Dell DL1000 Appliance

Bereitstellungshandbuch

DELL EMC

Anmerkungen, Vorsichtshinweise und Warnungen

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

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

WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

2016 - 09

Rev. A03

Inhaltsverzeichnis

1

Einführung der Dell DL1000

Das System Dell DL1000 kombiniert Sicherung und Replikation in einem einheitlichen Datenschutzprodukt. Es bietet eine zuverlässige Wiederherstellung von Anwendungsdaten anhand Ihrer Sicherungen zum Schutz von virtuellen und physischen Maschinen. Ihr Gerät ist in der Lage, Daten in der Größenordnung von Terabytes mit integrierter globaler Deduplizierung, Komprimierung, Verschlüsselung sowie Replikation in privaten oder öffentlichen Cloud-Infrastrukturen durchzuführen. Serveranwendungen und Daten können innerhalb von Minuten zu Datenaufbewahrungs- (Data Retention, DR) und Konformitätszwecken wiederhergestellt werden.

Ihr DL1000 unterstützt Multi-Hypervisor-Umgebungen auf VMware vSphere, Oracle VirtualBox und Microsoft Hyper-V für private und öffentliche Clouds.

Themen:

Dell DL1000-Kerntechnologien

Ihr Gerät kombiniert die folgenden Technologien:

Live-Wiederherstellung

Live-Wiederherstellung ist eine Technologie zur Sofortwiederherstellung für VMs oder Server, die nahezu ununterbrochenen Zugang zu Daten-Volumes auf virtuellen oder physischen Servern gewährt.

Die Sicherungs- und Replikationstechnologie des DL1000 erstellt simultane Snapshots von mehreren VMs oder Servern und liefert dadurch nahezu sofortigen Daten- und Systemschutz. Sie können die Verwendung des Servers durch die Bereitstellung eines Wiederherstellungspunkts wieder aufnehmen, ohne darauf zu warten, dass eine vollständige Wiederherstellung auf dem Produktionsspeicher ausgeführt wird.

Universal-Wiederherstellung

Die Universal-Wiederherstellung bietet uneingeschränkte Flexibilität bei der Maschinenwiederherstellung. Sie können Ihre Sicherungen auf folgenden Umgebungen wiederherstellen: von physischen Systemen auf virtuelle Maschinen, von virtuellen Maschinen auf virtuelle Maschinen, von virtuellen Maschinen auf physische Systeme oder von physischen Systemen auf physische Systeme. Darüber hinaus können Sie Bare-Metal-Wiederherstellungen auf unterschiedliche Hardware ausführen.

Die Universal-Wiederherstellung-Technologie beschleunigt auch plattformübergreifende Verschiebungen zwischen virtuellen Maschinen, zum Beispiel von VMware zu Hyper-V bzw. von Hyper-V zu VMware. Sie umfasst die Wiederherstellung auf Anwendungs-, Element- und Objektebene von einzelnen Dateien, Ordnern, E-Mails, Kalenderelementen, Datenbanken und Anwendungen.

True Global Deduplication

Mithilfe der echten globalen Deduplizierung werden redundante und doppelte Daten durch inkrementelle Sicherungen auf Blockebene der Maschine eliminiert.

Das typische Datenträgerlayout eines Servers besteht aus dem Betriebssystem, der Anwendung und den Daten. In den meisten Umgebungen nutzen die Administratoren für eine effektive Bereitstellung und Verwaltung oftmals eine allgemeine Konfiguration des Servers und Desktops, der bzw. die auf mehreren Systemen ausgeführt werden. Wenn die Sicherung auf Blockebene für mehrere Maschinen durchgeführt wird, erhalten Sie einen genaueren Überblick darüber, welche Inhalte in die Sicherung aufgenommen wurden und welche nicht, unabhängig von der Quelle. Zu diesen Daten gehören das Betriebssystem, die Anwendungen und die Anwendungsdaten in der Umgebung.

Abbildung 1. Diagramm der echten globalen Deduplizierung

Verschlüsselung

Das DL1000 bietet Verschlüsselung, um Sicherungen sowie gespeicherte Daten vor nicht autorisiertem Zugriff und unbefugter Nutzung zu schützen und gewährleistet damit Ihren Datenschutz. Sie können die Daten über den Verschlüsselungsschlüssel entschlüsseln und darauf zugreifen. Die Verschlüsselung wird inline auf Snapshot-Daten durchgeführt, und zwar mit Verbindungsgeschwindigkeiten, die die Leistung nicht beeinträchtigen.

Dell DL1000-Datenschutzfunktionen

Dell DL1000-Kern

Der Kern ist die zentrale Komponente der DL1000-Bereitstellungsarchitektur. Er speichert und verwaltet die Systemsicherungen und bietet Services für Sicherung, Wiederherstellung, Aufbewahrung, Replikation, Archivierung und Verwaltung. Der Kern ist ein eigenständiges Netzwerk und eine adressierbare Maschine, auf der eine 64-Bit-Version der Microsoft Windows Server 2012 R2 Foundation Edition und Standard-Betriebssysteme ausgeführt werden. Das Gerät führt zielbasierte Inline-Komprimierung, Verschlüsselung und Datendeduplizierung

der Daten aus, die vom Agenten empfangen werden. Der Kern speichert anschließend die Snapshot-Sicherungen in das Repository, das sich auf dem Gerät befindet. Kerne werden für die Replikation gekoppelt.

Das Repository befindet sich auf einem internen Speicher innerhalb des Kerns. Der Kern wird durch den Zugriff auf die folgende URL von einem JavaScript-fähigen Webbrowser verwaltet: **https://CORENAME:8006/apprecovery/admin**.

Dell DL1000 Smart Agent

Der Smart Agent ist auf der Maschine installiert, die durch den Kern geschützt wird. Er verfolgt die geänderten Blöcke auf dem Datenträger-Volume und erstellt ein Snapshot-Abbild der geänderten Blöcke in einem vordefinierten Schutzintervall. Der Ansatz eines fortlaufenden inkrementellen Snapshots auf Blockebene verhindert das wiederholte Kopieren der gleichen Daten von der geschützten Maschine auf den Kern.

Nachdem der Agent konfiguriert ist, verwendet er Smart-Technologie, um geänderte Blöcke auf geschützten Datenträger-Volumes nachzuverfolgen. Wenn der Snapshot bereit ist, wird er schnell mithilfe intelligenter mehrinstanzenfähiger, socketbasierter Verbindungen auf den Kern übertragen.

Snapshot-Prozess

Der DL1000-Schutzvorgang beginnt, wenn ein Basisabbild von einer geschützten Maschine auf den Kern übertragen wird. In dieser Phase wird eine vollständige Kopie der Maschine im Normalbetrieb über das Netzwerk transportiert, gefolgt von fortlaufenden inkrementellen Snapshots. Der DL1000-Agent für Windows nutzt den Microsoft Volume-Schattenkopie-Dienst (Volume Shadow Copy Service, VSS) für das Einfrieren und Stilllegen von Anwendungsdaten auf Datenträgern, um eine Dateisystem-konsistente und eine Anwendungs-konsistente Sicherung zu erfassen. Wenn ein Snapshot erstellt wird, verhindert der VSS-Generator auf dem Zielserver, dass Inhalte auf den Datenträger geschrieben werden. Während das Schreiben von Inhalten auf den Datenträger angehalten ist, werden alle Datenträger-E/A-Vorgänge in eine Warteschlange gestellt und erst wieder fortgesetzt, nachdem der Snapshot fertig erstellt ist, während alle derzeit ausgeführten Vorgänge abgeschlossen und alle geöffneten Dateien geschlossen werden. Der Prozess zum Erstellen einer Schattenkopie beeinträchtigt die Leistung des Produktionssystems nicht wesentlich.

Ihr DL1000 verwendet Microsoft VSS, da das Gerät über integrierten Support für alle Windows-internen Technologien wie NTFS, Registry, Active Directory verfügt, um Daten vor der Erstellung des Snapshots auf der Festplatte zu speichern. Außerdem verwenden andere Unternehmensanwendungen wie Microsoft Exchange und SQL die VSS-Generator-Plug-Ins, um benachrichtigt zu werden, wenn ein Snapshot vorbereitet wird und wenn sie ihre verwendeten Datenbankseiten auf dem Datenträger speichern müssen, um die Datenbank in einen konsistenten Transaktionsstatus zu versetzen. Die erfassten Daten werden schnell auf den Kern übertragen und gespeichert.

Replikation – Notfall-Wiederherstellungsstandort oder Dienstanbieter

Bei der Replikation handelt es sich um einen Prozess des Kopierens der Wiederherstellungspunkte von einem Rapid Recovery-Kern und des Übertragens dieser Punkte auf einen anderen Rapid Recovery-Kern auf einem separaten Speicherort zur Notfall-Wiederherstellung. Für diesen Prozess benötigen Sie eine gekoppelte Quell-Ziel-Beziehung zwischen zwei oder mehr Kernen.

Der Quellkern kopiert die Wiederherstellungspunkte der ausgewählten geschützten Maschinen und überträgt die inkrementellen Snapshot-Daten asynchron und dauerhaft auf den Zielkern an einem Remote-Notfall-Wiederherstellungsstandort. Sie können eine ausgehende Replikation auf ein unternehmenseigenes Rechenzentrum oder auf einen Remote-Notfall-Wiederherstellungsstandort (selbstverwalteter Zielkern) konfigurieren. Außerdem können Sie eine ausgehende Replikation auch auf einen MSP-Standort (Managed Service Provider) eines Drittanbieters oder auf einen Cloud-Anbieter, der externe Backups und einen Notfall-Wiederherstellungsservice bereitstellt, konfigurieren. Bei der Replikation auf einen Zielkern eines Drittanbieters können Sie integrierte Arbeitsabläufe verwenden, über die Sie Verbindungen anfordern und automatische Rückmeldungen erhalten können.

Replikation wird auf Basis jeder geschützten Maschine verwaltet. Jede Maschine (oder alle Maschinen), die auf einem Quellkern geschützt oder repliziert sind, können für die Replikation auf einen Zielkern konfiguriert werden.

Die Replikation ist selbstoptimierend mit einem einzigartigen Read-Match-Write (RMW)-Algorithmus, der eng mit der Deduplizierung verknüpft ist. Bei der RMW-Replikation gleicht der Quell- und Zielreplikation-Service die Schlüssel vor der Datenübertragung ab und repliziert dann nur die komprimierten – verschlüsselten – deduplizierten Daten über das WAN, was eine 10-fache Reduzierung der Bandbreitenanforderungen bedeutet.

Die Replikation beginnt mit dem Seeding: Die anfängliche Übertragung von deduplizierten Basisabbildern und inkrementellen Snapshots der geschützten Maschinen, die sich auf Hunderte oder Tausende Gigabytes von Daten summieren können. Die erste Replikation kann mithilfe externer Medien auf dem Zielkern platziert werden. Üblicherweise ist das bei großen Datensätzen oder Standorten mit langsamer Verbindung nützlich. Die Daten im Seeding-Archiv sind komprimiert, verschlüsselt und dedupliziert. Wenn die Gesamtgröße des Archivs den auf dem Wechseldatenträger verfügbaren Speicherplatz überschreitet, kann sich das Archiv, je nach verfügbarem Speicherplatz auf dem Datenträger, über mehrere Geräte erstrecken. Während des Seeding-Vorgangs werden die inkrementellen Wiederherstellungspunkte am Zielstandort repliziert. Nachdem der Zielkern das Seeding-Archiv konsumiert, werden die neu replizierten inkrementellen Wiederherstellungspunkte automatisch synchronisiert.

Wiederherstellung

Eine Wiederherstellung kann am lokalen Standort oder am replizierten Remote-Standort durchgeführt werden. Nachdem sich die Bereitstellung in einem stabilen Zustand mit lokalem Schutz und optionaler Replikation befindet, ermöglicht Ihnen der DL1000-Kern Wiederherstellungsvorgänge mithilfe von Verified Recovery, Universal-Wiederherstellung oder Live-Wiederherstellung.

Recovery-as-a-Service (RaaS)

Anbieter von verwalteten Diensten (MSPs) können das DL1000 vollständig als Plattform für die Bereitstellung der Wiederherstellung als Service (RaaS, Recovery-as-a-Service) nutzen. RaaS ermöglicht eine vollständige Wiederherstellung in der Cloud (Recovery-in-the-Cloud), indem die physischen und virtuellen Server des Kunden repliziert werden. Die Clouds des Dienstanbieters werden als virtuelle Maschinen zur Unterstützung von Wiederherstellungstests oder tatsächlichen Wiederherstellungsvorgängen verwendet. Kunden, die eine Wiederherstellung in der Cloud durchführen möchten, können die Replikation auf ihren geschützten Maschinen auf den lokalen Kernen zu einem Rapid Recovery-Dienstanbieter konfigurieren. In einem Notfall können die MSPs sofort virtuelle Maschinen für den Kunden bereitstellen.

Das DL1000 selbst ist nicht mandantenfähig. Die MSPs können das DL1000 jedoch an mehreren Standorten verwenden und eine mandantenfähige Umgebung an ihrem Ende erstellen.

Virtualisierung und Cloud

Der DL1000-Kern ist Cloud-fähig und ermöglicht Ihnen, die Rechenkapazität der Cloud für die Wiederherstellung und Archivierung zu nutzen.

Das DL1000 kann alle geschützten oder replizierten Maschinen auf lizenzierte Versionen von VMware oder Hyper-V exportieren. Bei fortlaufenden Exporten wird die virtuelle Maschine inkrementell nach jedem Snapshot aktualisiert. Die inkrementellen Aktualisierungen erfolgen schnell und stellen Standby-Klone bereit, die mit einem Mausklick auf eine Schaltfläche eingeschaltet werden können. Die folgenden Exporte für virtuelle Maschinen werden unterstützt:

- VMware Workstation oder Server in einem Ordner
- Direkter Export auf einen VSphere- oder VMware ESXi-Host
- Export zu Oracle VirtualBox
- Microsoft Hyper-V-Server auf Windows Server 2008 (x64)
- Microsoft Hyper-V Server auf Windows Server 2008 R2

- Microsoft Hyper-V Server auf Windows Server 2012 R2

Sie können nun Ihre Repository-Daten in die Cloud archivieren. Verwenden Sie dazu Plattformen wie Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage oder andere OpenStack-basierte Cloud-Dienste.

Dell DL1000-Bereitstellungsarchitektur

Die DL1000-Bereitstellungsarchitektur besteht aus lokalen Komponenten und Remote-Komponenten. Die Remote-Komponenten sind möglicherweise für Umgebungen optional, die keinen Notfallwiederherstellungsstandort oder keinen Anbieter verwalteter Dienste für eine externe Wiederherstellung erfordern. Eine einfache lokale Bereitstellung besteht aus einem Sicherungsserver, der Kern genannt wird, und mindestens einer geschützten Maschine, die als Agent bezeichnet wird. Die externe Komponente wird mithilfe von Replikation aktiviert, die umfassende Wiederherstellungsfähigkeiten am Notfall-Wiederherstellungsstandort bietet. Der DL1000-Kern verwendet Basisabbilder und inkrementelle Snapshots, um die Wiederherstellungspunkte der geschützten Agenten zu kompilieren.

Darüber hinaus ist das DL1000 in der Lage, vorhandene Microsoft Exchange- und SQL-Anwendungen und ihre entsprechenden Datenbanken und Protokolldateien zu erkennen (Anwendungserkennung). Sicherungen werden mithilfe anwendungsspezifischer Snapshots auf Blockebene durchgeführt. Das DL1000 führt die Kürzung des Protokolls des geschützten Microsoft Exchange-Server durch.

Das folgende Diagramm stellt eine einfache DL1000-Bereitstellung dar. DL1000-Agenten sind auf Maschinen installiert, z. B. auf Dateiservern, E-Mail-Servern oder Datenbankservern, oder virtuelle Maschinen sind mit einem einzigen DL1000-Kern verbunden, der aus einem zentralen Repository besteht, und werden durch diesen geschützt. Das Dell Software License Portal verwaltet Lizenzabonnements, Gruppen und Benutzer für die Agenten und Kerne in Ihrer Umgebung. Das License Portal ermöglicht Ihnen, sich anzumelden, Konten zu aktivieren, Software herunterzuladen und Agenten und Kerne gemäß Ihrer Lizenz für Ihre Umgebung bereitzustellen.

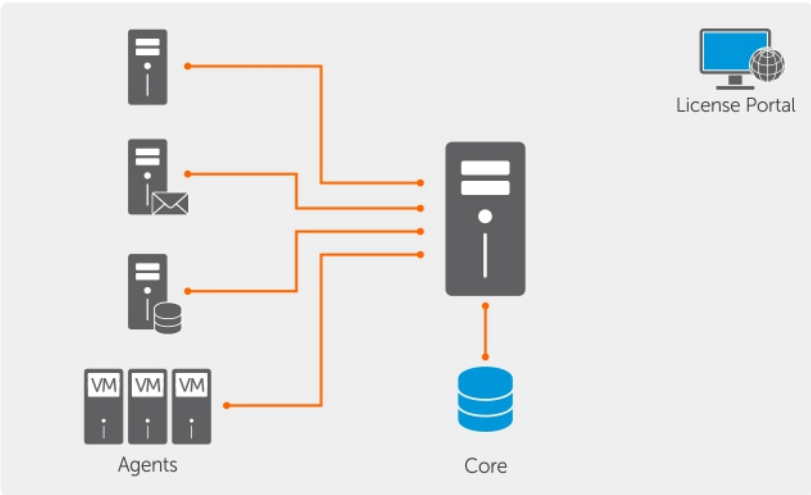

Abbildung 2. Dell DL1000-Bereitstellungsarchitektur

Sie können auch mehrere DL1000-Kerne bereitstellen, wie im folgenden Diagramm beschrieben. Eine zentrale Konsole verwaltet mehrere Kerne.

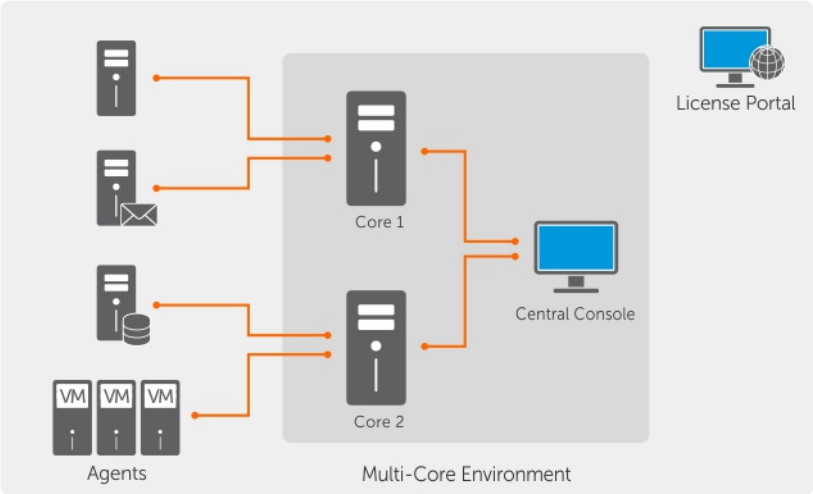

Abbildung 3. DL1000-Bereitstellungsarchitektur mit mehreren Kernen

Weitere nützliche Informationen

ANMERKUNG: Rufen Sie für alle Dokumente zu Dell OpenManage die Seite Dell.com/openmanagemanuals auf.

ANMERKUNG: Wenn auf der Website Dell.com/support/home aktualisierte Dokumente vorliegen, lesen Sie diese immer zuerst, denn frühere Informationen werden damit gegebenenfalls ungültig.

ANMERKUNG: Dokumentation zu Dell OpenManage Server Administrator finden Sie unter Dell.com/openmanage/manuals.

