DL4000 Dell PowerVault Backup to Disk Appliance Bereitstellungshandbuch – Für Capacity-Lizenzen

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG liefert wichtige Informationen, mit denen Sie den Computer 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.

2013 - 10

Rev. A02

Inhaltsverzeichnis

1

Einrichten des DL Backup to Disk-Systems

Einführung

Das Dell PowerVault DL Backup to Disk-System ist die neueste Generation eines Systems zur Sicherung auf der Festplatte mit Unterstützung von Dell AppAssure-Software. Das DL Backup to Disk-System ermöglicht:

- Skalierbare Speicherfunktionen zur Unterstützung von Organisationen jeglicher Größe
- 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

Das DL Backup to Disk-System ist in zwei Konfigurationen erhältlich: Standard-Edition und Edition mit hoher Kapazität. Kapazitätskonfigurationen sind wie folgt:

Tabelle 1. Kapazitätskonfigurationen der DL4000 Standard-Edition

Kapazität	Hardwarekonfiguration
5 TB	DL4000 mit nur internem Speicher
10 TB	DL4000 mit internem Speicher und 1 x MD1200 mit 12 x 1-TB-Festplatten
20 TB	DL4000 mit internem Speicher und 1 x MD1200 mit 12 x 2-TB-Festplatten
40 TB	DL4000 mit internem Speicher und 1 x MD1200 mit 12 x 4-TB-Festplatten

Tabelle 2. Kapazitätskonfigurationen der DL4000-Edition mit hoher Kapazität

Kapazität	Hardwarekonfiguration
20 TB	DL4000 mit internem Speicher und 1 x MD1200 mit 12 x 2-TB-Festplatten
40 TB	DL4000 mit internem Speicher und 1 x MD1200 mit 12 x 4-TB-Festplatten
60 TB	DL4000 mit internem Speicher und 2 x MD1200 • Erste MD1200 mit 12 x 4-TB-Laufwerken (40 TB) • Zweite MD1200 mit 12 x 2-TB-Laufwerken (20 TB)
80 TB	DL4000 mit internem Speicher und 2 x MD1200 • Erste MD1200 mit 12 x 4-TB-Laufwerken (40 TB) • Zweite MD1200 mit 12 x 4-TB-Laufwerken (40 TB)

ANMERKUNG: Alle Modelle außer dem Modell der Standard-Edition 5TB verwenden den internen Speicher auf dem DL4000 für VM-, Archivierungs-, oder andere Scratch Space-Speicher.

ANMERKUNG: Zusätzlicher Speicher kann durch Erweiterungsfächer hinzugefügt werden (Dell PowerVault MD1200). Zusätzlicher Speicher kann nur dem Standard Edition 5 TB-Modell hinzugefügt werden und ermöglicht ein Erweiterungsfach, und den 20 TB- und 40 TB-Modellen hoher Kapazität, die zwei Erweiterungsfächer ermöglichen.

Jede Konfiguration umfasst auch die folgende Hardware und Software:

- Dell PowerVault DL4000-System
- Dell PowerEdge RAID-Controller (PERC)
- Vorinstalliertes Betriebssystem sowie Dell OpenManage-System- und Speicherverwaltungssoftware.
- AppAssure 5-Software

ANMERKUNG: Wenn die Systemkonfiguration keine PowerVault MD1200-Speichergehäuse umfasst, können Sie die in diesem Dokument genannten Referenzen zu PowerVault MD1200 und Speichergehäusen ignorieren.

Weitere Informationen über jede Konfiguration finden Sie im *Dell PowerVault DL4000 Owner's Manual* (Benutzerhandbuch Dell PowerVault DL4000) unter **dell.com/support/manuals.**

Die für Ihre IT-Umgebung spezifischen Erstanforderungen müssen eingegeben werden, wenn Sie das System zum ersten Mal verwenden.

Die folgende Tabelle führt die in diesem Dokument verwendeten Begriffe auf, die sich auf die verschiedenen Hardware- und Softwarekomponenten der DL4000 Backup to Disk Appliance beziehen.

Tabelle 3. Hardware- und Softwarekomponenten des DL Backup to Disk-Systems

Komponente	Verwendete Begriffe
DL4000 Backup to Disk Appliance	Appliance
PowerVault DL4000-System	DL4000-System
PowerVault MD1200-Speichergehäuse	Speichergehäuse
Dell AppAssure 5-Software	AppAssure 5

Installationsvoraussetzungen

Netzwerkanforderungen

Für den Betrieb des PowerVault DL Backup to Disk-Systems 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

Dell empfiehlt Organisationen die Verwendung von1 GigE Backbone für eine effiziente Leistung bei der Verwendung von AppAssure 5 und 10 GigE-Netzwerke für extrem stabile Umgebungen.

Einrichten der Hardware

Das System wird mit einem einzelnen PowerVault DL4000-System geliefert. Lesen Sie das mit dem System mitgelieferte Handbuch *Getting Started Guide* (Erste Schritte) für das PowerVault DL4000-System. Packen Sie die DL Backup to Disk-Systemhardware aus und richten Sie diese 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 DL Backup to Disk-Systemhardware ein.

1. Montieren Sie das PowerVault DL4000-System und das bzw. die Speichergehäuse im Rack und verkabeln Sie alle Geräte.
2. Schalten Sie das bzw. die Speichergehäuse, und anschließend das PowerVault DL4000-System ein.

Installation des Systems in einem Rack

Wenn das PowerVault DL4000-System ein Schienen-Kit beinhaltet, dann machen Sie die *Anweisungen für die Rack-Installation* ausfindig, die mit dem Schienen-Kit mitgeliefert werden. Befolgen Sie die Anweisungen, um die Schienen in der Rackeinheit, und das PowerVault DL4000-System und Speichergehäuse im Rack zu installieren.

Verkabelung des Systems

Machen Sie das mit dem System mitgelieferte PowerVault DL4000-Handbuch *Getting Started Guide* (Erste Schritte) ausfindig und befolgen Sie die Anweisungen zum Anschluss:

- Der Tastatur-, Maus-, Monitor-, Strom- und Netzwerkkabel an das PowerVault DL4000-System
- Der Stromversorgungskabel

Einstellen des Konfigurationsschalters für das Speichergehäuse

Stellen Sie den Speichermodus für das Speichergehäuse auf den einheitlichen Modus ein, wie in den folgenden Abbildungen gezeigt.

