Dell DL1300 Appliance
Bereitstellungshandbuch

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.

2016 - 05

Rev. A01

Inhaltsverzeichnis

1

Einführung in Dell DL1300

Das System Dell DL1300 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 DL1300 unterstützt Multi-Hypervisor-Umgebungen auf VMware vSphere, Oracle VirtualBox und Microsoft Hyper-V für private und öffentliche Clouds.

Dell DL1300-Kerntechnologien

Ihr Gerät kombiniert die folgenden Technologien:

- Live Recovery
- Universal Recovery
- True Global Deduplication
- Verschlüsselung

Live Recovery

Live Recovery 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 DL1300 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 Recovery

Die Universal Recovery 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 Recovery-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 DL1300 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 DL1300-Datenschutzfunktionen

Dell DL1300-Kern

Der Kern ist die zentrale Komponente der DL1300-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 DL1300 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 DL1300-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 DL1300-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 DL1300 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 – Notfallwiederherstellungsstandort oder Dienstanbieter

Bei der Replikation handelt es sich um einen Prozess des Kopierens der Wiederherstellungspunkte von einem AppAssure-Kern und des Übertragens dieser Punkte auf einen anderen AppAssure-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-Notfallwiederherstellungsstandort. Sie können eine ausgehende Replikation auf ein

unternehmenseigenes Rechenzentrum oder auf einen Remote-Notfallwiederherstellungsstandort (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-Wiederherstellungs-Service 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 DL1300-Kern Wiederherstellungsvorgänge mithilfe von Verified Recovery, Universal Recovery oder Live Recovery.

Recovery-as-a-Service (RaaS)

Anbieter von verwalteten Diensten (MSPs) können DL1300 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), bei der die physischen und virtuellen Server des Kunden zusammen 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 AppAssure-Dienstanbieter konfigurieren. In einem Notfall können die MSPs sofort virtuelle Maschinen für den Kunden bereitstellen.

Das DL1300 selbst ist nicht mandantenfähig. Die MSPs können das DL1300 jedoch an mehreren Standorten verwenden und eine mandantenfähige Umgebung an ihrem Ende erstellen.

Virtualisierung und Cloud

Der DL1300-Kern ist Cloud-fähig und ermöglicht Ihnen, die Rechenkapazität der Cloud für die Wiederherstellung und Archivierung zu nutzen.

Das DL1300 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 DL1300-Bereitstellungsarchitektur

Die DL1300-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 DL1300-Kern verwendet Basisabbilder und inkrementelle Snapshots, um die Wiederherstellungspunkte der geschützten Agenten zu kompilieren.

Darüber hinaus ist das DL1300 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 DL1300 führt die Kürzung des Protokolls des geschützten Microsoft Exchange-Server durch.

Das folgende Diagramm stellt eine einfache DL1300-Bereitstellung dar. DL1300-Agenten sind auf Maschinen installiert, z. B. auf Dateiservern, E-Mail-Servern oder Datenbankservern, oder virtuelle Maschinen sind mit einem einzigen DL1300-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.

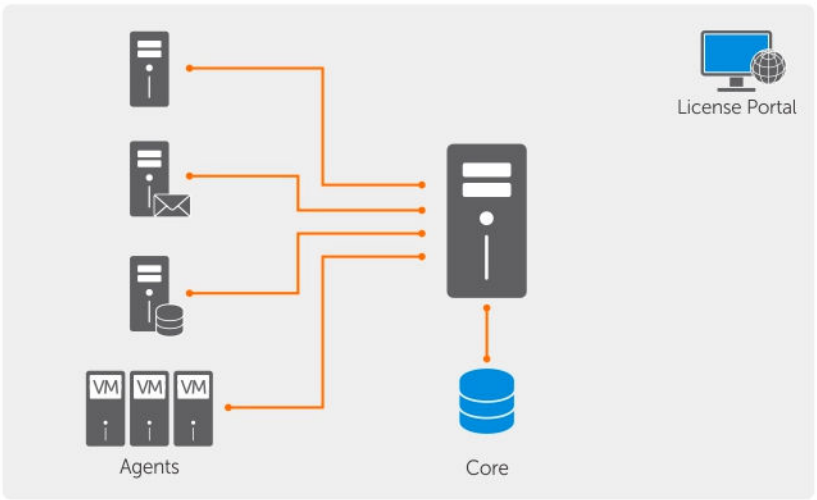

Abbildung 2. Dell DL1300-Bereitstellungsarchitektur

Sie können auch mehrere DL1300-Kerne bereitstellen, wie im folgenden Diagramm beschrieben. Eine zentrale Konsole verwaltet mehrere Kerne.

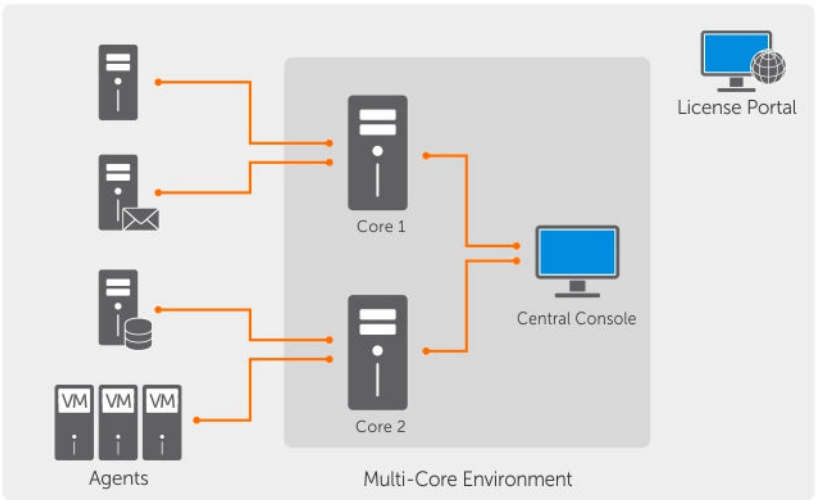

Abbildung 3. DL1300-Bereitstellungsarchitektur mit mehreren Kernen

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 DL1300-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 Ihres Dell DL1300

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
2 TB	Vier 4TB-HDDs mit 2 TB nutzbarem Repository-Speicherplatz
3 TB mit zwei virtuellen Maschinen	Vier 4TB-HDDs mit 3 TB nutzbarem Repository-Speicherplatz und einstellbarem VM-Speicherplatz
4 TB mit zwei virtuellen Maschinen	Vier 4TB-HDDs mit 4 TB nutzbarem Repository-Speicherplatz und einstellbarem VM-Speicherplatz

Jede Konfiguration umfasst die folgende Hard- und Software:

- Dell DL1300-System
- Dell PowerEdge RAID-Controller (PERC)
- Dell AppAssure-Software

Installationsübersicht

Die DL1300-Installation umfasst die Installation des AppAssure-Kerns und der AppAssure 5-Agent-Services auf den Systemen, die geschützt werden sollen. Wenn zusätzliche Kerne eingerichtet werden, müssen die zentralen AppAssure 5-Verwaltungskonsolendienste installiert werden.
Führen Sie zur Installation des DL1300 die folgenden Schritte aus:

1. Besorgen Sie sich den permanenten Lizenzschlüssel ein. Über die Core-Konsole können Sie Ihre DL1300-Lizenzen direkt verwalten, den Lizenzschlüssel ändern und den Lizenzserver kontaktieren. Außerdem können Sie über die Seite „Licensing" (Lizenzierung) der Core-Konsole auf das Dell AppAssure License Portal (Lizenzportal) 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 Software-Voraussetzungen (Konfigurationsassistent für das AppAssure-System).
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

Zur Erzielung einer effizienten Leistung empfiehlt Dell Unternehmen, mit AppAssure Switches mit mindestens 1 GbE zu verwenden.

Einrichten der Hardware

Das Gerät wird mit einem einzelnen DL1300-System geliefert. Lesen Sie das mit dem Gerät gelieferte Handbuch zum Einstieg *Getting Started Guide* für Ihr System. Packen Sie die DL1300-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 DL1300-Hardware ein:

1. Bauen Sie das DL1300-System in ein Rack ein, und verkabeln Sie es.
2. Schalten Sie das DL1300-System ein.

Installieren des DL1300-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 DL1300 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 DL1300 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.

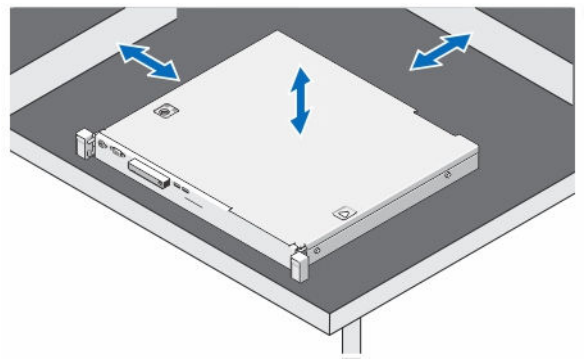

Abbildung 4. Verwenden des Systems ohne ein Rack

Verkabelung des Systems

Lesen Sie das Handbuch zum Einstieg für das DL1300-System *Dell DL1300 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 DL1300-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 des DL1300-Geräts

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

ANMERKUNG: Es wird empfohlen, das System zur Sicherstellung einer maximalen Zuverlässigkeit und Verfügbarkeit an eine unterbrechungsfreie Stromversorgung (USV) anzuschließen. Weitere Informationen finden Sie im Handbuch zum Einstieg für das DL1300-Gerät *Dell DL1300 Getting Started Guide* unter **Dell.com/support/manuals**.

Anfänglicher Software-Setup

Nach dem ersten Einschalten des Geräts und Ändern des Systemkennworts wird automatisch der AppAssure-Konfigurationsassistent**AppAssure Appliance Configuration wizard** 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**.
6. Scrollen Sie von dem Bildschirm **Dell readme.htm** nach unten und klicken Sie auf **Fortfahren**.
   Nach der Eingabe des Kennworts wird der Bildschirm **Drücken Sie STRG+ALT+ENTF, um sich anzumelden** angezeigt.
7. Melden Sie sich mit dem geänderten Administratorkennwort an.
   Der Bildschirm **Sprache für AppAssure-Gerät auswählen** wird angezeigt.
8. Wählen Sie die Sprache für Ihr Gerät aus der Liste der unterstützten Sprachen aus.
   Daraufhin wird das Fenster **EULA** angezeigt.
9. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung, indem Sie auf **EULA akzeptieren** klicken.

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

Der Begrüßungsbildschirm des **AppAssure Appliance Configuration wizard** (AppAssure-Gerätekonfigurationsassistenten) wird angezeigt.

