Description
Symbolleiste: Symbol „Ereignisse“	**Ereignisse**. Klicken Sie auf das Symbol „Ereignisse“, um ein Protokoll aller Systemereignisse für den Rapid Recovery Core anzuzeigen.
Symbolleiste: Symbol „Einstellungen“	**Einstellungen**. Klicken Sie auf das Symbol „Einstellungen“, um Einstellungen für den Rapid Recovery Core anzuzeigen oder zu verwalten. Sie können Core-Konfigurationseinstellungen sichern oder wiederherstellen. Stellen Sie allgemeine Einstellungen zur Steuerung von Anschlüssen oder zur Anzeige von Aspekten einstellen. Zusätzlich können Sie Einstellungen in den folgenden Kategorien konfigurieren: automatische Updates, nächtliche Jobs, Einstellungen für die Übertragungswarteschlange, Client-Zeitüberschreitungseinstellungen, DVM-Deduplizierungs-Cache-Einstellungen, Replay Engine-Einstellungen, und Bereitstellungseinstellungen. Sie können Datenbankverbindungen, Einstellungen für den SMTP-Server und Cloud-Speicherkonten anzeigen oder ändern und Schriftart-Einstellungen für Berichte ändern. Sie können Set SQL-Anfügbarkeitseinstellungen, Core-Job-Einstellungen, Lizenzeinstellungen, SNMP-Einstellungen und vSphere-Einstellungen einrichten.
Symbolleiste: Symbol „Mehr“	**Mehr.** Klicken Sie auf das Symbol „Mehr“ für den Zugriff auf andere wichtige Funktionen. Jede besitzt ein eigenes Symbol, die beide nachfolgend aufgeführt sind.
Symbolleiste: Symbol „Mehr“	Systeminformat  n	**Systeminformationen**. Klicken Sie auf „Systeminformationen“, um Daten über den Rapid Recovery Core-Server anzuzeigen. Angezeigt werden Hostname, Betriebssystem, Architektur und Arbeitsspeicher für den Core. Sie können den in der Core Console angezeigten Name sehen. Darüber hinaus können Sie den vollqualifizierten Domänennamen des Core im Netzwerk sowie den Pfad für die Cachemetadaten und die Deduplizierungscaches anzeigen. Weitere Informationen zum Ändern des Anzeigenamens finden Sie unter Grundlegende Informationen über Systeminformationen für den Core. Weitere Informationen zum Deduplizierungscache finden Sie unter Grundlegende Informationen zu Deduplizierungscache und Speicherorten. Informationen zum Anpassen der Einstellungen finden Sie unter Konfigurieren von DVM-Deduplizierungscache-Einstellungen.
Symbolleiste: Symbol „Mehr“	Archive 	**Archive**. Rapid Recovery ermöglicht Ihnen die Verwaltung von Archiven mit Informationen zum Core. Sie können Informationen zu geplanten oder angehängten Archiven anzeigen und Sie können Archive hinzufügen, überprüfen oder importieren.
Symbolleiste: Symbol „Mehr“	Bereitstellunger 	**Bereitstellungen**. Ermöglicht das Anzeigen und die Aufhebung lokaler Bereitstellungen, sowie Remote-Bereitstellungen anzeigen und trennen.

UI-Element	Description
Symbolleiste: Symbol „Mehr“	Start-CDs  **Start-CDs.** Ermöglicht Ihnen die Verwaltung von Boot-CDs, die in der Regel für eine Bare-Metal-Wiederherstellung (Bare Metal Restore, BMR) verwendet werden. Sie können ein Start-CD-ISO-Image erstellen, ein vorhandenes Image löschen oder auf den Pfad für das Bild klicken, das Sie öffnen oder speichern möchten.
Symbolleiste: Symbol „Mehr“	Repositorys  **Repositorys.** Ermöglicht das Anzeigen und Verwalten von Repositorys im Zusammenhang mit Ihrem Core.
Symbolleiste: Symbol „Mehr“	Verschlüsselun hlüssel  **Verschlüsselungsschlüssel.** Hiermit können Sie Verschlüsselungscodes anzeigen, verwalten, importieren oder hinzufügen, die Sie auf geschützte Maschinen anwenden können. Wenn nicht verwendet, können Sie Verschlüsselungsschlüssel löschen.
Symbolleiste: Symbol „Mehr“	Cloud-Konten  **Cloud-Konten**. Ermöglicht Ihnen Anzeige und Verwaltung von Verbindungen zwischen Ihren Core- und Cloud-Storage Konten.
Symbolleiste: Symbol „Mehr“	Datei suchen  **Datei suchen**. Ermöglicht Ihnen das Durchsuchen von Wiederherstellungspunkten für Dateien, die Sie dann auf einem lokalen Datenträger wiederherstellen können.
Symbolleiste: Symbol „Mehr“	Aufbewahrungs tlinie  **Aufbewahrungsrichtlinie.** Ermöglicht das Anzeigen und Ändern der Core-Aufbewahrungsrichtlinie, einschließlich wie lange Wiederherstellungspunkte vor dem Rollup aufbewahrt und schließlich gelöscht werden.
Symbolleiste: Symbol „Mehr“	Benachrichtigur  **Benachrichtigungen.** Hiermit können Sie Benachrichtigungen über Core-Ereignisse konfigurieren, SMTP-Server-Einstellungen für E-Mail-Benachrichtigungen definieren und Wiederholungsreduzierung zur Unterdrückung wiederholter Benachrichtigungen über dasselbe Ereignis.
Symbolleiste: Symbol „Mehr“	E-Mail-Wiederherstellu g  **E-Mail-Wiederherstellung**. Ermöglicht Ihnen das Durchsuchen von Exchange Server-Datenbanken, um E-Mail-Nachrichten zu suchen und wiederherzustellen.
Symbolleiste: Symbol „Mehr“	Downloads  **Downloads**. Sie können das Internet-Installationsprogramm der Agentensoftware, das Local Mount Utility bzw. MIB-Dateien, die Ereignisinformationen für die Verwendung in einer SNMP-Browser enthalten, herunterladen.
Symbolleiste: Symbol „Mehr“	Berichte  **Berichte**. Hiermit können Sie auf Core-Berichte oder Zeitplan-Berichte auf fortlaufender Basis zugreifen.
Symbolleiste: Symbol „Mehr“	Core-Protokoll  **Core-Protokoll**. Hiermit können Sie die Core-Protokolldatei für Diagnosezwecke herunterladen.

Menü des linken Navigationsbereichs

Der vollständige Satz der Menüs, die im linken Navigationsbereich angezeigt werden können, ist in der folgenden Tabelle beschrieben:

Tabelle 171. Menüoptionen des linken Navigationsbereichs

Beschreibungen der Optionen, die für die Typen der im linken Navigationsbereich aufgeführten Maschinen verfügbar sind.

UI-Element	Description
Menü „Maschinen“	Das Menü „Maschinen“ (früher als „Geschützte Maschinen“ bezeichnet) wird als erstes Menü im linken Navigationsbereich angezeigt, wenn mindestens eine Maschine in Ihrem Core geschützt ist. Wenn Sie auf einen bestimmten Maschinennamen in diesem Bereich klicken, wird eine Übersichtsseite mit einer Zusammenfassung der Informationen zur ausgewählten Maschine angezeigt. Weitere Informationen zu den Aktionen, die Sie auf der Seite "Zusammenfassung" durchführen können, finden Sie unter Anzeigen von zusammenfassenden Informationen für eine geschützte Maschine.
Menü „Replicated machines“ (Replizierte Maschinen)	Wenn der Name eines anderen Rapid Recovery Core als übergeordnetes Navigationsmenü angezeigt wird, ist der Core, auf dem Sie die Core Console anzeigen, ein Ziel-Core. Das Menü „Replicated machines“ (Replizierte Maschinen) wird nach dem Quell-Core benannt, wobei jede darunter aufgeführte Maschine eine Maschine von dem Quell-Core darstellt, der auf dieses Ziel repliziert wird. Wenn dieser Ziel-Core Wiederherstellungspunkte von mehr als einem Quell-Core repliziert, wird jeder Quell-Core als eigenes navigierbares Menü im linken Navigationsbereich angezeigt. Wenn Sie auf eine bestimmte in einem „Replicated machines“-Menü (Replizierte Maschinen) angezeigten Maschinennamen klicken, wird eine Übersichtsseite mit zusammengefassten Informationen zu der ausgewählten replizierten Maschine angezeigt. Weitere Informationen zur Replikation finden Sie unter Replikation.
Menü „Nur Wiederherstellungspunkte“	Wenn ein REINES WIEDERHERSTELLUNGSPUNKTMENÜ angezeigt wird, behält Ihr Core Wiederherstellungspunkte für eine Maschine bei, die er einmal geschützt oder repliziert hat. Diese Maschine erfasst keine neuen Snapshots mehr, die zuvor auf Ihrem Core erfassten Wiederherstellungspunkte bleiben jedoch erhalten. Diese Wiederherstellungspunkte können für die Wiederherstellung auf Dateiebene, aber nicht für eine BMR-Wiederherstellung, die Wiederherstellung ganzer Volumes oder das Hinzufügen von Snapshot-Daten verwendet werden.
Menü für benutzerdefinierte Gruppen	Wenn Sie benutzerdefinierte Gruppen erstellt haben, wird ein Menü für benutzerdefinierte Gruppen im Navigationsmenü angezeigt. bei benutzerdefinierten Gruppen handelt es sich um logische Container, die zur Gruppierung von Maschinen verwendet werden (z. B. nach Funktion, Organisation oder geografischem Standort). Benutzerdefinierte Gruppen können heterogene Objekte enthalten (geschützte Maschinen, replizierte Maschinen und so weiter). Sie können die Bezeichnung für eine benutzerdefinierte Gruppe festlegen. Wie bei anderen Menüs wird der Namen im Menü in Großbuchstaben angezeigt. Sie können Aktionen für ähnliche Elemente in einer benutzerdefinierten Gruppe durch Klicken auf den Pfeil rechts neben dem Titel der benutzerdefinierten Gruppe durchführen. Zum Beispiel können Sie für jede geschützte Maschine in einer benutzerdefinierten Gruppe einen Snapshot erzwingen. Weitere Informationen über das Erstellen und Verwalten von benutzerdefinierten Gruppen finden Sie unter Grundlegende Informationen zu benutzerdefinierten Gruppen.