ANMERKUNG: Der Konfigurationsschalter muss vor dem Einschalten des Speichergehäuses eingestellt werden. Wird der Konfigurationsmodus nach Einschalten des Speichergehäuses geändert, hat dies erst dann eine Auswirkung auf die Gehäusekonfiguration, wenn das System aus- und wieder eingeschaltet wurde. Weitere Informationen finden Sie im **Dell PowerVault MD1200 Hardware-Benutzerhandbuch** unter support.dell.com/manuals.

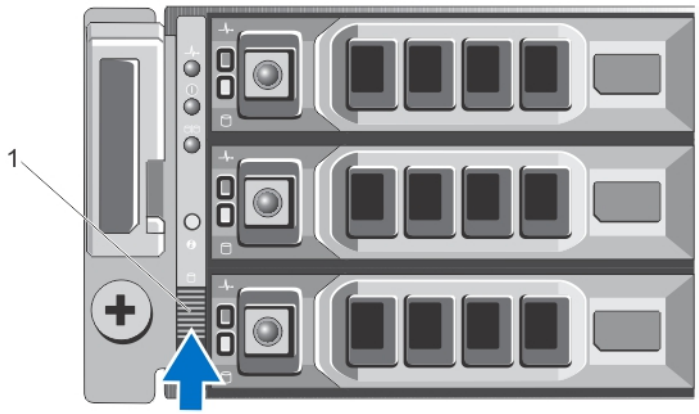

Abbildung 1. Einstellen des Konfigurationsschalters für das PowerVault MD1200-Speichergehäuse

1. Konfigurationsschalter

Anschließen des Speichergehäuses an das PowerVault DL4000-System

Verbinden Sie das SAS-Datenkabel des auf dem PowerVault DL4000-System installierten PowerEdge RAID-Controllers (PERC) mit dem primären EMM-SAS **In-**Anschluss (Enclosure Management Module, Gehäuseverwaltungsmodul) am Speichergehäuse. Beziehen Sie sich für weitere Informationen auf die untenstehende Abbildung.

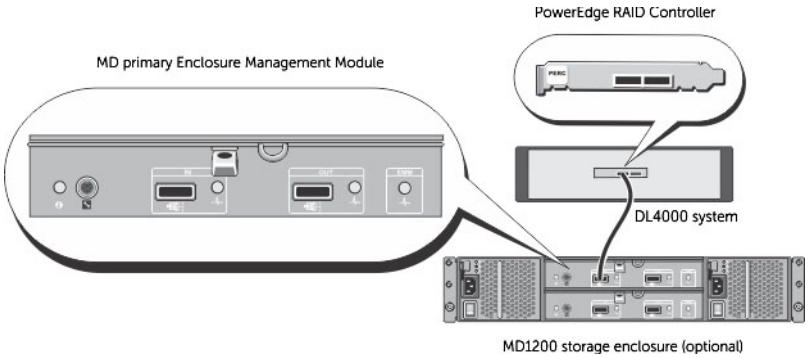

Abbildung 2. Anschließen des SAS-Kabels vom PowerVault DL4000-System an das PowerVault MD1200-Speichergehäuse

Anschließen des Kabelführungsarms (optional)

Falls Ihr System einen Kabelführungsarm enthält, nehmen Sie die *CMA Installation Instructions* (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 des DL Backup to Disk-Systems

Schalten Sie nach dem Verkabeln des Systems das MD1200-Speichergehäuse ein und schalten Sie anschließend das PowerVault DL4000-System ein.

ANMERKUNG: Es wird empfohlen, das System für eine maximale Zuverlässigkeit und Verfügbarkeit an eine unterbrechungsfreie Stromversorgung (USV) anzuschließen. Weitere Informationen finden Sie im *Benutzerhandbuch* des Systems unter **dell.com/support/manuals**.

PowerVault DL4000-Laufwerkskonfigurationen

Das PowerVault DL4000 unterstützt ausschließlich SAS- und Nearline-SAS-Laufwerke. Das Betriebssystem befindet sich auf einem auf den Steckplätzen 0 und 1 befindlichen (gespiegelten) virtuellen RAID1-Laufwerk. Lesen Sie für Informationen zu diesen Laufwerken das *Dell PowerVault DL4000 Benutzerhandbuch* auf **dell.com/support/manuals**. Steckplätze 2 bis 9 stehen für die automatische Konfiguration zur Verfügung, können jedoch manuell konfiguriert werden (falls erforderlich). Die Laufwerke werden automatisch als RAID 6 bereitgestellt. Optional ist eine Kapazitätserweiterung unter Nutzung eines MD1200-Speichergehäuses möglich.

2

Konfigurieren von AppAssure 5

Nach Ändern des Systemkennworts wird beim ersten Einschalten des Systems automatisch der **AppAssure-Systemkonfigurationsassistent** ausgeführt.

1. Nach Einschalten des Systems wird das Dialogfeld **Windows einrichten** angezeigt. Wählen Sie **Ich akzeptiere die Lizenzbedingungen** aus und klicken Sie auf **Start**.

   WARNUNG: Dell DL4000 ist aktuell so entwickelt, dass es mit Englisch als Systemstandardsprache funktioniert. Wählen Sie immer Englisch als Windows-Sprache aus und verwenden Sie keine Sprachpakete in anderen Sprachen. Die Verwendung eines Sprachpakets in einer anderen Sprache als Englisch resultiert in nicht ordnungsgemäßen Systemvorgängen. Sollten Sie, während dem Start von Windows ein Sprachpaket in einer anderen Sprache als Englisch ausgewählt haben, finden Sie Informationen zum Rekonfigurieren des Sprachpaketes zu Englisch unter Verwenden einer anderen Sprache als Englisch beim Windows-Start.

2. Klicken Sie bei der Meldung, die Sie zum Ändern Ihres Administrator-Kennworts auffordert auf **OK**.
3. Geben Sie das neue Kennwort ein und bestätigen Sie es.
   Sie werden von einer Meldung darauf hingewiesen, dass das Kennwort geändert wurde.
4. Klicken Sie auf **OK**.
5. Scrollen Sie von dem Bildschirm **Dell readme.htm** nach unten und klicken Sie auf **Fortfahren**.
6. Melden Sie sich bei Windows mit dem geänderten Administrator-Kennwort an.

Es wird der Begrüßungsbildschirm des **AppAssure-Systemkonfigurationsassistenten** angezeigt.

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

AppAssure-Systemkonfigurationsassistent

ANMERKUNG: Schließen Sie alle Schritte des **AppAssure-Systemkonfigurationsassistenten** ab, bevor Sie die Microsoft Windows-Aktualisierung verwenden. Der Windows-Aktualisierungsdienst wird während des Konfigurationsvorgangs vorübergehend deaktiviert.

Der **AppAssure-Systemkonfigurationsassistenten** führt Sie durch eine Reihe von Schritten zur Konfiguration der Systemsoftware.