Die Produktdokumentation beinhaltet:

Handbuch zum Einstieg	Bietet eine Übersicht über das Einrichten des Systems und die technischen Spezifikationen. Dieses Dokument wird auch mit dem System mitgeliefert.
System-Platzset	Enthält Informationen zum Einrichten der Hardware und Installieren der Software auf Ihrem Gerät.
Benutzerhandbuch	Bietet Informationen zu Systemfunktionen, zur Fehlerbehebung am System und zur Installation oder zum Austausch von Systemkomponenten.
Bereitstellungshandbuch	Enthält Informationen zur Hardwarebereitstellung und zur Erstbereitstellung der Appliance.
Benutzerhandbuch	Enthält Informationen über die Konfiguration und die Verwaltung des Systems.
Versionshinweise	Bietet Produktinformationen und weitere Informationen zum Dell DL1000-Gerät.
Interoperabilitätshandbuch	Enthält Informationen zur unterstützten Software und Hardware für Ihr DL1300-Gerät sowie Überlegungen, Empfehlungen und Richtlinien zur Nutzung.
OpenManageServer Administrator Benutzerhandbuch	Enthält Informationen über die Verwendung von Dell OpenManage Server Administrator zur Verwaltung des Systems.

2

Installieren der Dell DL1000

Einführung

Die DL Backup to Disk Applinace ermöglicht:

- Schnellere Sicherungen sowie schnellere Wiederherstellungsszenarien über herkömmliche Bandgeräte und Sicherungsmethoden.
- Optionale Möglichkeit zur Deduplizierung
- Permanenter Datenschutz für Rechenzentren und Server in Betriebsniederlassungen
- Schnelle und einfache Bereitstellung, dank der wichtige Daten sofort geschützt werden können

Verfügbare Konfigurationen

Die DL-Appliance ist in folgenden Konfigurationen verfügbar:

Tabelle 1. Verfügbare Konfigurationen

Kapazität	Hardwarekonfiguration
1 TB ohne virtuelle Maschinen	2-TB-Festplatte mit 200 GB-Betriebssystem-/Software-Partition und 1 TB nutzbarer Repository-Speicherplatz
2 TB ohne virtuelle Maschinen	3-TB-Festplatte mit 200 GB-Betriebssystem-/Software-Partition und 2 TB nutzbarer Repository-Speicherplatz
3 TB ohne virtuelle Maschinen	4-TB-Festplatte mit 200 GB-Betriebssystem-/Software-Partition und 3 TB nutzbarer Repository-Speicherplatz
3 TB mit zwei virtuellen Maschinen	4-TB-Festplatte mit 200 GB-Betriebssystem-/Software-Partition, einer 300-GB-Partition für den VM-Speicher und 3 TB nutzbarer Repository-Speicherplatz

Jede Konfiguration umfasst die folgende Hard- und Software:

- Dell DL1000-System
- Dell PowerEdge RAID-Controller (PERC)
- Dell AppAssure-Software

Installationsübersicht

Die DL1000-Installation umfasst die Installation des Rapid Recovery-Kerns und der Rapid Recovery Agenten-Dienste auf den zu schützenden Systemen. Wenn zusätzliche Kerne eingerichtet werden, müssen die Rapid Recovery Central Management Console-Dienste installiert werden.
Führen Sie zur Installation der DL1000 die folgenden Schritte aus:

1 Besorgen Sie sich den permanenten Lizenzschlüssel. Über die Core-Konsole können Sie Ihre DL1000-Lizenzen direkt verwalten, den Lizenzschlüssel ändern und den Lizenzserver kontaktieren. Außerdem können Sie auf das Rapid Recovery License Portal (Lizenzportal) von der Seite „Licensing“ (Lizenzierung) aus in der Core-Konsole zugreifen.

ANMERKUNG: Das System wird mit einer vorübergehenden 30-tägigen Lizenz konfiguriert und geliefert.

2 Prüfen der Voraussetzungen für die Installation.
3 Einrichten der Hardware.
4 Einrichten der anfänglichen Software (DL Appliance-Konfigurationsassistent).
5 Installieren der Kern-Verwaltungskonsole.

Installationsvoraussetzungen

Netzwerkanforderungen

Für Ihr Gerät muss die folgende Netzwerkumgebung vorhanden sein:

- Aktives Netzwerk mit verfügbaren Ethernet-Kabeln und -Verbindungen
- Eine statische IP-Adresse und die IP-Adresse eines DNS-Servers, falls nicht durch DHCP (Dynamic Host Configuration Protocol) zugewiesen
- Benutzername und Kennwort mit Administratorrechten

Empfohlene Netzwerkinfrastruktur

Vor einem Jahrzehnt wies die Standard-Backbone-Infrastruktur Geschwindigkeiten von 100 Megabit pro Sekunde auf. Anforderungen an den Netzwerkverkehr und Ein- und Ausgaben haben sich stetig und deutlich erhöht. Als Folge davon haben die Standards für Netzwerk-Backbones zugenommen, um den Anforderungen zu entsprechen. Moderne Netzwerk-Backbones unterstützen Geschwindigkeiten wie Gigabit-Ethernet (GbE), das Ethernet-Frames mit 1 Gigabit pro Sekunde überträgt, oder 10GbE, das zehnmal schneller ist.

Zur Ausführung von Rapid Recovery benötigt Dell eine minimale Netzwerkinfrastruktur von 1GbE für eine effiziente Leistung. Dell empfiehlt 10GbE-Netzwerke für robuste Umgebungen. 10GbE-Netzwerke werden ebenfalls empfohlen, wenn Server mit großen Volumen (5TB oder höher) geschützt werden.

Wenn mehrere Netzwerkschnittstellenkarten (NICs) auf der Kernmaschine zur Verfügung stehen, die NIC-Teaming (Zusammenfassung mehrerer physischer NICs zu einer einzigen logischen NIC) unterstützen, und wenn die Switches im Netzwerk es erlauben, dann kann die Verwendung von NIC-Teaming auf dem Kern zusätzliche Leistung bieten. In solchen Fällen kann das Zusammenarbeiten von Ersatznetzwerkkarten, die NIC-Teaming auf allen geschützten Maschinen unterstützen, soweit dies möglich ist, auch die Gesamtleistung erhöhen.

Wenn der Kern iSCSI- oder Network Attached Storage (NAS) verwendet, empfiehlt Dell die Verwendung von separaten NIC-Karten für den Speicher- und Netzwerkverkehr.

Verwenden Sie Netzwerkkabel mit der entsprechenden Nenngröße, um die erwartete Bandbreite zu erhalten. Dell empfiehlt das regelmäßige Testen der Netzwerkleistung und das entsprechende Anpassen der Hardware.

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

Einrichten der Hardware

Das Gerät wird mit einem einzelnen DL1000-System geliefert. Lesen Sie das mit dem Gerät gelieferte Handbuch zum Einstieg *Getting Started Guide* für Ihr System. Packen Sie die DL1000-Gerätehardware aus, und richten Sie sie ein.

ANMERKUNG: Die Software ist auf dem System vorinstalliert. Sämtliche im System enthaltenen Datenträger dürfen nur dann verwendet werden, wenn eine Systemwiederherstellung erforderlich ist.

So richten Sie die DL1000-Hardware ein:

1 Bauen Sie das DL1000-System in ein Rack ein, und verkabeln Sie es.
2 Schalten Sie das DL1000-System ein.

Installieren des DL1000-Geräts in ein Rack

Wenn Ihr System ein Schienen-Kit beinhaltet, lesen Sie die *Anweisungen für die Rack-Montage*, die mit dem Schienen-Kit geliefert wurden. Befolgen Sie die Anweisungen zum Installieren der Schienen und des DL1000 in das Rack.

Verwenden des Systems ohne ein Rack

Sie können das System ohne ein Server-Rack verwenden. Stellen Sie sicher, dass Sie, wenn Sie das System ohne ein Rack verwenden, die folgenden Richtlinien beachten:

- Das System muss auf eine solide und stabile Oberfläche, die das gesamte System unterstützt, platziert werden.

  ANMERKUNG: Das System darf nicht senkrecht aufgestellt werden.
- Platzieren Sie das System nicht auf dem Boden.
- Stellen oder legen Sie keine Gegenstände auf der Oberseite des Systems ab. Das obere Bedienfeld neigt sich eventuell unter dem Gewicht, was zu Schäden am System führen kann.
- Stellen Sie sicher, dass genügend Platz um das System herum zur Verfügung steht, um eine ausreichende Belüftung zu gewährleisten.
- Stellen Sie sicher, dass das System unter den Temperaturbedingungen installiert wurde, die in den technischen Daten im Abschnitt „Umgebung“ des DL1300-Benutzerhandbuchs *Dell DL1000 Appliance Owner's Manual* unter **Dell.com/support/home** empfohlen werden.

VORSICHT: Wenn Sie diese Richtlinien nicht befolgen, kann dies zu einer Beschädigung des Systems oder Verletzungen zur Folge haben.

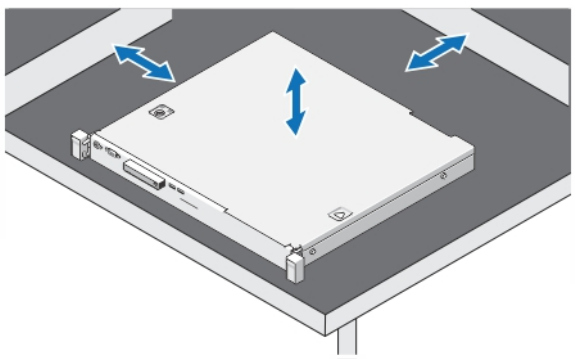

Abbildung 4. Verwenden des Systems ohne ein Rack

Verkabelung des Systems

Lesen Sie das Handbuch zum Einstieg für das DL1300-System *Dell DL1000 Appliance Getting Started Guide*, das mit dem Gerät geliefert wurde, und befolgen Sie die Anweisungen zum Anschließen der Tastatur-, Maus-, Monitor-, Strom- und Netzwerkkabel an das DL1000-System.

Anschließen des Kabelführungsarms (optional)

Falls Ihr System einen Kabelführungsarm (CMA) enthält, machen Sie die *Installationsanleitung für den Kabelführungsarm* ausfindig, die im Lieferumfang des Kits mit dem Kabelführungsarm enthalten ist, und befolgen Sie die Anweisungen zum Installieren des Kabelführungsarms.

Einschalten der DL1000 Appliance

Nachdem Sie das Gerät verkabelt haben, schalten Sie das System ein.

ANMERKUNG: Es wird empfohlen, das Gerät zur Sicherstellung einer maximalen Zuverlässigkeit und Verfügbarkeit an eine unterbrechungsfreie Stromversorgung (USV) anzuschließen. Weitere Informationen finden Sie im *Dell DL1000 Getting Started Guide (Handbuch zum Einstieg)* unter Dell.com/support/manuals.

Anfängliches Software-Setup

Nach dem ersten Einschalten des Geräts und Ändern des Systemkennworts wird automatisch der **AppAssure Appliance-Konfigurationsassistent** ausgeführt.

1 Wählen Sie nach dem Einschalten des Systems Ihre Betriebssystem-Sprache aus den Windows-Sprachoptionen aus.
   Die Microsoft EULA (Endbenutzer-Lizenzvereinbarung) wird auf der Seite **Einstellungen** angezeigt.
2 Übernehmen Sie die Endbenutzer-Lizenzvereinbarung, indem Sie auf **Ich stimme zu** klicken.
   Eine Seite zum Ändern des Administratorkennworts wird angezeigt.
3 Klicken Sie bei der Meldung, die Sie zum Ändern Ihres Administrator-Kennworts auffordert auf **OK**.
4 Geben Sie das neue Kennwort ein und bestätigen Sie es.
   Sie werden von einer Meldung darauf hingewiesen, dass das Kennwort geändert wurde.
5 Klicken Sie auf **OK**.
   Nach der Eingabe des Kennworts wird der Bildschirm **Drücken Sie STRG+ALT+ENTF, um sich anzumelden** angezeigt.
6 Melden Sie sich mit dem geänderten Administratorkennwort an.
   Der Bildschirm **Select the language for Appliance (Sprache für das Gerät auswählen)** wird angezeigt.
7 Wählen Sie die Sprache für Ihr Gerät aus der Liste der unterstützten Sprachen aus.
   Daraufhin wird das Fenster **EULA** angezeigt.
8 Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung, indem Sie auf **EULA akzeptieren** klicken.

   ANMERKUNG: Sie können den Konfigurationsassistenten für die AppAssure Appliance nur ausführen, wenn Sie die EULA akzeptiert haben. Andernfalls meldet Sie das Gerät unmittelbar ab.

Der Startbildschirm **AppAssure Appliance-Konfigurationsassistent** wird angezeigt.

ANMERKUNG: Es kann bis zu 30 Sekunden dauern, bis der AppAssure Appliance-Konfigurationsassistent auf der Systemkonsole angezeigt wird.

AppAssure Appliance Configuration Wizard (Konfigurationsassistent)

VORSICHT: Stellen Sie sicher, dass Sie alle Schritte des AppAssure Appliance-Konfigurationsassistenten abgeschlossen haben, bevor Sie einen anderen Vorgang auf dem Gerät ausführen oder Einstellungen auf dem Gerät vornehmen. Nehmen Sie keine Änderungen über die Systemsteuerung vor, vermeiden Sie die Verwendung von Microsoft Windows Update, und vermeiden Sie außerdem die Aktualisierung der AppAssure-Software bzw. die Installation von Lizenzen, bis der Assistent beendet ist. Der Windows-Aktualisierungsdienst wird während des Konfigurationsvorgangs vorübergehend deaktiviert. Wenn Sie den Konfigurationsassistenten für die AppAssure Appliance beenden, bevor der Konfigurationsvorgang abgeschlossen ist, können Systemfehler auftreten.

Der **AppAssure Appliance-Konfigurationsassistent** führt Sie durch die weiteren Schritte zum Konfigurieren der Software auf dem Gerät:

- Konfiguration der Netzwerkschnittstelle
- Konfiguration der Host-Namen- und Domain-Einstellungen
- Konfigurieren der SNMP-Einstellungen
- Speicherbereitstellung

Nach Abschluss der Installation mithilfe des Assistenten startet die Kern-Konsole automatisch.

Konfiguration der Netzwerkschnittstelle

So konfigurieren Sie die vorhandenen Netzwerkschnittstellen:

1 Klicken Sie auf dem **Begrüßungsbildschirm des AppAssure-Systemkonfigurationsassistenten** auf **Weiter**.
Die Seite **Netzwerkschnittstellen** zeigt die verfügbaren verbundenen Netzwerkschnittstellen an.

2 Wählen Sie die Netzwerkschnittstellen aus, die Sie konfigurieren wollen.

ANMERKUNG: Der AppAssure Appliance Configuration wizard (AppAssure-Gerätekonfigurationsassistent) konfiguriert Netzwerkschnittstellen als einzelne Ports (ohne Teaming). Für eine Verbesserung der Aufnahmeleistung können Sie einen größeren Aufnahmekanal durch Teaming der NICs erstellen. Dies muss jedoch nach der Erstkonfiguration des Systems vorgenommen werden.

3 Falls erforderlich, verbinden Sie die zusätzlichen Nezwerkschnittstellen und klicken Sie auf **Aktualisieren**.
Es werden die zusätzlich verbundenen Netzwerkschnittstellen angezeigt.

4 Klicken Sie auf **Weiter**.
Es wird die Seite **Ausgewählte Netzwerkschnittstelle konfigurieren** angezeigt.

5 Wählen Sie für die ausgewählte Schnittstelle das entsprechende Internetprotokoll aus.
Sie können **IPv4** oder **IPv6** auswählen.

Es werden die Netzwerkeinzelheiten entsprechend Ihrer Auswahl des Internetprotokolls angezeigt.

6 Verwenden Sie zum Zuweisen der Internetprotokolleinzelheiten eine der folgenden Vorgehensweisen:
- Wählen Sie zum automatischen Zuweisen der Internetprotokolleinzelheiten **IPV4-Adresse automatisch beziehen**.
- Wählen Sie zum manuellen Zuweisen der Netzwerkverbindung **Folgende IPv4-Adresse verwenden** aus und geben Sie die folgenden Details ein:
  - **IPv4 Adresse** oder **IPv6-Adresse**
  - **Subnetzmaske** für IPv4 und **Subnetzpräfixlänge** für IPv6
  - **Standard-Gateway**

7 Verwenden Sie zum Zuweisen der DNS-Server-Einzelheiten eine der folgenden Vorgehensweisen:
- Wählen Sie zum automatischen Zuweisen der DNS-Server-Einzelheiten **DNS-Server-Adresse automatisch beziehen**.

- Wählen Sie zum manuellen Zuweisen des DNS-Servers **Folgende DNS-Server-Adresse verwenden** und geben Sie die folgenden Details ein:
  - **Bevorzugter DNS-Server**
  - **Alternativer DNS-Server**

8 Klicken Sie auf **Weiter**.

Es wird die Seite **Hostnamen- und Domain-Einstellung** angezeigt.

Beziehen Sie sich für Informationen zum NIC-Teaming auf Teaming von Netzwerkkarten.

Konfiguration der Host-Namen- und Domain-Einstellungen

Dem System muss ein Host-Name zugewiesen werden. Es wird empfohlen, dass der Host-Name geändert wird, bevor Sicherungen gestartet werden. Standardmäßig ist der Host-Name der Systemname, wie er durch das Betriebssystem zugewiesen wird.

ANMERKUNG: Wenn Sie vorhaben, den Host-Namen zu ändern, wird empfohlen, dass Sie den Host-Namen zu diesem Zeitpunkt ändern. Das Ändern des Host-Namens nach Abschluss des AppAssure Appliance Configuration wizard (AppAssure-Gerätekonfigurationsassistenten) erfordert die Durchführung mehrerer Schritte.

Konfigurieren Sie den Host-Namen und die Domäneneinstellungen:

1 Geben Sie auf der Seite **Configure host name and domain setting** (Host-Namen- und Domain-Einstellungen konfigurieren) im Textfeld **New host name** (Neuer Host-Name) einen geeigneten Host-Namen ein.

2 Wenn Sie nicht wollen, dass das System mit einer Domäne verbunden wird, dann wählen Sie in **Do you want this appliance to join a domain?** (Wollen Sie, dass dieses System einer Domäne beitritt?) die Option **No** (Nein) aus.

ANMERKUNG: Wenn Ihr DL1000 im Installationsumfang der Microsoft Windows Server 2012 Foundation Edition enthalten ist, wird die Option zum Beitreten zu einer Domäne deaktiviert.

Standardmäßig ist **Ja** voreingestellt.

3 Wenn Sie Ihre Anwendung mit einer Domäne verbinden möchten, geben Sie die folgenden Details ein:

- **Domänenname**
- **Domain-Benutzername**

ANMERKUNG: Der Domain-Benutzername muss über lokale Administratorrechte verfügen.

- **Domain-Benutzerkennwort**

4 Klicken Sie auf **Weiter**.

ANMERKUNG: Das Ändern des Host-Namens oder der Domäne erfordert einen Neustart. Nach dem Neustart wird automatisch der AppAssure Appliance Configuration wizard (AppAssure-Gerätekonfigurationsassistent) gestartet. Wenn das System mit einer Domäne verbunden ist, müssen Sie sich nach dem Neustart als Domänenbenutzer mit Administratorberechtigungen am System anmelden.

Es wird die Seite **SNMP-Einstellungen konfigurieren** angezeigt.

Konfigurieren der SNMP-Einstellungen

Simple Network Management Protocol (SNMP) ist ein häufig verwendetes Netzwerkverwaltungsprotokoll, das SNMP-kompatible Verwaltungsfunktionen ermöglicht, wie z.B. die Geräteermittlung, Überwachung und Ereignisgenerierung. SNMP bietet die Netzwerkverwaltung des TCP/IP-Protokolls.

So konfigurieren Sie SNMP-Warnungen für das Gerät:

1 Wählen Sie auf der Seite **SNMP-Einstellungen konfigurieren** die Option **Auf diesem Gerät SNMP konfigurieren** aus.

ANMERKUNG: Heben Sie die Auswahl von Auf diesem Gerät SNMP konfigurieren auf, wenn Sie auf dem Gerät keine SNMP-Details und Warnungen einrichten wollen und fahren Sie mit Schritt 6 fort.