UI-Element	Description
Menü „Angehängte Archive“ 	Wenn Sie Ihrem Core Archive beifügen, werden die einzelnen Archive im linken Navigationsmenü aufgeführt. Seine Bezeichnung ist der Name des Archivs. In dieser Liste sind alle im Archiv enthaltenen Maschinen aufgeführt.

Details zu den Elementen im linken Navigationsbereich werden in der folgenden Tabelle angezeigt.

Tabelle 172. linker Navigationsbereich und Menüs

Beschreibungen der Menüs, die für die Typen der im linken Navigationsbereich aufgeführten Maschinen verfügbar sind.

UI-Element	Description
Textfilter Menü „Maschinen“ 	Der Textfilter ist ein Textfeld, mit dem Sie die Elemente filtern können, die in den Menüs „Maschinen“, „Replizierte Maschinen“ und „Nur Wiederherstellungspunkte-Maschinen“ angezeigt werden. Wenn Sie Ihre Kriterien in diesen Filter eingeben, werden nur die Maschinen, die Ihre Kriterien erfüllen in den jeweiligen Menüs angezeigt.
Details erweitern und verkleinern 	Klicken Sie auf den Pfeil rechts vom Textfilter, um Details für die Menüs „Maschinen“, „Replizierte Maschinen“ und „Nur Wiederherstellungspunkte-Maschinen“ zu erweitern oder zu verkleinern.
Menü „Maschine     	Das Menü „Maschinen“ wird im linken Navigationsbereich der Benutzeroberfläche angezeigt. In diesem Menü können Sie alle geschützten Maschinen, geschützten Cluster oder replizierte Maschinen anzeigen, die im Core konfiguriert sind. Wenn geschützte Gruppen oder „Nur Wiederherstellungspunkte-Maschinen“ vorhanden sind, werden diese ebenfalls in diesem Menü angezeigt. **NOTE:** Wenn ein vSphere/ESXi-Hypervisor Maschinen unter Schutz hat, wird der Host ebenfalls in diesem Menü angezeigt, mit allen seinen VMs als Kinder, auch wenn der Host nicht geschützt ist. Sie können die Ansicht für alle geschützten Maschinen im Core reduzieren oder erweitern, indem Sie auf den Pfeil auf der linken Seite dieser Menübeschriftung klicken. Das angezeigte Symbol porträtiert den Maschinentyp: • Ein einfaches Maschinensymbol stellt eine physische Maschine oder eine geschützte VM mit installierter Rapid Recovery Agentensoftware dar. Das gleiche Symbol wird für eine Maschine verwendet, die nur Wiederherstellungspunkte enthält. • Ein Multi-Maschinen-Symbol porträtiert ein geschütztes Cluster. • Ein leeres Doppelmaschinen-Symbol porträtiert eine VMware-VM mit agentenlosem Schutz. • Ein leeres Drei-Maschinen-Symbol porträtiert einen VMware vCenter-Host. • Ein Symbol mit zwei gestapelten Servern porträtiert einen Hyper-V-Host. • Ein Symbol mit einem einzigen Server porträtiert eine Hyper-V-VM, die agentenlos geschützt wird. Wenn Sie auf das Menü „Maschinen“ klicken, wird die Seite „ Maschinen“ angezeigt, auf der alle durch diesen Core geschützten Maschinen im Fensterbereich „Maschinen“ angezeigt werden. Weitere Informationen hierzu finden Sie unter Anzeigen des Menüs "Geschützte Maschinen".

UI-Element	Description
Menü „Replizierte Maschinen“	Bei der Replikation von Maschinen eines anderen Rapid Recovery Core wird der Name dieses Core als separater Menüeintrag unter dem Maschinen-Menü angezeigt. Jede auf diesem Ziel-Core replizierte Maschine aus dem aufgeführten Quell-Core erscheint unter diesem Menü. Für jede replizierte Maschine zeigt das Symbol den Typ der Maschine, die repliziert wird. Wenn zum Beispiel eine einzelne Maschine repliziert wird, zeigt das Symbol eine Maschine. Bei Replikation von einem Server-Cluster, steht das Symbol für einen Cluster. Sie können die Ansicht für diese replizierten Maschinen reduzieren oder erweitern, indem Sie auf den Pfeil auf der linken Seite dieser Menübeschriftung klicken. Im Menü „Replizierte Maschinen“ können Sie Aktionen für alle replizierten Maschinen durchführen. Wenn Sie auf das Menü „Replizierte Maschinen“ klicken, wird die Seite „Maschinen“ angezeigt. Diese Seite zeigt alle Maschinen, die auf einem anderen (Quell) Core geschützt sind und auf diesen Ziel-Core repliziert werden. Weitere Informationen hierzu finden Sie unter Anzeigen von replizierten Maschinen über das Navigationsmenü.
Menü „Nur Wiederherstellungspunkte“	Wenn Maschinen, die vorher im Core geschützt wurden, aus dem Schutz entfernt wurden, sie Wiederherstellungspunkte aber nicht gelöscht wurden, wird das Menü „Nur Wiederherstellungspunkte“ angezeigt. Es ist kein Menü-Symbol vorhanden. Jede der zuvor geschützten Maschinen mit aufbewahrten Wiederherstellungspunkten wird in dieser Liste angezeigt. Die Maschine mit nur Wiederherstellungspunkten weist das Symbol einer standardmäßigen geschützten Maschine auf. Sie können die Ansicht für „Nur Wiederherstellungspunkte-Maschinen“ reduzieren oder erweitern, indem Sie auf den Pfeil auf der linken Seite dieser Menübeschriftung klicken. Im Menü „Nur Wiederherstellungspunkte“ können Sie Wiederherstellungspunkte für alle „Nur Wiederherstellungspunkte“-Maschinen des Core entfernen. Wenn Sie auf das Menü „Nur Wiederherstellungspunkte“ klicken, wird die Seite „Maschinen“ mit den Maschinen angezeigt, für die Wiederherstellungspunkte gespeichert wurden. Weitere Informationen hierzu finden Sie unter Anzeigen des Menüs „Nur Wiederherstellungspunkte“.
Menü für benutzerdefinierte Gruppen	Wenn der Core benutzerdefinierte Gruppen umfasst, enthält der linke Navigationsbereich ein Menü für benutzerdefinierte Gruppen. Jedes der Objekte in dieser benutzerdefinierten Gruppe wird in dieser Liste angezeigt. Sie können die Ansicht für alle benutzerdefinierten Gruppen im Core reduzieren oder erweitern, indem Sie auf den Pfeil auf der linken Seite dieser Menübeschriftung klicken. Im Menü für benutzerdefinierte Gruppen können Sie Aktionen für gleichartige Elemente in der Gruppe durchführen. Wenn Sie auf das Menü für benutzerdefinierte Gruppen klicken, wird die Seite „Maschinen“ mit einem Fensterbereich für die einzelnen Rapid Recovery Objekte angezeigt, die in der benutzerdefinierten Gruppe enthalten sind: „Geschützte Maschinen“, „Replizierte Maschinen“ und „Nur Wiederherstellungspunkte-Maschinen“. Weitere Informationen hierzu finden Sie unter Anzeigen des Menüs für benutzerdefinierte Gruppen.
Menü „Angehängte Archive“	Wenn Sie Archive mit Ihrem Core verbunden haben, dann enthält der linke Navigationsbereich ein Menü für jedes verbundene Archiv. Jede der geschützten Maschinen im Archiv wird in dieser Liste angezeigt. Die Menübeschriftung verwendet den Namen, der angegeben wurde, als das Archiv gespeichert wurde.

UI-Element	Description
	Sie können die Ansicht für alle mit Ihrem Core verbunden Archive reduzieren oder erweitern, indem Sie auf den Pfeil auf der linken Seite dieser Menübeschriftung klicken. Im Menü für verbundene Archive können Sie Aktionen für gleichartige Elemente in der Gruppe durchführen. Wenn Sie auf das Menü für verbundene Archive klicken, wird die Seite „Maschinen“ mit einem Fensterbereich für die einzelnen Rapid Recovery Objekte angezeigt, die in der benutzerdefinierten Gruppe enthalten sind: „Geschützte Maschinen“, „Replizierte Maschinen“ und „Nur Wiederherstellungspunkte-Maschinen“. Weitere Informationen hierzu finden Sie unter Anzeigen des Menüs für benutzerdefinierte Gruppen.