ANMERKUNG: Es kann bis zu 30 Sekunden dauern, bis der **AppAssure Appliance Configuration wizard** (AppAssure-Gerätekonfigurationsassistenten) auf der Systemkonsole angezeigt wird.

AppAssure-Systemkonfigurationsassistent

VORSICHT: Stellen Sie sicher, dass Sie alle Schritte des AppAssure Appliance Configuration Wizard (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 abgeschlossen 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 Configuration wizard** (AppAssure-Gerätekonfigurationsassistent) führt Sie durch die weiteren Schritte zum Konfigurieren der Software im System:

- Konfiguration der Netzwerkschnittstelle
- Konfiguration der Host-Namen- und Domain-Einstellungen

- Konfigurieren der SNMP-Einstellungen

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 DL1300 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.

Recovery and Update Utility

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

RUU besteht aus aktualisierten Versionen von den Windows Server-Rollen und -Funktionen ASP .NET MVC3, LSI-Provider, DL-Anwendungen, OpenManage Server Administrator und App Assure Core-Software. Darüber hinaus aktualisiert das Dienstprogramm Recovery and Update den Rapid Appliance Self Recovery (RASR)-Inhalt.

So laden Sie die aktuellste Version des RUU:

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

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

ANMERKUNG: Wenn Sie RUU # 184 verwenden und Ihr DL-Gerät über eine AppAssure Core-Version vor (älter als) 5.4.3.106 verfügt, wird der Kern auf AppAssure Core 5.4.3.106 aktualisiert.

ANMERKUNG: Wenn Sie auf RUU # 184 aktualisieren, sehen Sie möglicherweise einige Inkonsistenzen in zukünftigen Ausführungen von bereits geplanten Windows-Sicherungen (durch RASR), oder Sie sind möglicherweise nicht in der Lage, eine Windows-Backup-Richtlinie zu erstellen. Diese Inkonsistenzen treten aufgrund von Platzmangel an Ihrem Windows-Backup-Speicherort auf.

Andere potenzielle Ursachen für diese Ausfälle umfassen:

1. Aktualisierung auf Rapid Recovery, besonders, wenn mehr als der minimale Deduplizierungs-Cache verwendet wird.
2. Installation oder Aktualisierung von Software (z. B. Outlook) auf dem Gerät.
3. Installation von Windows-Aktualisierungen.
4. Hinzufügen/Vergrößern von Datendateien (wie z. B. Deduplizierungs-Cache).

5. Kombinationen dieser Vorgänge.

Appliance-Schnellselbstwiederherstellung

Bei der Appliance-Schnellselbstwiederherstellung (Rapid Appliance Self Recovery, RASR) handelt es sich um einen Bare-Metal-Wiederherstellungsprozess, bei dem die Laufwerke des Betriebssystems und die Datenlaufwerke zum Wiederherstellen der Werkseinstellungen herangezogen werden.

Erstellen des RASR-USB-Sticks

So erstellen Sie einen RASR-USB-Speicherstick:

1. Navigieren Sie zur Registerkarte **Appliance** (Gerät).
2. Wählen Sie im Navigationsbereich auf der linken Seite 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 auf **Create RASR USB Drive now** (RASR-USB-Laufwerk jetzt erstellen).

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

   Nachdem Sie die Voraussetzungen überprüft wurden, zeigt das Fenster **Create the RASR USB Drive** (RASR-USB-Laufwerk erstellen) die Mindestgröße für die Erstellung des USB-Laufwerks und **listet alle möglichen Zielpfade** auf.
4. Wählen Sie das Ziel aus, und klicken Sie auf **Create** (Erstellen).

   Es wird ein Warndialogfeld angezeigt.
5. Klicken Sie auf **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. Anderenfalls wird der Inhalt auf dem USB-Stick möglicherweise beschädigt und der USB-Stick funktioniert nicht wie erwartet.

   Entfernen Sie den Stick, kennzeichnen Sie ihn, und heben Sie ihn für die künftige Verwendung auf.

Ausführen von RASR

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

Anhand der folgenden Schritte können Sie die Werkseinstellungen wiederherstellen.

.

So führen Sie die RASR durch:

1. Setzen Sie den erstellten RASR-USB-Schlüssel ein.
2. Führen Sie einen Neustart des Geräts durch, und wählen Sie den Startmanager **Boot Manager (F11)** aus.
3. Wählen Sie im **Hauptmenü des Startmanagers** das Startmenü **One-shot BIOS Boot Menu** 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 Startbildschirm wird angezeigt.
8. Klicken Sie auf **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 **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 **Weiter**.

    Die folgende Warnmeldung wird in einem Dialogfeld angezeigt: `This operation will recover the operating system. All OS disk data will be overwritten` (Durch diesen Vorgang wird das Betriebssystem wiederhergestellt. Alle Daten der BS-Festplatte werden überschrieben).
12. Klicken Sie auf **Ja**.

    Der Betriebssystemdatenträger beginnt mit der Wiederherstellung der Werkseinstellungen.
13. Klicken Sie nach Abschluss des Wiederherstellungsvorgangs im Bildschirm **RASR Completed** (RASR abgeschlossen) auf **Finish** (Fertig stellen).

3

Konfigurieren Ihres Dell DL1300

Konfigurationsübersicht

Die Konfiguration umfasst Aufgaben wie das Konfigurieren von Browsern für den Remote-Zugriff auf die DL1300-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: Während der Verwendung des DL1300 Backup to Disk-Systems wird empfohlen, den Kern über die Registerkarte **Appliance** (Gerät) zu konfigurieren.

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 von dem Bildschirm **Internet Options** (Internetoptionen) die Registerkarte **Security** (Sicherheit).
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 AppAssure 5 Core*> (Hostname oder die IP-Adresse des Geräteservers, der den AppAssure 5-Kern 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 DL1300 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**.

Lizenzverwaltung

Sie können Ihre DL1300-Lizenzen direkt über die Core Console verwalten. Über die Konsole können Sie den Lizenzschlüssel ändern und den Lizenzserver kontaktieren. Sie können das License Portal (Lizenzportal) auch über die Seite Licensing (Lizenzierung) der Core Console unter **https://licenseportal.com** aufrufen.

Die Seite Licensing (Lizenzierung) enthält die folgenden Informationen:

- Lizenztyp
- Lizenzstatus
- Details des Repositorys
- Master-Kerne der Replikation (eingehend)
- Slave-Kerne der Replikation (ausgehend)
- Gleichzeitige Rollups
- Rollup-Aufbewahrungsrichtlinie
- Verschlüsselungscodes
- Virtuelle Standby-Exporte
- Bereitstellungsprüfungen
- Kürzung Exchange-Protokoll
- Kürzung SQL-Protokoll
- Mindestwert für Snapshot-Intervall

Kontaktieren des Lizenzportalservers

Die Core Console kontaktiert den Portalserver, um Änderungen, die im Lizenzportal vorgenommen wurden, zu aktualisieren. Die Kommunikation mit dem Portalserver findet automatisch in bestimmten Intervallen statt. Sie können die Kommunikation jedoch auch bei Bedarf starten.

So kontaktieren Sie den Portalserver:

1. Navigieren Sie zur Core Console, und klicken Sie auf **Configuration (Konfiguration)** → **Licensing (Lizensierung)**.

   Die Seite **Licensing** (Lizenzierung) wird angezeigt.
2. Klicken Sie in der Option **License Server** (Lizenzserver) auf **Contact Now** (Jetzt kontaktieren).

Ändern eines Lizenzschlüssels

So ändern Sie einen Lizenzschlüssel:

1. Navigieren Sie zur Core Console, und wählen Sie **Configuration (Konfiguration)** → **Licensing (Lizenzierung)**aus.

Die Seite **Licensing** (Lizenzierung) wird angezeigt.

2. Klicken Sie auf der Seite **License Details** (Lizenzdetails) auf **Change License** (Lizenz ändern).

   Das Dialogfeld **Change License** (Lizenz ändern) wird angezeigt.

3. Aktualisieren Sie den neuen Lizenzschlüssel wie folgt:
   - Wählen Sie den jeweiligen Lizenzschlüssel aus, indem Sie die Registerkarte **Browse** (Durchsuchen) im Feld `Upload License File` (Lizenzdatei hochladen) verwenden.

     So laden Sie die entsprechende Lizenz herunter:

     1. Wechseln Sie zur Website **www.rapidrecovery.licenseportal.com**.
     2. Wählen Sie im Drop-Down-Menü **Software** oben links die Option **Appliance** (Gerät) aus.

        Alle verfügbaren Lizenzen und die zugehörigen Informationen werden angezeigt.
     3. Klicken Sie in der Spalte **Actions** (Maßnahmen) auf das Symbol für Herunterladen.

        Die Lizenz wird auf Ihr System heruntergeladen.
   - Geben Sie den Lizenzschlüssel in das Feld `Enter License Key` (Lizenzschlüssel eingeben) ein.

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

   Die Lizenz auf Ihrem System wird aktualisiert.

Manuelles Ändern der AppAssure-Sprache

AppAssure ermöglicht Ihnen das Ändern der Sprache, die Sie bei der Ausführung des AppAssure-Gerätekonfigurationsassistenten ausgewählt haben, in eine andere unterstützte Sprache.
So ändern Sie die vorhandene AppAssure-Sprache in die gewünschte Sprache:

1. Starten Sie den Registrierungseditor mit dem Befehl `regedit`.
2. Navigieren Sie zu **HKEY_LOCAL_MACHINE → SOFTWARE → AppRecovery → Core (Kern) → Localization (Lokalisierung)**.
3. Öffnen Sie **Lcid**.
4. Wählen Sie **decimal** (dezimal) aus.
5. Geben Sie den gewünschten Sprachwert in das Datenfeld `Value` (Wert) ein. Folgende Sprachwerte werden unterstützt:

   a. Englisch: 1033
   b. Portugiesisch (Brasilien): 1046
   c. Spanisch: 1034
   d. Französisch: 1036
   e. Deutsch: 1031
   f. Vereinfachtes Chinesisch: 2052
   g. Japanisch: 1041
   h. Koreanisch: 1042
6. Klicken Sie mit der rechten Maustaste, und starten Sie die Dienste in der angegebenen Reihenfolge neu:

   a. Windows-Verwaltungsinstrumentierung
   b. SRM-Webdienst
   c. App Assure-Kern
7. Löschen Sie den Browser-Cache.
8. Schließen Sie den Browser, und starten Sie die Core Console über das Desktop-Symbol neu.