2 Geben Sie in **Communities** einen oder mehrere SNMP-Community-Namen ein.

Verwenden Sie Kommas zum Trennen mehrerer Community-Namen.

3 Geben Sie in **SNMP-Pakete von diesen Hosts akzeptieren** die Namen von Hosts ein, mit denen das Gerät kommunizieren kann.

Trennen Sie die Host-Namen mit Kommas oder lassen Sie dieses Feld unausgefüllt, um eine Kommunikation mit allen Hosts zu erlauben.

4 Geben Sie zum Konfigurieren von SNMP-Warnungen den **Community-Namen** und die **Trap-Ziele** für die SNMP -Warnungen ein und klicken Sie auf **Hinzufügen**.

Wiederholen Sie diesen Schritt, um weitere SNMP-Adressen hinzuzufügen.

5 Wählen Sie zum Entfernen einer konfigurierten SNMP-Adresse in **Konfigurierte SNMP-Adressen** die entsprechende SNMP-Adresse aus und klicken Sie auf **Entfernen**.

6 Klicken Sie auf **Weiter**.

Es wird die Seite **Vielen Dank** angezeigt.

7 Um die Konfiguration abzuschließen, klicken Sie auf **Weiter**.

8 Klicken Sie auf der Seite **Configuration Complete** (Konfiguration abgeschlossen) auf **Exit** (Beenden).

Die Kern-Konsole wird in Ihrem Standard-Web-Browser geöffnet.

Speicherbereitstellung

So schließen Sie die Laufwerksbereitstellung für alle verfügbaren Speicher zum Erstellen eines neuen AppAssure-Repository ab:

1 Klicken Sie auf der Seite **Provisioning** (Bereitstellung) auf **Next** (Weiter).

Die Seite **Provisioning** (Bereitstellung) zeigt die vorhandene Speicherkapazität für Bereitstellung an. Diese Kapazität wird dazu verwendet, ein neues AppAssure Repository zu erstellen.

> **ANMERKUNG: Für das DL1000 3 TB (2 VM)-Konfigurationssystem können Sie Speicherplatz den Standby-VMs zuordnen.**

Die Laufwerksbereitstellung für Ihr System ist abgeschlossen, und ein neues Repository wird erstellt.

2 Klicken Sie auf **Next** (Weiter).

Die Seite **Configuration Complete** (Konfiguration abgeschlossen) wird angezeigt, klicken Sie auf **Exit** (Beenden).

DL Appliance-Konfigurationsassistent

> **ANMERKUNG: Sie können den DL Appliance-Konfigurationsassistenten nur sehen, wenn Sie Ihr Gerät mit dem neuesten RUU aktualisieren.**

> **VORSICHT: Stellen Sie sicher, dass Sie alle Schritte des DL Appliance-Konfigurationsassistenten abgeschlossen haben, bevor Sie einen anderen Vorgang auf dem Gerät ausführen oder Einstellungen auf dem Gerät vornehmen. Nehmen Sie keine Änderungen über die Systemsteuerung vor, vermeiden Sie die Verwendung von Microsoft Windows Update, die Aktualisierung der Rapid Recovery-Software bzw. die Installation von Lizenzen, bis der Assistent beendet ist. Der Windows-Aktualisierungsdienst wird während des Konfigurationsvorgangs vorübergehend deaktiviert. Wenn Sie den Konfigurationsassistenten für die DL Appliance beenden, bevor der Konfigurationsvorgang abgeschlossen ist, können Systemfehler auftreten.**

Der DL Appliance-Konfigurationsassistent führt Sie durch die nachfolgenden Schritte, um die Software auf dem Gerät zu konfigurieren:

- Konfiguration der Netzwerkschnittstelle
- Registrierung und Host-Einstellungen
- Warnungen und Überwachung
- Zugang und Verwaltung
- Konfigurieren des Windows-Backups
- Speicherbereitstellung
- Konfigurieren der Aufbewahrungsrichtlinien und Aktualisierungsoptionen

ANMERKUNG: Nach Abschluss der Appliance-Konfiguration können Sie entweder den Assistenten überspringen oder mit Machine protection (Maschinenschutz), Replication (Replikation), Virtual Machine Exports/Standby (VM-Exporte/Standby) fortfahren. Wenn Sie sich entschieden haben, den Assistenten zu überspringen, startet die Core-Konsole automatisch, und Sie können den Maschinenschutz, die Replikation und Exporte für virtuelle Maschinen in den späteren Phasen durchführen.

Weitere Informationen zur Durchführung des Maschinenschutzes, der Replikation und der Exporte für virtuelle Maschinen finden Sie im *Benutzerhandbuch zu Rapid Recovery auf DL Appliances* unter **www.dell.com/support/home**.

Konfiguration der Netzwerkschnittstelle

So konfigurieren Sie die vorhandenen Netzwerkschnittstellen:

1 Klicken Sie auf dem Bildschirm **DL Appliance Configuration Wizard Welcome (Willkommen zum DL Appliance-Konfigurationsassistenten)** auf **Next (Weiter)**.

Der Bildschirm **Lizenzvereinbarung** wird angezeigt.

2 Um die Vereinbarung anzunehmen, klicken Sie auf **I accept license agreement (Ich akzeptiere die Lizenzvereinbarung)**, und klicken Sie dann auf **Next (Weiter)**.

Die Seite **Network Settings (Netzwerkeinstellungen)** zeigt die verfügbaren verbundenen Netzwerkschnittstellen an.

3 Falls erforderlich, verbinden Sie die zusätzlichen Nezwerkschnittstellen und klicken Sie auf **Refresh (Aktualisieren)**.

Es werden die zusätzlich verbundenen Netzwerkschnittstellen angezeigt.

4 Wählen Sie die gewünschten Netzwerkschnittstellen aus, die für Ihre Umgebung geeignet sind.

Es stehen Ihnen folgende Optionen zur Verfügung: IPV4 und IPV6.

Es werden die Netzwerkeinzelheiten entsprechend Ihrer Auswahl des Internetprotokolls angezeigt.

5 Um IPV4 zu aktivieren, wählen Sie **Enable an IPv4 interface (IPv4-Schnittstelle aktivieren)** aus.

a Um die Daten des Internetprotokolls der IPv4-Schnittstelle zuzuweisen, wählen Sie eine der folgenden Optionen:

- Wählen Sie zum automatischen Zuweisen der Internetprotokolleinzelheiten **IPV4-Adresse automatisch beziehen**.
- Um die Netzverbindung manuell zuzuweisen, wählen Sie **Set manually IPV4 address (IPv4-Adresse manuell festlegen)** aus und geben Sie die folgenden Details ein:
  - **IPv4-Adresse**
  - **Subnetzmaske**
  - **Standard-Gateway**

6 Um IPV6 zu aktivieren, wählen Sie **Enable an IPv6 interface (IPv6-Schnittstelle aktivieren)** aus.

a Um die Daten des Internetprotokolls der IPv6-Schnittstelle zuzuweisen, wählen Sie eine der folgenden Optionen:

- Um die Daten des gewählten Internetprotokolls automatisch zuzuweisen, wählen Sie **Obtain an IPV6 address automatically (IPv6-Adresse automatisch beziehen)** aus.
- Um die Netzverbindung manuell zuzuweisen, wählen Sie **Set manually IPV6 address (IPv6-Adresse manuell festlegen)** aus und geben Sie die folgenden Details ein:
  - **IPv6-Adresse**
  - **Länge des Subnetz-Präfix**
  - **Standard-Gateway**

7 Zum Aktivieren von NIC-Teaming wählen Sie **Enable NIC teaming (NIC-Teaming aktivieren)** aus.

Weitere Informationen zum NIC-Teaming finden Sie unter Teaming Network Adapters (Teaming von Netzwerkadaptern) .

8 Klicken Sie auf **Next (Weiter)**.

Die Seite **Registrierung** wird angezeigt.

Registrierung und Host-Einstellungen

Registrieren Sie Ihr Gerät mit dem entsprechenden Lizenzschlüssel, um die Funktionen entsprechend zu nutzen. Es wird empfohlen, den Host-Namen zu ändern, bevor Sicherungen gestartet werden. Standardmäßig entspricht der Host-Name dem Systemnamen, der vom Betriebssystem zugewiesen wird.

ANMERKUNG: Wenn Sie den Host-Namen ändern möchten, wird empfohlen, dies zu diesem Zeitpunkt zu tun. Die Änderung des Host-Namens nach Abschluss des DL Appliance Configuration Wizard (DL Appliance-Konfigurationsassistenten) erfordert die Durchführung mehrerer Schritte.

1 Sie müssen auf der Seite **Registration (Registrierung)** eine der nachstehenden Optionen wählen:

- **Register now (Jetzt registrieren)** – zum Registrieren Ihres Geräts mit der erworbenen Lizenz. Geben Sie die folgenden Daten ein: Lizenznummer in das Textfeld `License number (Lizenznummer)` und die gültige E-Mail-Adresse in das Textfeld `Email address (E-Mail-Adresse)`.
- **Use trial license (Testlizenz verwenden)** – zum Registrieren Ihres Geräts mit der Testlizenz. Die Testlizenz läuft nach 30 Tagen ab. Um das Produkt weiterhin ohne Unterbrechung zu verwenden, registrieren Sie Ihr Gerät innerhalb dieses Zeitraums.

2 Klicken Sie auf **Next (Weiter)**.

Die Seite **Host Settings (Host-Einstellungen)** wird angezeigt.

3 Der Hostname Ihres Geräts wird standardmäßig im Feld `Host Name (Host-Name)` angezeigt. Um den Hostnamen Ihres Geräts zu ändern, geben Sie den `appropriate name (geeigneter Name)` im Textfeld **Host Name (Host-Name)** ein.

4 Wenn Sie Ihr Gerät mit einer Domäne verknüpfen möchten, markieren Sie das Kontrollkästchen **Join this system do a domain (dieses System mit einer Domäne verknüpfen)** und geben Sie die folgenden Informationen an:

Andernfalls fahren Sie mit Schritt 5 fort.

ANMERKUNG: Die Verknüpfung mit einer Domäne ist unter Windows Server 2012 R2 Foundation Edition nicht möglich. In diesem Fall ist das Kontrollkästchen Join this system do a domain (dieses System mit einer Domäne verknüpfen) deaktiviert.

Textfeld	Beschreibung
Domänen-Adresse	Adresse der Domäne, zu der Sie Ihr System hinzufügen möchten
Domänen-Administrator	Domänen-Administrator
Kennwort	Kennwort

5 Klicken Sie auf **Next (Weiter)**.

Die Seite **Alerts and Monitoring (Warnungen und Überwachung)** wird angezeigt.

Warnungen und Überwachung

Um Warnungen für Hardware- und Softwareänderungen zu aktivieren, stehen Ihnen zwei Optionen zur Verfügung – SNMP und SMTP. Das SNMP (Simple Network Management Protocol) ist ein häufig verwendetes Netzwerkverwaltungsprotokoll, das SNMP-kompatible Verwaltungsfunktionen ermöglicht, wie z.B. Geräteermittlung, Überwachung und Ereignisgenerierung. SNMP ermöglicht die Netzwerkverwaltung des TCP/IP-Protokolls. Sie können SNMP (Simple Network Management Protocol) oder SMTP (Simple Mail Transfer Protocol) verwenden, um Warn- und Überwachungsfunktionen für Ihr Gerät einzurichten.
Um Benachrichtigungen zu erhalten, konfigurieren Sie diese Optionen:

ANMERKUNG: Es wird empfohlen, Warnungen zu konfigurieren. Sie haben auch die Möglichkeit, die Konfiguration von Warnungen zu überspringen. Um die Konfiguration von Warnungen zu überspringen, fahren Sie mit Schritt 3 fort.

1 Es stehen Ihnen folgende Optionen für die Aktivierung von Warnungen zur Verfügung:

- Um SNMP-Systemwarnungen zu aktivieren, wählen Sie **Enable system SNMP alerts (SNMP-Systemwarnungen aktivieren)**.
  1 Geben Sie unter `SNMP Community` einen oder mehrere Namen für die SNMP-Community ein. Verwenden Sie Kommas, um mehrere Community-Namen zu trennen.
  2 Geben Sie unter `SNMP Trap destinations (SNMP-Trap-Ziele)` die Trap-Ziele ein und klicken Sie auf **Add (Hinzufügen)**.
- Um SNMP-Software-Warnungen zu aktivieren, wählen Sie die Option **Enable software SNMP alerts (SNMP-Software-Warnungen aktivieren)**.
  1 Geben Sie unter `SNMP Community` einen oder mehrere Namen für die SNMP-Community ein. Verwenden Sie Kommas, um mehrere Community-Namen zu trennen.
  2 Geben Sie unter `SNMP Trap destinations (SNMP-Trap-Ziele)` die Trap-Ziele ein und klicken Sie auf **Add (Hinzufügen)**.

2 Um Software-Warnungen über E-Mail einzurichten, wählen Sie die Option **Notify via email (per E-Mail benachrichtigen)** und geben Sie eine gültige E-Mail-Adresse ein.

3 Klicken Sie auf **Next (Weiter)**.

Die Seite `Access and Management (Zugang und Verwaltung)` wird angezeigt.

Zugang und Verwaltung

Um Zugang zu Ihrem Gerät zu erhalten und dieses zu verwalten, müssen Sie die Zugangs- und Verwaltungseinstellungen konfigurieren. So konfigurieren Sie die Zugangs- und Verwaltungseinstellungen Ihres Geräts:

1 Aktivieren oder deaktivieren Sie auf der Seite **Access and Management (Zugang und Verwaltung)** die folgenden Optionen für Zugang und Verwaltung Ihres Geräts durch nachfolgende Schritte:

- Aktivieren Sie den Remote-Desktop
- Aktivieren Sie die Windows-Firewall
- Aktivieren Sie die verstärkte Sicherheit für IE
- Aktivieren Sie die Windows-Updates
- Verwenden Sie einen Proxy-Server

2 Wenn Sie **Use Proxy Server (Proxy-Server verwenden)** auswählen, geben Sie die Proxy-Adresse in das Textfeld `Proxy address (Proxy-Adresse)` und die Portnummer in das Textfeld `Port` ein.

3 **ANMERKUNG: Wenn Sie die Zugangs- und Verwaltungseinstellungen auf die Standardoptionen einstellen möchten, klicken Sie auf die Schaltfläche Reset to Default (Auf Standardeinstellungen zurücksetzen).**

Klicken Sie auf **Next (Weiter)**.

Die Seite **Appliance Configuration Backup Options (Sicherungsoptionen der Appliance-Konfiguration)** wird angezeigt.

Konfigurieren des Windows-Backups

ANMERKUNG: Alle DL-Varianten, mit Ausnahme von DL 1000, unterstützen die Windows-Backup-Funktion.

Die **Appliance configuration backup options (Sicherungsoptionen der Appliance-Konfiguration)** ermöglichen das Festlegen der Häufigkeit, mit der Ihre Appliance-Konfiguration gesichert wird. Die Daten des Windows-Backups unterstützen die Wiederherstellung Ihrer Appliance-Konfigurationseinstellungen von einem beliebigen Zustand vor dem Ausfall.

1 Wählen Sie unter den **Appliance Configuration Backup Options (Sicherungsoptionen der Appliance-Konfiguration)** die Option **Perform Appliance configuration backup (Sicherung der Appliance-Konfiguration durchführen)**.

Es stehen Ihnen folgende Optionen zur Verfügung: Täglich, Wöchentlich und Monatlich.

2 Um die Häufigkeit des Windows-Backups einzustellen, wählen Sie eine der folgenden Optionen:

Option	Beschreibung
Täglich	Sichert täglich Ihre Konfigurationseinstellungen, mit Beginn um 12:01 Uhr
Weekly (Wöchentlich)	Sichert wöchentlich Ihre Konfigurationseinstellungen, mit Beginn jeden Sonntag um 12:01 Uhr
Monthly (Monatlich)	Sichert monatlich Ihre Konfigurationseinstellungen, mit Beginn jeden Sonntag um 12:01 Uhr

3 Klicken Sie auf **Next (Weiter)**.

Die Seite **Storage Provisioning (Speicherbereitstellung)** wird angezeigt.

Speicherbereitstellung

Ihr Gerät ermöglicht die Bereitstellung seines internen Speichers zur Erstellung der virtuellen Laufwerke (VDs) zum Hosten von Repositories und virtuellem Standby, Archiven oder zu anderen Zwecken.

1 Wählen Sie auf der Seite **Storage Provisioning (Speicherbereitstellung)** die folgenden Konfigurationsoptionen für Ihren Speicher aus.

Der `Repository-Name` wird standardmäßig als **Repository 1** angezeigt.

ANMERKUNG: Die Größe des Repositorys hängt von der Lizenz ab, die während der Registrierung Ihres Geräts angewendet wird.

- Wenn Sie während der Registrierung Ihres Geräts eine Testlizenz angewendet haben, gibt es keine Einschränkungen in der Repository-Größe.
- Wenn Sie während der Registrierung Ihres Geräts eine gekaufte Lizenz angewendet haben, entspricht die Größe des Repositorys dem Modell. Beispiel: Bei der DL 1000 1 TB Appliance wird ein Repository der Größe von 1 TB erstellt.

2 Wählen Sie **Allocate a portion of your storage for Virtual Standby, archives, or other purposes (Weisen Sie einen Anteil Ihres Speichers für virtuellen Standby, Archive oder andere Zwecke zu)** aus.

3 Ordnen Sie den Prozentsatz des Speicherplatzes, der nach dem Erstellen des Repositorys zur Verfügung steht, mithilfe des Schiebereglers zu. Sie können auch die genaue Größe über das Feld `Size (Größe)` angeben.

Es wird eine virtuelle Festplatte der angegebenen Kapazität zum Hosten von virtuellen Standby-VMs, Archiven oder zu anderen Zwecken erstellt.

4 Klicken Sie auf **Next (Weiter)**.

Das anfängliche Repository sowie die VDs zum Hosten von VMs oder zu anderen Zwecken werden erstellt.

Die Seite **Retention Policy (Aufbewahrungsrichtlinie)** wird angezeigt.

Konfigurieren der Aufbewahrungsrichtlinien und Aktualisierungsoptionen

Aufbewahrungsrichtlinien schreiben die Zeiträume vor, für die Sicherungen auf (schnellen und teuren) Kurzzeitmedien gespeichert werden. Mitunter machen geschäftliche und technische Anforderungen eine längere Aufbewahrung dieser Sicherungen erforderlich. Schnelle Speicher sind jedoch teuer. Aufbewahrungsrichtlinien können in Ihrem Gerät angepasst werden, um den Zeitraum festzulegen, für den ein Backup-Wiederherstellungspunkt aufbewahrt werden soll. Wenn das Alter der Wiederherstellungspunkte das Ende des Aufbewahrungszeitraums erreicht, werden sie als veraltet aus dem Aufbewahrungspool entfernt.

ANMERKUNG: Wenn die Lizenz der Aufbewahrungsrichtlinie standardmäßig eingeschränkt ist, kann die Aufbewahrungsrichtlinie nicht konfiguriert werden, um den Aufbewahrungszeitraum auf länger als drei Monate einzustellen. Wenn Sie dies versuchen, wird eine Fehlermeldung angezeigt.

1 Anhand der folgenden Optionen können Sie die Zeiträume festlegen, für welche die Backup-Snapshots von geschützten Maschinen gespeichert werden, und den Rollup-Prozess der Zusammenführung und Löschung alter Backups ändern. Die Seite **Retention Policy (Aufbewahrungsrichtlinie)** zeigt die folgenden Optionen an:

Tabelle 2. Zeitplanoptionen für die Standard-Aufbewahrungsrichtlinie

Textfeld	Beschreibung
Alle Wiederherstellungspunkte beibehalten für n [Aufbewahrungsdauer]	Gibt die Aufbewahrungsdauer für die Wiederherstellungspunkte an. Geben Sie eine Zahl für die Aufbewahrungsdauer ein und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist 3 Tage.