Anzeigen geschützter Maschinen

Von der **Startseite** auf Rapid Recovery Core Console können beim Betrachten der Zusammenfassungstabellen Zusammenfassungsinformationen für alle Maschinen, die durch den Core geschützt sind, im Fensterbereich der geschützten Maschinen angezeigt werden.

NOTE: Ein Software-Agent erledigt für den Benutzer die jeweiligen Aktionen. Geschützte Maschinen werden bisweilen als Agenten bezeichnet, da sie die Rapid Recovery Agent Software ausführen, um Datensicherung und -replikation auf Rapid Recovery Core zu ermöglichen.

Die folgenden Informationen werden angezeigt: Status, Anzeigename der einzelnen Maschinen, das verwendete Repository, Datum und Uhrzeit des letzten Snapshots, Anzahl der vorhandenen Wiederherstellungspunkte im Repository für die Maschine sowie der insgesamt von den Snapshots belegte Speicherplatz im Repository.

Sie können eine geschützte Maschine verwalten, indem Sie zu der geschützten Maschine navigieren, die Sie anzeigen, konfigurieren oder verwalten möchten. Von der **Startseite** gibt es drei Möglichkeiten, zu einer geschützten Maschine zu navigieren:

- Sie können auf die IP-Adresse oder den Anzeigenamen einer geschützten Maschine aus dem Fensterbereich der geschützten Maschinen klicken. Daraufhin wird die Seite „Zusammenfassung“ für die ausgewählte Maschine angezeigt.
- Im linken Navigationsbereich können Sie auf den Titel des Menüs **Geschützte Maschinen** klicken. Die Seite **Geschützte Maschinen** wird angezeigt. Auf dieser Seite werden Übersichtsinformationen zu den einzelnen Maschinen angezeigt. Eine ausführliche Beschreibung dieser Seite finden Sie unter Anzeigen von zusammenfassenden Informationen für eine geschützte Maschine.
- Sie können im linken Navigationsbereich unter dem Menü „Geschützte Maschinen“ auf die IP-Adresse oder den Anzeigenamen einer geschützten Maschine klicken. Daraufhin wird die Seite **Zusammenfassung** für die ausgewählte Maschine angezeigt. Eine ausführliche Beschreibung dieser Seite finden Sie unter Anzeigen von zusammenfassenden Informationen für eine geschützte Maschine.

Anzeigen von Ereignissen für eine geschützte Maschine

Auf der Seite **Ereignisse** können Sie die Jobs anzeigen, die auf der ausgewählten geschützten Maschine durchgeführt wurden oder werden. Über die Schaltflächen oben auf der Seite können Sie zu Joblisten in den folgenden drei Aktivitätskategorien navigieren:

- **Aufgaben.** Ein Job, den Rapid Recovery durchführen muss, damit die einwandfreie Funktionsweise gewährleistet ist.
- **Warnungen.**Eine Benachrichtigung für eine Aufgabe oder ein Ereignis mit Fehlern oder Warnungen.
- **Journal.**Eine Zusammenstellung aller Aufgaben und Ereignisse der geschützten Maschine.

Die folgende Tabelle enthält Beschreibungen der Schaltflächen auf der Seite **Ereignisse**.

Tabelle 173. Elemente der Seite „Ereignisse“

UI-Element	Description
Stichwortsuche	Bietet die Möglichkeit, ein bestimmtes Element in der jeweiligen Kategorie zu suchen. Nur für Tasks verfügbar.
Von	Um die Suchergebnisse einzugrenzen, können Sie ein Datum eingeben, an dem die Suche beginnen soll. Nur für Tasks verfügbar.
Bis	Um die Suchergebnisse einzugrenzen, können Sie ein Datum eingeben, an dem die Suche enden soll. Nur für Tasks verfügbar.
Statussymbole	Jedes Symbol stellt einen anderen Jobstatus dar. Für Tasks und Warnungen können Sie durch Klicken auf eines der Symbole die Liste anhand dieses Status filtern und so einen Bericht erzeugen. Wenn Sie ein zweites Mal auf das Symbol klicken, wird der Filter für den betreffenden Status entfernt. Sie können nach mehr als einem Status filtern. Die Status umfassen: • **Aktiv.**Ein Job, der gerade durchgeführt wird. • **In Warteschlange.** Ein Job, der auf den Abschluss eines anderen Jobs wartet, damit er eingeleitet werden kann. • **Wartend.**Ein Job der auf eine Genehmigung oder den Abschluss eines Vorgangs wartet, z. B. Bereitstellung eines Seed-Laufwerks. (Weitere Informationen zu Seed-Laufwerken finden Sie unter Replikation.) • **Abgeschlossen.**Ein Job, der erfolgreich durchgeführt wurde. • **Fehlgeschlagen.** Ein fehlgeschlagener Job, der nicht abgeschlossen wurde.
Dienstsymbol	Über diese Schaltfläche wird die Jobliste um Dienstjobs erweitert. Wenn Sie auf dieses Symbol klicken, wird in jedem Statussymbol ein kleineres Dienstsymbol angezeigt, damit Sie nach Dienstjobs mit dem jeweiligen Status filtern können (sofern vorhanden). Beispiele für Dienstjobs sind das Löschen von Indexdateien oder das Entfernen einer Maschine aus der Schutzfunktion.

UI-Element	Description
Dropdown-Liste „Exporttyp“	Die Dropdown-Liste enthält die Formate, in die der Ereignisbericht exportiert werden kann. Nur für Tasks verfügbar. Sie umfasst folgende Formate: • PDF • HTML • CSV • XLS • XLSX
(Exportsymbol)	Konvertiert den Ereignisbericht in das ausgewählte Format. Nur für Tasks verfügbar.
Seitenauswahl	Ereignisberichte können verschiedene Jobs auf mehreren Seiten enthalten. Mit den Zahlen und Pfeilen unten in der Seite **Ereignisse** können Sie zu den Seiten des Berichts navigieren.

Auf der Seite **Ereignisse** werden alle Ereignisse in einer Tabelle angezeigt. Die folgende Tabelle führt die angezeigten Informationen zu jedem Element auf.

Tabelle 174. Detaillierte Informationen zur Übersichtstabelle „Ereignisse“

UI-Element	Description
Status	Zeigt den Status der Task, Warnung oder des Journalelements an. Verfügbar für Warnungen oder Journalelemente. Kicken Sie auf die Kopfzeile, um die Ergebnisse nach Status zu filtern.
Name	Nur für Tasks verfügbar. Dieses Textfeld gibt den Tasktyp an, der für diese geschützte Maschine abgeschlossen wurde. Beispiele sind die Übertragung von Volumes, die Wartung des Repository, Durchführen eines Rollups, Überprüfung der Bereitstellungsfähigkeit, Durchführen von Prüfsummen-Überprüfungen usw.
Startzeit	Verfügbar für Tasks, Warnungen und Journalelemente. Zeigt das Datum und die Uhrzeit an, an dem bzw. zu der der Job oder die Task begann.
Endzeit	Nur für Tasks verfügbar. Zeigt das Datum und die Uhrzeit an, an dem bzw. zu der die Task beendet wurde.
Jobdetails	Nur für Tasks verfügbar. Öffnet das Dialogfeld**Aktive Task überwachen**, so dass Sie Details des spezifischen Job oder der Task anzeigen können. Diese Details umfassen eine ID für den Job, die Geschwindigkeit, mit der die Daten vom Core übertragen wurden (falls relevant), die zum Abschluss des Jobs verwendete Zeit, der Gesamtaufwand in Anzahl an Gigabyte sowie alle untergeordneten Aufgaben im Zusammenhang mit dem Job.
Meldung	Verfügbar für Warnungen und Journalelemente. Dieses Textfeld enthält einen beschreibenden Inhalt der Warnung oder des Journalelements.

Anzeigen des Menüs „Mehr“ für eine geschützte Maschine

Das Menü **Mehr** bietet weitere Optionen, um Sie bei der Verwaltung der ausgewählten geschützten Maschine zu unterstützen. Für den Zugang auf diese Tools klicken Sie auf das Drop-Down-Menü „Mehr“ und wählen Sie eine der in der folgenden Tabelle beschriebenen Optionen aus:

Tabelle 175. Tools, die über das Menü „Mehr“ für eine geschützte Maschine zur Verfügung stehen

UI-Element	Description
Systeminformationen	Zeigt Informationen zur geschützten Maschine (Systeminformationen, Volumes, Prozessoren, Netzwerkadapter und IP-Adressen für die jeweilige Maschine). Weitere Informationen hierzu finden Sie unter Anzeigen von Systeminformationen für eine geschützte Maschine.
Bereitstellungen	Im Bereich „Lokale Bereitstellungen“ können Sie lokal bereitgestellte Volumes anzeigen oder unmounten (Bereitstellung aufheben). Im Bereich „Remote-Bereitstellungen“ können Sie Volumes, die mit dem Local Mount Utility bereitgestellt wurden, anzeigen oder unmounten. Weitere Informationen zum Aufheben der Bereitstellung von Volumes finden Sie unter Aufheben der Bereitstellung von Wiederherstellungspunkten. Weitere Informationen zur lokalen Bereitstellung von Wiederherstellungspunkten finden Sie unter Bereitstellen eines Wiederherstellungspunkts bzw. Bereitstellen eines Wiederherstellungspunkt-Volumes für eine Linux-Maschine.
Aufbewahrungsrichtlinie	Ermöglicht die Angabe einer Aufbewahrungsrichtlinie für die ausgewählte Maschine. Sie können die Standardrichtlinie des Core verwenden oder für diese Maschine eine ganz bestimmte Aufbewahrungsrichtlinie angeben. Weitere Informationen hierzu finden Sie unter Anpassen der Aufbewahrungsrichtlinieneinstellungen für eine geschützte Maschine.
Benachrichtigungen	Ermöglicht die Angabe einer benutzerdefinierten Benachrichtigungsgruppe für Ereignisse im Zusammenhang mit der ausgewählten Maschine. Diese ändert nichts an den Benachrichtigungen, die bereits auf dem Core eingestellt wurden. Weitere Informationen hierzu finden Sie unter Konfigurieren von Benachrichtigungsgruppen.
Agentenprotokoll	Mit dieser Option können Sie die Protokolldatei für eine Maschine, die durch Rapid Recovery Agent-Software geschützt ist, herunterladen und anzeigen. Weitere Informationen hierzu finden Sie unter Herunterladen und Anzeigen der Protokolldatei für eine geschützte Maschine.