Ändern der Betriebssystemsprache während der Installation

Bei einer laufenden Microsoft Windows-Installation können Sie über die Systemsteuerung Sprachpakete auswählen und zusätzliche internationale Einstellungen konfigurieren.
So ändern Sie die Sprache des Betriebssystems (BS):

ANMERKUNG: Es wird empfohlen, die gleiche Sprache für das Betriebssystem und AppAssure auszuwählen, da anderenfalls bestimmte Meldungen gemischt in zwei unterschiedlichen Sprachen angezeigt werden.

ANMERKUNG: Es wird empfohlen, zuerst die Sprache für das Betriebssystem und dann die für AppAssure zu ändern.

1. Geben Sie auf der Seite **Start** den Eintrag `language` (Sprache) ein, und stellen Sie sicher, dass der Suchumfang auf „Settings" (Einstellungen) gesetzt ist.
2. Wählen Sie im Bereich **Results** (Ergebnisse) den Wert **Language** (Sprache) aus.
3. Wählen Sie im Bereich **Change your language preferences** (Spracheinstellungen ändern) die Option **Add a language** (Sprache hinzufügen) aus.
4. Navigieren Sie zu der Sprache, die Sie installieren möchten, oder suchen Sie nach ihr.

   Wählen Sie z. B. **Catalan** (Katalanisch) aus und dann **Add** (Hinzufügen). Katalanisch wird daraufhin als eine Ihrer Sprachen angezeigt.
5. Wählen Sie im Bereich „Change your language preferences" (Spracheinstellungen andern) die Option **Options** (Optionen) neben der Sprache aus, die Sie hinzugefügt haben.
6. Wenn ein Sprachpaket für Ihre Sprache verfügbar ist, wählen Sie `Download and install language pack` (Sprachpaket herunterladen und installieren) aus.
7. Wenn das Sprachpaket installiert ist, wird die Sprache als verfügbare Anzeigesprache für Windows angezeigt.
8. Um diese Sprache als Anzeigesprache festzulegen, verschieben Sie sie an die erste Stelle der Sprachenliste.
9. Melden Sie sich bei Windows ab und wieder an, damit die Änderung wirksam wird.

Verschlüsseln der Agent Snapshot-Daten

Der Kern kann Agenten-Snapshot-Daten im Repository verschlüsseln. Anstelle einer Verschlüsselung des gesamten Repositorys ermöglicht Ihnen das DL1300 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.

Feld	Beschreibung
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 DL1300 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 DL1300 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.

Textfeld	Beschreibung
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**.

4

Vorbereiten des Schutzes Ihres Servers

Übersicht

Um Ihre Daten mithilfe des DL1300 zu schützen, müssen Sie die zu schützenden Workstations und Server (z. B. Ihren Exchange-Server, den SQL-Server, Linux-Server) zur Kern-Konsole hinzufügen.

In der Kern-Konsole können Sie die Maschine bestimmen, 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 Kern-Konsole für den Schutz von Workstations und Servern finden Sie unter Schützen von Maschinen.

Schützen von Maschinen

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

So schützen Sie eine Maschine:

1. Wechseln Sie zur Kern-Konsole und wählen Sie die Registerkarte **Machines** (Maschinen) aus.
2. Klicken Sie im Drop-Down-Menü **Actions** (Maßnahmen) auf **Protect Machine** (Maschine schützen).

   Das Dialogfeld **Connect** (Verbinden) wird angezeigt.
3. Geben Sie die Informationen über die Maschine, mit der Sie Verbindung aufnehmen wollen, im Dialogfeld **Connect** (Verbinden) ein, wie in der folgenden Tabelle beschrieben.

Host	Der Hostname oder die IP-Adresse der Maschine, die Sie schützen möchten.
Schnittstelle	Die Schnittstellennummer, über die der 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 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 DL1300-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 DL1300-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 DL1300 sichern.

Teaming von Netzwerkkarten

Standardmäßig sind die Netzwerkkarten (NICs) auf der DL1300 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 DL1300-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.

Einstellen gleichzeitiger 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.

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 die Agent-Software außerdem während des Schutzvorgangs der Maschine für die Agent-Maschine bereitstellen. Diese Option ist für Maschinen verfügbar, auf denen die Agent-Software noch nicht installiert ist. Weitere Informationen zum Bereitstellen der Agent-Software während des Schutzes einer Maschine finden Sie im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**.

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.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 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 beim Schutz einer Maschine

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. Navigieren Sie zu **Protect Machine** (Maschine schützen) → **Connect** (Verbinden), nachdem Sie die entsprechenden Verbindungseinstellungen im Dialogfeld eingegeben haben.
2. Klicken Sie auf **Connect** (Verbinden).

   Das Dialogfeld **Deploy Agent** (Agenten bereitstellen) wird angezeigt.
3. Klicken Sie auf **Yes** (Ja), um die Agent Software per Remote auf der Maschine bereitzustellen.

   Das Dialogfeld **Deploy Agent** (Agenten bereitstellen) wird angezeigt.
4. Geben Sie die Anmelde- und Schutzeinstellungen wie folgt ein:
   - **Host name** (Hostname) - Legt den Hostnamen oder die IP-Adresse der Maschine fest, die Sie schützen möchten.
   - **Port** (Port) – Legt die Portnummer fest, auf der der Kern mit dem Agenten auf der Maschine kommuniziert. Der Standardwert ist 8006.
   - **User name** (Benutzername) - Legt den Benutzernamen, der zum Verbinden der Maschine verwendet wird, fest; z. B. administrator.

- **Passwort** (Kennwort) - Legt das Kennwort, das zur Verbindung dieser Maschine verwendet wird, fest.
- **Display name** (Anzeigename) – Name der Maschine, die auf der Kern-Konsole angezeigt wird. Der Anzeigename kann der gleiche Name sein wie der Hostname.
- **Protect machine after install** (Maschine nach der Installation schützen) – Wenn Sie diese Option auswählen, kann das DL1300 einen Basis-Snapshot der Daten erstellen, nachdem Sie die Maschine zum Schutz hinzugefügt haben. Diese Option ist standardmäßig ausgewählt. Sollten Sie diese Option deaktivieren, müssen Sie einen Snapshot manuell beim Start des Datenschutzes erzwingen. Weitere Informationen zum manuellen Erzwingen eines Snapshots finden Sie unter „Forcing A Snapshot" (Erzwingen eines Snapshots) im DL1300-Benutzerhandbuch*Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**.
- **Repository** (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.
- **Encryption Key** (Verschlüsselungsschlüssel) - Bestimmt ob die Verschlüsselung auf die Daten für jedes in dem Repository gespeicherte Volumen auf dieser Maschine angewendet werden soll.

  ANMERKUNG: Sie können Verschlüsselungseinstellungen für ein Repository auf der Registerkarte **Configuration** (Konfiguration) in der Core Console definieren.

5. Klicken Sie auf **Deploy** (Bereitstellen).

   Das Dialogfeld **Deploy Agent** (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 .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 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**.

   Es wird das Dialogfeld **Download Agent** angezeigt.

2. Klicken Sie neben der Version des Installationsprogramms, die Sie herunterladen möchten, auf **Download** (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: Dell unterstützt die oben aufgeführten Linux-Distributionen, wobei die veröffentlichten Kernel-Versionen getestet wurden.

   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 unter Verwendung der Kernmaschine finden Sie unter „Deploying An Agent (Push Install)" (Bereitstellen eines Agenten (Push-Installation)) im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**.

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 Kerns schützen wollen. Sie können die Installationsprogramme unter **https://licenseportal.com** vom Lizenzportal herunterladen. Weitere Informationen finden Sie unter 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

Weitere Informationen zum Schützen einer Maschine finden Sie im Abschnitt „Protecting a Machine" (Schützen einer Maschine) im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**.

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
- Installation des Agenten auf Red Hat Enterprise Linux und CentOS
- Installieren des Agenten auf SUSE Linux Enterprise Server

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 Agenten zum Zugriff auf den Zugangsagenten für TCP-Ports 8006 und 8009 für den 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
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

Komponente	Speicherort/Pfad
	• /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`
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 directory** heruntergeladen haben.

Zum Installieren des Agenten auf Ubuntu:

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_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 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: Informationen zu den durch den Agenten benötigten Dateien finden Sie unter Agenten-Abhängigkeiten.

Nachdem der Installationsprozess abgeschlossen ist, wird der Ubuntu-Agent auf Ihrem Computer installiert. Lesen Sie den Abschnitt „Protecting Workstations and Servers“ (Schützen von Workstations und Servern) im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter DL1300, um weitere Informationen zum 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 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.

Informationen zu den durch den Agenten benötigten Dateien finden Sie unter Agenten-Abhängigkeiten.

Nachdem das Installationsprogramm abgeschlossen wurde, wird der Agent auf Ihrem Computer ausgeführt. Lesen Sie das Thema „Protecting Workstations and Servers" (Schützen von Workstations und Servern) im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter DL1300, um weitere Informationen zum 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 directory** 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 DL1300-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 DL1300-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.

   Informationen zu den durch den Agenten benötigten Dateien finden Sie unter Agenten-Abhängigkeiten.
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 der Maschine ausgeführt. Lesen Sie den Abschnitt „Protecting Workstations and Servers" (Schutz von Workstations und Servern) im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**, um weitere Informationen zum Schutz dieser Maschine mit dem Kern zu erhalten.

5

Allgemeine Anwendungsfälle

In diesem Abschnitt werden die häufigsten Anwendungsbeispiele für das DL1300-System und eine allgemeine Übersicht über die Informationen und Vorgehensweisen für die einzelnen Szenarios vorgestellt. Soweit erforderlich, sind Verweise auf weitere Informationen angegeben.

Schützen von Maschinen

Die AppAssure Sicherungs- und Replikationstechnologie bietet einen erweiterten Schutz von VMs oder Servern und gleichzeitig eine flexible Wiederherstellung von Anwendungen und Daten. Wenn eine Maschine geschützt ist, werden vollständige und inkrementelle Snapshots erfasst und im Kern-Repository gespeichert. Der AppAssure-Schutzvorgang nutzt zwei zentrale Technologien, die im Folgenden näher beschrieben werden: Snapshots und den Dell DL1300 Smart Agent.

Snapshots

Der AppAssure Agent für Windows verwendet den Microsoft Volumeschattenkopie-Dienst (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 wird, 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. Weitere Informationen finden Sie im Thema Snapshot-Prozess.

Dell DL1300 Smart Agents

Der Smart Agent ist auf den Maschinen installiert, die durch den DL1300-Kern geschützt werden. Er überwacht die geänderten Blöcke auf dem Festplatten-Volume und erstellt in einem vordefinierten Schutzintervall ein Snapshot-Abbild der geänderten Blöcke. Durch das Konzept fortlaufender inkrementeller Snapshots auf Blockebene wird das wiederholte Kopieren der gleichen Daten von der geschützten Maschine auf den Kern verhindert. Wenn der Snapshot bereit ist, wird er mithilfe von intelligenten mehrinstanzfähigen, socketbasierten Verbindungen schnell auf den Kern übertragen. Weitere Informationen finden Sie unter dem Thema Dell DL1300 Smart Agent.