Textfeld	Beschreibung
	Sie können unter Folgendem auswählen: Tage, Wochen, Monate oder Jahre
...und anschließend einen Wiederherstellungspunkt pro Stunde beibehalten für n [Aufbewahrungsdauer]	Gibt eine genauere Aufbewahrungsstufe an. Diese Option wird zusammen mit der primären Einstellung als Baustein zur weiteren Definition dafür verwendet, wie lange Wiederherstellungspunkte beibehalten werden sollen. Geben Sie eine Zahl für die Aufbewahrungsdauer ein und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist 2 Tage. Sie können unter Folgendem auswählen: Tage, Wochen, Monate oder Jahre
...und anschließend einen Wiederherstellungspunkt pro Tag beibehalten für n [Aufbewahrungsdauer]	Gibt eine genauere Aufbewahrungsstufe an. Diese Option wird zusammen mit der primären Einstellung als Baustein zur weiteren Definition dafür verwendet, wie lange Wiederherstellungspunkte beibehalten werden sollen. Geben Sie eine Zahl für die Aufbewahrungsdauer ein und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist 4 Tage. Sie können unter Folgendem auswählen: Tage, Wochen, Monate oder Jahre
...und anschließend einen Wiederherstellungspunkt pro Woche beibehalten für n [Aufbewahrungsdauer]	Gibt eine genauere Aufbewahrungsstufe an. Diese Option wird zusammen mit der primären Einstellung als Baustein zur weiteren Definition dafür verwendet, wie lange Wiederherstellungspunkte beibehalten werden sollen. Geben Sie eine Zahl für die Aufbewahrungsdauer ein und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist 3 Wochen. Sie können unter Folgendem auswählen: Wochen, Monate oder Jahre
...und anschließend einen Wiederherstellungspunkt pro Monat beibehalten für n [Aufbewahrungsdauer]	Gibt eine genauere Aufbewahrungsstufe an. Diese Option wird zusammen mit der primären Einstellung als Baustein zur weiteren Definition dafür verwendet, wie lange Wiederherstellungspunkte beibehalten werden sollen. Geben Sie eine Zahl für die Aufbewahrungsdauer ein und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist 2 Monate. Sie können unter Folgendem auswählen: Monate oder Jahre
...und anschließend einen Wiederherstellungspunkt pro Jahr beibehalten für n [Aufbewahrungsdauer]	Geben Sie eine Zahl für die Aufbewahrungsdauer ein und wählen Sie dann die Zeitdauer aus. Sie können Folgendes auswählen: Jahre

2 Klicken Sie auf **Next (Weiter)**.

Die Seite **Update Options (Aktualisierungsoptionen)** wird angezeigt.

3 Um nach einer Gerätesoftware-Aktualisierung zu suchen, wählen Sie die Option **Check for appliance software update (Nach einer Gerätesoftware-Aktualisierung suchen)** aus.

Wenn eine Aktualisierung vorhanden ist, wird sie heruntergeladen und nach Beendigung des Assistenten installiert.

4 Um Rapid Recovery Core-Aktualisierungen zu aktivieren, wählen Sie **Enable Rapid Recovery Core updates (Rapid Recovery Core-Aktualisierungen aktivieren)** und dann eine der folgenden Optionen aus:

- Updates nicht automatisch installieren, sondern Benachrichtigung erhalten
- Updates automatisch installieren

5 Klicken Sie auf **Finish (Fertigstellen)**.

Die Geräteeinstellungen werden übernommen.

Appliance-Schnellselbstwiederherstellung

Bei der Appliance-Schnellselbstwiederherstellung (RASR) handelt es sich um einen Bare-Metal-Wiederherstellungsprozess, bei dem die Laufwerke des Betriebssystems auf das werkseitig voreingestellte Image neu erstellt werden.

Erstellen des RASR-USB-Sticks

So erstellen Sie einen RASR-USB-Speicherstick:

1 Navigieren Sie zur Registerkarte **Appliance (Gerät)**.

2 Wählen Sie im linken Navigationsbereich die Optionen **Appliance (Gerät)** > **Backup** aus.

Daraufhin wird das Fenster **Create RASR USB Drive (RASR-USB-Laufwerk erstellen)** angezeigt.

ANMERKUNG: Fügen Sie einen 16 GB oder grösseren USB-Stick ein, bevor Sie versuchen, einen RASR-Stick zu erstellen.

3 Klicken Sie nach dem Einsetzen eines USB-Sticks mit mindestens 16 GB auf **Create RASR USB Drive now (RASR-USB-Laufwerk jetzt erstellen)**.

Daraufhin wird die Meldung **Prerequisite Check (Überprüfung der Voraussetzung)** angezeigt.

Nachdem die Voraussetzungen überprüft wurden, zeigt das Fenster **Create the RASR USB Drive (RASR-USB-Laufwerk erstellen)** die erforderliche Mindestgröße für die Erstellung des USB-Laufwerks und die **List of Possible target paths (Liste aller möglichen Zielpfade)** an.

4 Wählen Sie das Ziel aus, und klicken Sie auf **Create (Erstellen)**.

Es wird ein Warndialogfeld angezeigt.

5 Klicken Sie auf **Yes (Ja)**.

Der RASR-USB-Laufwerks-Stick wurde erstellt.

6

ANMERKUNG: Verwenden Sie die Windows-Funktion zum Auswerfen des Laufwerks, um den USB-Stick auf das Entfernen vorzubereiten. Andernfalls könnte der Inhalt auf dem USB-Stick beschädigt werden und der USB-Stick nicht erwartungsgemäß funktionieren.

Entfernen Sie den für jede DL Appliance erstellten RASR-USB-Stick, kennzeichnen Sie ihn, und bewahren Sie ihn für die zukünftige Verwendung auf.

Ausführen von RASR

ANMERKUNG: Dell empfiehlt, dass Sie den RASR-USB-Stick erstellen, nachdem Sie das Gerät eingerichtet haben. Weitere Informationen zum Erstellen des RASR-USB-Sticks finden Sie im Abschnitt Erstellen des RASR-USB-Sticks.

ANMERKUNG: Stellen Sie sicher, dass Sie über das neueste RUU verfügen und dieses auf Ihrem Gerät zugänglich ist.

.

ANMERKUNG: Weitere Informationen zur Ausführung der Systemwiederherstellung mit RASR finden Sie im Dokument *Wiederherstellen einer Dell™ DL Backup and Recovery-Appliance mit Rapid Appliance Self Recovery (RASR)* unter Dell.com/support/home.

So setzen Sie das Gerät auf die Werkseinstellungen zurück:

1 Setzen Sie den erstellten RASR-USB-Stick ein.

2 Führen Sie einen Neustart des Geräts durch, und wählen Sie den **Startmanager (F11)** aus.

3 Wählen Sie im **Hauptmenü des Startmanagers** das **einmalige BIOS-Startmenü** aus.

4 Wählen Sie im **Startmenü des Startmanagers** das angeschlossene USB-Laufwerk aus.

5 Wählen Sie das Tastaturlayout aus.

6 Klicken Sie auf **Troubleshoot (Fehlerbehebung)** > **Rapid Appliance Self Recovery (Appliance-Schnellselbstwiederherstellung)**.

7 Wählen Sie das Ziel-Betriebssystem (BS) aus.

RASR wird gestartet, und der **Willkommens**bildschirm wird angezeigt.

8 Klicken Sie auf **Next (Weiter)**.

Der Bildschirm zum Überprüfen der **Prerequisites (Voraussetzungen)** wird angezeigt.

ANMERKUNG: Stellen Sie sicher, dass alle Hardware- und sonstigen Voraussetzungen überprüft werden, bevor Sie die RASR ausführen.

9 Klicken Sie auf **Next (Weiter)**.

Der Bildschirm **Recovery Mode Selection (Auswahl des Wiederherstellungsverfahrens)** wird mit den folgenden drei Optionen angezeigt:

- **System Recovery (Systemwiederherstellung)**
- **Windows Recovery Wizard (Assistent zur Windows-Wiederherstellung)**
- **Factory Reset (Auf Werkseinstellungen zurücksetzen)**

10 Wählen Sie die Option **Factory Reset (Auf Werkseinstellungen zurücksetzen)** aus.

Mit dieser Option setzen Sie den Betriebssystemdatenträger wieder auf die Werkseinstellungen zurück.

11 Klicken Sie auf **Next (Weiter)**.

Die folgende Warnmeldung wird in einem Dialogfeld angezeigt: `This operation will recover the operating system. All OS disk data will be overwritten.`

12 Klicken Sie auf **Yes (Ja)**.

Der Betriebssystemdatenträger beginnt mit der Wiederherstellung der Werkseinstellungen.

13 Die Seite **RASR Completed (RASR abgeschlossen)** wird nach Abschluss des Wiederherstellungsprozesses angezeigt. Klicken Sie auf **Finish (Fertigstellen)**.

14 Starten Sie das System nach dem Wiederherstellen.

15 **ANMERKUNG: Fahren Sie nur fort, wenn Sie den AppAssure Appliance Configuration Wizard (AppAssure Appliance-Konfigurationsassistent) sehen. Andernfalls wechseln Sie zu Schritt 17.**

Warten Sie, bis der AppAssure Appliance-Konfigurationsassistent geladen wird, um ihn schließen zu können. Schließen Sie den Assistenten über den Windows Task-Manager.

16 Führen Sie die Datei **launchRUU.exe** im RUU-Paket aus. Folgen Sie den Anweisungen, wählen Sie die Option zum Fortfahren der RUU-Installation und schließen Sie diese ab.

17 Der **DL Appliance Configuration Wizard (DL Appliance-Konfigurationsassistent)** wird gestartet und führt Sie durch den verbleibenden Wiederherstellungsprozess.

Ihr Gerät funktioniert jetzt normal.

Dienstprogramm zur Wiederherstellung und Aktualisierung

Das RUU (Recovery and Update Utility) ist ein All-in-One-Installationsprogramm zur Wiederherstellung und Aktualisierung der DL Appliances-Software (DL1000, DL1300, DL4000 und DL4300). Es enthält die Rapid Recovery Core-Software und gerätespezifische Komponenten.

RUU besteht aus aktualisierten Versionen der Windows Server-Rollen und -Funktionen, .Net 4.5.2, LSI-Provider, DL-Anwendungen, OpenManage Server Administrator und Rapid Recovery Core-Software. Darüber hinaus aktualisiert das Dienstprogramm den RASR-Inhalt (Geräte-Schnellselbstwiederherstellung).

ANMERKUNG: Wenn Sie derzeit eine der AppAssure Core-Versionen, die Rapid Recovery Core-Version 6.0.2.144 oder früher verwenden, erzwingt RUU eine Aktualisierung auf die neueste verfügbare Version in der Payload. Es ist nicht möglich, die Aktualisierung zu überspringen, und diese Aktualisierung ist nicht rücksetzbar. Wenn Sie kein Upgrade der Core-Software durchführen möchten, dann führen Sie das RUU nicht aus.

So installieren Sie die aktuellste Version des RUU:

1 Gehen Sie zum Lizenzportal unter dem Abschnitt „Downloads" oder gehen Sie zu **support.dell.com** und laden Sie das RUU-Installationsprogramm herunter.

2 Um den RUU-Prozess zu starten, führen Sie die Datei **launchRUU.exe** im RUU-Paket aus.

ANMERKUNG: Es ist möglich, dass das System während des RUU-Aktualisierungsvorgangs neu gestartet wird.

3

Konfigurieren Ihres Dell DL1000

Konfigurationsübersicht

Führen Sie nach Abschluss des DL Appliance- Konfigurationsassistenten die folgenden Verfahren durch, um sicherzustellen, dass Ihr Backup-Gerät und die durch das Gerät gesicherten Server korrekt konfiguriert wurden.

Die Konfiguration umfasst Aufgaben wie das Konfigurieren von Browsern für den Remote-Zugriff auf die DL1000 Core-Konsole, die Verwaltung von Lizenzen und das Einrichten von Warnungen und Benachrichtigungen. Sobald Sie die Konfiguration des Kerns abgeschlossen haben, können Sie Agenten schützen und Wiederherstellungen durchführen.

ANMERKUNG: Das Gerät ist mit einer 30-tägigen temporären Rapid Recovery-Softwarelizenz konfiguriert. Um einen permanenten Lizenzschlüssel anzufordern, melden Sie sich auf dem Dell Data Protection | Rapid Recovery Lizenzportal unter www.dell.com/DLActivation an. Weitere Informationen zum Ändern des Lizenzschüssels finden Sie unter dem Thema "Aktualisieren oder Ändern einer Lizenz" im *Benutzerhandbuch zu Rapid Recovery 6.0 auf DL Appliances* unter dell.com/support/home.

ANMERKUNG: Während der Verwendung der DL1000 Backup to Disk-Appliance wird empfohlen, den Kern über die Registerkarte Appliance (Gerät) zu konfigurieren.

Zurücksetzen des Betriebssystems auf die Standardeinstellungen

Zum Zurücksetzen des Betriebssystems auf die Standardeinstellungen führen Sie Folgendes durch:

1 Melden Sie sich als Administrator an und öffnen Sie ein Fenster zur Befehlseingabe.
2 Navigieren Sie zu **c:\windows\system32\sysprep** und führen Sie den Befehl **sysprep.exe/generalize/oobe/reboot** aus.
3 Wählen Sie folgendermaßen:
   - **Englisch** als Sprache
   - **Vereinigte Staaten** als Land/Region
   - **US** als Tastaturlayout

Konfigurieren von Browsern für den Remote-Zugriff auf die DL1300-Kern-Konsole

Bevor Sie erfolgreich von einem Remote-System auf die Kern-Konsole zugreifen können, müssen Sie Ihre Browser-Einstellungen ändern. Die folgenden Verfahren beschreiben, wie Internet Explorer-, Google Chrome- und Mozilla Firefox-Browser-Einstellungen geändert werden.

ANMERKUNG: Um Browser-Einstellungen zu ändern, müssen Sie mit Administrator-Zugriffsrechten an der Maschine angemeldet sein.

ANMERKUNG: Weil Chrome die Einstellungen von Internet Explorer verwendet, müssen Sie die Änderungen für Chrome unter Verwendung von Internet Explorer vornehmen.

ANMERKUNG: Stellen Sie sicher, dass Internet Explorer Enhanced Security aktiviert ist, wenn Sie lokal oder im Remote-Zugriff auf die Kern-Webkonsole zugreifen. Öffnen Sie zum Aktivieren von Internet Explorer Enhanced Security Server Manager > Lokaler Server > IE Enhanced Security Configuration (IE-verstärkte Sicherheitskonfiguration) und vergewissern Sie sich, dass die Option On (Aktiviert) ist.

Konfiguration der Browser-Einstellungen für Internet Explorer und Chrome:

Um die Browser-Einstellungen für Internet Explorer und Chrome zu ändern, führen Sie die folgenden Schritte aus:

1 Wählen Sie auf dem Bildschirm **Internet Options (Internetoptionen)** die Registerkarte **Security (Sicherheit)** aus.

2 Klicken Sie auf **Trusted Sites (Vertrauenswürdige Seiten)** und klicken Sie dann auf **Sites (Seiten)**.

3 Deaktivieren Sie die Option **Require server verification (https:) for all sites in the zone (Serverüberprüfung erforderlich (https:) für alle Websites in der Zone)** und fügen sie dann http://*<hostname or IP Address of the Appliance server hosting the Rapid Recovery Core> (Hostname oder IP-Adresse des Geräteservers, der den Rapid Recovery Core hostet)* auf **Trusted Sites (Vertrauenswürdige Sites)** hinzu.

4 Klicken sie auf **Close (Schließen)**, wählen Sie **Trusted Sites (Vertrauenswürdige Sites)** aus und klicken Sie dann auf **Custom Level (Benutzerdefinierte Stufe)**.

5 Scrollen Sie zu **Miscellaneous** → **Display Mixed Content** (Verschiedenes → Gemischten Inhalt anzeigen) und klicken Sie auf **Enable (Aktivieren)**.

6 Scrollen Sie auf dem Bildschirm nach unten zu **User Authentication** → **Logon** (Benutzerauthentifizierung → Anmelden) und wählen Sie dann **Automatic logon with current user name and password (Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort)**.

7 Klicken Sie auf **OK** und wählen Sie dann die Registerkarte **Advanced (Erweitert)**.

8 Scrollen Sie zu **Multimedia** und wählen Sie **Play animations in webpages (Auf Webseiten Animationen abspielen)** aus.

9 Scrollen Sie zu **Security (Sicherheit)**, markieren Sie **Enable Integrated Windows Authentication (Integrierte Windows-Authentifizierung)** und klicken Sie dann auf **OK**.

Konfigurieren der Browser-Einstellungen in Firefox

So ändern Sie Browser-Einstellungen in Firefox:

1 Geben Sie in die Firefox-Adresszeile **about:config** ein und klicken Sie dann, wenn aufgefordert, auf **I'll be careful, I promise** (Ich verspreche, ich werde vorsichtig sein).

2 Suchen Sie nach dem Begriff **ntlm**.

Die Suche sollte mindestens drei Ergebnisse aufzeigen.

3 Doppelklicken Sie auf **network.automatic-ntlm-auth.trusted-uris** und geben Sie die folgende Einstellung entsprechend Ihrer Maschine ein:

- Geben Sie für lokale Maschinen den Hostnamen ein.
- Geben Sie für Remote-Maschinen den Host-Namen oder die IP-Adresse des Gerätesystems, das den Kern hostet, durch Kommas getrennt ein; Beispiel: *IP-Adresse*, *Host-Name*.

4 Starten Sie Firefox neu.

Zugreifen auf die DL1000 Core Console

Stellen Sie sicher, dass Sie vertrauenswürdige Seiten, wie im Thema Aktualisieren von vertrauenswürdigen Seiten im Internet Explorer behandelt, aktualisieren und Ihre Browser wie im Thema Konfigurieren von Browsern für den Remote-Zugriff auf die DL1300-Kern-Konsole behandelt, konfigurieren. Nachdem Sie die vertrauenswürdigen Seiten in Internet Explorer aktualisiert und Ihre Browser konfiguriert haben, führen Sie einen der folgenden Schritte für den Zugriff auf die Core-Konsole aus:

- Melden Sie sich lokal bei Ihrem Kern-Server an, und doppelklicken Sie dann auf das Symbol für die **Kern-Konsole**.
- Geben Sie eine der folgenden URLs in den Webbrowser ein:
  - **https://<yourCoreServerName>:8006/apprecovery/admin/core oder**
  - **https://<yourCoreServerIPaddress>:8006/apprecovery/admin/core**

Aktualisieren von vertrauenswürdigen Seiten im Internet Explorer

So aktualisieren Sie vertrauenswürdige Seiten in Internet Explorer:

1 Öffnen Sie Internet Explorer.
2 Wenn die **File** (Datei) **Edit View** (Anzeige bearbeiten) und andere Menüs nicht angezeigt werden, drücken Sie auf <F10>.
3 Klicken Sie auf das Menü **Tools** (Extras) und wählen Sie **Internet Options** (Internetoptionen) aus.
4 Klicken Sie im Fenster **Internet Options** (Internetoptionen) auf die Registerkarte **Security** (Datenschutz).
5 Klicken Sie auf **Trusted Sites** (Vertrauenswürdige Seiten) und klicken Sie dann auf **Sites** (Seiten).
6 Geben Sie in **Add this website to the zone** (Diese Website zur Zone hinzufügen) unter Verwendung des Namens, den Sie als Anzeigenamen bereitgestellt haben, Folgendes ein: **https://[Display Name]** (https://[Anzeigenamen]).
7 Klicken Sie auf **Hinzufügen**.
8 Geben Sie in **Add this website to the zone**, (Diese Website zur Zone hinzufügen) Folgendes ein: **about:blank**.
9 Klicken Sie auf **Hinzufügen**.
10 Klicken Sie auf **Close** (Schließen) und dann auf **OK**.