Third-party contributions

This product contains the third-party components listed below. For third-party license information, go to http://quest.com/legal/license-agreements.aspx. Source code for components marked with an asterisk (*) is available at http://opensource.quest.com.

Table 176. List of third-party contributions

Component	License or acknowledgment	Notes
AlphaFS 2.0.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
AlphaVSS 1.2.4000	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
ANTLR 3.3.3	BSD ANTLR 3	Copyright (c) 2003-2007, Terence Parr A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
ANTLR 4.0.2	BSD ANTLR 4	Copyright (c) 2012 Terence Parr and Sam Harwell A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
AWS SDK for .NET 3.3.37	Apache 2.0	A copy of this license can be found at Apache 2.0.
Azure SDK for .NET 2.4	Apache 2.0	A copy of this license can be found at Apache 2.0
Bootstrap 3.0.0	Apache 2.0	Bootstrap.js by @fat & @mdo Copyright 2012 Twitter, Inc. A copy of this license can be found at Apache 2.0
Bundletransformer 1.9.138	Apache 2.0	Copyright (c) 2012-2015 Andrey Taritsyn A copy of this license can be found at Apache 2.0
Caliburn.Micro 2.0.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Castle Windsor 2.5.2	Apache 2.0	A copy of this license can be found at Apache 2.0.
Chromium 43.0.2312	Chromium BSD License N/A	Copyright 2014 The Chromium Authors. All rights reserved. A copy of this license can be found at Chromium BSD License N/A.

Component	License or acknowledgment	Notes
CLAP 4.2	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Common Library for Hyak Code Generator 1.0.2	Apache 2.0	A copy of this license can be found at Apache 2.0.
curlpp 0.7.2	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
EcmaScript.Net 1.0.1	Mozilla Public License (MPL) 1.1	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Far Manager 3.0.4242	Far Manager BSD License N/A	Copyright (c) 1996 Eugene Roshal Copyright (c) 2000 Far Group All rights reserved. A copy of this licenses can be found at Far Manager BSD License N/A.
fio 2.18*	GPL (GNU General Public License) 2.0	This component is not used in the application. It is provided with the product for customer convenience. A copy of this license can be found at GPL (GNU General Public License) 2.0.
FlotCharts 0.8.3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Google APIs Client Library for .NET 1.9.2	Apache 2.0	Copyright 2011 Google Inc A copy of this license can be found at Apache 2.0.
HTML Renderer 1.5.0.6	BSD CodePlex	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
html5-placeholder-shim.jquery.js 1.0.58	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
ISOLINUX 4.05 20120131*	GPL (GNU General Public License) 2.0	A copy of this license can be found at GPL (GNU General Public License) 2.0.
JavaScriptEngineSwitcher 1.2.4	Apache 2.0	Copyright (c) 2013-2015 Andrey Taritsyn A copy of this license can be found at Apache 2.0.
jqGrid 4.4.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jqrowl 1.2.6	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Component	License or acknowledgment	Notes
JQuery 1.8.2	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery File Upload Plugin 5	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery knob 1.2.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Templates 1.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Templates 1.0.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
JQuery UI 1.9.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Validation 1.9.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Viewport 1.0.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Viewport 1.0.0.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.fileDownload 1.3.3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.hotkeys 0.7.9	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.mCustomScrollbar 3.0.7	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquerey.mousewheel 3.1.12	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.splitter 0.14.0	GNU LGPL Version 3, 29 June 2007	Copyright (C) 2010-2013 Jakub Jankiewicz A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.tagsinput 1.3.3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Json.NET 4.5	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Component	License or acknowledgment	Notes
jsTree 1.0-rc3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.11.3*	GNU LGPL Version 3, 29 June 2007	Copyright © 2006–2015 SUSE LLC and contributors. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.12*	GNU LGPL Version 3, 29 June 2007	Copyright © 2002 Red Hat, Inc. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.15*	GNU LGPL Version 3, 29 June 2007	Copyright © 2015 Canonical Ltd. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.17*	GNU LGPL Version 3, 29 June 2007	Copyright © 2002 Red Hat, Inc. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.19*	GNU LGPL Version 3, 29 June 2007	Copyright © 2006–2015 SUSE LLC and contributors. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Libc.so.6 2.7*	LGPL (GNU Lesser General Public License) 2.1	A copy of this license can be found at LGPL (GNU Lesser General Public License) 2.1.
libext2fs 1.42.12*	GNU Lesser General Public License 2.1	Copyright (C) 1993, 1994, 1995, 1996 Theodore Ts'o. A copy of this license can be found at LGPL (GNU Lesser General Public License) 2.1.
libssh2 1.4.3	BSD-style N/A	Portions Copyright 2002-2010 Atsuhiko Yamanaka, JCraft,Inc. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Log4Net 1.2.10	Apache 2.0	A copy of this license can be found at Apache 2.0.
MarkdownSharp 1.13	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
matchMedia 2.72	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
memtest86+ 4.20*	GPL (GNU General Public License) 2.0	A copy of this license can be found at GPL (GNU General Public License) 2.0.
Microsoft Azure Compute	Apache 2.0	A copy of this license can be found at Apache 2.0.

Component	License or acknowledgment	Notes
Management Library 12.0.0		
Microsoft Reactive Extensions for .NET 2.1	Apache 2.0	A copy of this license can be found at Apache 2.0.
Moment.js 2.6.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
MongoDB 2.0.6*	GNU Affero GPL 3.0	A copy of this license can be found at GNU AFFERO GENERAL PUBLIC LICENSE
MongoDB 10gen driver 2.4.1	Apache 2.0	A copy of this license can be found at Apache 2.0.
Mono 5.2*	LGPL (GNU Lesser General Public License) 2.1	Copyright (C) 1991, 1999 Free Software Foundation, Inc. A copy of this license can be found at LGPL (GNU Lesser General Public License) 2.1.
MsieJavaScriptEngine 1.4.3*	Mozilla Public License (MPL) 1.1	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
NBD various*	GPL (GNU General Public License) 2.0	This component is not used in the application. It is provided with the product for customer convenience. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
NDesk.Options 0.2.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Newtonsoft.Json.dll 6.0.8	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
NLog 4.4.12	BSD - Kowalski 2011	Copyright (c) 2004-2011 Jaroslaw Kowalski <jaak@jkowwalski.net>. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
OpenSSL 1.1.0e	OpenSSL 1.0	This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved. A copy of this license can be found at OpenSSL 1.0.
OpenStack.NET 1.4.0.2	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Component	License or acknowledgment	Notes
PowerCollections 2007*	Eclipse Public License 1.0	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Prism 4.0	Microsoft patterns & practices license N/A	Contains software or other content adapted from Microsoft patterns & practices ObjectBuilder, © 2006 Microsoft Corporation. All rights reserved. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
ProductionStackTrace 1.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Protobuf-net 2.0.0.627	Apache 2.0	A copy of this license can be found at Apache 2.0.
PuTTY 0.63	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Quartz.NET 2.1.2	Apache 2.0	A copy of this license can be found at Apache 2.0.
Raphaël—JavaScript Library 2.1.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
RazorGenerator 2.1	Apache 2.0	A copy of this license can be found at Apache 2.0.
Resize Floating Popup Control Revision 3	Code Project Open License (CPOL) 1.02	A copy of this license can be found at Code Project Open License (CPOL) 1.02 .
respond.js 1.3.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
SignalR 1.2.2	Apache 2.0	Copyright (c) .NET Foundation. All rights reserved. A copy of this license can be found at Apache 2.0.
SimpleRestServices 1.2.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
SimpleRestServices 1.3.0.3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Sparsehash 1.11	BSD CodePlex	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
SSH.Net 2013.4.7	BSD CodePlex	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Component	License or acknowledgment	Notes
TextFileEncodingDetector 1.0	BSD TextFileEncodingDetector 1.0	Copyright 2002-2008 Xiph.org Foundation Copyright 2002-2008 Jean-Marc Valin Copyright 2005-2007 Analog Devices Inc. Copyright 2005-2008 Commonwealth Scientific and Industrial Research Organisation (CSIRO) Copyright 1993, 2002, 2006 David Rowe Copyright 2003 EpicGames Copyright 1992-1994 Jutta Degener, Carsten Bormann A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
trip 2.1.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Tri-state tree view Revision 9 (30-May-2011)	Code Project Open License (CPOL) 1.02	A copy of this license can be found at Code Project Open License (CPOL) 1.02 .
Virtual Box SDK 4.2.14*	LGPL (GNU Lesser General Public License) 2.1	c 2004-2015 Oracle Corporation A copy of this license can be found at LGPL (GNU Lesser General Public License) 2.1.
WebGrease 1.5.2	Apache 2.0	A copy of this license can be found at Apache 2.0.
Yahoo! UI Library: YUI Compressor .Net 2.7.0	BSD CodePlex	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
zlib 1.2.5	zlib 1.2.5	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Apache 2.0

License Text

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places:

within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Chromium BSD License N/A

License Text

Copyright 2014 The Chromium Authors. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code Project Open License (CPOL) 1.02

License Text

Preamble

This License governs Your use of the Work. This License is intended to allow developers to use the Source Code and Executable Files provided as part of the Work in any application in any form.