Bereitstellen von Smart Agenten

Sie müssen den AppAssure-Agenten auf jeder vom DL1300-Kern geschützten Maschine in der Umgebung installieren.

ANMERKUNG: Die folgenden Verfahren stellen lediglich eine Übersicht dar. Detaillierte Informationen und spezifische Anleitungen für Linux-Agenten finden Sie im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide*.

Schritt 1: Beziehen der Agent-Software

Die Smart Agent-Software kann auf eine der folgenden Vorgehensweisen bezogen werden:

- **Herunterladen vom AppAssure-Kern** – Melden Sie sich an der Kern-Konsole an, und laden Sie die Software auf die Agent-Maschine herunter. Klicken Sie auf der Registerkarte **Tools** (Extras) auf **Downloads**, und laden Sie dann das Web-Installationsprogramm für die Agent-Komponente herunter.
- **Herunterladen vom AppAssure-Lizenzportal** – Wenn Sie die Software im Dell Software-Lizenzportal registriert haben, können Sie sich am Lizenzportal anmelden und die Software auf die Agent-Maschine herunterladen.
- **Bereitstellen der Agent-Software beim Schutz einer Maschine** – Sie können die Agent-Software mit dem **Protect a Machine Wizard** (Assistenten zum Schützen einer Maschine) auf der Maschine bereitstellen, die Sie schützen möchten.
- **Verwenden der Funktion zur Massenbereitstellung** – Wenn der Kern installiert ist, können Sie die Agent-Software auf mehreren Maschinen bereitstellen, indem Sie die Funktion **Bulk deploy** (Massenbereitstellung) verwenden, die in der Kern-Konsole auf der Registerkarte **Tools** (Extras) verfügbar ist.

Schritt 2: Installieren der Agent-Software

Starten Sie das Installationsprogramm wie unten stehend beschrieben, um die Software auf jeder Maschine zu installieren, die Sie im Kern schützen möchten. So installieren Sie die Agent-Software auf Windows-Maschinen:

1. Doppelklicken Sie auf der Maschine, die Sie schützen möchten, auf die Installationsdatei für den Agenten.
2. Klicken Sie auf der Seite **Welcome** (Willkommen) auf **Next** (Weiter), um die Installation fortzusetzen.
3. 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 dann auf **Next** (Weiter).

   ANMERKUNG: Das Agent-Installationsprogramm überprüft, ob die erforderlichen Dateien vorhanden sind. Falls die erforderlichen Dateien nicht vorhanden sind, ermittelt das Agent-Installationsprogramm, welche Dateien benötigt werden und zeigt die Ergebnisse entsprechend an, z. B.: Microsoft System CLR-Typen für SQL Server 2008 R2 (x64).
4. Klicken Sie auf **Install Prerequisites** (Voraussetzungen installieren).
5. Wenn die Installation der erforderlichen Dateien abgeschlossen ist, klicken Sie auf **Next** (Weiter).
6. Überprüfen Sie auf der Seite **Installation Options** (Installationsoptionen) die Installationsoptionen. Falls erforderlich, ändern Sie sie wie unten beschrieben:
   a. 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, und klicken Sie auf **OK**.
   b. Geben Sie im Textfeld **Port Number** (Schnittstellennummer) eine Schnittstellennummer ein, die für die Kommunikation zwischen dem Agenten und dem Kern verwendet werden soll.

      ANMERKUNG: Der Standardwert ist 8006. Wenn Sie die Schnittstellennummer ändern, notieren Sie sich diese für den Fall, dass Sie die Konfigurationseinstellungen später ändern müssen.

7. Überprüfen Sie die Installationsoptionen, und klicken Sie auf **Install** (Installieren). Nach Abschluss der Installation wird die Seite **Completed** (Abgeschlossen) angezeigt.
8. Wählen Sie eine der folgenden Optionen, und klicken Sie anschließend auf **Finish** (Fertig stellen): Yes, I want to restart my computer now (Ja, Computer jetzt neu starten). No, I will restart my computer later (Nein, Computer später neu starten).

ANMERKUNG: Sie müssen das System neu starten, bevor Sie die Agent-Software verwenden können.

Konfigurieren von Schutz-Jobs

Wenn Sie Schutz hinzufügen, müssen Sie Informationen über die Verbindung definieren, z. B. die IP-Adresse und die Schnittstelle, sowie die Anmeldeinformationen für die Maschine eingeben, die Sie schützen möchten. Optional können Sie einen Anzeigenamen eingeben, der in der Kern-Konsole anstelle der IP-Adresse angezeigt wird. Sie können auch den Zeitplan für den Schutz der Maschine definieren.

ANMERKUNG: Die folgenden Verfahren stellen lediglich eine Übersicht dar. Detaillierte Informationen finden Sie im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**.

Schützen einer Maschine

In diesem Thema wird beschrieben, wie Sie beginnen können, die Daten auf einer von Ihnen angegebenen Maschine zu schützen.

ANMERKUNG: Damit eine Maschine geschützt werden kann, muss auf ihr die AppAssure Agent-Software installiert sein. Sie können die Agent-Software vor diesem Vorgang installieren oder aber dem Agenten die Software bereitstellen, wenn Sie im Dialogfeld **Connection** (Verbindung) den Schutz definieren. Informationen zur Installation der Agent-Software während des Vorgangs zum Schützen einer Maschine finden Sie im Abschnitt „Deploying The Agent Software When Protecting An Agent'" (Bereitstellen der Agent-Software beim Schutz eines Agenten) im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide*.

Wenn Sie die Maschine um Schutz ergänzen, müssen Sie den Namen oder die IP-Adresse der zu schützenden Maschine und die Volumes auf dieser Maschine angeben sowie den Schutzzeitplan für jedes Volume definieren.

Informationen zum Schützen mehrerer Maschinen gleichzeitig finden Sie im Abschnitt über den Schutz von mehreren Maschinen im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide*.

So schützen Sie eine Maschine:

1. Starten Sie die Maschine neu, auf dem die AppAssure-Agentensoftware installiert ist, wenn Sie dies nicht bereits getan haben.
2. Klicken Sie in der Core-Konsole auf der Kern-Maschine auf der Symbolleiste auf die Optionen **Protect (Schützen)** → **Protect Machine** (Maschine schützen).

   Der **Protect Machine Wizard** (Assistent zum Schützen einer Maschine) wird angezeigt.
3. 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 nicht möchten, dass die Seite **Welcome** (Willkommen) des **Protect Machine Wizard** (Assistent zum Schützen einer Maschine) in Zukunft angezeigt wird, wählen Sie die Option **Skip this Welcome page the next time the wizard opens** (Willkommen-Seite überspringen, wenn der Assistent beim nächsten Mal aufgerufen wird).

4. Klicken Sie auf **Weiter**.
5. Geben Sie auf der Seite **Connection** (Verbindung) die Informationen zu der Maschine ein, zu dem Sie eine Verbindung herstellen möchten. Richten Sie sich dabei an die folgenden Tabelle:

Textfeld	Beschreibung
Host	Der Hostname oder die IP-Adresse der Maschine, die Sie schützen möchten.
Schnittstelle	Die Portnummer, über die der AppAssure-Kern mit der Maschine kommuniziert. Der standardmäßige Port ist 8006.
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.

6. Klicken Sie auf **Next** (Weiter). Wenn als nächstes die Seite **Protection** (Schutz) im **Protect Machine Wizard** (Assistenten zum Schützen einer Maschine) angezeigt wird, fahren Sie fort mit Schritt 7.

   ANMERKUNG: Wenn die Seite **Install Agent** (Agent installieren) als Nächstes im **Assistenten zum Schützen des Rechners** angezeigt wird, bedeutet dies, dass die Agentensoftware noch nicht auf der designierten Maschine installiert ist. Klicken Sie auf **Next** (Weiter), um die Agentensoftware zu installieren. Die Agentensoftware muss auf der Maschine installiert sein, die Sie schützen möchten; diese muss neu gestartet werden, bevor sie auf dem Kern gesichert werden kann. Damit das Installationsprogramm der Agentenmaschine neu starten kann, wählen Sie die Option **After installation, restart the machine automatically (recommended)** (Maschine nach Abschluss der Installation automatisch neu starten (empfohlen)) aus, und klicken Sie dann auf **Next** (Weiter).
7. Der Hostname oder die IP-Adresse, die Sie im Dialogfeld **Connect** (Verbinden) angegeben haben, erscheint in diesem Dialogfeld. Geben Sie optional einen neuen Namen für die Maschine ein, die in der Core Console angezeigt werden soll.
8. Wählen Sie den entsprechenden Zeitplan für den Schutz aus:
   - Um den Standard-Schutzzeitplan zu verwenden, wählen Sie unter **Schedule Settings** (Zeitplaneinstellungen) die Option **Default protection (hourly snapshots of all volumes)** (Standard-Schutz (Erstellung von 3-Stunden-Snapshots von allen Volumes) aus. Bei einem Standard-Schutzzeitplan erstellt der Kern alle drei Stunden Snapshots der Agentenmaschine. Snapshots der Agentenmaschine können mindestens einmal pro Stunde erstellt werden. Zum Ändern der Sicherheitseinstellungen zu einem beliebigen Zeitpunkt, nachdem Sie den Assistenten geschlossen haben, einschließlich der Entscheidung, welche Volumes geschützt werden sollen, gehen Sie zu der Registerkarte „Summary" (Zusammenfassung) für die jeweilige Agentenmaschine.
   - Um einen anderen Schutzzeitplan zu definieren, wählen Sie unter **Schedule Settings** (Zeitplaneinstellungen) die Option **Custom Protection** (Benutzerdefinierter Schutz) aus.
9. Wählen Sie eine der folgenden Optionen:
   - Wenn Sie im **Protect Machine Wizard** (Assistenten zum Schützen einer Maschine) „Typical configuration" (Typische Konfiguration) ausgewählt und Standard-Schutz angegeben haben, klicken Sie anschließend auf **Finish** (Fertig stellen), um die Auswahl zu bestätigen, den Assistenten zu schließen und die angegebene Maschine zu schützen.
   - Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, beginnt ein Basisabbild (welches ein Snapshot aller Daten im geschützten Volume ist) sofort mit der Übertragung zum Repository auf dem Kern, außer, wenn Sie angegeben haben, anfänglich den Schutz anzuhalten.
   - Wenn Sie eine typische Konfiguration für den **Protect Machine Wizard** (Assistenten zum Schützen der Maschine) ausgewählt und einen benutzerdefinierten Schutz angegeben haben, klicken Sie auf **Next** (Weiter), um einen benutzerdefinierten Schutzzeitplan einzurichten. Weitere Informationen über das Definieren eines benutzerdefinierten Schutzzeitplans finden Sie unter „Erstellen von benutzerdefinierten Schutzzeitplänen".