Verschlüsseln der Agent Snapshot-Daten

Der Kern kann Agenten-Snapshot-Daten im Repository verschlüsseln. Anstelle einer Verschlüsselung des gesamten Repositorys ermöglicht Ihnen das DL1000 die Spezifizierung eines Verschlüsselungsschlüssels während des Schutzes eines Agenten in einem Repository, was eine erneute Verwendung des Schlüssels für unterschiedliche Agenten erlaubt.

Zum Verschlüsseln von Agenten-Snapshot-Daten:

1 Klicken Sie vom Kern auf **Configuration** (Konfiguration) → **Manage** (Verwalten) → **Security** (Sicherheit).
2 Klicken Sie auf **Actions** (Maßnahmen), und klicken Sie dann auf **Add Encryption Key** (Verschlüsselungsschlüssel hinzufügen).
Die Seite **Create Encryption Key** (Verschlüsselungsschlüssel erstellen) wird angezeigt.
3 Vervollständigen Sie die folgenden Informationen:

Feld	Beschreibung
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein.
Kommentar	Geben Sie eine Anmerkung für den Verschlüsselungsschlüssel ein. Sie wird zur Bereitstellung zusätzlicher Details für den Verschlüsselungsschlüssel genutzt.
Passphrase	Geben Sie eine Passphrase ein. Sie wird zur Steuerung des Zugriffs verwendet.
Passphrase bestätigen	Geben Sie die Passphrase erneut ein. Dies wird zur Bestätigung der Passphraseneingabe verwendet.

ANMERKUNG: **Es wird empfohlen, die Verschlüsselungspassphrase zu speichern, da der Verlust der Passphrase die Daten unzugänglich macht. Weitere Informationen finden Sie im Kapitel zum Verwalten der Sicherheit im DL1300-Benutzerhandbuch *Dell DL1000 Appliance User's Guide*.**

Konfigurieren eines E-Mail-Servers und einer E-Mail-Benachrichtigungsvorlage

Sollten Sie E-Mail-Benachrichtigungen über Ereignisse erhalten wollen, konfigurieren Sie einen E-Mail-Server und eine E-Mail-Benachrichtigungsvorlage.

ANMERKUNG: Sie müssen außerdem Einstellungen für Benachrichtigungsgruppen konfigurieren und die Option Notify by email (Per E-Mail benachrichtigen) aktivieren, damit E-Mail-Benachrichtigungen gesendet werden. Weitere Informationen zum Festlegen von Ereignissen, die eine E-Mail-Benachrichtigung auslösen, finden Sie unter „Configuring Notification Groups For System Events“ (Konfigurieren von Benachrichtigungsgruppen für Systemereignisse) im DL1300-Benutzerhandbuch *Dell DL1000 Appliance User's Guide* unter Dell.com/support/home.

So konfigurieren Sie einen E-Mail-Server und eine E-Mail-Benachrichtigungsvorlage:

1 Wählen Sie im Kern die Registerkarte **Configuration** (Konfiguration) aus.
2 Klicken Sie unter **Manage** (Verwalten) auf die Option **Events** (Ereignisse).
3 Klicken Sie im Fensterbereich **Email SMTP Settings** (E-Mail-SMTP-Einstellungen) auf **Change** (Ändern).
Das Dialogfeld **Edit Email Notification Configuration** (Konfiguration der E-Mail-Benachrichtigung bearbeiten) wird angezeigt.
4 Wählen Sie **Enable Email Notifications** (E-Mail-Benachrichtigungen aktivieren) aus und geben dann die E-Mail-Serverdetails, wie folgend beschrieben, ein:

Textfeld	Beschreibung
SMTP-Server	Geben Sie den Namen des E-Mail-Servers, der von der E-Mail-Benachrichtigungsvorlage verwendet werden soll, ein. Die Benennungskonvention umfasst Hostname, Domain und Suffix; z.B. **smtp.gmail.com.**
Schnittstelle	Geben Sie eine Schnittstellennummer ein. Sie wird zur Identifizierung der Schnittstelle für den E-Mail-Server verwendet. Zum Beispiel ist die Schnittstelle 587 für Gmail. Die Standardeinstellung ist 25.
Zeitüberschreitung (Sekunden)	Geben Sie einen Wert ein, um festzulegen, wie lange ein Verbindungsaufbau versucht wird, bevor eine Zeitüberschreitung eintritt. Diese Option wird zur Festlegung der Zeit in Sekunden verwendet, bevor beim Versuch, eine Verbindung mit dem E-Mail-Server herzustellen, eine Zeitüberschreitung eintritt. Die Standardeinstellung ist 30 Sekunden.
TLS	Verwenden Sie diese Option, wenn der E-Mail-Server eine sichere Verbindung, wie Transport Layer Security (TLS) oder Secure Sockets Layer (SSL) verwendet.
Benutzername	Geben Sie einen Benutzernamen für den E-Mail-Server ein.
Kennwort	Geben Sie ein Kennwort für den Zugriff auf den E-Mail-Server ein.
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**.
E-Mail-Betreff	Geben Sie einen Betreff für die E-Mail-Vorlage ein. Er wird zur Definition des Betreffs der E-Mail-Benachrichtigungsvorlage verwendet; z.B. `<hostname> - <level> <name>`.
E-Mail	Geben Sie Informationen für den Nachrichtentext der Vorlage ein, mit denen das Ereignis, der Ereigniszeitpunkt und der Schweregrad beschrieben werden.

5 Klicken Sie auf **Send Test Email** (Test-E-Mail senden), und prüfen Sie die Ergebnisse.
6 Wenn Sie mit den Ergebnissen des Tests zufrieden sind, klicken Sie auf **OK**.

Anpassen der Anzahl der Streams

Standardmäßig ist Rapid Recovery so konfiguriert, dass drei gleichzeitige Streams auf dem Gerät zulässig sind. Es wird empfohlen, die Anzahl der Streams auf 10 bis 15 einzustellen, um eine optimale Leistung zu erzielen.

So ändern Sie die Anzahl der gleichzeitigen Streams:

1 Wählen Sie die Registerkarte **Konfiguration** aus und klicken Sie dann auf **Einstellungen**.
2 Wählen Sie in **Übertragungen-Warteschlange** „Ändern“ aus.

3 Ändern Sie die Option **Maximum Concurrent Transfers (Maximale Anzahl der gleichzeitigen Übertragungen)** auf eine Zahl zwischen 10 und 15, um eine optimale Leistung zu erzielen. Sollte die Leistung unzureichend sein, versuchen Sie diese manuell abzustimmen.

4

Vorbereitung zum Schutz Ihrer Server

Übersicht

Um Ihre Daten mithilfe von DL 1000 zu schützen, müssen Sie die zu schützenden Workstations und Server (z. B. Ihren Exchange-Server, den SQL-Server, Linux-Server, usw.) in der Core-Konsole hinzufügen.

In der Core-Konsole können Sie die Maschine ermitteln, auf der ein Agent installiert ist, und angeben, welche Volumes geschützt werden sollen (z. B. ein Microsoft Windows-Speicherplatz). Sie können die Zeitpläne für den Schutz definieren, weitere Sicherheitsmaßnahmen wie Verschlüsselung hinzufügen und vieles mehr. Weitere Informationen über den Zugriff auf die Core-Konsole für den Schutz von Workstations und Servern finden Sie unter Schützen einer Maschine.

Themen:

Installieren von Agenten auf Clients

Auf allen durch das DL 1000-System gesicherten Clients muss der Rapid Recovery-Agent installiert sein. Über die Rapid Recovery Core-Konsole können Sie Agenten auf Maschinen bereitstellen. Das Bereitstellen von Agenten auf Maschinen erfordert die Vorkonfiguration der Einstellungen zur Auswahl eines Agententypen, der auf die Clients aufgespielt (Push) werden soll. Diese Methode funktioniert, wenn auf allen Clients das gleiche Betriebssystem ausgeführt wird. Sind jedoch unterschiedliche Versionen von Betriebssystemen vorhanden, ist es für Sie möglicherweise einfacher, die Agenten auf den Maschinen zu installieren.

Sie können die Agenten-Software auch während des Vorgangs zum Schützen einer Maschine für die Agenten-Maschine bereitstellen. Diese Option ist für Maschinen verfügbar, auf denen die Agenten-Software noch nicht installiert ist. Weitere Informationen zum Bereitstellen der Agenten-Software während des Schützens einer Maschine finden Sie im *Benutzerhandbuch zu Rapid Recovery auf DL Appliance* unter **Dell.com/support/home**.

Bereitstellen der Agenten-Software beim Schützen eines Agenten

Sie können Agenten während des Vorgangs des Hinzufügens eines Agenten herunterladen und bereitstellen.

ANMERKUNG: Dieser Vorgang ist nicht erforderlich, wenn Sie die Agenten-Software auf einer zu schützenden Maschine bereits installiert haben. Wenn die Agenten-Software vor dem Schützen einer Maschine nicht installiert wurde, können Sie keine spezifischen Volumes für den Schutz als Teil dieses Assistenten auswählen. In diesem Fall werden standardmäßig alle Volumes auf der Agenten-Maschine in den Schutz einbezogen. Rapid Recovery unterstützt den Schutz und die Wiederherstellung von Maschinen, die mit EISA-Partitionen konfiguriert wurden. Die Unterstützung gilt auch für Windows 8 und 8.1, sowie Windows 2012- und 2012 R2-Maschinen, die Windows RE (Windows Wiederherstellungsumgebung) verwenden.

1 Führen Sie einen der folgenden Vorgänge aus:

- Wenn Sie mit dem Assistenten zum Schützen der Maschine beginnen, fahren Sie mit Schritt 2 fort . .

- Wenn Sie mit der Rapid Recovery Core-Konsole beginnen, klicken Sie in der Schaltflächenleiste auf **Protect (Schützen)**.

Daraufhin wird der **Protect Machine Wizard (Assistent zum Schützen der Maschine)** angezeigt.

2 Wählen Sie auf der Seite **Welcome (Willkommen)** die entsprechenden Installationsoptionen aus:

- Wenn Sie kein Repository definieren oder eine Verschlüsselung aufbauen müssen, wählen Sie **Typical (Typisch)**.
- Wenn Sie ein Repository erstellen, ein anderes Repository für Sicherungen der ausgewählten Maschine angeben oder die Verschlüsselung mit dem Assistenten einrichten müssen, wählen Sie **Advanced (show optional steps) (Erweitert (optionale Schritte anzeigen))**.
- Wenn die Seite **Welcome (Willkommen)** für den Assistenten zum Schützen der Maschine künftig nicht angezeigt werden soll, wählen Sie die Option **Skip this Welcome page the next time the wizard opens (Seite „Willkommen“ beim nächsten Öffnen des Assistenten ignorieren)** aus.

3 Wenn Sie mit Ihrer Auswahl auf der Begrüßungsseite zufrieden sind, klicken Sie auf **Next (Weiter)**.

Die Seite **Connection (Verbindung)** wird angezeigt.

4 Geben Sie auf der Seite **Connection (Verbindung)** die Informationen zur Maschine ein, zu der Sie eine Verbindung herstellen möchten. Richten Sie sich dabei an die folgende Tabelle und klicken Sie anschließend auf **Next (Weiter)**.

Tabelle 3. Verbindungseinstellungen für Maschinen

Textfeld	Beschreibung
Host	Der Hostname oder die IP-Adresse der Maschine, die Sie schützen möchten.
Port	Die Portnummer, über die der Rapid Recovery-Kern mit dem Agenten auf der Maschine kommuniziert. Die Standardportnummer ist 8006.
Benutzername	Der Benutzername, der für die Verbindung mit dieser Maschine verwendet wird, z. B. Administrator (oder, falls sich der Computer in einer Domäne befindet: [Domänenname]\Administrator).
Kennwort	Das Kennwort, das für die Verbindung mit dieser Maschine verwendet wird.

Wenn die Seite **Install Agent (Agent installieren)** als Nächstes im Assistenten zum Schützen der Maschine angezeigt wird, bedeutet das, dass Rapid Recovery nicht den Rapid Recovery-Agenten auf der Maschine erkennt und die aktuelle Version der Software installieren wird.

5 **ANMERKUNG: Die Agenten-Software muss auf der zu schützenden Maschine installiert sein und diese Maschine muss neu gestartet werden, bevor sie im Kern gesichert werden kann. Damit das Installationsprogramm die geschützte Maschine neu startet, wählen Sie die Option After installation, restart the machine automatically (recommended) (Maschine nach der Installation automatisch neu starten (empfohlen)) aus, bevor Sie auf Next (Weiter) klicken.**

Klicken Sie auf **Next (Weiter)**.

Installieren der Rapid Recovery Agenten-Software auf Windows-Maschinen

Stellen Sie die Rapid Recovery Agenten-Installationsdatei für die Maschine bereit, die Sie schützen möchten, und verwenden Sie hierfür eine der Methoden, die im Thema „Installieren der Rapid Recovery Agenten-Software“ im *Dell Data Protection | Rapid Recovery 6.0 Installations- und Aktualisierungshandbuch* beschrieben wird. Starten Sie anschließend das Installationsprogramm, wie nachstehend beschrieben, um die Software auf jeder Windows-Maschine, die Sie im Rapid Recovery-Kern schützen möchten, zu installieren oder zu aktualisieren.

ANMERKUNG: Sie müssen das Installationsprogramm mit lokalen Administratorrechten ausführen.

1 Doppelklicken Sie auf der Maschine, die Sie schützen möchten, auf die ausführbare Rapid Recovery Agenten-Installationsdatei, um das Installationsprogramm zu starten.

Je nach Konfiguration Ihrer Maschine können die Fenster „Benutzerkontensteuerung“ oder „Sicherheitswarnung wegen geöffneter Datei“ angezeigt werden.

2 Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass Sie das Installationsprogramm ausführen und Änderungen am System vornehmen möchten.

3 Wenn .NET-Komponenten fehlen oder aktualisiert werden müssen, akzeptieren Sie die Eingabeaufforderung zum Herunterladen und Installieren des Frameworks.

4 Wählen Sie im Feld „Sprache“ die entsprechende Sprache aus und klicken Sie auf **OK**.

5 Wählen Sie eine der folgenden Optionen:

- Wenn die Rapid Recovery Agenten-Software zum ersten Mal auf dieser Maschine installiert wird, bereitet das Installationsprogramm die Installation vor. Anschließend wird der Rapid Recovery Agenten-Installationsassistent angezeigt. Fahren Sie mit Schritt 6 fort.
- Wenn auf dieser Maschine eine frühere Version der AppAssure- oder Rapid Recovery Agenten-Software installiert ist, sehen Sie eine Meldung mit der Frage, ob Sie ein Upgrade auf die aktuelle Version durchführen möchten.
  1 Klicken Sie auf **Yes (Ja)**.

    Der Rapid Recovery Agenten-Installationsassistent erscheint und zeigt die Seite **Progress (Fortschritt)** des Assistenten an. Die Anwendung wird in den Zielordner heruntergeladen, wobei der Fortschritt im Fortschrittsbalken angezeigt wird. Wenn der Download abgeschlossen ist, wechselt der Assistent automatisch auf die Seite **Completed (Abgeschlossen)**.

  2 Fahren Sie mit Schritt 12 fort.

6 Klicken Sie im Rapid Recovery Agenten-Installationsassistenten, auf der Seite **Welcome (Willkommen)** auf **Next (Weiter)**, um mit der Installation fortzufahren.

Die Seite **License Agreement (Lizenzvereinbarung)** wird angezeigt.

7 Klicken Sie auf der Seite **License Agreement (Lizenzvereinbarung)** auf **I accept the terms in the license agreement (Ich stimme den Bedingungen der Lizenzvereinbarung zu)** und klicken Sie anschließend auf **Next (Weiter)**.

Die Seite **Prerequisites (Erforderliche Komponenten)** wird angezeigt.

8 Das Rapid Recovery Agenten-Installationsprogramm überprüft, ob die erforderlichen Dateien vorhanden sind.

- Falls die erforderlichen Dateien vorhanden sind, wird eine Meldung angezeigt, dass alle erforderlichen Komponenten auf dieser Maschine installiert sind.
- Falls die erforderlichen Dateien nicht vorhanden sind, ermittelt das Rapid Recovery Agenten-Installationsprogramm die benötigten Dateien und zeigt die entsprechenden Ergebnisse an, z. B. CRT-2013 (x64) ENU (Verteilbarer Code für Microsoft Visual Studio®), oder Microsoft System CLR-Typen für SQL Server 2008 R2 (x64). Klicken Sie auf **Install Prerequisites (Erforderliche Komponenten installieren)**.

9 Wenn die Installation der erforderlichen Dateien abgeschlossen ist, klicken Sie auf **Next (Weiter)**.

Die Seite **Installation Options (Installationsoptionen)** wird angezeigt.

10 Überprüfen Sie auf der Seite **Installation Options** die Installationsoptionen. Falls erforderlich, ändern Sie sie wie unten beschrieben:

- Prüfen Sie im Textfeld **Destination Folder (Zielordner)** den Zielordner für die Installation. Wenn Sie den Speicherort ändern möchten, gehen Sie wie folgt vor:
  - Klicken Sie auf das Ordner-Symbol.
  - Wählen Sie im Dialogfeld **Browse to Destination (Ziel suchen)** einen neuen Speicherort aus.
  - Klicken Sie auf **OK**.
- Geben Sie im Textfeld **Port Number (Portnummer)** eine Portnummer ein, über die der Datenaustausch zwischen der Agenten-Software auf der geschützten Maschine und dem Rapid Recovery-Kern erfolgt.

  ANMERKUNG: Der Standardwert ist 8006. Wenn Sie die Portnummer ändern, notieren Sie sich diese für den Fall, dass Sie die Konfigurationseinstellungen später ändern müssen.
- Wählen Sie **Allow Agent to automatically send diagnostic and usage information to Dell Inc. (Automatisches Senden von Diagnose- und Nutzerinformationen durch Agenten an Dell Inc. erlauben)**. Wenn Sie die Informationen nicht senden möchten, löschen Sie diese Option.

11 Wenn Sie mit den Installationsoptionen zufrieden sind, klicken Sie auf **Install (Installieren)**.

Die Seite **Progress (Fortschritt)** wird angezeigt und enthält eine Statusleiste, über die Sie den Installationsfortschritt verfolgen können.

Nach Abschluss der Installation wird die Seite **Completed (Abgeschlossen)** angezeigt. Fahren Sie mit Schritt 12 fort.

12 Wenn Sie auf der Seite **Completed (Abgeschlossen)** eine Meldung sehen, dass das System neu gestartet werden muss, bevor die Installation wirksam wird, führen Sie einen der folgenden Schritte aus:

- Um jetzt neu zu starten, wählen Sie **Yes, I want to restart my computer now (Ja, Computer jetzt neu starten)**.
- Um später neu zu starten, löschen Sie die Option **Yes, I want to restart my computer now (Ja, Computer jetzt neu starten)**.

13 Klicken Sie auf der Seite **Completed (Abgeschlossen)** auf **Finish (Fertigstellen)**.
Der Installationsassistent wird geschlossen, und die Installation des Agenten ist beendet.

Bereitstellen der Rapid Recovery Agenten-Software auf einer oder mehreren Maschinen

Sie können die Aufgabe der Bereitstellung der Rapid Recovery Agenten-Software auf einer oder mehreren Windows-Maschinen durch Verwendung des Deploy Agent Software Wizard (Assistent zur Bereitstellung der Agenten-Software) vereinfachen.

ANMERKUNG: Früher wurde diese Funktion auch „Bulk Deploy“ (Massenbereitstellung) genannt.