Der Assistent unterstützt Sie bei Folgendem:

- Einrichten der Netzwerkschnittstellen
- Konfigurieren des Hostnamens und der Domäneneinstellungen
- Konfigurieren der SNMP-Einstellungen

Nach Abschluss aller Schritte des Systemkonfigurationsassistenten wird automatisch die **AppAssure 5 Kern**-Konsole gestartet.

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 Systemkonfigurationsassistent 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**.
   Die zusätzlich verbundenen Netzwerkschnittstellen werden angezeigt.
4. Klicken Sie auf **Weiter**.
   Die Seite **Konfigurieren der ausgewählten Netzwerkschnittstellen** wird 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 konfigurieren** angezeigt.

Weitere Informationen zu NIC-Teamvorgang finden Sie unter 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 Systemkonfigurationsassistenten erfordert die manuelle Durchführung mehrerer Schritte.

Konfigurieren Sie den Host-Namen und die Domäneneinstellungen:

1. Ändern Sie den Host-Namen des Systems auf der Seite **Host-Namen- und Domain-Einstellungen konfigurieren.** Geben Sie zum Ändern des Host-Namens des Systems in **Neuer Host-Name** einen geeigneten Host-Namen ein.
2. Wenn Sie nicht wollen, dass das System einer Domain beitritt, dann wählen Sie in **Wollen Sie, dass dieses System einer Domain beitritt? Nein** aus

   Standardmäßig ist **Ja** voreingestellt.
3. Geben Sie die folgenden Einzelheiten ein, um das System einer Domain beitreten zu lassen:
   - **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 Domain erfordert einen Neustart. Nach dem Neustart wird automatisch der AppAssure-Systemkonfigurationsassistent gestartet. Wenn das System einer Domain beigetreten ist, müssen Sie sich nach dem Neustart als Domainnutzer mit Administratorberechtigungen am System anmelden.

   Die Seite **Konfiguration der SNMP-Einstellungen** wird 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 Auf diesem Gerät SNMP konfigurieren** [auf der Seite **SNMP-Einstellungen 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**.

   Die Seite **Vielen Dank** wird angezeigt.

7. Um die SNMP-Konfiguration abzuschließen, klicken Sie auf **Weiter** und auf der Seite **Konfiguration beendet** ebenfalls auf **Weiter**.

   Die AppAssure 5 Core-Konsole wird in Ihrem Standard-Web-Browser geöffnet.

   Sie werden durch eine Meldung aufgefordert, Ihren Microsoft Windows-Administratorbenutzernamen und das Kennwort einzugeben.

8. Geben Sie Ihren Microsoft Windows-Administratorbenutzernamen und das Kennwort ein und klicken Sie auf **OK**.

9. Fahren Sie mit dem Konfigurationsprozess durch Speicherbereitstellung fort.

Speicherbereitstellung

Das System konfiguriert automatisch den im DL4000 intern verfügbaren Speicher und alle verbundenen externen Speichergehäuse für:

- AppAssure-Repositories
- Virtuelles Standby der geschützten Maschinen

ANMERKUNG: Nur MD1200s mit 1TB-, 2TB-, 3TB-, oder 4TB- (für hohe Kapazität) Treibern, mit H810-Controllern verbunden, werden unterstützt. Ein MD1200 wird für das Standard-Gerät unterstützt und zwei MD1200s werden auf dem Leistungsgerät unterstützt.

Bevor Sie damit anfangen, Speicher auf dem Laufwerk bereitzustellen, bestimmen Sie, wie viel Speicher Sie für die virtuellen Standby-Maschinen brauchen. Sie können einen beliebigen Prozentsatz der verfügbaren Kapazität zum Hosten virtueller Standby-Maschinen zuordnen. Wenn Sie zum Beispiel Storage Resource Management (SRM) verwenden, können Sie bis zu 100 Prozent Kapazität auf ein Gerät, das auf virtuelle Maschinen bereitgestellt ist, zuordnen. Diese Maschinen können unter Verwendung der Live-Wiederherstellungsfunktion von AppAssure verwendet werden, um beliebige Server wiederherzustellen, die durch das DL4000 geschützt werden.

Basierend auf einer mittelgroßen Umgebung die keine virtuellen Standby-Maschinen braucht, können Sie den ganzen Speicher dazu verwenden eine erhebliche Anzahl von Agenten zu sichern. Wenn Sie jedoch weitere Ressourcen für virtuelle Standby-Maschinen benötigen und eine kleinere Anzahl von Agentenmaschinen sichern, können Sie den größeren VMs mehr Ressourcen zuweisen.

Wenn Sie die Registerkarte **Gerät** auswählen, findet die AppAssure Appliance-Software den verfügbaren Speicher für alle unterstützten Controller im System und bestätigt, dass die Hardware den Anforderungen entspricht.

So schließen Sie die Laufwerksbereitstellung für alle verfügbaren Speicher ab:

1. Klicken Sie in der Registerkarte **Gerät** auf **Tasks**.

   Der Bildschirm **Tasks** zeigt die verfügbare interne Speicherkapazität des Systems an. Diese Kapazität wird zum Erstellen eines neuen AppAssure-Repositories verwendet

   VORSICHT: Bevor Sie in diesem Vorgang mit Schritt 2 weiterfahren, klicken Sie zum Öffnen des Fensters „Speicherbereitstellung“ auf Bereitstellung in der Spalte „Maßnahme“ neben dem Speicher, den Sie bereitstellen möchten. Stellen Sie im Abschnitt Bereitstellungstask-Maßnahme sicher, dass das Kontrollkästchen neben Tun Sie dies nur für einen Bereitstellungstask, wenn mehr als ein Task auf einmal bereitgestellt wird markiert ist, außer, wenn Sie auf dem ersten Gehäuse eine Reserve haben möchten. (In diesem Fall würden Sie diese Einstellung markiert lassen). Wählen Sie im Abschnitt Optionale Speicher-Reserve das Kästchen neben Stellen Sie einen Teil des Speichers für virtuelle Standby-Maschinen oder andere Zwecke bereit und geben Sie einen Prozentsatz zum Zuordnen an. Andernfalls wird der Prozentsatz des Speichers, der im Abschnitt Optionale Speicher-Reserve angegeben wird, von allen angebrachten Laufwerken genommen.