The main points subject to the terms of the License are:

Source Code and Executable Files can be used in commercial applications;

Source Code and Executable Files can be redistributed; and

Source Code can be modified to create derivative works.

No claim of suitability, guarantee, or any warranty whatsoever is provided. The software is provided "as-is".

The Article(s) accompanying the Work may not be distributed or republished without the Author's consent

This License is entered between You, the individual or other entity reading or otherwise making use of the Work licensed pursuant to this License and the individual or other entity which offers the Work under the terms of this License ("Author").

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CODE PROJECT OPEN LICENSE ("LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HEREIN, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE AUTHOR GRANTS YOU THE RIGHTS CONTAINED HEREIN IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO ACCEPT AND BE BOUND BY THE TERMS OF THIS LICENSE, YOU CANNOT MAKE ANY USE OF THE WORK.

Definitions.

"Articles" means, collectively, all articles written by Author which describes how the Source Code and Executable Files for the Work may be used by a user.

"Author" means the individual or entity that offers the Work under the terms of this License.

"Derivative Work" means a work based upon the Work or upon the Work and other pre-existing works.

"Executable Files" refer to the executables, binary files, configuration and any required data files included in the Work.

"Publisher" means the provider of the website, magazine, CD-ROM, DVD or other medium from or by which the Work is obtained by You.

"Source Code" refers to the collection of source code and configuration files used to create the Executable Files.

"Standard Version" refers to such a Work if it has not been modified, or has been modified in accordance with the consent of the Author, such consent being in the full discretion of the Author.

"Work" refers to the collection of files distributed by the Publisher, including the Source Code, Executable Files, binaries, data files, documentation, whitepapers and the Articles.

"You" is you, an individual or entity wishing to use the Work and exercise your rights under this License.

Fair Use/Fair Use Rights. Nothing in this License is intended to reduce, limit, or restrict any rights arising from fair use, fair dealing, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

License Grant. Subject to the terms and conditions of this License, the Author hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

You may use the standard version of the Source Code or Executable Files in Your own applications.

You may apply bug fixes, portability fixes and other modifications obtained from the Public Domain or from the Author. A Work modified in such a way shall still be considered the standard version and will be subject to this License.

You may otherwise modify Your copy of this Work (excluding the Articles) in any way to create a Derivative Work, provided that You insert a prominent notice in each changed file stating how, when and where You changed that file.

You may distribute the standard version of the Executable Files and Source Code or Derivative Work in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution.

The Articles discussing the Work published in any form by the author may not be distributed or republished without the Author's consent. The author retains copyright to any such Articles. You may use the Executable Files and Source Code pursuant to this License but you may not repost or republish or otherwise distribute or make available the Articles, without the prior written consent of the Author.

Any subroutines or modules supplied by You and linked into the Source Code or Executable Files this Work shall not be considered part of this Work and will not be subject to the terms of this License.

Patent License. Subject to the terms and conditions of this License, each Author hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, import, and otherwise transfer the Work.

Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

You agree not to remove any of the original copyright, patent, trademark, and attribution notices and associated disclaimers that may appear in the Source Code or Executable Files.

You agree not to advertise or in any way imply that this Work is a product of Your own.

The name of the Author may not be used to endorse or promote products derived from the Work without the prior written consent of the Author.

You agree not to sell, lease, or rent any part of the Work. This does not restrict you from including the Work or any part of the Work inside a larger software distribution that itself is being sold. The Work by itself, though, cannot be sold, leased or rented.

You may distribute the Executable Files and Source Code only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy of the Executable Files or Source Code You distribute and ensure that anyone receiving such Executable Files and Source Code agrees that the terms of this License apply to such Executable Files and/or Source Code. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute the Executable Files or Source Code with any

technological measures that control access or use of the Work in a manner inconsistent with the terms of this License.

You agree not to use the Work for illegal, immoral or improper purposes, or on pages containing illegal, immoral or improper material. The Work is subject to applicable export laws. You agree to comply with all such laws and regulations that may apply to the Work after Your receipt of the Work.

Representations, Warranties and Disclaimer. THIS WORK IS PROVIDED "AS IS", "WHERE IS" AND "AS AVAILABLE", WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OR GUARANTEES. YOU, THE USER, ASSUME ALL RISK IN ITS USE, INCLUDING COPYRIGHT INFRINGEMENT, PATENT INFRINGEMENT, SUITABILITY, ETC. AUTHOR EXPRESSLY DISCLAIMS ALL EXPRESS, IMPLIED OR STATUTORY WARRANTIES OR CONDITIONS, INCLUDING WITHOUT LIMITATION, WARRANTIES OR CONDITIONS OF MERCHANTABILITY, MERCHANTABLE QUALITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY OF TITLE OR NON-INFRINGEMENT, OR THAT THE WORK (OR ANY PORTION THEREOF) IS CORRECT, USEFUL, BUG-FREE OR FREE OF VIRUSES. YOU MUST PASS THIS DISCLAIMER ON WHENEVER YOU DISTRIBUTE THE WORK OR DERIVATIVE WORKS.

Indemnity. You agree to defend, indemnify and hold harmless the Author and the Publisher from and against any claims, suits, losses, damages, liabilities, costs, and expenses (including reasonable legal or attorneys' fees) resulting from or relating to any use of the Work by You.

Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL THE AUTHOR OR THE PUBLISHER BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK OR OTHERWISE, EVEN IF THE AUTHOR OR THE PUBLISHER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Termination.

This License and the rights granted hereunder will terminate automatically upon any breach by You of any term of this License. Individuals or entities who have received Derivative Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 6, 7, 8, 9, 10 and 11 will survive any termination of this License.

If You bring a copyright, trademark, patent or any other infringement claim against any contributor over infringements You claim are made by the Work, your License from such contributor to the Work ends automatically.

Subject to the above terms and conditions, this License is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, the Author reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

Publisher. The parties hereby confirm that the Publisher shall not, under any circumstances, be responsible for and shall not have any liability in respect of the subject matter of this License. The Publisher makes no warranty whatsoever in connection with the Work and shall not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. The Publisher reserves the right to cease making the Work available to You at any time without notice

Miscellaneous

This License shall be governed by the laws of the location of the head office of the Author or if the Author is an individual, the laws of location of the principal place of residence of the Author.

If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this License, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

This License constitutes the entire agreement between the parties with respect to the Work licensed herein. There are no understandings, agreements or representations with respect to the Work not specified herein. The Author

shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Author and You.

Far Manager BSD License N/A

License Text

Copyright (c) 1996 Eugene Roshal

Copyright (c) 2000 Far Group

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions

are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

EXCEPTION:

Far Manager plugins that use only the following header files from this distribution (none or any): farcolor.hpp, farkeys.hpp, plugin.hpp, farcolorW.pas, farkeysW.pas and pluginW.pas; can be distributed under any other possible license with no implications from the above license on them.

GNU AFFERO GENERAL PUBLIC LICENSE

Version 3, 19 November 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/> Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU Affero General Public License is a free, copyleft license for software and other kinds of works, specifically designed to ensure cooperation with the community in the case of network server software.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, our General Public Licenses are intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

Developers that use our General Public Licenses protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License which gives you legal permission to copy, distribute and/or modify the software.

A secondary benefit of defending all users' freedom is that improvements made in alternate versions of the program, if they receive widespread use, become available for other developers to incorporate. Many developers of free software are heartened and encouraged by the resulting cooperation. However, in the case of software used on network servers, this result may fail to come about. The GNU General Public License permits making a modified version and letting the public access it on a server without ever releasing its source code to the public.

The GNU Affero General Public License is designed specifically to ensure that, in such cases, the modified source code becomes available to the community. It requires the operator of a network server to provide the source code of the modified version running there to the users of that server. Therefore, public use of a modified version, on a publicly accessible server, gives the public access to the source code of the modified version.

An older license, called the Affero General Public License and published by Affero, was designed to accomplish similar goals. This is a different license, not a version of the Affero GPL, but Affero has released a new version of the Affero GPL which permits relicensing under this license.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU Affero General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component,

and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from

a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms. "Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available

network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Remote Network Interaction; Use with the GNU General Public License.

Notwithstanding any other provision of this License, if you modify the Program, your modified version must prominently offer all users interacting with it remotely through a computer network (if your version supports such interaction) an opportunity to receive the Corresponding Source of your version by providing access to the Corresponding Source from a network server at no charge, through some standard or customary means of facilitating copying of software. This Corresponding Source shall include the Corresponding Source for any work covered by version 3 of the GNU General Public License that is incorporated pursuant to the following paragraph.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the work with which it is combined will remain governed by version 3 of the GNU General Public License.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU Affero General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU Affero General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU Affero General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU Affero General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU Affero General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Affero General Public License for more details.