Bei Verwendung des Assistenten zur Bereitstellung der Agenten-Software kann Rapid Recovery automatisch Maschinen auf einem Host erkennen und Ihnen die Auswahl der Maschine ermöglichen, auf der Sie die Software bereitstellen möchten. Für Maschinen auf anderen Domänen oder Hosts als Active Directory oder vCenter oder ESX(i) können Sie manuell eine Verbindung zu einzelnen Maschinen herstellen, indem Sie deren IP-Adressen und die entsprechenden Anmeldeinformationen eingeben. Sie können auch Push-Installationen von Upgrades der Software auf Maschinen durchführen, die bereits vom lokalen Rapid Recovery-Kern geschützt werden.

Von der Core-Konsole aus können Sie die folgenden Aufgaben durchführen:

- Bereitstellen für Maschinen auf einer Active Directory-Domäne
- Bereitstellen für Maschinen auf einem virtuellen Host des VMware vCenter/ESX(i)

ANMERKUNG: Dell empfiehlt, dass Sie die Anzahl der Maschinen für eine gleichzeitige Bereitstellung auf 50 oder weniger beschränken. So können Ressourcenengpässe vermieden werden, die zu fehlerhaften Bereitstellungsvorgängen führen können.

Installieren von Microsoft Windows-Agenten auf dem Client

So installieren Sie die Agenten:

1 Überprüfen Sie, dass auf dem Client das Microsoft .NET 4-Framework installiert ist:
   a Starten Sie auf dem Client den **Windows Server-Manager**.
   b Klicken Sie auf **Konfiguration** > **Dienste.**
   c Stellen Sie sicher, dass in der Liste mit den Diensten das Microsoft .NET Framework angezeigt wird.
   Wenn es nicht installiert ist, können Sie eine Kopie von **microsoft.com** beziehen.

2 Installieren des Agenten:
   a Geben Sie auf Ihrem Gerät das Verzeichnis **C:\Program Files\AppRecovery** an die Clients weiter, die Sie sichern wollen.
   b Ordnen Sie auf dem Client-System ein Laufwerk zu **C:\Program Files\AppRecovery** auf Ihrer DL Appliance zu.
   c Öffnen Sie das Verzeichnis **C:\Program Files\AppRecovery** auf dem Client-System und doppelklicken Sie auf den für das System geeigneten Agenten, um mit der Installation zu beginnen.

Bereitstellen für Maschinen auf einer Active Directory-Domäne

Verwenden Sie dieses Verfahren, um die Rapid Recovery Agenten-Software gleichzeitig auf einer oder mehreren Maschinen auf einer Active Directory-Domäne bereitzustellen.
Bevor Sie diesen Vorgang starten, müssen Sie über die Domänen-Informationen und die Anmeldeinformationen für den Active Directory-Server verfügen.

1 Klicken Sie auf der Rapid Recovery Core-Konsole auf das Drop-Down-Menü **Protect (Schützen)** und klicken Sie dann auf **Deploy Agent Software (Agenten-Software bereitstellen)**.

Der Deploy Agent Software Wizard (Assistent zur Bereitstellung der Agenten-Software) wird geöffnet.

2 Wählen Sie auf der Seite **Connection (Verbindung)** des Assistenten, aus der Drop-Down-Liste **Source (Quelle)** die Option **Active Directory** aus.

3 Geben Sie die Domänen-Informationen und die Anmeldeinformationen ein, wie in der folgenden Tabelle beschrieben:

Tabelle 4. Domänen-Informationen und Anmeldeinformationen

Textfeld	Beschreibung
Host	Hostname oder IP-Adresse der Active Directory-Domäne.
Benutzername	Der Benutzername, der für die Verbindung mit dieser Domäne verwendet wird, z. B. Administrator, oder, falls sich der Computer in einer Domäne befindet: [Domänenname]\Administrator).
Kennwort	Das sichere Kennwort, das für die Verbindung mit dieser Domäne verwendet wird.

4 Klicken Sie auf **Next (Weiter)**.

5 Wählen Sie auf der Seite **Machines (Maschinen)** die Maschinen aus, für die Sie die Rapid Recovery Agenten-Software bereitstellen möchten.

6 Um die geschützten Maschinen nach der Installation des Agenten automatisch neuzustarten, können Sie wahlweise **After Agent installation, restart the machines automatically (Recommended) (die Maschinen nach Installation des Agenten automatisch neustarten (empfohlen))** auswählen.

7 Klicken Sie auf **Finish (Fertigstellen)**.

Das System überprüft automatisch jede Maschine, die Sie ausgewählt haben.

Wenn Rapid Recovery etwaige Probleme bei der automatischen Überprüfung entdeckt, führt Sie der Assistent zu einer Warnseite, auf der Sie Maschinen aus der Auswahl löschen und die gewählten Maschinen manuell überprüfen können. Wenn die hinzugefügten Maschinen die automatische Überprüfung bestehen, erscheinen sie im Fensterbereich „Deploy Agent to Machines“ (Agenten für Maschinen bereitstellen).

8 Wenn die Warnseite angezeigt wird und Sie dennoch zufrieden mit Ihrer Auswahl sind, klicken Sie erneut auf **Finish (Fertigstellen)**.

Die Rapid Recovery Agenten-Software wird auf den angegebenen Maschinen bereitgestellt. Die Maschinen sind noch nicht geschützt. Informationen zum Schutz der Maschinen finden Sie im Thema „Mehrere Maschinen auf der Active Directory-Domäne schützen“ im *Benutzerhandbuch zu Rapid Recovery 6.0 auf DL Appliances*.

Bereitstellen für Maschinen auf einem virtuellen Host des VMware vCenter/ESX(i)

Verwenden Sie dieses Verfahren, um die Rapid Recovery Agenten-Software gleichzeitig für eine oder mehrere Maschinen auf einem virtuellen Host des VMware vCenter/ESX(i) bereitzustellen.
Bevor Sie diesen Vorgang starten, müssen Sie die folgenden Informationen bereit haben:

- Anmeldeinformationen für den virtuellen Host des VMware vCenter/ESX(i).
- Host-Standort.
- Anmeldeinformationen für jede Maschine, die Sie schützen möchten.

ANMERKUNG: Alle virtuellen Maschinen müssen VMware-Tools installiert haben, oder Rapid Recovery kann den Hostnamen der virtuellen Maschine nicht erkennen, auf der bereitgestellt werden soll. Anstelle des Hostnamens verwendet Rapid Recovery den Namen der virtuellen Maschine, der zu Problemen führen kann, wenn der Hostname anders ist als der Name der virtuellen Maschine.

1 Klicken Sie auf der Rapid Recovery Core-Konsole auf das Drop-Down-Menü **Protect (Schützen)** und klicken Sie dann auf **Deploy Agent Software (Agenten-Software bereitstellen)**.

Der **Deploy Agent Software Wizard (Assistent zur Bereitstellung der Agenten-Software)** wird geöffnet.

2 Auf der Seite **Connection (Verbindung)** des Assistenten, von der Drop-Down-Liste **Source (Quelle)** wählen Sie **vCenter / ESX(i)** aus.

3 Geben Sie die Host-Informationen und die Anmeldeinformationen ein, wie in der folgenden Tabelle beschrieben:

Tabelle 5. Einstellungen der vCenter/ESX(i)-Verbindung

Textfeld	Beschreibung
Host	Der Name oder die IP-Adresse des virtuellen Hosts des VMware vCenter Server/ESX(i).
Port	Der Port, der für die Verbindung mit dem virtuellen Host verwendet wird. Die Standardeinstellung ist 443.
Benutzername	Der Benutzername, der für die Verbindung mit dem virtuellen Host verwendet wird, z. B. Administrator, oder, falls sich der Computer in einer Domäne befindet: [Domänenname]\Administrator).
Kennwort	Das sichere Kennwort, das für die Verbindung mit diesem virtuellen Host verwendet wird.

4 Klicken Sie auf **Next** (Weiter).

5 Wählen Sie auf der Seite **Maschinen** des Assistenten eine der folgenden Optionen aus dem Drop-Down-Menü aus:
- Hosts und Cluster
- Virtuelle Maschinen und Vorlagen

6 Erweitern Sie die Liste der Machinen und wählen Sie dann die virtuellen Maschinen aus, auf denen Sie die Software bereitstellen möchten.

Es wird eine Benachrichtigung angezeigt, wenn Rapid Recovery erkennt, dass eine Maschine offline ist oder VMware-Tools nicht installiert sind.

7 Wenn Sie die Maschinen nach der Bereitstellung automatisch neu starten möchten, wählen Sie **After Agent installation, restart the machines automatically (Recommended) (Maschinen nach der Installation des Agenten automatisch neu starten (empfohlen))**.

8 Klicken Sie auf **Next (Weiter)**.

Rapid Recovery prüft automatisch jede Maschine, die Sie ausgewählt haben.

9 Geben Sie auf der Seite **Adjustments (Anpassungen)** des Assistenten die Anmeldeinformationen für jede Maschine im folgenden Format ein: `hostname::username::password`.

ANMERKUNG: Geben Sie eine Maschine in jede Zeile ein.

10 Klicken Sie auf **Finish (Fertigstellen)**.

Das System überprüft automatisch jede Maschine, die Sie ausgewählt haben.

Wenn Rapid Recovery etwaige Probleme bei der automatischen Überprüfung entdeckt, führt Sie der Assistent zu einer Warnseite, auf der Sie Maschinen aus der Auswahl löschen und die gewählten Maschinen manuell überprüfen können. Wenn die hinzugefügten Maschinen die automatische Überprüfung bestehen, erscheinen sie im Fensterbereich „Deploy Agent to Machines“ (Agenten für Maschinen bereitstellen).

11 Wenn die Warnseite angezeigt wird und Sie dennoch zufrieden mit Ihrer Auswahl sind, klicken Sie erneut auf **Finish (Fertigstellen)**.

Die Rapid Recovery Agenten-Software wird auf den angegebenen Maschinen bereitgestellt.

Installieren der Agenten-Software auf Linux-Maschinen

Beim Installieren der Agenten-Software auf Linux-Maschinen, die Sie schützen möchten, verwenden Sie die folgenden Anleitungen. Nach Abschluss der Installation konfigurieren Sie den Agenten, wie unter dem Thema „Konfigurieren des Rapid Recovery Agent auf einer Linux-Maschine“ im *Dell Data Protection | Rapid Recovery 6.0 Installations- und Aktualisierungshandbuch* beschrieben.

VORSICHT: Nach der Konfiguration der neu installierten Agenten-Software auf einer Linux-Maschine starten Sie den Computer neu. Durch den Neustart wird sichergestellt, dass die richtige Kernel-Treiberversion zum Schützen der Maschine verwendet wird.

Das Verfahren zum Installieren und Entfernen der Agenten-Software auf Linux-Maschinen hat sich geändert. Ab Version 6.0.1 gelten die folgenden Faktoren:

- Ein Satz mit Anweisungen gilt für Installationen des Agenten auf einer Linux-Maschine mit aktuellem Zugang zum Internet. Dies bezeichnet man als Online-Installation. Statt Verwendung von Shell-Skripten werden Paket-Manager verwendet, um die Rapid Recovery-Software von einem Repository, auf das auf der lokalen Linux-Maschine verwiesen wird, zu installieren oder zu entfernen.

ANMERKUNG: Das Repository wird für das Staging der Dateien für den entsprechenden Paket-Manager verwendet. Dieses Repository bezieht sich nicht auf das Rapid Recovery-Repository.

- Wenn der Agent auf einer Linux-Maschine ohne Zugriff auf das Internet (wie z. B. eine air-gapped oder gesicherte eigenständige Maschine) installiert wird, bezeichnet man dies als Offline-Installation. Für dieses Verfahren müssen Sie zuerst ein Installationspaket von einer Linux-Maschine mit Internetzugang herunterladen und anschließend diese Installationsdateien auf den geschützten Computer für die Installation bewegen.

Da die verschiedenen unterstützten Linux-Verteilungen andere Paket-Manager für die Online-Installation verwenden, hängt das Verfahren zur Installation, Erweiterung oder Entfernung des Agenten auf/von einem der unterstützten Linux-Betriebssysteme vom verwendeten Paket-Manager ab. Die Paket-Manager und die Linux-Verteilungen, die sie unterstützen, werden in der folgenden Tabelle beschrieben.

Tabelle 6. Paket-Manager und die Linux-Verteilungen, die sie unterstützen

Paket-Manager	Linux-Verteilung
yum	Linux-Verteilungen basierend auf Red Hat Enterprise Linux (RHEL), einschließlich RHEL, CentOS und Oracle Linux.
zypper	SUSE Linux Enterprise Server (SLES), Versionen 11, 12.
apt	Linux-Verteilungen basierend auf Debian, einschließlich Debian 7 bzw. 8 und Ubuntu 12.04 und höher.

Als einmaliger Setup-Schritt müssen Sie für jede Linux-Maschine Ihr lokales Software-Repository so konfigurieren, dass es auf den Speicherort zeigt, an dem der Paket-Manager Dell Rapid Recovery-Installationsdateien abruft.

ANMERKUNG: Dieser Prozess wird durch die Schritte 1 bis 4 in jedem der Installationsverfahren dargestellt. Bei der Aktualisierung künftiger Ausgaben des Rapid Recovery Agenten auf einer Linux-Maschine mit konfiguriertem Repository müssen Sie keinen dieser Schritte ausführen.

Nach der Konfiguration eines Software-Repositorys auf Ihrer Linux-Maschine ist der Paket-Manager in der Lage, die Pakete, die zur Installation oder Deinstallation der Rapid Recovery Agenten-Software und zugehöriger Komponenten, wie z. B. aamount (jetzt 'Lokale Bereitstellung' genannt), aavdisk (jetzt 'rapidrecovery-vdisk' genannt), und Mono (ein Open Source, Ecma-Standard-kompatibler, .NET Framework-kompatibler Werkzeugsatz, der für die Portierung der Agenten-Software auf Linux-Plattformen verwendet wird) erforderlich sind, abzurufen und zu installieren.

Für jeden Paket-Manager können Sie den entsprechenden Befehl an der Befehlszeile ausführen, um festzustellen, ob er jetzt so konfiguriert ist, dass Rapid Recovery-Pakete heruntergeladen werden können. Diese Befehle sind in der folgenden Tabelle aufgelistet.

Tabelle 7. Befehl zur Anzeige der Paket-Manager Repository-Konfiguration

Paket-Manager	Befehl zum Auflisten konfigurierter Repositories
yum	yum replolist
zypper	zypper repos
apt	ls /etc/apt/sources.list.d

Vorherige Versionen der AppAssure Agenten-Software müssen vollständig vor der Installation der Rapid Recovery Agenten-Version und zum Schutz der Linux-Maschine unter Verwendung des Rapid Recovery-Kerns von einer Linux-Maschine entfernt werden. Dies gilt für Online- oder Offline-Installationen. Für das Entfernen von AppAssure Agent werden Shell-Skripte genutzt. Abhängig von der verwendeten Linux-Verteilung variieren die Deinstallationsschritte. Weitere Informationen zur Deinstallation von AppAssure Agent von einer Linux-Maschine finden Sie unter "Deinstallieren der AppAssure Agenten-Software von einer Linux-Maschine" im *Dell Data Protection | Rapid Recovery 6.0 Installations- und Aktualisierungshandbuch*.

ANMERKUNG: Für das Entfernen der neuen Rapid Recovery Agenten-Software wird der Paket-Manager für jede Verteilung verwendet. Daher sehen Sie beim Deinstallieren einer Version von Rapid Recovery Agent im entsprechenden Verfahren unter dem Thema "Deinstalieren der Rapid Recovery Agenten-Software von einer Linux-Maschine" im *Dell Data Protection | Rapid Recovery 6.0 Installations- und Aktualisierungshandbuch* nach.

Wenn der Rapid Recovery Agent auf einer Linux-Maschine installiert wird, auf der nie AppAssure Agent installiert war, bestimmen Sie den geeigneten Paket-Manager von der vorhergehenden Tabelle. Folgen Sie dann dem entsprechenden Installationsverfahren.

Nach der Konfiguration der neu installierten Agenten-Software auf einer Linux-Maschine müssen Sie den Computer neu starten. Durch den Neustart wird sichergestellt, dass die richtige Kernel-Treiberversion zum Schützen der Maschine verwendet wird.

Deshalb umfasst der Installationsvorgang bei der Aktualisierung von AppAssure auf Rapid Recovery die folgenden Schritte:

- Entfernen der AppAssure Agenten-Software (nicht erforderlich bei Erstinstallation)
- Bestimmen des relevanten Paket-Managers für Ihre Linux-Verteilung
- Befolgen Sie das Verfahren für die Installation von Rapid Recovery Agent auf der Linux-Maschine, einschließlich Konfiguration des Software-Repositorys (Schritte 1 bis 4 des Installationsverfahrens)
- Führen Sie das Konfigurationsdienstprogramm aus, konfigurieren Sie Benutzer, führen Sie Firewall-Ausschlüsse hinzu, installieren Sie das Kernel-Modul und starten Sie den Agenten-Dienst
- Starten Sie die Linux-Maschine neu

Die Anweisungen für die Installation der Agenten-Software auf einer Linux-Maschine hängen jeweils von der verwendeten Linux-Verteilung ab. Weitere Informationen zur Vorbereitung auf und zum Installieren der Agenten-Software für eine Linux-Maschine, die mit dem Internet verbunden ist, finden Sie im entsprechenden Thema. Sie können zwischen folgenden Abschnitten wählen:

- Installieren der Rapid Recovery Agenten-Software auf Debian oder Ubuntu
- Installieren der Rapid Recovery Agenten-Software auf SUSE Linux Enterprise Server

Weitere Informationen zur Vorbereitung auf und zum Installieren der Agenten-Software für eine Linux-Maschine, die nicht mit dem Internet verbunden ist, finden Sie im Thema:

- Installieren der Agenten-Software auf Offline-Linux-Maschinen

Siehe die folgenden wichtigen Informationen vor Beginn der Installation der Agenten-Software: Herunterladen der Linux-Verteilung, Informationen zur Sicherheit, Speicherort von Linux Agenten-Dateien, Agenten-Abhängigkeiten, Linux Skript-Informationen, im *Dell Data Protection | Rapid Recovery 6.0 Installations- und Aktualisierungshandbuch*.

Speicherort von Linux Agent-Dateien

Es gibt verschiedene Dateien, die zur Unterstützung der Rapid Recovery Agent-Software auf einer Linux-Maschine benötigt werden. Für alle unterstützten Linux-Distributionen befinden sich diese Dateien in den folgenden Verzeichnissen:

- mono:
  `/opt/apprecovery/mono`
- agent:
  `/opt/apprecovery/agent`
- Lokale Bereitstellung:
  `/opt/apprecovery/local_mount`
- rapidrecovery-vdisk und aavdctl:
  `/usr/bin/aavdisk`
- Konfigurationsdateien für rapidrecovery-vdisk:
  `/etc/apprecovery/aavdisk.conf`
- Wrapper für Agent und local_mount
  `/usr/bin/agent`

  `/usr/bin/local_mount`
- Autorun-Skripts für Agent und rapidrecovery-vdisk:
  `/etc/init.d/rapidrecovery-agent`

  `/etc/init.d/rapidrecovery-vdisk`

Agenten-Abhängigkeiten

Die folgenden Abhängigkeiten sind erforderlich und werden mit dem Agenten-Installationsprogramm-Paket installiert:

- Für Debian und Ubuntu:
  - Der rapidrecovery-agent benötigt:

    ```
    dkms, gcc, make, linux-headers-‘uname-r‘
                    libc6 (>=2.7-18), libblkid1, libpam0g, libpcre3
    ```

  - Der rapidrecovery-mono benötigt:

    ```
    libc6 (>=2.7-18)
    ```

- Für Red Hat Enterprise Linux, CentOS und Oracle Linux:
  - Das nbd-dkms benötigt

    ```
    dkms, gcc, make, kernel-headers-‘uname-r‘ kernel-devel-‘uname-r‘
    ```

  - Der rapidrecovery-agent benötigt:

    ```
    dkms, gcc, make, kernel-headers-‘uname-r‘ kernel-devel-‘uname-r‘,
                    nbd-dkms, libblkid, pam, pcre
    ```

  - Der rapidrecovery-mono benötigt:

    ```
    glibc >=2.11
    ```

- Für SUSE Linux Enterprise Server:
  - Das nbd-dkms benötigt:

    ```
    dkms, gcc, make, kernel-syms
    ```

  - Der rapidrecovery-agent benötigt:

    ```
    dkms, kernel-syms, gcc, make, libblkid1, pam, pcre
    ```

  - Der rapidrecovery-mono benötigt:

    ```
    glibc >= 2.11
    ```

Installieren der Rapid Recovery Agenten-Software auf Debian oder Ubuntu

Die .deb-Datei des Rapid Recovery-Agenten ist ein Archiv mit Repository-Informationen, die speziell für den apt-Paketmanager vorgesehen sind. Führen Sie die folgenden Schritte aus, um eine Online-Installation des Rapid Recovery-Agenten auf Debian- oder Ubuntu-Maschinen vorzunehmen.