2. Klicken Sie auf **Alle Bereitstellen**.

ANMERKUNG: Wenn Sie zum Beispiel ausgewählt haben, 30 Prozent des Speichers den Standby-VMs zuzuordnen, wird der Befehl **Alle Bereitstellen** den internen Speicher als 70 Prozent für das Repository und 30 Prozent für Standby-VMs zuordnen. Wenn Sie die Einstellung **Tun Sie dies nur für einen Bereitstellungstask, wenn mehr als ein Task auf einmal bereitgestellt wird** deaktiviert haben, wird der ganze externe Speicher 100 Prozent dem Repository zugeordnet, das als extra Speicherplatz für das Repository hinzugefügt wird, das auf dem internen Speicher erstellt wird.

Breitstellung von ausgewählten Speichern

So stellen Sie ausgewählte Speicher bereit:

1. Klicken Sie in der Registerkarte **Gerät** auf **Tasks**.

   Der Bildschirm **Tasks** zeigt die verfügbare interne und externe Speicherkapazität für das Gerät an, ob es für die Bereitstellung verfügbar ist oder ob es schon bereitgestellt wurde oder ob ein Zustand besteht, der den Speicher davon abhält, automatisch bereitgestellt zu werden. Diese Kapazität wird zum Erstellen eines AppAssure 5-Repositories verwendet
2. Um nur einen Teil des verfügbaren Speichers bereitzustellen, klicken Sie auf **Bereitstellung** unter **Maßnahme** neben dem Speicherplatz, den Sie bereitstellen möchten.

   – Um ein neues Repository zu erstellen, wählen Sie **Ein neues Repository erstellen** und geben Sie einen Namen für das Repository ein.

     Standardmäßig wird Repository 1 im neuen Repository-Namen angezeigt. Sie können sich dazu entscheiden, den Namen zu überschreiben.

   – Wählen Sie **Aktuelles Repository erweitern** und das entsprechende Repository in der Liste **Aktuelle Repositorys** aus, um einem vorhandenen Repository Kapazität hinzuzufügen.

   ANMERKUNG: Um Kapazität hinzuzufügen wird empfohlen, dass sie ein aktuelles Repository erweitern, anstatt ein weiteres Repository hinzuzufügen. Speicherplatz wird von separaten Repositories nicht gleichermaßen effizient genutzt, weil eine Deduplizierung nicht über separate Repositories hinweg durchgeführt werden kann.
3. Sie können unter **Optionale Speicher-Reserve** die Option auswählen, einen Teil des Speichers für virtuelle Standby-Maschinen bereitzustellen, und dann den Prozentsatz des Speichers, den Sie für die VMs bereitstellen möchten, anzugeben.
4. Sie können sich dazu entscheiden, das Kontrollkästchen **Tun Sie dies nur für einen Bereitstellungstask, wenn mehr als ein Task auf einmal bereitgestellt wird** (Standardmäßig ausgewählt) zu löschen.

   Wenn Sie diese Option aufheben, wird der Prozentsatz des ausgewählten Speichers auf nur das ausgewählte Speichergerät angewendet. Die Auswahl dieser Option ermöglicht es Ihnen, den Prozentsatz des ausgewählten Speichers auf den internen Speicher und die externen Gehäuse anzuwenden.
5. Klicken Sie auf **Bereitstellung**.

   Die Laufwerksbereitstellung beginnt, und im Bereich **Status** des Bildschirms **Tasks** wird der Status der AppAssure-Repository-Erstellung angezeigt. Die **Statusbeschreibung** zeigt **Bereitgestellt** an.
6. Um die Details anzuzeigen nachdem die Laufwerksbereitstellung fertiggestellt wird, klicken Sie auf **>** neben der Statusanzeige.

   Die Seite **Tasks** wird erweitert und zeigt Status, Repository und virtuelle Festplattendetails (falls zugeteilt) an.

3

Aufgaben nach der Installation

Führen Sie nach Abschluss des AppAssure-Systemkonfigurationsassistenten und des AppAssure-Kerneinrichtungsassistenten die folgenden Verfahren durch, um sicherzustellen, dass Ihr Sicherungssystem und die durch das System gesicherten Server korrekt konfiguriert wurden.

ANMERKUNG: Das System ist mit einer 30-tägigen Testlizenz konfiguriert. Melden Sie sich zum Erhalt eines permanenten Lizenzschlüssels im Dell AppAssure License Portal unter **www.dell.com/DLActivation** an. Geben Sie die System-Service-Tag-Nummer, um den permanenten Lizenzschlüssel zu erhalten, ein und ändern Sie dann den Lizenzschlüssel in der AppAssure Software. Weitere Informationen zum Ändern des Lizenzschüssels in der AppAssure Software finden Sie im Abschnitt „Ändern eines Lizenzschlüssels“ im *DL4000 User's Guide* (Benutzerhandbuch DL4000) unter **dell.com/support.manuals**.

Eine andere Sprache als Englisch beim Start von Windows ausgewählt

Wenn Sie beim Start von Windows eine andere Sprache als Englisch ausgewählt haben, funktioniert das System nicht einwandfrei.

Zum Rekonfigurieren der Standardsprache des Systems in Englisch:

1. Melden Sie sich als Administrator an und öffnen Sie ein Befehlsfenster.
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

   ANMERKUNG: Es wird dringend empfohlen, dass Sie den Hostnamen durch Verwendung des AppAssure-Systemkonfigurationsassistenten ändern. Sobald der AppAssure-Systemkonfigurationsassistent beendet wurde, ändern Sie den Computernamen manuell auf den vorherigen Namen zurück.

Zugreifen auf die AppAssure 5-Core Console

Stellen Sie sicher, dass Sie vertrauenswürdige Seiten, wie im Thema Aktualisieren von vertrauenswürdigen Seiten in Internet Explorer behandelt, aktualisieren und den Browser, wie in Thema Konfigurieren des Browsers zum Remote-Zugriff auf die AppAssure 5 Core-Konsole behandelt, aktualisieren. Nachdem Sie die vertrauenswürdigen Seiten in Internet Explorer aktualisiert und Ihre Browser konfiguriert haben, führen Sie einen der folgenden Schritte zum Zugriff auf die AppAssure 5 Core-Konsole durch:

- Melden Sie sich lokal bei Ihrem AppAssure 5 Core-Server an und wählen Sie dann das Symbol für die **Core Console** (Kern-Konsole) aus.
- 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 in 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**.

Konfigurieren des Browsers zum Remote-Zugriff auf die AppAssure 5 Core-Konsole

Bevor Sie erfolgreich auf die AppAssure 5 Core Console von einem Remote-System zugreifen können, müssen Sie Ihre Browser-Einstellungen ändern. Die folgenden Verfahren beschreiben, wie Internet Explorer-, Google Chrome-, und Mozilla Firefox-Browser-Einstellungen geändert werden können.