You should have received a copy of the GNU Affero General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If your software can interact with users remotely through a computer network, you should also make sure that it provides a way for users to get its source. For example, if your program is a web application, its interface could display a "Source" link that leads users to an archive of the code. There are many ways you could offer source, and different solutions will be better for different programs; see section 13 for the specific requirements.

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU AGPL, see <http://www.gnu.org/licenses/>.

GPL (GNU General Public License) 2.0

License Text

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its

contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS"

WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

LGPL (GNU Lesser General Public License) 2.1

License Text

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is

especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will

automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

OpenSSL 1.0

License Text

License

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

==========

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

/

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 datenorientieren 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

Besuchen Sie uns bei Fragen zum Vertrieb oder für andere Anfragen unter der Adresse https://www.quest.com/contact.

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

Glossar

Agent

Beim Rapid Recovery Agent handelt es sich um Software, die auf einer physischen oder virtuellen Maschine installiert ist und die Möglichkeit bietet, die Maschine unter Schutz durch den Rapid Recovery Core zu stellen.

Basisimage

Die erste übertragene Sicherung, die im Core gespeichert wird, heißt Basisimage-Snapshot. Alle Daten auf allen angegebenen Volumes (einschließlich Betriebssystem, Anwendungen und Einstellungen) werden im Core gespeichert. Weitere Informationen finden Sie unter Snapshot.

Prüfsumme

Die Prüfsummenfunktion ermöglicht das Erstellen von Datenblöcken, mit denen unbeabsichtigte, bei der Übertragung oder Speicherung auftretende Fehlern ermittelt werden können.

Cluster

Siehe Windows-Failover-Cluster.

Fortlaufende Clusterreplikation (CCR)

Eine Failover-Cluster-Lösung für nicht freigegebenen Speicher, die eine integrierte, asynchrone Protokollversandtechnologie verwendet, die auf einem zweiten Server in einem Failover-Cluster eine Kopie jeder Speichergruppe erstellt und verwaltet. CCR ist als Lösung für ein oder zwei Rechenzentren ausgelegt, die eine hohe Verfügbarkeit sowie Ausfallsicherheit von Standorten bietet. Dabei handelt es sich um eine von zwei Bereitstellungsmöglichkeiten für Postfachclusterserver, die in Exchange 2007 verfügbar sind.

Cluster-Knoten

Eine einzelne Maschine, die Teil eines Windows-Failover-Clusters ist.

Komprimierung

Die Storage Networking Industry Association (SNIA) definiert die Komprimierung als Kodierung von Daten, um deren Größe zu reduzieren.

Core

Der Rapid Recovery Core ist die zentrale Komponente der Rapid Recovery Architektur. Der Core stellt die grundlegenden Dienste für Sicherung, Wiederherstellung, Aufbewahrung, Replikation, Archivierung und Verwaltung bereit. Im Kontext der Replikation wird der Core auch als Quell-Core bezeichnet. Der Quell-Core ist der Ursprung und der Ziel-Core ist das Ziel (ein anderer Rapid Recovery Core auf einem eigenen dedizierten Server, auf die geschützten Maschinen oder Cluster repliziert werden).

Core Console

Die Rapid Recovery Kern-Konsole ist eine webbasierte Schnittstelle, die eine umfassende Verwaltung des Rapid Recovery Kerns ermöglicht.

Datenbankverfügbarkeitsgruppe (DAG)

Eine Gruppe von bis zu 16 Microsoft Exchange Server 2010-Postfachservern, die eine automatische Wiederherstellung auf Datenbankebene bei Datenbank-, Server oder Netzwerkfehlern ermöglicht. DAGs verwenden die kontinuierliche Replikation und einen Teil der Windows-Technologien für Cluster-Failover, um hohe Verfügbarkeit und Ausfallsicherheit von Standorten zu gewährleisten. Die Postfachserver in einer DAG überwachen sich gegenseitig auf Fehler. Wenn ein Postfachserver einer DAG hinzugefügt wird, arbeitet er mit den anderen Servern in der DAG zusammen, um bei Datenbankfehlern eine automatische Wiederherstellung auf Datenbankebene zu ermöglichen.

Verschlüsselung

Daten werden verschlüsselt, damit sie nur für autorisierte Benutzer zugänglich sind, die über den entsprechenden Entschlüsselungsschlüssel verfügen. Die Datenverschlüsselung erfolgt mithilfe des 256-Bit-AES im CBC-Modus (Cipher Block Chaining). Im CBC-Modus wird jeder Datenblock vor der Verschlüsselung eine XOR-Operation mit dem vorherigen verschlüsselten Textblock ausgeführt. Auf diese Weise hängt jeder neue verschlüsselte Textblock von allen vorausgehenden unverschlüsselten Textblöcken ab. Als Initialisierungsvektor wird eine Passphrase verwendet.

Ereignis

Ein Ereignis ist ein Prozess, der vom Core aufgezeichnet wird. Ereignisse können innerhalb der Core Console durch Anklicken des Symbols  (Ereignisse) in der Symbolleiste eingesehen werden. Die Standardansicht zeigt beim Klicken auf dieses Symbol die Seite **Aufgaben** an. Diese Ansicht zeigt Ereignisse, die im Zusammenhang mit einem Job stehen. Prioritätsereignisse, über die Sie benachrichtigt werden, können auf der Seite **Warnungen** eingesehen werden. Ein Protokoll aller Ereignisse erscheint auf der Seite **Journal**. Durch Einrichten oder Ändern vorhandener Benachrichtigungsgruppen können Sie Benachrichtigungen für alle Ereignisse anpassen. Diese Maßnahme erhöht die Priorität des Ereignisses durch dessen Anzeige auf der Seite **Warnungen**. Mitglieder einer Benachrichtigungsgruppe werden unter Verwendung der Benachrichtigungsmethoden, die in den Meldungsoptionen für die Gruppe festgelegt wurden, über Ereignisse benachrichtigt.

Globale Deduplizierung

Die Storage Networking Industry Association (SNIA) definiert die Datendeduplizierung als das Ersetzen mehrerer Kopien von Daten – auf verschiedenen Granularitätsebenen – durch Verweise auf eine gemeinsame Kopie, um Speicherplatz oder Bandbreite einzusparen. Der Volume-Manager von Rapid Recovery führt die globale Datendeduplizierung in einem logischen Volume durch. Die Granularität der Deduplizierung beträgt 8 KB. Die Deduplizierung in Rapid Recovery ist auf geschützte Maschinen beschränkt, die das gleiche Repository und den gleichen Verschlüsselungsschlüssel verwenden.

Inkrementeller Snapshot

Inkrementelle Snapshots sind Sicherungen, die nur Daten umfassen, die seit der letzten Sicherung auf der geschützten Maschine geändert wurden. Sie werden regelmäßig basierend auf dem festgelegten Intervall (z. B. alle 60 Minuten) im Core gespeichert. Weitere Informationen finden Sie unter Snapshot.

Lizenzschlüssel

Ein Lizenzschlüssel ist eine mögliche Methode zum Registrieren einer Software oder eines Gerätes von Rapid Recovery. (Sie können auch eine Lizenzdatei verwenden.) Sie können Lizenzschlüssel oder Dateien erhalten, wenn Sie sich auf dem Rapid Recovery Lizenzportal für ein Konto registrieren. Weitere Informationen finden Sie unter Lizenzportal.

Lizenzportal

Über das Internet können Benutzer und Partner auf das Rapid Recovery Lizenzportal zugreifen und Software herunterladen, Rapid Recovery Appliances registrieren und ihre Lizenzabonnements verwalten. Benutzer des Lizenzportals können Konten einrichten, den Software-Kern und -Agenten für Rapid Recovery herunterladen, Gruppen verwalten, Gruppenaktivitäten nachverfolgen, Computer und Geräte registrieren sowie Benutzer einladen und Berichte erstellen. Weitere Informationen finden Sie im *Rapid Recovery Lizenzportal Benutzerhandbuch*.

Live Recovery

Rapid Recovery Live Recovery ist eine Technologie zur Sofortwiederherstellung für VMs und Server. Sie gewährt nahezu ununterbrochenen Zugriff auf Daten-Volumes von virtuellen oder physischen Servern und ermöglicht dadurch die Wiederherstellung kompletter Volumes in extrem kurzer RTO-Zeit und RPO-Zeiten von wenigen Minuten.

Local Mount Utility

Die Local Mount Utility (LMU) ist eine herunterladbare Anwendung, mit der Sie auf einer beliebigen Maschine im Remote-Zugriff einen Wiederherstellungspunkt in einem Rapid Recovery Core laden können.

Protokollkürzung

Bei der Protokollkürzung werden Protokolldatensätze aus dem Transaktionsprotokoll entfernt. Wenn Sie bei einer SQL-Server-Maschine die Kürzung der SQL-Server-Protokolle erzwingen, wird hierdurch der freie Speicherplatz

auf dem SQL-Server ermittelt. Wenn Sie bei einem Oracle Datenbankserver Protokolle kürzen (nach einem Zeitplan oder manuell nach Bedarf), werden Archiv-Protokolle gelöscht, wodurch Speicherplatz frei wird. Wenn Sie die Kürzung der Exchange Server-Protokolle erzwingen, wird dadurch gleichermaßen Speicherplatz auf dem Exchange-Server freigegeben.