- Wenn Sie „Advanced Configuration" (Erweiterte Konfiguration) für den **Protect Machine Wizard** (Assistenten zum Schützen der Maschine) und den Standardschutz ausgewählt haben, klicken Sie auf **Next** (Weiter), und fahren Sie mit Schritt 12 fort, um die Repository- und Verschlüsselungsoptionen anzuzeigen.
- Wenn Sie „Advanced configuration" (Erweiterte Konfiguration) im **Protect Machine Wizard** (Assistenten zum Schützen einer Maschine) und benutzerdefinierten Schutz ausgewählt haben, klicken Sie auf **Next** (Weiter), und fahren Sie mit Schritt 10 fort, um auszuwählen, welche Volumes geschützt werden sollen.

10. Wählen Sie auf der Seite **Protection Volumes** (Schutz-Volumes) die Volumes auf der Agent-Maschine aus, die Sie schützen möchten. Wenn Volumes aufgelistet sind, die Sie nicht in den Schutz aufnehmen möchten, klicken Sie in die Spalte zum Ankreuzen, um die Auswahl zu löschen. Klicken Sie anschließend auf **Next** (Weiter).

    ANMERKUNG: Es wird empfohlen, das durch das System reservierte Volume und das Volume mit dem Betriebssystem (in der Regel Laufwerk C) zu schützen.

11. Definieren Sie auf der Seite **Protection Schedule** (Schutzzeitplan) einen benutzerdefinierten Schutzzeitplan.
12. Wählen Sie auf der Seite **Repository** (Repository) die Option **Use an existing repository** (Vorhandenes Repository verwenden) aus.
13. Klicken Sie auf **Weiter**.

    Die Seite **Encryption** (Verschlüsselung) wird angezeigt.
14. Klicken Sie ggf. zum Aktivieren der Verschlüsselung auf **Enable Encryption** (Verschlüsselung aktivieren).

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

    ANMERKUNG: Wenn Sie die Verschlüsselung aktivieren, wird diese auf die Daten aller geschützten Volumes für diese Agentenmaschine angewendet. Sie können die Einstellungen später auf der Registerkarte „Configuration" (Konfiguration) in der AppAssure 5 Core-Konsole ändern.

    VORSICHT: AppAssure verwendet eine 256-Bit-AES-Verschlüsselung im CBC-Modus (Cipher Block Chaining) mit 256-Bit-Schlüsseln. Die Verwendung der Verschlüsselung ist optional, Dell empfiehlt jedoch dringend, dass Sie einen Verschlüsselungsschlüssel aufbauen und dass Sie die von Ihnen definierte Passphrase schützen. Speichern Sie die Passphrase an einem sicheren Ort, da sie für die Datenwiederherstellung von zentraler Bedeutung ist. Ohne Passphrase ist die Datenwiederherstellung nicht möglich.
15. Geben Sie die in der folgenden Tabelle beschriebenen Informationen ein, um einen Verschlüsselungsschlüssel für den Kern hinzuzufügen.

Textfeld	Beschreibung
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein.
Beschreibung	Geben Sie eine Beschreibung ein, um zusätzliche Details für den Verschlüsselungsschlüssel bereitzustellen.
Passphrase	Geben Sie die Passphrase zur Steuerung des Zugriffs ein.
Passphrase bestätigen	Geben Sie zuvor eingegebene Passphrase erneut ein.

16. Klicken Sie auf **Finish** (Fertig stellen), um Ihre Einstellungen zu speichern und zu übernehmen.

Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, beginnt ein Basisabbild (welches ein Snapshot aller Daten im geschützten Volume ist) sofort mit der Übertragung zum Repository auf dem AppAssure-Kern, außer, wenn Sie angegeben haben, anfänglich den Schutz anzuhalten.

Wiederherstellen von Daten

Mit dem DL1300 können Daten sowohl auf Windows- als auch auf Linux-Maschinen geschützt werden. Sicherungen geschützter Maschinen werden als Wiederherstellungspunkte im Kern gespeichert. Mit diesen können Ihre Daten wiederhergestellt werden. Ganze Volumes können von einem Wiederherstellungspunkt auf den Ziel-Maschinen wiederhergestellt und ausgetauscht werden. Zum Wiederherstellen von Daten anhand von Wiederherstellungspunkten kann eines der folgenden Verfahren ausgeführt werden:

- Wiederherstellung von Dateien und Ordnern
- Wiederherstellung von Datenvolumes mithilfe von Live Recovery
- Bare-Metal-Wiederherstellung mithilfe von Universal Recovery

Wiederherstellen von Verzeichnissen oder Dateien

Sie können Windows-Explorer verwenden, um Verzeichnisse und Dateien von einem bereitgestellten Wiederherstellungspunkt auf eine Windows-Maschine zu kopieren. Dies kann hilfreich sein, wenn Sie nur einen Teil eines Wiederherstellungspunkts für Benutzer freigeben möchten. Wenn Sie Verzeichnisse und Dateien kopieren, werden die Zugriffsberechtigungen des Benutzers verwendet, der den Kopiervorgang ausführt und auf die eingefügten Verzeichnisse und Dateien angewendet.
So stellen Sie ein Verzeichnis oder eine Datei mithilfe von Windows-Explorer wieder her:

1. Stellen Sie den Wiederherstellungspunkt bereit, der die wiederherzustellenden Daten enthält. Weitere Informationen finden Sie im Abschnitt zum Bereitstellen eines Wiederherstellungspunktes für eine Windows-Maschine im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide*.
2. Navigieren Sie in Windows Explorer zum bereitgestellten Wiederherstellungspunkt und wählen Sie die Verzeichnisse und Dateien aus, die Sie wiederherstellen möchten. Klicken Sie mit der rechten Maustaste, und wählen Sie **Copy** (Kopieren) aus.
3. Navigieren Sie im Windows-Explorer zur Maschine, auf der die Daten wiederhergestellt werden sollen. Klicken Sie mit der rechten Maustaste, und wählen Sie **Paste** (Einfügen) aus.

Wiederherstellen von Volumes

Von der Kern-Konsole können Sie ganze Volumes von einem systemfremden Wiederherstellungspunkt wiederherstellen, wobei die Volumes auf der Ziel-Maschine ersetzt werden.

ANMERKUNG: Das folgende Verfahren stellt eine vereinfachte Übersicht über das Wiederherstellungsverfahren dar. Ausführliche Informationen und Verfahren für zusätzliche Wiederherstellungsoptionen finden Sie im Abschnitt zum Wiederherstellen von Volumes anhand eines Wiederherstellungspunkts im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide*.

So stellen Sie Volumes aus einem Wiederherstellungspunkt wieder her:

1. Klicken Sie in der Core Console auf die Registerkarte **Restore** (Wiederherstellen).

   Der **Restore Machine Wizard** (Assistent zum Wiederherstellen einer Maschine) wird angezeigt.
2. Wählen Sie auf der Seite **Protected Machines** (Geschützte Maschinen) die geschützte Maschine aus, für die Sie Daten wiederherstellen möchten, und klicken Sie dann auf **Next** (Weiter).

ANMERKUNG: Auf der geschützten Maschine muss die Agentensoftware installiert sein, und Sie müssen über Wiederherstellungspunkte verfügen, von denen aus Sie die Wiederherstellung durchführen.

Die Seite **Recovery Points** (Wiederherstellungspunkte) wird angezeigt.

3. Suchen Sie in der Liste der Wiederherstellungspunkte den Snapshot, den Sie auf der Agentenmaschine wiederherstellen möchten.

   ANMERKUNG: Falls erforderlich, verwenden Sie die Navigationsschaltflächen am unteren Rand der Seite, um zusätzliche Wiederherstellungspunkte anzuzeigen. Wenn Sie die Anzahl der Wiederherstellungspunkte auf der Seite „Recovery Points" (Wiederherstellungspunkte) des Assistenten begrenzen möchten, können Sie nach Volumes (falls definiert) oder nach Datum der Erstellung des Wiederherstellungspunkts filtern.

4. Klicken Sie auf einen beliebigen Wiederherstellungspunkt, um ihn auszuwählen, und klicken Sie dann auf **Next** (Weiter).

   Die Seite **Destination** (Ziel) wird angezeigt.

5. Wählen Sie auf der Seite **Destination** (Ziel) die Maschine aus, die Sie wiederherstellen möchten. Gehen Sie dabei wie folgt vor:

   - Wenn Sie Daten vom ausgewählten Wiederherstellungspunkt auf der gleichen Agent-Maschine (z. B. Maschine1) wiederherstellen möchten, und wenn die Volumes, die Sie wiederherstellen möchten, nicht das System-Volume enthalten, wählen Sie **Recover to a protected machine (only non-system volumes)** (Wiederherstellung zu einer geschützten Maschine (ohne System-Volume)), überprüfen Sie, ob die Ziel-Maschine (Maschine1) ausgewählt ist, und klicken Sie dann auf **Next** (Weiter). Die Seite „Volume-Mapping" (Volume-Zuweisung) wird angezeigt. Fahren Sie fort mit Schritt 6.
   - Wenn Sie Daten vom ausgewählten Wiederherstellungspunkt auf einer anderen geschützten Maschine wiederherstellen möchten, z. B. wenn Sie den Inhalt von Maschine2 durch die Daten von Maschine1 ersetzen möchten, wählen Sie **Wiederherstellung auf einer geschützten Maschine (nur Nicht-System-Volumes)**, wählen Sie die Ziel-Maschine (z. B. Maschine2) aus der Liste aus, und klicken Sie dann auf **Weiter**. Die Seite „Volume-Zuweisung" wird angezeigt. Fahren Sie fort mit Schritt 6.
   - Wenn Sie von einem Wiederherstellungspunkt zu einem System-Volume wiederherstellen möchten (z. B. Laufwerk C: der Agent-Maschine mit dem Namen Maschine1), müssen Sie eine Bare-Metal-Wiederherstellung durchführen.

6. Wählen Sie auf der Seite „Volume-Zuweisung" für jedes Volume im Wiederherstellungspunkt, das Sie wiederherstellen möchten, das entsprechende Ziel-Volume aus. Falls Sie kein Volume wiederherstellen möchten, wählen Sie in der Spalte „Ziel-Volumes" die Option **Do not restore** (Nicht wiederherstellen) aus.