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

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

So ändern Sie Browser-Einstellungen für Internet Explorer und Chrome:

1. Wählen Sie von dem Bildschirm **Internetoptionen** die Registerkarte **Sicherheit**.
2. Klicken Sie auf **Vertrauenswürdige Seiten** und klicken Sie dann auf **Seiten**.
3. Deaktivieren Sie die Option **Serverüberprüfung erforderlich (https:) für alle Websites in der Zone** und fügen sie dann http://<*Hostname oder die IP-Adresse des Geräteservers, der den AppAssure 5-Kern hostet*> auf **Vertrauenswürdige Sites** hinzu.
4. Klicken sie auf **Schließen**, wählen Sie **Vertrauenswürdige Sites** aus und klicken Sie dann auf **Benutzerdefinierte Stufe**.
5. Scrollen Sie zu **Verschiedenes → Gemischten Inhalt anzeigen** und klicken Sie auf **Aktivieren**.
6. Scrollen Sie auf dem Bildschirm nach unten zu **Benutzerauthentifizierung → Anmelden** und wählen Sie dann **Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort** aus.
7. Klicken Sie auf **OK** und wählen Sie dann die Registerkarte **Erweitert**.
8. Scrollen Sie zu **Multimedia** und wählen Sie **Auf Webseiten Animationen abspielen** aus.
9. Scrollen Sie zu **Sicherheit**, markieren Sie **Integrierte Windows-Authentifizierung aktivieren** und klicken Sie dann auf **OK**.

So ändern Sie die Firefox Browser-Einstellungen:

1. Geben Sie in die Firefox-Adresszeile **about:config** ein und klicken Sie dann, wenn aufgefordert, auf **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, durch Kommas getrennt, des Gerätesystems ein, das den AppAssure 5-Kern hostet; zum Beispiel: *IPAddress*,*host name*.
4. Starten Sie Firefox neu.

Überprüfen der Beibehaltungszeiträume

AppAssure legt Standard-Beibehaltungszeiträume fest, die bestimmen, wie oft Snapshots erstellt werden und wie lange die Snapshots beibehalten werden. Die Beibehaltungszeiträume müssen jedoch auf den Anforderungen Ihrer Umgebung basieren. Wenn Sie z.B. Server sichern, die unternehmenskritische Daten ausführen, die häufigen Änderungen unterliegen und für die Geschäftskontinuität unerlässlich sind, dann müssen Snapshots häufiger erstellt werden.

Zum Überprüfen und Ändern der Beibehaltungszeiträume:

1. Öffnen Sie die AppAssure-Kern-Konsole.
2. Wählen Sie die Registerkarte **Konfiguration** aus, und klicken Sie dann auf **Beibehaltungsrichtlinie**.
3. Passen Sie die Beibehaltungsrichtlinie basierend auf den Anforderungen Ihrer Organisation an.
4. Klicken Sie auf **Anwenden**.

Verschlüsseln der Agent Snapshot-Daten

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

Zum Verschlüsseln von Agenten-Snapshot-Daten:

1. Klicken Sie vom AppAssure 5-Kern auf **Konfiguration** → **Verwalten** → **Sicherheit**.
2. Klicken Sie auf **Maßnahmen**, und klicken Sie dann auf **Verschlüsselungsschlüssel hinzufügen**.
   Die Seite **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.

Feld	Beschreibung
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, dass Sie die Verschlüsselungspassphrase speichern, da der Verlust der Passphrase die Daten unzugänglich macht.

Konfigurieren eines E-Mail-Servers und einer E-Mail-Benachrichtigungs-Vorlage

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

ANMERKUNG: Sie müssen ebenfalls die Benachrichtigungsgruppeneinstellungen, einschließlich der Option **Durch E-Mail benachrichtigen** aktivieren, bevor E-Mail-Benachrichtigungen gesendet werden. Weitere Informationen zum Festlegen von Ereignissen, um E-Mail-Benachrichtigungen zu erhalten, finden Sie unter „Konfigurieren von Benachrichtigungsgruppen für Systemereignisse“ im *Dell PowerVault DL4000 User's Guide* (Dell PowerVault DL4000-Benutzerhandbuch) unter **dell.com/support/manuals**.

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

1. Wählen Sie in AppAssure 5-Core die Registerkarte **Konfiguration** aus.
2. Klicken Sie unter **Verwalten** auf die Option **Ereignisse**.
3. Klicken Sie im Fensterbereich **E-Mail-SMTP-Einstellungen** auf **Ändern**.
   Das Dialogfeld „**Konfiguration der E-Mail-Benachrichtigung**“ wird angezeigt.
4. Wählen Sie **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.

Textfeld	Beschreibung
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 **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 AppAssure so konfiguriert, dass drei gleichzeitige Streams auf das System zugelassen werden. Es wird empfohlen, dass die Anzahl der Streams um eins höher ist als die Anzahl der von Ihnen gesicherten Maschinen (Agenten). Wenn Sie z.B. sechs Agenten sichern, muss die **Maximale Anzahl gleichzeitiger Übertragungen** auf sieben eingestellt werden.

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 **Maximale Anzahl gleichzeitiger Übertragungen** auf eine Zahl, die mindestens um eins höher ist als die Anzahl der Clients, die Sie sichern.

Das Schützen von Maschinen und das Überprüfen der Client-Konnektivität

Überprüfen Sie nach dem Konfigurieren des AppAssure-Systems und -Kerns (Core), dass Sie sich mit den Maschinen verbinden können, die Sie sichern wollen.

So schützen Sie eine Maschine:

1. Wechseln Sie zur AppAssure 5-Kern-Konsole und wählen Sie die Registerkarte **Maschine** aus.
2. Klicken Sie im Drop-Down-Menü **Maßnahmen** auf **Maschine schützen**.
   Das Dialogfeld **Verbinden** wird angezeigt.
3. Geben Sie die Informationen über die Maschine, mit der Sie Verbindung aufnehmen wollen, im Dialogfeld **Verbinden** ein, wie in der folgenden Tabelle beschrieben.

Host	Der Hostname oder die IP-Adresse der Maschine, die Sie schützen möchten.
Schnittstelle	Die Portnummer, über die der AppAssure 5-Kern mit dem Agenten auf der Maschine kommuniziert.
Benutzername	Der Benutzername, der für die Verbindung mit dieser Maschine verwendet wird, z. B. Administrator.
Kennwort	Das Kennwort, das für die Verbindung mit dieser Maschine verwendet wird.