Verwaltungsrollen

Die Rapid Recovery Zentrale Verwaltungskonsole umfasst ein neues Konzept für Verwaltungsrollen, mit dem zur Unterstützung einer sicheren und effizienten Delegierung von Verwaltungsaufgaben administrative Zuständigkeiten unter vertrauenswürdigen Daten- und Dienstadministratoren aufgeteilt sowie die Steuerung des Zugriffs ermöglicht werden.

Bereitstellbarkeit

Die Exchange-Bereitstellbarkeitkeitsprüfung ermöglicht die Ermittlung von Beschädigungen. Sie weist Administratoren auf mögliche Fehler hin und stellt sicher, dass alle Daten auf den Exchange-Servern bei einem Ausfall erfolgreich wiederhergestellt werden.

Objektdateisystem

Der skalierbare Objektspeicher von Rapid Recovery ist eine Objektdateisystemkomponente. Alle Datenblöcke, von denen Snapshots abgeleitet werden, werden als Objekte behandelt, die im Objektdateisystem gespeichert, abgerufen, verwaltet und repliziert werden. Das System ist so ausgelegt, dass eine skalierbare E/A-Leistung) zusammen mit globaler Datendeduplizierung, Verschlüsselung und Aufbewahrungsverwaltung bereitgestellt wird. Das Objektdateisystem verfügt über direkte Schnittstellen zu branchenüblichen Speichertechnologien.

Passphrase

Eine Passphrase ist ein Schlüssel, der bei der Datenverschlüsselung verwendet wird. Wenn die Passphrase verloren geht, können die Daten nicht wiederhergestellt werden.

Unzulässige Zeichen

Unzulässige Zeichen sind Zeichen, die in Namen von Objekten in der Rapid Recovery Kern-Konsole nicht verwendet werden dürfen. Beim Festlegen des Anzeigenamens für eine geschützte Maschine dürfen beispielsweise die folgenden Sonderzeichen nicht verwendet werden:

Tabelle 177. Unzulässige Zeichen

Zeichen	Zeichenname	Unzulässig in
?	Fragezeichen	Anzeigename von Maschinen, Verschlüsselungsschlüssel, Repository, Pfad
|	Senkrechter Strich	Anzeigename von Maschinen, Verschlüsselungsschlüssel, Repository, Pfad
:	Doppelpunkt	Anzeigename von Maschinen, Verschlüsselungsschlüssel, Repository Dieses Zeichen wird in Pfadangaben unterstützt, z. B. `c:\data`.
/	Vorwärtsschrägstrich	Anzeigename von Maschinen, Verschlüsselungsschlüssel, Repository, Pfad
\	Umgekehrter Schrägstrich	Anzeigename von Maschinen, Verschlüsselungsschlüssel, Repository Dieses Zeichen wird in Angaben für lokale Pfade oder Netzwerkpfade unterstützt, z. B. `c:\data` oder `\\ComputerName\SharedFolder\`
*	Sternzeichen	Anzeigename von Maschinen, Verschlüsselungsschlüssel, Repository, Pfad
"	Anführungszeichen	Anzeigename von Maschinen, Verschlüsselungsschlüssel, Repository, Pfad

Zeichen	Zeichenname	Unzulässig in
<	Öffnende spitze Klammer	Anzeigename von Maschinen, Verschlüsselungsschlüssel, Repository, Pfad
>	Schließende spitze Klammer	Anzeigename von Maschinen, Verschlüsselungsschlüssel, Repository, Pfad

Unzulässige Phrasen

Unzulässige Phrasen sind Phrasen (oder Zeichenfolgen), die nicht als Namen von Objekten in der Rapid Recovery Kern-Konsole verwendet werden dürfen, weil sie für das Betriebssystem reserviert sind. Die Verwendung dieser Phrasen sollte nach Möglichkeit komplett vermieden werden. Beim Festlegen des Anzeigenamens für eine geschützte Maschine dürfen beispielsweise die folgenden Phrasen nicht verwendet werden:

Tabelle 178. Unzulässige Phrasen

Phrase	Allgemeine Verwendung	Unzulässig in
con	Konsole	Anzeigename von Maschinen, Verschlüsselungsschlüssel, Repository, Pfad
prn	Druckeranschluss	Anzeigename von Computern, Verschlüsselungsschlüssel
aux	Hilfsanschluss	Anzeigename von Computern, Verschlüsselungsschlüssel
nul	NULL-Wert	Anzeigename von Computern, Verschlüsselungsschlüssel
com1, com2... bis com9	Kommunikationsanschlüsse	Anzeigename von Computern, Verschlüsselungsschlüssel
lpt1, lpt2... bis lpt9	LPT-Druckeranschlüsse	Anzeigename von Maschinen, Verschlüsselungsschlüssel, Repository, Pfad

Geschützte Maschine

Ein geschützter Computer – manchmal auch als "Agent" bezeichnet – ist ein physischer Computer oder ein virtueller Computer, der/die durch den Rapid Recovery Kern geschützt wird. Sicherungsdaten werden nach einem vordefinierten Schutzintervall vom geschützten Computer auf das im Kern angegebene Repository übertragen. Das Basis-Image überträgt alle Daten auf einem Wiederherstellungspunkt (einschließlich Betriebssystem, Anwendungen und Einstellungen). Jedes nachfolgende inkrementelle Snapshot bestätigt nur die geänderten Blöcke auf den angegebenen Datenträgervolumes des geschützten Computers. Auf softwarebasiert geschützten Computern ist die Rapid Recovery Agentensoftware installiert. Einige Virtual Machines können mit einigen Einschränkungen auch ohne Agenten ebenfalls geschützt werden.

Rapid Recovery

Rapid Recovery setzt neue Standards beim Datenschutz. Dazu werden Sicherung, Replikation und Wiederherstellung in einer Lösung kombiniert, die als extrem schnelle und zuverlässige Sicherungslösung zum Schutz von virtuellen Maschinen (VM) sowie von physischen und Cloud-Umgebungen konzipiert wurde.

Quorum

In einem Failover-Cluster ist ein Quorum die Anzahl der Elemente, die online sein müssen, damit ein bestimmter Cluster betriebsfähig bleibt. Die in diesem Kontext relevanten Elemente sind Cluster-Knoten. Dieser Begriff kann auch für Quorum-fähige Ressourcen verwendet werden, die für die Verwaltung der Konfigurationsdaten

ausgewählt wurden, die für die Wiederherstellung des Clusters notwendig sind. Diese Daten enthalten Einzelheiten aller Änderungen, die an der Cluster-Datenbank vorgenommen wurden. Im Allgemeinen können andere Cluster-Ressourcen auf die Quorum-Ressource zugreifen, sodass jeder Cluster-Knoten Zugriff auf die aktuellsten Datenbankänderungen hat. Standardmäßig gibt es nur eine Quorum-Ressource pro Server-Cluster. Eine besondere Quorum-Konfiguration (Einstellungen für einen Failover-Cluster) bestimmt den Punkt, an dem zu viele Fehler den Cluster-Betrieb unmöglich machen.

Wiederherstellungspunkte

Wiederherstellungspunkte sind eine Sammlung von Snapshots verschiedener Datenträger-Volumes. Zum Beispiel C:, D: und E:.

Wiederherstellungspunkte-nur Maschine

"Computer-nur Wiederherstellungspunkte" bezeichnet die Darstellung im Kern der Wiederherstellungspunkte eines Computers, der zuvor vom Kern geschützt, inzwischen aber entfernt wurde. Wenn Sie die Replikation entfernen, aber die Wiederherstellungspunkte behalten, erhalten Sie ebenfalls einen "Computer-nur Wiederherstellungspunkte". Informationen können auf Dateiebene angezeigt und wiederhergestellt werden. Sie können einen Computer-nur Wiederherstellungspunkte nicht verwenden, um eine BMR-Wiederherstellung vorzunehmen oder die vollen Volumes wiederherzustellen, noch können Sie weitere Daten zu einem Computer-nur Wiederherstellungspunkte hinzufügen.

Remote-Core

Ein Remote-Kern ist ein Rapid Recovery Kern, auf den durch einen nicht zum Kern gehörenden Computer mithilfe des Local Mount Utility oder der Zentralen Verwaltungskonsole zugegriffen wird.

Replikation

Replikation ist der Vorgang des Kopierens von Wiederherstellungspunkten von einem Rapid Recovery Core und deren Übertragung an einen anderen Rapid Recovery Core zur Notfall-Wiederherstellung. Dafür ist eine gekoppelte Quelle-Ziel-Beziehung zwischen zwei oder mehr Cores erforderlich. Die Replikation wird auf jeder geschützten Maschine einzeln verwaltet. Alle in einem Quell-Core geschützten oder auf einen Quell-Core replizierten Maschinen können für die Replikation auf einen Ziel-Core konfiguriert werden. Hierbei werden die Wiederherstellungspunkte in den Zielkern kopiert.

Repository

Ein Repository ist eine Sammlung von Basis-Images und inkrementellen Snapshots, die von den geschützten Computern eines Rapid Recovery Kerns erfasst werden. Repositorys müssen auf schnellen primären Speichergeräten gespeichert werden. Der Speicherort für eine DVM-Repository kann für den Kern-Computer lokal sein (in diesem Fall wird es nur auf einem unterstützten Windows-BS gehostet). Es kann Direct-Attach-Storage, ein Speicherbereichsnetzwerk oder einen über ein entsprechend gekennzeichnetes Netzwerk verbundenen Server nutzen.