7. Wählen Sie **Show advanced options** (Erweiterte Optionen anzeigen) aus, und führen Sie dann die folgenden Schritte aus:

   - Für Informationen zum Wiederherstellen auf Windows-Maschinen mit Live Recovery wählen Sie **Live Recovery** (Live Recovery) aus.

     Mithilfe der Live Recovery-Technologie zur Sofortwiederherstellung in AppAssure 5 können Sie Daten von gespeicherten Wiederherstellungspunkten für Windows-Maschinen sofort auf Ihren physischen Maschinen oder auf virtuellen Maschinen wiederherstellen, einschließlich Microsoft Windows Storage Spaces. Live Recovery ist für Linux-Computer nicht verfügbar.
   - Wenn Sie die Aufhebung der Bereitstellung erzwingen möchten, wählen Sie **Force Dismount** (Erzwungene Aufhebung der Bereitstellung) aus.

     Wenn Sie vor der Wiederherstellung von Daten eine Aufhebung der Bereitstellung nicht erzwingen, schlägt die Wiederherstellung mit einem Fehler, dass das Volume derzeit verwendet wird, unter Umständen fehl.

Wenn die Agent-Maschine von der Start-CD aus gestartet wird, wird die Universal Recovery Console (URC-)-Schnittstelle angezeigt. Diese Umgebung wird zur Wiederherstellung des Systemlaufwerks oder ausgewählter Volumes direkt vom Kern verwendet. Beachten Sie die IP-Adresse und den Authentifizierungsschlüssel im URC, die jedes Mal dann aktualisiert werden, wenn Sie von der Start-CD aus starten.

8. Wenn die Volumes, die Sie wiederherstellen möchten, SQL- oder Microsoft Exchange-Datenbanken enthalten, werden Sie auf der Seite **Dismount Databases** (Bereitstellung von Datenbanken aufheben) dazu aufgefordert, die Bereitstellung aufzuheben. Alternativ können Sie, wenn Sie diese Datenbanken nach Abschluss der Wiederherstellung erneut mounten, die Option **Automatically remount all databases after the recovery point is restored** (Alle Datenbanken nach der Wiederherstellung des Wiederherstellungspunktes automatisch erneut mounten) auswählen. Klicken Sie auf **Finish** (Fertig stellen).
9. Klicken Sie auf **OK**, um die Statusmeldung, dass der Wiederherstellungsprozess gestartet wurde, zu bestätigen.
10. Um den Fortschritt der Wiederherstellung zu überwachen, klicken Sie in der Core Console auf **Events** (Ereignisse).

Bare-Metal-Wiederherstellung

Mit AppAssure können Sie eine Bare-Metal-Wiederherstellung (BMR) für Windows- oder Linux-Maschinen durchführen. BMR ist ein Prozess, bei dem die gesamte Software-Konfiguration für ein spezifisches System wiederhergestellt wird. Der Begriff „Bare-Metal" bezieht sich darauf, dass beim Wiederherstellungsvorgang nicht nur die Daten vom Server wiederhergestellt, sondern auch das Festplattenlaufwerk neu formatiert und das Betriebssystem sowie alle Anwendungen neu installiert werden. Bei der Ausführung einer BMR geben Sie einen Wiederherstellungspunkt auf einer geschützten Maschine an und führen ein Rollback auf die angegebene physische oder virtuelle Maschine aus. Eine Bare-Metal-Wiederherstellung kommt u. a. auch dann in Frage, wenn Hardware-Aktualisierungen oder der Austausch eines Servers anstehen.

Eine BMR kann für physische oder virtuelle Maschinen durchgeführt werden. Ein zusätzlicher Vorteil besteht darin, dass AppAssure eine BMR auch dann ermöglicht, wenn die Hardware nur ähnlich oder gar unterschiedlich ist.

Voraussetzungen für eine Bare-Metal-Wiederherstellung für eine Windows-Maschine

Bevor Sie mit der Durchführung eines Bare-Metal-Wiederherstellungsvorgangs für eine Windows Maschine beginnen können, müssen Sie sicherstellen, dass die folgenden Bedingungen und Kriterien erfüllt sind:

- **Sicherungen der Maschine, die Sie wiederherstellen möchten** – Sie müssen über einen funktionsfähigen AppAssure-Kern verfügen, der die Wiederherstellungspunkte des geschützten Servers enthält, den Sie wiederherstellen möchten.
- **Hardware zur Wiederherstellung (neu oder alt, ähnlich oder unterschiedlich)** – Der Zielcomputer muss den Installationsanforderungen für einen Agenten entsprechen.
- **Image-Medien und Software** – Sie benötigen eine leere CD oder DVD sowie eine Brennersoftware oder eine Software zum Erstellen eines ISO-Images. Wenn Sie Maschinen per Remote-Zugriff unter Verwendung einer Virtual Network Computing-Software wie UltraVNC verwalten, benötigen Sie VNC Viewer.
- **Kompatible Speichertreiber und Netzwerkadaptertreiber** – Wenn Sie auf unterschiedliche Hardware wiederherstellen, benötigen Sie Windows 7 PE (32-Bit)-kompatible Treiber für Massenspeicher und

Netzwerkadapter für die Zielmaschine, ggf. einschließlich RAID, AHCI und Chipsatz-Treiber für das Zielbetriebssystem.

- **Speicherplatz und Partitionen je nach Bedarf** – Stellen Sie sicher, dass auf dem Laufwerk genug Speicherplatz zur Erstellung von Zielpartitionen auf der Zielmaschine vorhanden ist, um die Quellvolumes zu enthalten. Die Zielpartitionen müssen mindestens ebenso groß sein, wie die ursprüngliche Quellpartition.
- **Kompatible Partitionen** – Windows 8 und Windows Server 2012 Betriebssysteme, die von FAT32 EFI-Partitionen gestartet werden, sind für Schutz oder Wiederherstellung verfügbar, ebenso Resilient File System (ReFS)-Volumes. UEFI-Partitionen werden als einfache FAT32-Volumes behandelt. Inkrementelle Übertragungen werden vollständig unterstützt und geschützt. AppAssure 5 bietet Unterstützung für UEFI-Systeme für Bare Metal Recovery, einschl. automatischer Partitionierung von GPT-Festplatten.

Voraussetzungen für eine Bare-Metal-Wiederherstellung für eine Windows-Maschine

ANMERKUNG: Im Folgenden werden die grundlegenden Schritte für die Bare-Metal-Wiederherstellung (BMR) erläutert. Ausführliche Informationen zu den einzelnen Schritten finden Sie im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide*.

So führen Sie eine BMR (Bare-Metal-Wiederherstellung) für eine Windows-Maschine durch:

1. Erstellen Sie eine Start-CD
2. Brennen Sie das Abbild auf einen Datenträger.
3. Starten Sie den Zielserver von der Start-CD aus neu.
4. Stellen Sie eine Verbindung zum Wiederherstellungsdatenträger her.
5. Weisen Sie die Volumes zu.
6. Initiieren Sie die Wiederherstellung.
7. Überwachen Sie den Fortschritt.

Replizieren von Wiederherstellungspunkten

Replikation ist der Prozess des Kopierens von Wiederherstellungspunkten und des Übertragens dieser Punkte auf einen sekundären Speicherort, um diese für eine Notfallwiederherstellung verwenden zu können. Für diesen Prozess benötigen Sie eine gekoppelte Quell-Ziel-Beziehung zwischen zwei Kernen. Der Quellkern kopiert die Wiederherstellungspunkte der geschützten Agenten und überträgt diese asynchron und dauerhaft auf den Zielkern an einem Remote-Notfallwiederherstellungsort. Der Remote-Standort kann ein unternehmenseigenes Rechenzentrum (selbstverwalteter Kern) oder ein MSP-Standort (Managed Service Provider) eines Drittanbieters oder eine Cloud-Umgebung sein. Bei der Replikation auf einem MSP können Sie integrierte Arbeitsabläufe verwenden, über die Sie Verbindungen anfordern und automatische Rückmeldungen erhalten können. Mögliche Replikationsszenarien umfassen:

- **Replikation zu einem lokalen Standort** – Der Zielkern befindet sich in einem lokalen Rechenzentrum oder vor Ort und die Replikation wird zu jedem Zeitpunkt aufrecht erhalten. In dieser Konfiguration verhindert der Verlust des Kerns nicht die Wiederherstellung.
- **Replikation zu einem externen Standort** – Der Zielkern befindet sich in einer externen Einrichtung zur Notfallwiederherstellung, um im Verlustfall die Wiederherstellung zu gewährleisten.
- **Gegenseitige Replikation** – Zwei Rechenzentren an zwei unterschiedlichen Standorten enthalten jeweils einen Kern. Sie schützen Agenten und dienen sich gegenseitig als externe

Notfallwiederherstellungssicherung. In diesem Szenario repliziert jeder Kern die Agenten auf den Kern, der sich im anderen Rechenzentrum befindet.

- **Gehostete und Cloud-Replikation** – AppAssure MSP-Partner unterhalten mehrere Zielkerne in einem Rechenzentrum oder einer öffentlichen Cloud. Auf jedem dieser Kerne lässt der MSP-Partner gegen Gebühr seine Kunden Wiederherstellungspunkte von einem Quellkern am Kundenstandort auf den MSP-Zielkern replizieren.

Einrichten Ihrer Umgebung

Wenn die Bandbreite zwischen Quellkern und Zielkern die Übertragung von gespeicherten Wiederherstellungspunkten nicht aufnehmen kann, beginnt die Replikation mit dem Seeding des Zielkerns mit Basisabbildern und Wiederherstellungspunkten von den ausgewählten Servern, die auf dem Quellkern geschützt sind. Der Seeding-Vorgang kann jederzeit als Bestandteil der anfänglichen Übertragung der Daten ausgeführt werden, die als Grundlage für eine regelmäßige, geplante Replikation dient, oder im Falle einer Weidereinsetzung der Replikation für eine zuvor replizierte Maschine, deren Replikation angehalten oder gelöscht wurde. In diesem Fall können Sie mit der „Build RP Chain"-Option noch nicht replizierte Wiederherstellungspunkte auf ein Seed-Laufwerk replizieren.