ANMERKUNG: Dieses Verfahren gilt für eine Linux-Maschine, die mit dem Internet verbunden ist. Informationen zur Offline-Installation des Rapid Recovery-Agenten auf einer beliebigen Linux-Maschine finden Sie unter Installieren der Agenten-Software auf Offline-Linux-Maschinen.

1 Öffnen Sie eine Terminalsitzung mit Root-Zugriff.

2 Bestimmen Sie Ihr aktuelles Arbeitsverzeichnis durch Eingabe von PWD und drücken Sie die **Eingabetaste**. Ihr Verzeichnis könnte zum Beispiel **/home/rapidrecovery/** lauten.

3 Laden Sie die entsprechende .deb-Installationsdatei des Rapid Recovery-Agenten vom Lizenzportal unter https://licenseportal.com in Ihr aktuelles Arbeitsverzeichnis herunter.

Weitere Informationen über das Lizenzportal finden Sie im *Dell Datensicherung | Rapid Recovery License Portal Benutzerhandbuch*.

4 Um eine dauerhafte Verbindung zwischen Ihrer Linux-Maschine und der Dell Remote-Repository einzurichten, auf der die Rapid Recovery-Software und -Komponenten gespeichert sind, geben Sie den folgenden Befehl ein:

```
dpkg -i <.deb installation file you downloaded>
```

Beispiel: Wenn der Name der Installationsdatei „rapidrecovery-repo-6.0.2.999.deb“ im Verzeichnis **/home/rapidrecovery/** lautet, geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
dpkg -i rapidrecovery-repo-6.0.2.999.deb
```

Etwaige fehlende Pakete oder vom Agenten benötigte Dateien werden vom Remote-Repository heruntergeladen und automatisch als Teil des Skripts installiert.

ANMERKUNG: Weitere Informationen zu Abhängigkeiten für die Installation auf einer Linux-Maschine finden Sie unter Agenten-Abhängigkeiten.

5 Installieren Sie den Rapid Recovery-Agenten durch Aufrufen des apt-Paketmanagers, der den Repository Manager aktualisiert. Geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
apt-get update
```

6 Weisen Sie den Paketmanager an, die Rapid Recovery Agenten-Software zu installieren. Geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
apt-get install rapidrecovery-agent
```

7 Der Paketmanager bereitet die Installation aller abhängigen Dateien vor. Wenn Sie zur Bestätigung der Installation nicht signierter Dateien aufgefordert werden, geben Sie **y** (Ja) ein und drücken Sie die **Eingabetaste**.

Die Rapid Recovery Agenten-Dateien werden installiert.

Installieren der Rapid Recovery Agenten-Software auf SUSE Linux Enterprise Server

Die .rpm-Datei des Rapid Recovery-Agenten ist ein Archiv mit Repository-Informationen für SUSE Linux Enterprise Server (SLES). Diese Distribution verwendet den Zypper Paketmanager. Führen Sie die folgenden Schritte aus, um den Rapid Recovery-Agenten auf SLES zu installieren.

ANMERKUNG: Dieses Verfahren gilt für eine Linux-Maschine, die mit dem Internet verbunden ist. Informationen zur Offline-Installation des Rapid Recovery-Agenten auf einer beliebigen Linux-Maschine finden Sie unter Installieren der Agenten-Software auf Offline-Linux-Maschinen.

1 Öffnen Sie eine Terminalsitzung mit Root-Zugriff.

2 Bestimmen Sie Ihr aktuelles Arbeitsverzeichnis durch Eingabe von PWD und drücken Sie die **Eingabetaste**. Ihr Verzeichnis könnte zum Beispiel **/home/rapidrecovery/** lauten.

3 Laden Sie die entsprechende .rmp-Installationsdatei des Rapid Recovery-Agenten vom Lizenzportal unter https://licenseportal.com in Ihr aktuelles Arbeitsverzeichnis herunter.

Weitere Informationen über das Lizenzportal finden Sie im *Dell Datensicherung | Rapid Recovery License Portal Benutzerhandbuch*.

4 Um eine dauerhafte Verbindung zwischen Ihrer Linux-Maschine und der Dell Remote-Repository einzurichten, auf der die Rapid Recovery-Software und -Komponenten gespeichert sind, geben Sie den folgenden Befehl ein:

```
rpm -ivh <.rpm installation file you downloaded>
```

Beispiel: Wenn der Name der Installationsdatei „rapidrecovery-repo-6.0.2.999.rmp“ im Verzeichnis **/home/rapidrecovery/** lautet, geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
rpm -ivh rapidrecovery-repo-6.0.2.999.rpm
```

Etwaige fehlende Pakete oder vom Agenten benötigte Dateien werden vom Remote-Repository heruntergeladen und automatisch als Teil des Skripts installiert.

ANMERKUNG: Weitere Informationen zu Abhängigkeiten für die Installation auf einer Linux-Maschine finden Sie unter Agenten-Abhängigkeiten.

5 Installieren Sie den Rapid Recovery-Agenten durch Aufrufen des Zypper Paketmanagers, der den Repository Manager aktualisiert. Geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
apt-get update
```

6 Weisen Sie den Paketmanager an, die Rapid Recovery Agenten-Software zu installieren. Geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
apt-get install rapidrecovery-agent
```

7 Der Paketmanager bereitet die Installation aller abhängigen Dateien vor. Wenn Sie zur Bestätigung der Installation nicht signierter Dateien aufgefordert werden, geben Sie **y** (Ja) ein und drücken Sie die **Eingabetaste**.

Die Rapid Recovery Agenten-Dateien werden installiert.

Installation des Agenten auf Red Hat Enterprise Linux und CentOS

ANMERKUNG: Stellen Sie vor dem Durchführen dieser Schritte sicher, dass Sie das Red Hat- bzw. CentOS-Installationspaket in das Verzeichnis /home/system directory heruntergeladen haben. Die folgenden Schritte sind für 32-Bit und 64-Bit-Umgebungen gleich.

Zur Installation des Agenten auf Red Hat Enterprise Linux und CentOS:

1 Öffnen Sie eine Terminalsitzung mit Root-Zugriff.

2 Geben Sie den folgenden Befehl ein, um das Agent-Installationsprogramm ausführbar zu machen:

`chmod +x appassure-installer__rhel_amd64_5.x.x.xxxxx.sh` und drücken Sie anschließend <Eingabe>.

ANMERKUNG: Der Name des Installationsprogramms für 32-Bit-Umgebungen lautet `appassureinstaller__rhel_i386_5.x.x.xxxxx.sh`.

Die Datei wird ausführbar gemacht.

3 Geben Sie den folgenden Befehl ein, um den Agenten zu extrahieren und zu installieren:

`/appassure-installer_rhel_amd64_5.x.x.xxxxx.sh` und drücken Sie anschließend <Eingabe>.

Der Linux-Agent beginnt mit dem Extrahieren und dem Installationsvorgang. Etwaige fehlende Pakete oder durch den Agenten benötigte Pakete oder Dateien werden heruntergeladen und automatisch als Teil des Scripts installiert.

Lesen Sie Agenten-Abhängigkeiten, um Informationen zu den durch den Agenten benötigten Dateien zu erhalten.

Nach Abschluss des Installationsprogramms wird der Agent auf Ihrer Maschine ausgeführt. Weitere Informationen über den Schutz dieser Maschine durch den Kern finden Sie im Thema „Schützen von Workstations und Servern“ im *Benutzerhandbuch zu Rapid Recovery 6.0 auf DL Appliances* unter **Dell.com/support/home**.

Installieren der Agenten-Software auf Offline-Linux-Maschinen

Diese Aufgabe erfordert den Zugang zu einer Online-Linux-Maschine, zu Wechselspeichermedien und zur endgültigen Offline-Linux-Maschine. Wenn der AppAssure-Agent auf der Offline-Linux-Maschine installiert ist, müssen Sie ihn zuerst deinstallieren, bevor Sie den Rapid Recovery-Agenten installieren. Weitere Informationen finden Sie im Abschnitt „Deinstallieren der AppAssure Agenten-Software von einer Linux-Maschine" im *Dell Data Protection | Rapid Recovery Installations- und Aktualisierungshandbuch*.

Wenn Sie die Agenten-Software auf Linux-Maschinen installieren, die über keinen Zugang zum Internet verfügen, gehen Sie wie folgt vor. Konfigurieren Sie den Agenten nach Abschluss der Installation wie im Thema beschrieben Konfigurieren des Rapid Recovery Agent auf einer Linux-Maschine.

ANMERKUNG: Bei Installation auf mehreren Linux-Distributionen führen Sie dieses Verfahren für jede Distribution jeweils einmal aus.

1 Öffnen Sie auf einer Linux-Maschine mit Zugang zum Internet ein Terminalfenster und geben Sie den folgenden Befehl ein:

```
wget http://s3.amazonaws.com/repolinux/6.0.2/packages-downloader.sh
```

Das Shell-Skript wird in Ihr aktuelles Verzeichnis heruntergeladen.

2 Führen Sie das Shell-Skript durch Ausführung des folgenden Befehls aus:

```
bash packages-downloader.sh
```

Das Skript wird ausgeführt und fordert Sie dazu auf, eine bestimmte Linux-Distribution und Architektur zu wählen.

3 Geben Sie die Zahl des gewünschten Installationspakets ein und drücken Sie die **Eingabetaste**.

Beispiel: Um ein Installationspaket für Red Hat Enterprise Linux 7 abzurufen, geben Sie „3“ ein und drücken Sie die **Eingabetaste**.

Das entsprechende Installationsprogramm wird in das Verzeichnis **~/rapidrecovery.packages/** extrahiert.

ANMERKUNG: Die Tilde-Zeichen ~/ stehen für das Hauptverzeichnis.

4 Kopieren Sie die Pakete für den Rapid Recovery-Agenten auf einen Wechseldatenträger. Der spezifische Speicherort Ihres Wechseldatenträgers kann sich je nach Linux-Distribution unterscheiden. Geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
cp -R ~/rapidrecovery.packages/ <your_removable_media>
```

Beispiel: Wenn Sie einen USB-Wechseldatenträger verwenden, der im Speicherort „/media/USB-drive-1“ gemountet ist, geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
cp -R ~/rapidrecovery.packages /media/USB-drive-1
```

Alle erforderlichen Dateien werden auf das Wechselmedium kopiert.

5 Bringen Sie das Wechselmedium zur Offline-Linux-Maschine und bauen Sie das Laufwerk ein.

6 Kopieren Sie die Daten des eingebauten Geräts in Ihr Hauptverzeichnis oder einen anderen gewünschten Speicherort. Beispiel: Geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
cp -R /media/USB-drive-1 ~/rapidrecovery.packages
```

7 Wechseln Sie in das Verzeichnis Rapid Recovery. Beispiel: Geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
cd ~/rapidrecovery.packages
```

8 Führen Sie die Installation des Agenten mit Root-Rechten aus. Dieser Befehl unterscheidet sich je nach Linux-Distribution.

- Für Red Hat, SLES, Oracle und CentOS geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

  ```
  sudo rpm -i *.rpm
  ```

- Für Debian und Ubuntu geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

  ```
  sudo dpkg -i *.deb
  ```

Der lokale Paketmanager führt die Installation des Rapid Recovery-Agenten durch.

Nach Abschluss der Installation konfigurieren Sie den Agenten, wie im Thema Konfigurieren des Rapid Recovery Agent auf einer Linux-Maschine beschrieben.

VORSICHT: Nach der Konfiguration der neu installierten Agenten-Software auf einer Linux-Maschine müssen Sie den Computer neu starten. Durch den Neustart wird sichergestellt, dass die richtige Kernel-Treiberversion zum Schützen der Maschine verwendet wird.

Installieren der Agenten-Software auf Windows Server Core Edition-Maschinen

Führen Sie die Schritte im folgenden Verfahren aus, um die Agenten-Software auf einer Windows Server Core-Maschine zu installieren.

ANMERKUNG: Mit dem folgenden Verfahren wird die Agenten-Software im Konsolenmodus installiert. Um sie stattdessen im Silent-Modus zu installieren, hängen Sie `/silent` an den Dateinamen des Installationsprogramms in der Befehlszeile an. Zum Beispiel `Agent-X64-6.X.X.xxxxx.exe /silent`.

1 Laden Sie die Rapid Recovery Agenten-Installationsdatei vom Dell Datensicherung | Rapid Recovery License Portal oder vom Rapid Recovery Core herunter.

2 Von einer Eingabeaufforderung navigieren Sie zum Verzeichnis mit der Rapid Recovery Agenten-Installationsdatei und geben den Namen der Installationsdatei ein, um mit der Installation zu beginnen:

```
Agent-X64-6.x.x.xxxxx.exe
```

Das Installationsprogramm installiert die Agenten-Software und zeigt den Fortschritt in der Konsole an. Nach der Fertigstellung lösen neue Installationen einen automatischen Neustart der Maschine aus, während Agenten-Upgrades eventuell keinen Neustart der Maschine erfordern.

Konfigurieren des Rapid Recovery Agent auf einer Linux-Maschine

Führen Sie das Dienstprogramm zur Rapid Recovery-Konfiguration nach der Installation der Rapid Recovery Agenten-Software auf einer Linux-Maschine aus. Dieses kompiliert und installiert das Kernel-Modul auf der Linux-Maschine, die Sie schützen möchten, in Ihrem Core.

Das Konfigurationsprogramm bietet verschiedene Konfigurationsoptionen und Tipps für die nummerierten Schritte der Anweisungen, wenn es Ihre spezifischen Konfigurationsinformationen erkennt.

Führen Sie die folgenden Schritte zur Konfiguration der Rapid Recovery Agenten-Software auf einer beliebigen Linux-Maschine aus. Einige Konfigurationsoptionen unterscheiden sich je nach Linux-Verteilung, deren Installation Sie vornehmen.

1 Öffnen Sie eine Terminalsitzung mit Root-Zugriff.

2 Geben Sie den folgenden Befehl ein, um das Konfigurationsdienstprogramm zu starten und drücken Sie die Eingabetaste:

```
sudo /usr/bin/rapidrecovery-config
```

Das Konfigurationsdienstprogramm wird gestartet. Dieses enthält verschiedene Konfigurationsoptionen, die jeweils über eine Indexnummer zur Eingabe für den entsprechenden Konfigurationsschritt verfügen.

3 Konfigurieren Sie den Port für diese geschützte Maschine durch Eingabe des folgenden Befehls und drücken Sie dann die Eingabetaste. Die Standardportnummer ist 8006.

```
1 <agent_port>
```

Wenn zum Beispiel der Standardport verwendet wird, geben Sie folgenden Befehl ein:

```
1 8006
```

4 Konfigurieren Sie zum Schutz verfügbare Benutzer, indem Sie den folgenden Befehl eingeben, und drücken Sie dann die Eingabetaste:

```
1 <user_names_separated_by_comma>
```

Wenn Sie zum Beispiel die Benutzernamen Michael, Administrator und test_user1 verwenden, geben Sie den folgenden Befehl ein:

```
2 michael,administrator,test_user1
```

5 Konfigurieren Sie die Firewall-Regeln für die Auswahl eines Firewall-Konfigurationsmanagers. Darin werden Firewall-Ausnahmen für den in Schritt 1 genannten Port erstellt.

Wenn das Dienstprogramm einen oder mehrere Firewall-Konfigurationsmanager erkennt (wie z. B. lokkit oder firewalld), so wird jeder im Dienstprogramm in Zeile 3 aufgeführt. Wählen Sie den entsprechenden Konfigurationsmanager aus und geben Sie ihn ein, und zwar beginnend mit der Befehlsnummer (3), und drücken Sie dann die Eingabetaste:

```
3 <firewall_configuration>
```

Wenn Sie z. B. firewalld verwenden, geben Sie den folgenden Befehl ein:

```
3 firewalld
```

6 Fragen Sie die Liste kompatibler Kernel-Module vom Dienstprogramm mit Eingabe folgender Befehlsnummer ab und drücken Sie dann die Eigabetaste:

```
4
```

Ein Unterverzeichnis mit Shell gibt alle für die Installation kompatiblen Kernel-Module zurück. So konnten zum Beispiel die folgenden zurückgegeben werden:

```
Searching for all available for installation kernels.
This might take a while, depending on the Internet connection speed.
Kernels compatible for module installation:
 0 - linux-image-3.16.0.23-generic
 1 - linux-image-3.16.0.31-generic
 2 - linux-image-3.16.0.33-generic
 3 - linux-image-3.16.0.34-generic
Input indices of the kernel modules you wish to install, delimited by space; use 'all' to
install into all supported kernels, or 'q' to quit.
```

7 Konfigurieren Sie das entsprechende Rapid Recovery Kernel-Modul.

Beispiel: Um Kernel-Module für 3.16.0-23 und 3.16.0-34 einzugeben, geben Sie `1 4` ein und drücken die Eingabetaste.

Um alle Kernel-Module einzugeben, geben Sie `all` ein und drücken die Eingabetaste.

8 Nach der Konfiguration der neu installierten Agenten-Software starten Sie den Computer neu. Durch den Neustart wird sichergestellt, dass die richtige Kernel-Treiberversion zum Schützen der Maschine verwendet wird.

Nach Abschluss dieses Vorgangs wird das lokale Repository auf dieser Linux-Maschine konfiguriert. Die Agenten-Software ist installiert und das Kernel-Modul geladen.

Im nächsten Schritt wird die Maschine auf dem Rapid Recovery Core geschützt.

Schützen einer Maschine

Wenn Sie die Rapid Recovery Agenten-Software auf der zu schützenden Maschine bereits installiert, die Maschine aber noch nicht neu gestartet haben, starten Sie sie jetzt neu.

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.

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-Konsole anstelle der IP-Adresse angezeigt wird. Wenn Sie diese Änderung vornehmen, wird für die geschützte Maschine bei Anzeige der Details in der Core-Konsole keine IP-Adresse angezeigt. Sie legen auch den Schutzzeitplan für die Maschine fest.

Der Workflow des Schutzassistenten kann abhängig von der jeweiligen Umgebung geringfügig abweichen. Wenn beispielsweise die Rapid Recovery Agenten-Software 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.

1 Führen Sie einen der folgenden Vorgänge aus:

- Wenn Sie mit dem Assistenten zum Schützen der Maschine beginnen, fahren Sie mit Schritt 2 fort.
- Wenn Sie mit der Rapid Recovery Core-Konsole beginnen, klicken Sie in der Schaltflächenleiste auf **Protect (Schützen)**.

Daraufhin wird der **Protect Machine Wizard (Assistent zum Schützen der Maschine)** angezeigt.