REST-APIs

Representational State-Transfers (REST) ist eine einfache statusfreie Software-Architektur, die auf Skalierbarkeit ausgelegt ist. Rapid Recovery verwendet diese Architektur zur Unterstützung seiner Application Program Interfaces (APIs), um bestimmte Funktionen und Tasks zu automatisieren und anzupassen. Es gibt einen separaten Satz von REST-APIs für Core-Funktionen und für geschützte Maschinenfunktionalität (Agent).

wiederherstellen

Bei einer Wiederherstellung werden Speicher-Volumes auf einer Maschine aus Wiederherstellungspunkten wiederhergestellt, die im Rapid Recovery Core gespeichert sind. Dieser Vorgang wurde früher Rollback genannt.

Aufbewahrung

Die Aufbewahrung definiert den Zeitraum, für den Sicherungs-Snapshots der geschützten Maschinen im Rapid Recovery Core gespeichert werden. Der Rollup-Prozess sorgt dafür, dass die Aufbewahrungsrichtlinie für die Wiederherstellungspunkte eingehalten wird.

Rollup

Der Rollup-Prozess ist ein internes, nachts durchgeführtes Wartungsverfahren, das durch Komprimieren und Entfernen veralteter Wiederherstellungspunkte für die Einhaltung der Aufbewahrungsrichtlinie sorgt. Rapid Recovery reduziert das Rollup auf nur Metadatenvorgänge.

Seeding

Hierbei handelt es sich um die Erstübertragung von deduplizierten Basisimages und inkrementellen Snapshots von geschützten Agenten bei der Replikation, die sich auf hunderte oder tausende Gigabytes an Daten summieren kann. Die Anfangsreplikation kann auf dem Ziel-Core mithilfe externer Datenträger erledigt werden, was bei umfangreichen Daten oder Standorten mit langsamer Verbindung sinnvoll ist.

Server-Cluster

Siehe Windows-Failover-Cluster.

SharePoint-Sicherung

Bei einer SharePoint-Sicherung handelt es sich um eine Datenkopie, die für die Wiederherstellung der Daten auf einem SharePoint-Server nach einem Systemausfall verwendet wird. Anhand der SharePoint-Sicherung können Sie die ganze SharePoint-Farm oder einzelne Komponenten der Farm wiederherstellen.

Einzelkopiecluster

Eine Failover-Cluster-Lösung für Speicher, die eine einzelne Kopie einer Speichergruppe im Speicher verwendet, die von den Knoten im Cluster gemeinsam genutzt wird. Dabei handelt es sich um eine von zwei Bereitstellungsmöglichkeiten für Postfachclusterserver, die in Exchange 2007 verfügbar sind.

Smart Agent

Der Rapid Recovery Smart Agent ist auf den Maschinen installiert, die durch den Rapid Recovery Core geschützt werden. Der Smart Agent protokolliert die geänderten Blöcke auf dem Datenträger-Volume und erstellt in einem vordefiniertem Schutzintervall Snapshots der geänderten Blöcke.

Snapshot

Snapshot ist ein in der Branche gebräuchlicher Ausdruck, mit dem die Fähigkeit zur Erfassung und Speicherung des Zustands eines Datenträger-Volumes zu einem bestimmten Zeitpunkt definiert wird, während Anwendungen ausgeführt werden. Der Snapshot ist entscheidend, wenn eine Systemwiederherstellung aufgrund eines Systemausfalls oder -fehlers erforderlich ist. Die Rapid Recovery Snapshots sind anwendungskonsistent, d. h., dass alle offenen Transaktionen und laufenden Transaktionsprotokolle abgeschlossen und die Cache-Speicher geleert werden, bevor der Snapshot erstellt wird. Rapid Recovery verwendet die Funktionalität der Microsoft Volume Shadow Services (VSS), um konsistente Snapshots beim Absturz von Anwendungen zu ermöglichen.

SQL-Anfügbarkeit

Die SQL-Anfügbarkeit ist ein Test, der im Rapid Recovery Core durchgeführt wird, um sicherzustellen, dass alle SQL-Wiederherstellungspunkte fehlerfrei und im Falle eines Fehlers für die Sicherung verfügbar sind.

SQL-Sicherung

Bei einer SQL-Sicherung handelt es sich um eine Datenkopie, die für die Wiederherstellung der Daten auf einem SQL-Server nach einem Systemausfall verwendet wird. Anhand der SQL-Sicherung können Sie die ganze SQL-Datenbank oder einzelne Komponenten der SQL-Datenbank wiederherstellen.

Differenzielle SQL-Sicherung

Eine differenzielle Datenbanksicherung ist eine kumulative Kopie aller geänderten Daten seit der letzten Vollsicherung der SQL-Datenbank. Die Erstellung differenzieller Sicherungen ist normalerweise schneller als die Erstellung von Vollsicherungen. Darüber hinaus wird die Anzahl der erforderlichen Transaktionsprotokolle für die Wiederherstellung der Datenbank verringert.

Ziel-Core

Der Ziel-Kern, der manchmal auch als Replikat-Kern bezeichnet wird, ist der Rapid Recovery Kern, der die replizierten Daten (Wiederherstellungspunkte) vom Quell-Kern erhält.

Transport Layer Security

TLS (Transport Layer Security) ist ein modernes kryptografisches Netzwerkprotokoll, um eine sichere Kommunikation über das Internet zu gewährleisten. Dieses Protokoll, das von der IETF (Internet Engineering Task Force) definiert wurde, ist der Nachfolger von Secure Sockets Layer (SSL). Im Allgemeinen wird weiterhin der Begriff SSL verwendet. Die beiden Protokolle sind jedoch kompatibel (ein TLS-Client kann mit einem SSL-Server kommunizieren).

True Scale

True Scale ist die skalierbare Architektur von Rapid Recovery.

Universal Recovery

Die Universelle Wiederherstellungstechnologie von Rapid Recovery bietet unbegrenzte Flexibilität bei der Wiederherstellung von Computern. Sie ermöglicht die Durchführung monolithischer Wiederherstellungen auf und von beliebigen physischen oder virtuellen Plattformen sowie die inkrementelle Aktualisierung von Wiederherstellung auf virtuellen Maschinen von jeder physischen oder virtuellen Quelle aus. Darüber hinaus können Sie mit dieser Technologie auf Anwendungs-, Element- und Objektebene Wiederherstellungen von einzelnen Dateien, Ordnern, E-Mails, Kalenderelementen, Datenbanken und Anwendungen durchführen.

Verified Recovery

Mit der Verified Recovery-Technologie werden automatisierte Wiederherstellungstests durchgeführt und Sicherungen überprüft. Sie unterstützt unterschiedliche Dateisysteme und Server.

Virtual Standby

Virtual Standby ist ein Prozess, bei dem ein virtueller Klon-Computer des geschützten Computers erstellt wird. Der ursprüngliche Quell-Computer kann physisch oder virtuell sein, aber das Ergebnis ist immer virtuell. Sie können einen virtuellen Standby einmal bei Bedarf erstellen oder Sie können Anforderungen zur Erstellung einer startfähigen VM definieren und diese nach jedem Snapshot, der auf dem ursprünglichen geschützten Computer erfasst, ständig aktualisieren.

Volume-Manager

Der Rapid Recovery Volume-Manager verwaltet und speichert Objekte und stellt sie anschließend als logisches Volume dar. Er nutzt eine dynamische Pipeline-Architektur, um True Scale-Skalierbarkeit, Parallelität und ein asynchrones E/A-Modell für hohen Durchsatz mit minimaler E/A-Latenz zu liefern.

White-Labeling

Rapid Recovery bietet bestimmten Anbietern von Sicherungs- und Notfallwiederherstellungsdiensten die Möglichkeit, Rapid Recovery ohne Markenaufdruck zu nutzen (White-Labeling) oder mit eigenem Logo zu versehen (Rebranding) und als eigenes Produkt oder als eigenen Dienst zu verkaufen oder zu vertreiben.

Die Option des White-Labelings von Rapid Recovery ist nur für Organisationen verfügbar, deren Quest Softwarelizenzvereinbarungen die Berechtigung zum Rebranding ausdrücklich erteilen. Optionen zum Lizenzieren, Unterlizenzieren und/oder Weiterverkauf dieser Software stehen auch nur Organisationen zur Verfügung, mit denen eine bestimmte Lizenzvereinbarung getroffen wurde, die diese Rechte gewähren. Quest Software behält sich alle Rechte an Rapid Recovery vor. Die Option des White-Labelings gewährt zu keinem Zeitpunkt irgendwelche Rechte des geistigen Eigentums an Rapid Recovery. Wenn Sie diese Funktionalität in Ihrer Organisation nutzen möchten, wenden Sie sich bitte an Ihren Quest Software-Vertreter.

Windows-Failover-Cluster

Eine Gruppe unabhängiger Computer, die zusammenarbeiten, um die Verfügbarkeit von Anwendungen und Diensten zu erhöhen. Die geclusterten Server (so genannte Knoten) sind durch physische Kabel und durch Software miteinander verbunden. Wenn einer der Cluster-Knoten ausfällt, übernimmt ein anderer Knoten die Bereitstellung des Dienstes (dieser Prozess ist als Failover bekannt). Benutzer nehmen nur minimale Dienstunterbrechungen wahr. Rapid Recovery unterstützt den Schutz mehrerer verschiedener SQL Server- und Exchange Server-Clustertypen.