Beim Vorbereiten der Replikation sollten Sie die folgenden Faktoren beachten:

- **Änderungsrate** – Die Änderungsrate ist die Rate, zu der sich die Menge der geschützten Daten ansammelt. Die Rate hängt von der Menge der Daten ab, die auf geschützten Volumes geändert werden, und vom Schutzintervall auf den Volumes. Wenn ein Satz an Blöcken auf dem Volume geändert wird, wird durch Reduzieren des Schutzintervalls auch die Änderungsrate reduziert.
- **Bandbreite** – Die Bandbreite ist die verfügbare Übertragungsgeschwindigkeit zwischen dem Quellkern und dem Zielkern. Es ist entscheidend, dass die Bandbreite größer ist als die Änderungsrate bei der Replikation, damit die von den Snapshots erstellten Wiederherstellungspunkte aufrechterhalten werden können. Aufgrund der von Kern zu Kern übertragenen Datenmenge sind eventuell mehrere parallele Ströme erforderlich, um Drahtgeschwindigkeiten bis zur Geschwindigkeit einer 1-GB-Ethernet-Verbindung zu erreichen.

  ANMERKUNG: Die vom Internetdienstanbieter angegebene Bandbreite ist die verfügbare Gesamtbandbreite. Die ausgehende Bandbreite wird von allen Geräten im Netzwerk geteilt. Stellen Sie sicher, dass für die Replikation ausreichend freie Bandbreite für die Änderungsrate zur Verfügung steht.
- **Anzahl der Agenten**: Es ist wichtig, die Anzahl der Agenten in Betracht zu ziehen, die pro Quellkern geschützt werden sollen, und wie viele Sie davon auf das Ziel replizieren möchten. Mit DL1300 können Sie die Replikation pro geschütztem Server durchführen, sodass Sie auswählen können, ob Sie bestimmte Server replizieren möchten. Wenn alle geschützten Server repliziert werden müssen, beeinflusst dies die Änderungsrate erheblich, vor allem dann, wenn die Bandbreite zwischen Quell- und Zielkernen für Menge und Größe der replizierten Wiederherstellungspunkte unzureichend ist.

  Abhängig von Ihrer Netzwerkkonfiguration kann die Replikation ein zeitaufwendiger Vorgang sein.

  Die Maximale Änderungsrate für WAN-Verbindungstypen wird in der Tabelle unten mit Beispielen für die notwendige Bandbreite pro Gigabyte für eine angemessene Änderungsrate angezeigt.

Tabelle 2. Maximale Änderungsrate für WAN-Verbindungstypen

Breitband	Bandbreite	Max. Änderungsrate
DSL	768 KBit/s und höher	330 MB pro Stunde
Kabel	1 MBit/s und höher	429 MB pro Stunde

T1	1,5 MBit/s und höher	644 MB pro Stunde
Fiber	20 MBit/s und höher	8,38 GB pro Stunde

Für optimale Ergebnisse befolgen Sie bitte die Empfehlungen in der obigen Tabelle. Im Falle eines Verbindungsausfalls während der Datenübertragung wird die Replikation vom letzten Fehlerpunkt der Übertragung wieder aufgenommen, wenn die Verbindungsfunktionalität wiederhergestellt ist.

Schritte für das Konfigurieren der Replikation

ANMERKUNG: Die folgenden Informationen bieten einen allgemeinen Überblick über die Schritte, die zur Durchführung einer Replikation erforderlich sind. Die vollständigen Anweisungen finden Sie im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **dell.com/support/home**.

Um Daten mit AppAssure zu replizieren, müssen Sie die Quell- und Zielkerne für die Replikation konfigurieren. Wenn Sie die Replikation konfiguriert haben, können Sie Agentendaten replizieren, die Replikation überwachen und verwalten und Wiederherstellungen durchführen. Das Ausführen der Replikation in AppAssure umfasst die folgenden Schritte:

- **Selbstverwaltende Replikation konfigurieren**: Weitere Informationen über die Replikation zu einem selbstverwaltenden Zielkern finden Sie im Abschnitt zum Replizieren zu einem selbstverwaltenden Zielkern im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**.
- **Drittanbieter-Replikation konfigurieren**: Weitere Informationen über die Replikation zu einem Zielkern eines Drittanbieters finden Sie im Abschnitt über das Verfahren zum Replizieren zu einem Zielkern eines Drittanbieters im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**.
- **Bestehenden Agenten replizieren**: Weitere Informationen über die Replikation eines Agenten, der bereits vom Quellkern geschützt wird, finden Sie im Abschnitt zum Hinzufügen einer Maschine zu einer bestehenden Replikation im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**.
- **Seed-Laufwerk verarbeiten**: Weitere Informationen zum Verarbeiten von Daten des Seed-Laufwerks auf dem Zielkern finden Sie im Abschnitt zum Verarbeiten des Seed-Laufwerks auf einem Zielkern im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**.
- **Replikationspriorität für einen Agenten einstellen**: Weitere Informationen zur Priorisierung der Replikation von Agenten finden Sie im Abschnitt zum Einstellen der Replikationspriorität für einen Agenten im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**.
- **Replikationszeitplan für einen Agenten einstellen**: Weitere Informationen zur Festlegung eines Replikationszeitplans finden Sie im Abschnitt zum Planen der Replikation im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**.
- **Replikation nach Bedarf überwachen**: Weitere Informationen zur Überwachung der Replikation finden Sie im Abschnitt zum Überwachen der Replikation im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**.
- **Replikation nach Bedarf verwalten**: Weitere Informationen zum Verwalten der Replikation finden Sie im Abschnitt zum Verwalten der Replikationseinstellungen im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**.
- **Wiederherstellen von replizierten Daten im Notfall oder bei Datenverlust**: Weitere Informationen zur Wiederherstellung replizierter Daten finden Sie im Abschnitt zum Wiederherstellen von replizierten

Daten im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**

Verwenden des virtuellen Standby

AppAssure unterstützt sowohl einmaligen als auch dauerhaften Export (Unterstützung von virtuellem Standby) von Windows-Sicherungsinformationen in eine virtuelle Maschine. Das Exportieren Ihrer Daten auf eine virtuelle Standby-Maschine bietet Ihnen eine hochverfügbare Kopie der Daten. Wenn eine geschützte Maschine ausfällt, können Sie die virtuelle Maschine starten, um eine Wiederherstellung auszuführen.

Wenn Sie auf eine virtuelle Maschine exportieren, werden alle Sicherungsdaten von einem Wiederherstellungspunkt sowie die für den Schutzzeitplan definierten Parameter für Ihre Maschine exportiert. Sie können auch ein „virtuelles Standby" erstellen, indem geschützte Daten fortlaufend von Ihrer geschützten Maschine auf eine virtuelle Maschine exportiert werden.

ANMERKUNG: Nur die DL1300-Konfiguration mit 3 TB und 2 VMs bzw. 4 TB und 2 VMs unterstützen den einmaligen und kontinuierlichen Export auf virtuellen Standby-VMs.

Ausführen eines einmaligen Hyper-V-Exports

So führen Sie einen einmaligen Hyper-V-Export aus:

1. Navigieren Sie in der Core Console zu der Maschine, die Sie exportieren möchten.
2. Klicken Sie auf der Registerkarte „Summary" (Zusammenfassung) auf **Actions (Aktionen)** → **Export (Exportieren)** → **One-time (Einmalig)**.

   Der **Assistent zum Exportieren** wird auf der Seite **Protected Machines** (Geschützte Maschinen) angezeigt.
3. Wählen Sie eine Maschine zum Exportieren aus, und klicken Sie dann auf **Next** (Weiter).
4. Wählen Sie auf der Seite **Recovery Points** (Wiederherstellungspunkte) den Wiederherstellungspunkt aus, den Sie exportieren möchten, und klicken Sie dann auf **Next** (Weiter).

Definieren von einmaligen Einstellungen für das Ausführen eines Hyper-V-Exports

So definieren Sie die einmaligen Einstellungen für das Ausführen eines Hyper-V-Exports:

1. Klicken Sie über das Dialogfeld „Hyper-V" auf die Option **Use local machine** (Lokale Maschine verwenden), um den Hyper-V-Export auf eine lokale Maschine durchzuführen, der die Hyper-V-Rolle zugewiesen wurde.
2. Klicken Sie auf die Option **Remote host** (Remote-Host) um anzugeben, dass sich der Hyper-V-Server auf einer Remote-Maschine befindet. Wenn Sie die Option Remote host auswählen, geben Sie die Parameter für den Remote-Host wie nachfolgend beschrieben ein.

Textfeld	Beschreibung
Host-Name	Geben Sie eine IP-Adresse oder einen Hostnamen für den Hyper-V-Server ein. Er steht für eine IP-Adresse oder einen Hostnamen des Remote-Hyper-V-Servers.
Schnittstelle	Geben Sie eine Portnummer für die Maschine ein. Sie steht für den Port, über den der Kern mit dieser Maschine kommuniziert.
Benutzername	Geben Sie den Benutzernamen für den Benutzer mit Administratorberechtigungen für die Workstation mit dem Hyper-V-Server ein.

Textfeld	Beschreibung
	Das Kennwort wird zur Angabe der Anmeldeinformationen für die virtuelle Maschine verwendet.
Kennwort	Geben Sie das Kennwort für das Benutzerkonto mit den Administratorberechtigungen auf der Workstation mit Hyper-V-Server an. Das Kennwort wird zur Angabe der Anmeldeinformationen für die virtuelle Maschine verwendet.

3. Klicken Sie auf **Weiter**.
4. Geben Sie auf der Seite **Virtual Machines Options** (Optionen der virtuellen Maschine) im Textfeld **VM Machine Location** (Speicherort der VM-Maschine) den Pfad oder Speicherort für die virtuelle Maschine ein, zum Beispiel **D:\export**. Der VM-Speicherort muss über ausreichend Speicherplatz verfügen, um die VM-Metadaten und die virtuellen Laufwerke zu beherbergen, die für die virtuelle Maschine erforderlich sind.
5. Geben Sie den Namen für die virtuelle Maschine in das Textfeld **Virtual Machine Name** (Name der virtuellen Maschine) ein.

   Der Name, den Sie eingeben, erscheint in der Liste der virtuellen Maschinen in der Hyper-V-Manager-Konsole.
6. Klicken Sie auf eine der folgenden Optionen:
   - **Use the same amount of RAM as the source machine** (Gleiche RAM-Größe verwenden wie Quellmaschine), um anzugeben, dass die RAM-Nutzung bei virtuellen und Quellmaschinen identisch ist.
   - **Use a specific amount of RAM** (Bestimmte RAM-Größe verwenden), um anzugeben, über wie viel Speicherplatz die virtuelle Maschine nach dem Export verfügen soll; z. B. 4096 MB (empfohlen).
7. Um das Laufwerkformat anzugeben, klicken Sie neben **Disk Format** (Laufwerkformat) auf eine der folgenden Optionen:
   - **VHDX**
   - **VHD**

   ANMERKUNG: Hyper-V-Export unterstützt VHDX-Laufwerkformate, wenn die Zielmaschine mit Windows 8 (Windows Server 2012) oder höher ausgeführt wird. Wenn der VHDX für Ihre Umgebung nicht unterstützt wird, ist die Option deaktiviert.
8. Wählen Sie auf der Seite **Volumes** (Datenträger) den bzw. die Datenträger aus, die exportiert werden sollen. Schließen Sie das Boot-Laufwerk der geschützten Maschine ein, damit die virtuelle Maschine ein erfolgreiches Backup der geschützten Maschine darstellen kann. Beispiel: C: \.