4. Klicken Sie auf **Verbinden**.

5. 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 AppAssure-Dienste und RPC ausgeführt werden.
   d) Überprüfen Sie die DNS-Lookups (falls vorhanden)

Überprüfen der Netzwerkkonnektivität

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, dann überprüfen Sie, ob die Firewall-Einstellungen ein Ausführen der AppAssure-Komponenten zulassen.

Überprüfen der Firewall-Einstellungen

Wenn der Client ordnungsgemäß mit dem Netzwerk verbunden ist, jedoch durch die AppAssure-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 AppAssure-Kern und alle Clients, die dieser sichert:

1. Klicken Sie auf dem AppAssure-Gerät auf **Start → 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 AppAssure-Kern und die Ports in der Spalte **Aktiviert Ja** angezeigt wird.
6. Wenn die Regel nicht aktiviert ist, dann klicken Sie mit der rechten Maustaste auf den AppAssure-Kern und wählen Sie **Regel aktivieren** aus.
7. Klicken Sie auf **Ausgehende Regeln** und überprüfen Sie den AppAssure-Kern in gleicher Weise .

Überprüfen der Namensauflösung (falls vorhanden)

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 AppAssure-System in **C:\Windows\system32\drivers\etc** Hosts.
2. Geben Sie die IP-Adressen aller Clients ein, die auf das DL4000 sichern.

Teaming von Netzwerkkarten

Standardmäßig sind die Netzwerkkarten (NICs) auf dem DL4000 Backup to Disk-System 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.**
   Das InstallShield Wizard wird angezeigt.
2. Klicken Sie auf **Weiter**.
3. Klicken Sie auf **Ändern, Hinzufügen oder Entfernen**.
   Das Fenster **Benutzerdefiniertes Setup** 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**.

Erstellen des NIC-Teams

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

So erstellen Sie NIC-Teaming:

1. Wechseln Sie zu **Start → Search → 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 → Zu Team-Ansicht wechseln aus.**
3. Klicken Sie in der **Hosts-Liste** auf der linken Seite mit der rechten Maustaste auf den Host-Namen des DL4000-Systems und wählen Sie **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: Die Erstellung des Teams nimmt etwa 5 Minuten in Anspruch.

4

Installieren von Agenten auf Clients

Auf allen durch das AppAssure-System gesicherten Clients muss der AppAssure-Agent installiert sein. Mittels der AppAssure 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 (PUSH) aufgespielt 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 ebenfalls die Agentensoftware während des Schutzvorgangs der Maschine auf an die Agenten-Maschine bereitstellen. Diese Option ist für Maschinen verfügbar, die die Agentensoftware noch nicht installiert haben. Weitere Informationen zum Bereitstellen der Agentensoftware, während des Schutzes einer Maschine, finden Sie im *DL4000 User's Guide* (Benutzerhandbuch DL4000) unter **dell.com/support/manuals**.

Remote-Installation von Agenten (Push)

So führen Sie eine Remote-Installation (Push) von Agenten durch:

1. Wenn der Client eine Betriebssystemversion ausführt, die älter ist als Windows Server 2012, dann überprüfen Sie, dass auf dem Client das Microsoft.NET4-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 für die Installation eine Kopie von **microsoft.com** beziehen.
2. Überprüfen und/oder ändern Sie den Pfad zu den Agenten-Installationspaketen:
   a) Klicken Sie in der AppAssure-Kern-Konsole auf die Registerkarte **Konfiguration** und klicken Sie anschließend im linken Fensterbereich auf **Einstellungen**.
   b) Klicken Sie im Bereich **Einstellungen anwenden** auf **Ändern**.
   c) Vervollständigen Sie die folgenden Informationen zum Speicherort des Agenten:

Feld	Beschreibung
Agenten-Installationsprogrammname	Spezifiziert den exakten Pfad zum **folder\file** des Agenten.
Kern-Adresse	Spezifiziert die IP-Adresse des Systems, auf dem der AppAssure-Kern ausgeführt wird. **ANMERKUNG:** Standardmäßig ist **Kern-Adresse** unausgefüllt. Das Feld **Kern-Adresse** benötigt keine IP-Adresse, da die Installationsdateien auf dem System installiert werden.

   d) Klicken Sie auf **OK**.
3. Klicken Sie auf die Registerkarte **Extras** und klicken Sie anschließend im linken Fensterbereich auf **Massenbereitstellung**.

ANMERKUNG: Sollte der Client bereits einen Agenten installiert haben, überprüft das Installationsprogramm die Version des Agenten. Ist der von Ihnen hinzugefügte Agent neuer als die installierte Version, bietet Ihnen das Installationsprogramm eine Aktualisierung des Agenten an. Sollte der Host die aktuelle Agentenversion installiert haben, stellt die Massenbereitstellung den Schutz zwischen dem AppAssure-Kern und dem Agenten her.

4. Wählen Sie in der Liste mit den Clients alle Clients aus und klicken Sie auf **Überprüfen**, um sicherzustellen, dass die Maschine aktiv ist und dass der Agent bereitgestellt werden kann.
5. Klicken Sie auf **Bereitstellen**, wenn in der Spalte **Meldung** bestätigt wird, dass die Maschine bereit ist.
6. Wählen Sie die Registerkarte **Ereignisse** aus, um den Status der Bereitstellung zu überprüfen.

   Nach Bereitstellen des Agenten wird automatisch mit einer Sicherung des Clients begonnen.

Bereitstellen der Agent Software bei dem Schutz eines Agenten

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

ANMERKUNG: Dieser Vorgang ist nicht erforderlich, wenn Sie bereits die Agent Software auf einer Maschine, die Sie beschützen wollen, installiert haben.

Zum Bereitstellen der Agenten während des Vorgangs des Hinzufügens eines Agenten zum Schutz:

1. Klicken Sie von dem Dialogfeld **Maschine schützen → Verbinden**, nachdem Sie die entsprechenden Verbindungseinstellungen eingegeben haben, auf **Verbinden**.

   Das Dialogfeld **Agenten bereitstellen** wird angezeigt.
2. Klicken Sie auf **Ja**, um die Agent Software per Remote auf der Maschine bereitzustellen.