2 Wählen Sie auf der Seite **Welcome (Willkommen)** die entsprechenden Installationsoptionen aus:

- Wenn Sie kein Repository definieren oder eine Verschlüsselung aufbauen müssen, wählen Sie **Typical (Typisch)**.
- Wenn Sie ein Repository erstellen, ein anderes Repository für Sicherungen der ausgewählten Maschine angeben oder die Verschlüsselung mit dem Assistenten einrichten müssen, wählen Sie **Advanced (show optional steps) (Erweitert (optionale Schritte anzeigen))**.
- Wenn die Seite **Welcome (Willkommen)** für den Assistenten zum Schützen der Maschine künftig nicht angezeigt werden soll, wählen Sie die Option **Skip this Welcome page the next time the wizard opens (Seite „Willkommen“ beim nächsten Öffnen des Assistenten ignorieren)** aus.

3 Wenn Sie mit Ihrer Auswahl auf der Begrüßungsseite zufrieden sind, klicken Sie auf **Next (Weiter)**.

Die Seite **Connection (Verbindung)** wird angezeigt.

4 Geben Sie auf der Seite **Connection (Verbindung)** die Informationen zur Maschine ein, zu der Sie eine Verbindung herstellen möchten. Richten Sie sich dabei an die folgende Tabelle und klicken Sie anschließend auf **Next (Weiter)**.

Tabelle 8. Verbindungseinstellungen für Maschinen

Textfeld	Beschreibung
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, der für die Verbindung mit dieser Maschine verwendet wird, z. B. Administrator (oder, falls sich der Computer in einer Domäne befindet: [Domänenname]\Administrator).
Kennwort	Das Kennwort, das für die Verbindung mit dieser Maschine verwendet wird.

Wenn die Seite **Install Agent (Agent installieren)** als Nächstes im Assistenten zum Schützen der Maschine angezeigt wird, bedeutet dies, dass Rapid Recovery nicht den Rapid Recovery-Agenten auf der Maschine erkennt und die aktuelle Version der Software installieren wird. Gehen Sie zu Schritt 7.

Wenn im Assistenten als Nächstes die Seite **Upgrade Agent (Agent aktualisieren)** angezeigt wird, bedeutet dies, dass eine ältere Version der Agenten-Software auf der zu schützenden Maschine vorhanden ist.

ANMERKUNG: Die Agenten-Software muss auf der zu schützenden Maschine installiert sein und diese Maschine muss neu gestartet werden, bevor sie im Kern gesichert werden kann. Damit das Installationsprogramm die geschützte Maschine neu startet, wählen Sie die Option After installation, restart the machine automatically (recommended) (Maschine nach der Installation automatisch neu starten (empfohlen)) aus, bevor Sie auf Next (Weiter) klicken.

5 Führen Sie auf der Seite **Upgrade Agent (Agent aktualisieren)** eine der folgenden Aktionen aus:

- Um die neue Version der Agenten-Software bereitzustellen (die mit der Version des Rapid Recovery Core übereinstimmt), wählen Sie **Upgrade the Agent to the latest version of the software (Agent auf die neueste Version der Software aktualisieren)** aus.
- Wenn die Maschine weiterhin geschützt werden soll, ohne die Agenten-Softwareversion zu aktualisieren, wählen Sie die Option **Upgrade the Agent to the latest version of the software (Agent auf die neueste Version der Software aktualisieren)** ab.

6 Klicken Sie auf **Next (Weiter)**.

7 Sie können ggf. auf der Seite **Protection (Schutz)**, wenn in der Rapid Recovery Core-Konsole anstelle der IP-Adresse ein Name für die geschützte Maschine angezeigt werden soll, im Feld **Display Name (Anzeigename)** einen Namen in das Dialogfeld eingeben.

Sie können bis zu 64 Zeichen eingeben. Verwenden Sie keine Sonderzeichen (siehe Beschreibung im Abschnitt „Unzulässige Zeichen“ im *Benutzerhandbuch zu Rapid Recovery auf DL Appliances*). Darüber hinaus darf der Anzeigename nicht mit den Zeichenkombinationen beginnen, die im Abschnitt „Unzulässige Wortgruppen“ im *Benutzerhandbuch zu Rapid Recovery auf DL Appliances* aufgeführt sind.

8 Wählen Sie den entsprechenden Schutzzeitplan aus (siehe nachstehende Beschreibung):

- Um den Standard-Schutzzeitplan zu verwenden, wählen Sie unter „Schedule Settings“ (Zeitplaneinstellungen) die Option **Default protection (Standardschutz)** aus.

Im Standard-Schutzzeitplan erstellt der Core jede Stunde Snapshots aller Volumes der geschützten Maschine. Auf der Seite „Summary“ (Zusammenfassung) für die jeweilige geschützte Maschine können Sie jederzeit die Schutzeinstellungen ändern, nachdem der Assistent beendet wurde, und auch die zu schützenden Volumes auswählen.

- Um einen anderen Schutzzeitplan zu definieren, wählen Sie unter „Schedule Settings“ (Zeitplaneinstellungen) die Option **Custom protection (Benutzerdefinierter Schutz)** aus.

9 Fahren Sie mit der Konfiguration wie folgt fort:

- Wenn Sie im Assistenten zum Schützen der Maschine eine typische Konfiguration ausgewählt und den Standardschutz angegeben haben, klicken Sie auf **Finish (Fertigstellen)**, um die ausgewählten Einstellungen zu bestätigen, den Assistenten zu schließen und die angegebene Maschine zu schützen.

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 anzuhalten.

- Wenn Sie im Assistenten zum Schützen der Maschine eine typische Konfiguration ausgewählt und den benutzerdefinierten Schutz angegeben haben, klicken Sie auf **Next (Weiter)**, um einen benutzerdefinierten Schutzzeitplan einzurichten. Ausführliche Informationen zum Festlegen eines benutzerdefinierten Schutzzeitplans finden Sie unter "Erstellen benutzerdefinierter Schutzzeitpläne" im *Benutzerhandbuch zu Rapid Recovery 6.0 auf DL Appliances*.
- Wenn Sie „Advanced Configuration“ (Erweiterte Konfiguration) für den Assistenten zum Schützen der Maschine und den Standardschutz ausgewählt haben, klicken Sie auf **Next (Weiter)**, und fahren Sie mit Schritt 14 fort, um die Repository- und Verschlüsselungsoptionen anzuzeigen.
- Wenn Sie „Advanced Configuration“ (Erweiterte Konfiguration) für den Assistenten zum Schützen der Maschine und den benutzerdefinierten Schutz ausgewählt haben, klicken Sie auf **Next (Weiter)**, und fahren Sie mit Schritt 11 fort, um auszuwählen, welche Volumes geschützt werden sollen.

10 Wählen Sie auf der Seite **Protection Volumes (Schutz-Volumes)** die Volumes aus, die Sie schützen möchten. Klicken Sie in der Spalte „Check“ (Überprüfen) auf die aufgelisteten Volumes, die nicht geschützt werden sollen, um die Auswahl aufzuheben. Klicken Sie anschließend auf **Next (Weiter)**.

ANMERKUNG: In der Regel sollten zumindest das Volume „System-reserviert“ und das Volume mit dem Betriebssystem (normalerweise Laufwerk C:) geschützt werden.

11 Legen Sie auf der Seite **Protection Schedule (Schutzzeitplan)** einen benutzerdefinierten Schutzzeitplan fest und klicken Sie dann auf **Next (Weiter)**. Ausführliche Informationen zum Festlegen eines benutzerdefinierten Schutzzeitplans finden Sie unter "Erstellen benutzerdefinierter Schutzzeitpläne" im *Benutzerhandbuch zu Rapid Recovery 6.0 auf DL Appliances*.

Wenn Sie bereits Repository-Informationen konfiguriert und die Option „Advanced“ (Erweitert) in Schritt 1 gewählt haben, wird die Seite „Encryption“ (Verschlüsselung) angezeigt. Fahren Sie mit Schritt 13 fort.

12 Wählen Sie ggf. auf der Seite **Encryption (Verschlüsselung)** zum Aktivieren der Verschlüsselung **Enable Encryption (Verschlüsselung aktivieren)** aus.

Die Felder für die Verschlüsselungsschlüssel werden auf der Seite **Encryption (Verschlüsselung)** angezeigt.

ANMERKUNG: Wenn Sie die Verschlüsselung aktivieren, werden die Daten aller geschützten Volumes für diese Maschine verschlüsselt. Sie können Verschlüsselungseinstellungen später von der Rapid Recovery Core-Konsole ändern. Weitere Informationen zur Verschlüsselung finden Sie im Abschnitt "Grundlegendes zu Verschlüsselungsschlüssel" im *Benutzerhandbuch zu Rapid Recovery 6.0 auf DL Appliances* unter www.dell.com/support/home.

VORSICHT: 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 Dell 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.

13 Wählen Sie auf der Seite **Encryption (Verschlüsselung)** eine der folgenden Optionen aus:

- Wenn Sie diese geschützte Maschine mit einem Verschlüsselungsschlüssel verschlüsseln möchten, der bereits in diesem Rapid Recovery Core definiert ist, wählen Sie **Encrypt data using an existing Encryption key (Daten mit einem vorhandenen Verschlüsselungsschlüssel verschlüsseln)** und dann den entsprechenden Schlüssel im Dropdown-Menü aus. Fahren Sie mit dem nächsten Schritt fort.
- Wenn Sie einen neuen Verschlüsselungsschlüssel zum Core hinzufügen und für diese geschützte Maschine verwenden möchten, geben Sie die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 9. Einstellungen für Verschlüsselungsschlüssel

Textfeld	Beschreibung
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein. Namen für Verschlüsselungsschlüssel müssen 1 bis 130 alphanumerische Zeichen umfassen. Sie dürfen keine Sonderzeichen wie umgekehrter Schrägstrich, Vorwärtsschrägstrich, senkrechter Strich, Doppelpunkt, Sternzeichen, Anführungszeichen, Fragezeichen, linke oder rechte Klammern, Und-Zeichen

Textfeld	Beschreibung
	(&) oder Rautezeichen (#) verwenden. Diese Informationen werden im Beschreibungsfeld angezeigt, wenn Verschlüsselungsschlüssel von der Core-Konsole angezeigt werden.
Beschreibung	Geben Sie eine Anmerkung für den Verschlüsselungsschlüssel ein. Diese Informationen werden im Beschreibungsfeld angezeigt, wenn Verschlüsselungsschlüssel von der Core-Konsole angezeigt werden.
Passphrase	Geben Sie die Passphrase für die Zugriffssteuerung ein. Sie sollten die oben aufgeführten Sonderzeichen nicht verwenden. Bewahren Sie die Passphrase an einem sicheren Ort auf. Der Dell Support kann eine Passphrase nicht wiederherstellen. Wenn Sie einen Verschlüsselungsschlüssel erstellt und für eine oder mehrere geschützte Maschine(n) verwendet haben, können Sie keine Daten mehr wiederherstellen, wenn die Passphrase verloren geht.
Passphrase bestätigen	Geben Sie zuvor eingegebene Passphrase erneut ein.

14 Klicken Sie auf **Finish (Fertigstellen)**, um Ihre 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 anzuhalten.

15 Wenn Sie eine Fehlermeldung erhalten, kann sich das Gerät nicht mit der Maschine verbinden, um diese zu sichern. So beheben Sie den Fehler:

a Überprüfen Sie die Netzwerkkonnektivität.
b Überprüfen Sie die Firewall-Einstellungen.
c Überprüfen Sie, ob die Rapid Recovery Services und RPC ausgeführt werden.
d Überprüfen Sie die DNS-Lookups (falls vorhanden)

Überprüfen der Netzwerk-Verbindungsfähigkeit

So überprüfen Sie die Netzwerkkonnektivität:

1 Öffnen Sie auf dem Client-System, mit dem Sie sich verbinden wollen eine Befehlszeilenschnittstelle.
2 Führen Sie den Befehl **ipconfig** aus und notieren Sie sich die IP-Adresse des Clients.
3 Öffnen Sie auf dem System eine Befehlszeilenschnittstelle.
4 Führen Sie den Befehl **ping <IP address of client>** aus.
5 Verfahren Sie je nach Ergebnis wie folgt:
- Wenn der Client auf das Ping nicht antwortet, dann überprüfen Sie die Konnektivität des Servers und die Netzwerkeinstellungen.
- Wenn der Client antwortet, überprüfen Sie, ob die Firewall-Einstellungen das Ausführen der DL1000-Komponenten zulassen.

Überprüfen der Firewall-Einstellungen

Wenn der Client ordnungsgemäß mit dem Netzwerk verbunden ist, jedoch durch die Kern-Konsole nicht erkannt wird, dann überprüfen Sie die Firewall, um sicherzugehen, dass eingehende und ausgehende Kommunikationen erlaubt sind.

So überprüfen Sie die Firewall-Einstellungen auf dem Kern und alle Clients, die dieser sichert:

1 Klicken Sie auf dem DL1000-Gerät auf **Start** > **Control Panel (Systemsteuerung).**
2 Klicken Sie in der **Systemsteuerung** auf **System und Sicherheit**, und klicken Sie unter **Windows Firewall** auf **Firewall-Status überprüfen**.
3 Klicken Sie auf **Erweiterte Einstellungen**.

4 Klicken Sie auf dem Bildschirm **Windows Firewall mit erweiterter Sicherheit** auf **Eingehende Regeln**.
5 Vergewissern Sie sich, dass für den Kern und die Ports in der Spalte **Enabled** (Aktiviert) **Yes** (Ja) angezeigt wird.
6 Wenn die Regel nicht aktiviert ist, dann klicken Sie mit der rechten Maustaste auf den Kern und wählen Sie **Enable Rule** (Regel aktivieren) aus.
7 Klicken Sie auf **Outbound Rules** (Ausgehende Regeln) und überprüfen Sie den Kern in gleicher Weise.

Überprüfen der DNS-Auflösung

Wenn die Maschine, die Sie sichern wollen DNS verwendet, dann überprüfen Sie, ob Forward- und Reverse Lookups korrekt sind.
So stellen Sie sicher, dass die Reverse Lookups korrekt sind:

1 Gehen Sie im System auf **C:\Windows\system32\drivers\etc** Hosts.
2 Geben Sie die IP-Adressen aller Clients ein, die auf DL1000 sichern.

Teaming von Netzwerkkarten

Standardmäßig sind die Netzwerkkarten (NICs) auf der DL1000 Appliance nicht verbunden, was sich auf die Leistung des Systems auswirkt. Es wird empfohlen, dass Sie die NICs als einzelne Schnittstelle teamen (oder: zusammenlegen). Für das Teaming der NICs ist folgendes erforderlich:

- Neuinstallation der Broadcom Advanced Control Suite (Software-Suite für die erweiterte Broadcom-Konfiguration).
- Erstellung des NIC-Teams

Neuinstallation der Broadcom Advanced Configuration Suite (Software-Suite für die erweiterte Broadcom-Konfiguration)

So installieren Sie die Broadcom Advanced Configuration Suite erneut:

1 Gehen Sie zu **C:\Install\BroadcomAdvanced** und doppelklicken Sie auf **Setup.**
Der **InstallShield-Assistent** wird angezeigt.
2 Klicken Sie auf **Weiter**.
3 Klicken Sie auf **Ändern, Hinzufügen oder Entfernen**.
Das Fenster **Benutzerdefinierte Einrichtung** wird angezeigt.
4 Klicken Sie auf **CIM-Anbieter** und wählen Sie anschließend **Diese Funktion wird auf der lokalen Festplatte installiert** aus.
5 Klicken Sie auf **BASP** und wählen Sie anschließend **Diese Funktion wird auf der lokalen Festplatte installiert** aus.
6 Klicken Sie auf **Weiter**.
7 Klicken Sie auf **Installieren**.
8 Klicken Sie auf **Fertigstellen**.

Erstellung des NIC-Teams

ANMERKUNG: Es wird empfohlen, die native Teamschnittstelle in Windows 2012 Server nicht zu verwenden. Der Teaming-Algorithmus ist für ausgehenden und nicht für eingehenden Verkehr optimiert. Er bietet schlechte Leistung mit Sicherungsauslastung, sogar mit mehr Netzwerk-Ports im Team.

So erstellen Sie NIC-Teaming:

1 Wechseln Sie zu **Start** > **Search (Suche)** > **Broadcom Advanced Control Suite**

ANMERKUNG: **Bei dem Verwenden der Broadcom Advanced Control Suite wählen Sie nur die Broadcom Netzwerkkarten aus.**

2 Wählen Sie in der **Broadcom Advanced Control Suite (Software-Suite für die erweiterte Broadcom-Konfiguration) Teams** > **Go to Team View (Zu Team-Ansicht wechseln).**

3 Klicken Sie in der **Hosts list** (Host-Liste) auf der linken Seite mit der rechten Maustaste auf den Host-Namen des DL1000-Geräts, und wählen Sie **Create Team** (Team erstellen) aus.

Das Fenster **Broadcom Teaming-Assistent** wird angezeigt.

4 Klicken Sie auf **Weiter**.

5 Geben Sie einen Namen für das Team ein und klicken Sie auf **Weiter**.

6 Wählen Sie den **Team-Typ** aus und klicken Sie auf **Weiter**.

7 Wählen Sie einen Adapter aus, den Sie zu einem Teil des Teams machen wollen und klicken Sie auf **Hinzufügen**.

8 Wiederholen Sie diese Schritte für alle anderen Adapter, die Teil des Teams sind.

9 Wenn alle Adapter für das Team ausgewählt wurden, klicken Sie auf **Weiter**.

10 Wählen Sie eine Standby-NIC aus, falls Sie eine NIC wollen, die als Standard-NIC verwendet wird, wenn das Team ausfällt.

11 Wählen Sie aus, ob **LiveLink** konfiguriert werden soll und klicken Sie anschließend auf **Weiter**.

12 Wählen Sie **VLAN-Verwaltung überspringen** aus und klicken Sie auf **Weiter**.

13 Wählen Sie **Änderungen auf System anwenden** aus und klicken Sie auf **Fertig stellen**.

14 Klicken Sie auf **Ja**, wenn Sie gewarnt werden, dass die Netzwerkverbindung unterbrochen wurde.

ANMERKUNG: **Das Erstellen des NIC-Teams dauert etwa fünf Minuten.**

5

Wie Sie Hilfe bekommen

Suche nach Dokumentation und Software-Aktualisierungen

Direkte Links zur Rapid Recovery- und DL1000 Appliance-Dokumentation und zu Software-Aktualisierungen finden Sie in der Core-Konsole.

Dokumentation

So greifen Sie auf den Link für die Dokumentation zu:

1 Klicken Sie in der Core-Konsole auf die Registerkarte **Appliance (Gerät)**.

2 Öffnen Sie im linken Fensterbereich den Link unter**Appliance (Gerät)** > **Documentation (Dokumentation)**.

Software updates (Software-Aktualisierungen)

So greifen Sie auf den Link für Software-Aktualisierung zu:

1 Klicken Sie in der Core-Konsole auf die Registerkarte **Appliance (Gerät)**.

2 Navigieren Sie im linken Fensterbereich zum Link**Appliance (Gerät)** > **Software Updates (Software-Aktualisierungen)**.

Kontaktaufnahme mit Dell

ANMERKUNG: Wenn Sie nicht über eine aktive Internetverbindung verfügen, können Sie Kontaktinformationen auch auf Ihrer Auftragsbestätigung, dem Lieferschein, der Rechnung oder im Dell-Produktkatalog finden.

Dell bietet verschiedene online- und telefonisch basierte Support- und Serviceoptionen an. Wenn Sie über keine aktive Internetverbindung verfügen, so finden Sie Kontaktinformationen auf der Eingangsrechnung, dem Lieferschein, der Rechnung oder im Dell Produktkatalog. Die Verfügbarkeit ist abhängig von Land und Produkt und einige Dienste sind in Ihrem Gebiet möglicherweise nicht verfügbar. Um sich bei Problemen zum Vertrieb, technischen Support oder zum Kundendienst mit Dell in Verbindung zu setzen, gehen Sie zu **software.dell.com/support**

Feedback zur Dokumentation

Klicken Sie auf allen Seiten der Dell Dokumentation auf den Link **Feedback (Rückmeldung)**, füllen Sie das Formular aus und klicken Sie auf **Submit (Senden)**, um uns Ihre Rückmeldung zukommen zu lassen.