   Das Dialogfeld **Agenten bereitstellen** wird angezeigt.
3. Geben Sie die Anmelde- und Schutzeinstellungen, wie folgt ein:

   - **Hostname** - Legt den Hostnamen oder die IP-Adresse der Maschine fest, die Sie schützen möchten.
   - **Schnittstelle** - Bestimmen Sie die Schnittstellennummer auf welcher AppAssure 5 Core mit dem Agenten oder der Maschine kommuniziert. Der Standardwert ist 8006.
   - **Benutzername** - Legt den Benutzernamen, der zur Verbindung dieser Maschine verwendet wird, fest; z. B. administrator.
   - **Kennwort** - Legt das Kennwort, das zur Verbindung dieser Maschine verwendet wird, fest.
   - **Anzeigename** - Legt den Namen für die Maschine, der auf der AppAssure 5 Core-Konsole angezeigt wird, fest. Der Anzeigename kann der gleiche wie der Hostname sein.
   - **Schützen der Maschine nach Installation** - Die Auswahl dieser Option ermöglicht AppAssure 5 ein Basis-Snapshot der Daten, nachdem Sie die Maschine zum Schutz hinzugefügt haben, vorzunehmen. Diese Option ist standardmäßig ausgewählt. Sollten Sie diese Option deaktivieren, müssen Sie ein Snapshot manuell beim Start des Datenschutzes erzwingen. Weitere Informationen zum manuellen Erzwingen eines Snapshots finden Sie unter „Erzwingen eines Snapshots“ in *Dell PowerVault DL4000 User's Guide* (Dell PowerVault DL4000-Benutzerhandbuch) unter **dell.com/support/manuals**.
   - **Repository** - Wählen Sie das Repository aus, in welchem die Daten für diesen Agenten gespeichert werden sollen.

     ANMERKUNG: Sie können Daten von mehreren Agenten in einem einzelnen Repository speichern.
   - **Verschlüsselungsschlüssel** - Bestimmt, ob die Verschlüsselung auf die Daten für jedes in dem Repository gespeicherte Volumen auf dieser Maschine angewendet werden soll.

     ANMERKUNG: Sie können die Verschlüsselungseinstellungen für ein Repository auf der Registerkarte **Konfiguration** in der AppAssure 5-Core-Konsole definieren.

4. Klicken Sie auf **Bereitstellen**.

   Das Dialogfeld **Agenten bereitstellen** wird geschlossen. Es kann zu einer Verzögerung kommen, bevor der ausgewählte Agent in der Liste der geschützten Maschinen aufgeführt wird.

Installieren von Microsoft Windows-Agenten auf dem Client

So installieren Sie die Agenten:

1. Überprüfen Sie, dass auf dem Client das Microsoft .NET4 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 im AppAssure-System das Verzeichnis **C:\install\AppAssure** für den bzw. die Client(s) frei, den bzw. die Sie sichern wollen.
   b) Weisen Sie ein Laufwerk auf dem Client-System **C:\install\AppAssure** auf dem AppAssure-System zu.
   c) Öffnen Sie das Verzeichnis **C:\install\AppAssure** auf dem Client-System und doppelklicken Sie auf den für das System geeigneten Agenten, um mit der Installation zu beginnen.

Hinzufügen eines Agenten durch Verwenden des Lizenzportals

ANMERKUNG: Zum Herunterladen und Hinzufügen von Agenten müssen Sie Administratorrechte besitzen.

So fügen Sie einen Agenten hinzu:

1. Wählen Sie von der **Startseite des AppAssure 5-Lizenzportals** aus eine Gruppe aus und klicken Sie dann auf **Agenten herunterladen**.

   Das Dialogfeld **Agenten herunterladen** wird angezeigt.
2. Klicken Sie neben der Version des Installationsprogramms, die Sie herunterladen möchten, auf **Herunterladen**.

   Folgende Optionen stehen zur Auswahl:

   - 32-Bit Windows-Installationsprogramm
   - 64-Bit Windows-Installationsprogramm
   - 32-Bit Red Hat Enterprise Linux 6.3, 6.4-Installationsprogramm
   - 64-Bit Red Hat Enterprise Linux 6,3, 6.4-Installationsprogramm
   - 32-Bit CentOS 6.3, 6.4-Installationsprogramm
   - 64-Bit CentOS 6,3, 6.4-Installationsprogramm
   - 32-Bit Ubuntu 12.04 LTS, 13.04-Installationsprogramm
   - 64-Bit Ubuntu 12.04 LTS, 13.04-Installationsprogramm
   - 32-Bit SUSE Linux Enterprise Server 11 SP2, SP3-Installationsprogramm
   - 64-Bit SUSE Linux Enterprise Server 11 SP2, SP3-Installationsprogramm
   - Microsoft Hyper-V Server 2012

   ANMERKUNG: Wir unterstützen diese Linux-Bereitstellungen und haben sie unter Verwendung der aktuellsten Kernel-Versionen getestet.

   ANMERKUNG: Agenten installiert auf Microsoft Hyper-V Server 2012 werden in dem Modus „Core Edition" von Windows Server 2012 betrieben.

   Die Datei mit dem **Agenten** wird heruntergeladen.

3. Klicken Sie im Dialogfeld des **Installationsprogramms** auf **Ausführen**.

   ANMERKUNG: Weitere Informationen zum Hinzufügen von Agenten durch Verwendung der Kernmaschine finden Sie unter „Bereitstellen eines Agenten (Push-Installation)“ im *Dell PowerVault DL4000 User's Guide* (Dell PowerVault DL4000-Benutzerhandbuch) unter **dell.com/support/manuals**.

Installieren von Agenten auf Linux-Maschinen

Laden Sie das verteilungsspezifische 32-Bit oder 64-Bit-Installationsprogramm auf alle Linux-Server herunter, die Sie unter Verwendung des AppAssure 5-Kerns schützen wollen. Sie können die Installationsprogramme unter **https://licenseportal.com** vom AppAssure 5-Lizenzportal herunterladen. Beziehen Sie sich für weitere Informationen auf Hinzufügen eines Agenten durch Verwenden des Lizenzportals .

ANMERKUNG: Die Sicherheit beim Schutz einer Maschine basiert in Linux auf dem Pluggable Authentication Module (PAM). Nachdem ein Benutzer unter Verwendung von **libpam** authentifiziert wurde, ist der Benutzer nur dann zum Schutz der Maschine autorisiert, wenn er einer der folgenden Gruppen angehört:

- sudo
- admin
- appassure
- wheel

Beziehen Sie sich für Informationen über den Schutz einer Maschine auf den Abschnitt „Schutz einer Maschine“ im *Dell DL4000 Benutzerhandbuch* auf **dell.com/support/manuals.**

Die Installationsanweisungen sind je nach der von Ihnen verwendeten Linux-Verteilung unterschiedlich. Beziehen Sie sich für weitere Informationen zum Installieren des Linux-Agenten auf Ihrer Verteilung auf folgendes:

- Installieren des Agenten auf Ubuntu 12.04 LTS
- Installieren des Agenten auf Red Hat Enterprise Linux 6.3 und CentOS 6.3
- Installieren des Agenten auf SUSE Linux Enterprise Server 11 SP2

ANMERKUNG: Wir unterstützen diese Linux-Distributionen und haben sie unter den meisten der freigegebenen Kernelversion gestestet.

ANMERKUNG: Die Installation des Linux Agent überschreibt alle Firewall-Regeln, die nicht durch UFW, Yast2 oder **system-config-firewall** angewandt wurden.

Wenn Sie manuell Firewall-Regeln hinzugefügt haben, müssen Sie die AppAssure-Ports nach der Installation manuell hinzufügen. Eine Sicherung der bestehenden Regeln wird unter **/var/lib/appassure/backup.fwl** geschrieben.

Sie müssen die Firewall-Ausnahmen auf allen Servern, die den AppAssure-Agenten zum Zugriff auf den Zugangsagenten für TCP-Ports 8006 und 8009 für den AppAssure 5-Kern verwenden, hinzufügen.

Speicherort der Linux-Agenten-Dateien

Die Linux-Agenten-Dateien befinden sich bei allen Verteilungen in den folgenden Verzeichnissen:

Komponente	Speicherort/Pfad
mono	/opt/appassure/mono
Agent	/opt/appassure/aagent
aamount	/opt/appassure/amount

Komponente	Speicherort/Pfad
aavdisk and aavdctl	/usr/bin
configuration files for aavdisk	/etc/appassure/aavdisk.conf
wrappers for aamount and agent	• /usr/bin/aamount • /usr/bin/aagent
autorun scripts for aavdisk and agent	• /etc/init.d/appassure-agent • /etc/init.d/appassure-vdisk

Agenten-Abhängigkeiten

Die folgenden Abhängigkeiten werden benötigt und werden als Teil des Agenten-Installationsprogrammpakets installiert:

Für Ubuntu	Abhängigkeit
Das appassure-vss benötigt	`dkms, gcc, make, linux-headers-‘uname-r‘`
Das appassure-aavdisk benötigt	`libc6 (>=2.7-18), libblkid1, libpam0g, libpcre3`
Das appassure-mono benötigt	`libc6 (>=2.7-18)`

Für Red Hat Enterprise Linux und CentOS	Abhängigkeit
Das nbd-dkms benötigt	`dkms, gcc, make, kernel-headers-‘uname-r‘ kernel-devel-‘uname-r‘`
Das appassure-vss benötigt	`dkms, gcc, make, kernel-headers-‘uname-r‘ kernel-devel-‘uname-r‘`
Das appassure-aavdisk benötigt	`nbd-dkms, libblkid, pam, pcre`
Das appassure-mono benötigt	`glibc >=2.11`

Für SUSE Linux Enterprise Server	Abhängigkeit
Das nbd-dkms benötigt	`dkms, gcc, make, kernel-syms`
Das appassure-vss benötigt	`dkms, kernel-syms, gcc, make`

Für SUSE Linux Enterprise Server	Abhängigkeit
Das appassure-aavdisk benötigt	`libblkid1, pam, pcre`
Das appassure-mono benötigt	`glibc >=2.11`

Installieren des Agenten auf Ubuntu

ANMERKUNG: Stellen Sie vor dem Durchführen dieser Schritte sicher, dass Sie das Ubuntu-spezifische Installationspaket in das Verzeichnis **/home/system** heruntergeladen haben.

Zum Installieren des AppAssure 5 Agenten auf Ubuntu:

1. Öffnen Sie eine Terminalsitzung mit Root-Zugriff.
2. Geben Sie den folgenden Befehl ein, um das AppAssure 5-Agenten-Installationsprogramm ausführbar zu machen:
   `chmod +x appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh` und drücken Sie anschließend <Eingabe>.
   Die Datei wird ausführbar gemacht.

   ANMERKUNG: Der Name des Installationsprogramms für 32-Bit-Umgebungen lautet **appassureinstaller_ubuntu_i386_5.x.x.xxxxx.sh**
3. Geben Sie den folgenden Befehl ein, um den AppAssure 5-Agenten zu extrahieren und zu installieren:
   `/appassure-installer_ubuntu_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.

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

Nachdem das Installationsprogramm abgeschlossen wurde, wird der Agent auf Ihrem Computer ausgeführt. Lesen Sie den Abschnitt „Schutz von Workstations und Servern“ im *Dell DL4000 User's Guide* (Benutzerhandbuch Dell DL4000) auf **dell.com/support/manuals**, um weitere Informationen über den Schutz dieses Computers durch den Kern zu erhalten.

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** 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 AppAssure 5-Agenten-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 AppAssure 5-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.

Nachdem das Installationsprogramm abgeschlossen wurde, wird der Agent auf Ihrem Computer ausgeführt. Lesen Sie den Abschnitt „Schutz von Workstations und Servern" im *AppAssure 5 User Guide* (Benutzerhandbuch Dell AppAssure) auf **dell.com/support/manuals**, um weitere Informationen über den Schutz dieses Computers durch den Kern zu erhalten.

Installieren des Agenten auf SUSE Linux Enterprise Server

ANMERKUNG: Stellen Sie vor dem Durchführen dieser Schritte sicher, dass Sie das SUSE Linux Enterprise Server (SLES) Installationspaket in das Verzeichnis **/home/system** heruntergeladen haben. Die folgenden Schritte sind für 32-Bit und 64-Bit-Umgebungen gleich.

Zum Installieren des Agenten auf SLES:

1. Öffnen Sie eine Terminalsitzung mit Root-Zugriff.
2. Geben Sie den folgenden Befehl ein, um das AppAssure 5-Agenten-Installationsprogramm ausführbar zu machen:

   `chmod +x appassure-installer_sles_amd64_5.x.x.xxxxx.sh` und drücken Sie anschließend <Eingabe>.

   ANMERKUNG: Der Name des Installationsprogramms für 32-Bit-Umgebungen lautet `appassureinstaller__ sles_i386_5.x.x.xxxxx.sh`

   Die Datei wird ausführbar gemacht.
3. Geben Sie den folgenden Befehl ein, um den AppAssure 5-Agenten zu extrahieren und zu installieren:

   `/appassure-installer_sles_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.
4. Geben Sie bei Aufforderung zum Installieren der neuen Pakete `y` ein und drücken Sie anschließend <Eingabe>.

   Das System schließt den Installationsvorgang ab.

Nachdem das Installationsprogramm abgeschlossen wurde, wird der Agent auf Ihrem Computer ausgeführt. Lesen Sie den Abschnitt „Schutz von Workstations und Servern" im *Dell DL4000 User Guide* (Benutzerhandbuch Dell DL4000) auf **dell.com/support/manuals**, um weitere Informationen über den Schutz dieses Computers durch den Kern zu erhalten.