   Die von Ihnen ausgewählten Volumes dürfen bei VHD nicht größer als 2040 GB sein. Wenn die ausgewählten Volumes größer sind als 2040 GB und das VHD-Format ausgewählt wurde, wird eine Fehlermeldung angezeigt.
9. Klicken Sie auf der Seite **Summary** (Zusammenfassung) auf **Finish** (Fertig stellen), um den Assistenten zu beenden und den Export zu starten.

Ausführen eines dauerhaften Hyper-V-Exports (virtueller Standby)

ANMERKUNG: Nur die DL1300-Konfiguration mit 3 TB und 2 VMs bzw. 4 TB und 2 VMs unterstützen den einmaligen Export und den kontinuierlichen Export auf virtuellen Standby-VMs.

So führen Sie einen dauerhaften Hyper-V-Export (virtueller Standby) aus:

1. Klicken Sie in der Core Console auf der Registerkarte **Virtual Standby** (Virtueller Standby) auf **Add** (Hinzufügen), um den **Export Wizard** (Assistenten zum Exportieren) zu starten. Auf der Seite **Protected Machines** (Geschützte Maschinen) des **Export Wizard** (Assistenten zum Exportieren).
2. Wählen Sie die zu exportierende Maschine aus, und klicken Sie dann auf **Next** (Weiter).
3. Klicken Sie auf der Registerkarte **Summary** (Zusammenfassung) auf **Export (Exportieren)** → **Virtual Standby**(Virtueller Standby).
4. Klicken Sie über das Dialogfeld „Hyper-V" auf die Option **Use local machine** (Lokale Maschine verwenden), um den Hyper-V-Export auf eine lokale Maschine durchzuführen, der die Hyper-V-Rolle zugewiesen wurde.
5. Klicken Sie auf die Option **Remote host** (Remote-Host) um anzugeben, dass sich der Hyper-V-Server auf einer Remote-Maschine befindet. Wenn Sie die Option Remote host auswählen, geben Sie die Parameter für den Remote-Host wie nachfolgend beschrieben ein.

Textfeld	Beschreibung
Host-Name	Geben Sie eine IP-Adresse oder einen Hostnamen für den Hyper-V-Server ein. Er steht für eine IP-Adresse oder einen Hostnamen des Remote-Hyper-V-Servers.
Schnittstelle	Geben Sie eine Portnummer für die Maschine ein. Sie steht für den Port, über den der Kern mit dieser Maschine kommuniziert.
Benutzername	Geben Sie den Benutzernamen für den Benutzer mit Administratorberechtigungen für die Workstation mit dem Hyper-V-Server ein. Das Kennwort wird zur Angabe der Anmeldeinformationen für die virtuelle Maschine verwendet.
Kennwort	Geben Sie das Kennwort für das Benutzerkonto mit den Administratorberechtigungen auf der Workstation mit Hyper-V-Server an. Das Kennwort wird zur Angabe der Anmeldeinformationen für die virtuelle Maschine verwendet.

6. Geben Sie auf der Seite **Virtual Machines Options** (Optionen der virtuellen Maschine) im Textfeld **VM Machine Location** (Speicherort der VM-Maschine) den Pfad oder Speicherort für die virtuelle Maschine ein, zum Beispiel D:\export. Der VM-Speicherort muss über ausreichend Speicherplatz verfügen, um die VM-Metadaten und die virtuellen Laufwerke zu beherbergen, die für die virtuelle Maschine erforderlich sind.
7. Geben Sie den Namen für die virtuelle Maschine in das Textfeld **Virtual Machine Name** (Name der virtuellen Maschine) ein.

   Der Name, den Sie eingeben, erscheint in der Liste der virtuellen Maschinen in der Hyper-V-Manager-Konsole.
8. Klicken Sie auf eine der folgenden Optionen:
   - **Use the same amount of RAM as the source machine** (Gleiche RAM-Größe verwenden wie Quellmaschine), um anzugeben, dass die RAM-Nutzung bei virtuellen und Quellmaschinen identisch ist.
   - **Use a specific amount of RAM** (Bestimmte RAM-Größe verwenden), um anzugeben, über wie viel Speicherplatz die virtuelle Maschine nach dem Export verfügen soll; z. B. 4096 MB (empfohlen).
9. Klicken Sie auf eine der folgenden Optionen, um die Generation anzugeben:
   - Generation 1 (empfohlen)
   - Generation 2
10. Um das Laufwerkformat anzugeben, klicken Sie neben **Disk Format** (Laufwerkformat) auf eine der folgenden Optionen:

- **VHDX** (Standardeinstellung)
- **VHD**

ANMERKUNG: Hyper-V-Export unterstützt VHDX-Laufwerkformate, wenn die Zielmaschine mit Windows 8 (Windows Server 2012) oder höher ausgeführt wird. Wenn VHDX für Ihre Umgebung nicht unterstützt wird, ist die Option deaktiviert. Wählen Sie auf der Seite „Network Adapters" (Netzwerkadapter) den virtuellen Adapter aus, der mit einem Schalter verbunden werden soll.

11. Wählen Sie auf der Seite **Volumes** (Datenträger) den bzw. die Datenträger aus, die exportiert werden sollen. Schließen Sie das Boot-Laufwerk der geschützten Maschine ein, damit die virtuelle Maschine ein erfolgreiches Backup der geschützten Maschine darstellen kann. Beispiel: C: \.

    Die von Ihnen ausgewählten Volumes dürfen bei VHD nicht größer als 2040 GB sein. Wenn die ausgewählten Volumes größer sind als 2040 GB und das VHD-Format ausgewählt wurde, wird eine Fehlermeldung angezeigt.

12. Klicken Sie auf der Seite **Summary** (Zusammenfassung) auf **Finish** (Fertig stellen), um den Assistenten zu beenden und den Export zu starten.

    ANMERKUNG: Sie können den Status und Fortschritt des Exports über das Anzeigen der Registerkarten **Virtual Standby** (Virtueller Standby) oder **Events** (Ereignisse) anzeigen.

Verwalten von Wiederherstellungspunkten

Auf dem Kern sammeln sich die regelmäßig von allen geschützten Servern erstellten Sicherungs-Snapshots an. Die Aufbewahrungsrichtlinien werden zur Aufbewahrung von Sicherungs-Snapshots für längere Zeiträume sowie zur Unterstützung bei der Verwaltung dieser Sicherungs-Snapshots verwendet. Eine Aufbewahrungsrichtlinie wird durch einen nachts durchgeführten Rollup-Prozess umgesetzt, der bei der Bestimmung der Fälligkeit und beim Löschen alter Sicherungen hilft.

Archivieren von Daten

Aufbewahrungsrichtlinien erzwingen die Zeitdauer, für die Sicherungen auf (schnellen und teuren) Kurzzeitmedien gespeichert werden. Mitunter machen geschäftliche und technische Anforderungen eine längere Aufbewahrung dieser Sicherungen erforderlich, schnelle Speicherung ist jedoch unerschwinglich teuer. Deshalb wird durch diese Anforderung (langsame und kostengünstige) Langzeitspeicherung notwendig. Unternehmen verwenden Langzeitspeicherung oftmals zur Archivierung von konformen sowie nicht-konformen Daten. Die Archivierungsfunktion in AppAssure wird zur Unterstützung der verlängerten Aufbewahrung für konforme und nicht-konforme Daten verwendet. Außerdem können Sie mit dieser Funktion Replikationsdaten auf einem Remote-Replikatkern platzieren.

Erstellen eines Archivs

So erstellen Sie ein Archiv:

1. Klicken Sie in der Core Console auf **Tools (Extras)** → **Archive (Archiv)** → **Create (Erstellen)**.

    Daraufhin wird das Dialogfeld **Add Archive Wizard** (Archivassistent hinzufügen) angezeigt.

2. Wählen Sie auf der Seite Create (Erstellen) des Add Archive Wizard (Assistenten zum Hinzufügen von Archiven) eine der folgenden Optionen aus der Drop-Down-Liste Location Type (Speicherorttyp) aus:
    - Lokal
    - Netzwerk
    - Cloud

3. Geben Sie die in der folgenden Tabelle beschriebenen Details für das Archiv auf Basis der Position, die Sie in Schritt 3 ausgewählt haben, ein.

Tabelle 3. Erstellen eines Archivs

Option	Textfeld	Beschreibung
Lokal	Output location (Ausgabespeicherort)	Geben Sie den Speicherort für die Ausgabe ein. Er wird für die Definition des Pfades verwendet, auf dem sich das Archiv befinden soll, zum Beispiel „d:\work\archive“.
Netzwerk	Output location (Ausgabespeicherort)	Geben Sie den Speicherort für die Ausgabe ein. Er wird für die Definition des Pfades verwendet, auf dem sich das Archiv befinden soll, zum Beispiel „\\servername \sharename“.
	Benutzername	Geben Sie einen Benutzernamen ein. Es wird zur Festlegung von Anmeldeinformationen für die Netzwerkfreigabe verwendet.
	Kennwort	Geben Sie ein Kennwort für den Netzwerkpfad ein. Es wird zur Festlegung von Anmeldeinformationen für die Netzwerkfreigabe verwendet.
Cloud	Account (Konto)	Wählen Sie ein Konto aus der Drop-Down-Liste aus. **ANMERKUNG:** Zum Auswählen eines Cloud-Kontos müssen Sie dieses zuerst zur Kern-Konsole hinzufügen. Siehe hierzu den Abschnitt zum Hinzufügen eines Cloud-Kontos im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide*.
	Container	Wählen Sie einen Container, der mit Ihrem Konto verknüpft ist, aus dem Drop-Down-Menü aus.

Option	Textfeld	Beschreibung
	Ordnername	Geben Sie einen Namen für den Ordner ein, in dem die archivierten Daten gespeichert werden sollen. Der Standardname ist „AppAssure-5-Archivierung – [ERSTELLT AM] – [ERSTELLTE UM]“.

4. Klicken Sie auf **Weiter**.
5. Wählen Sie auf der Seite Machines (Maschinen) des Assistenten aus, welche geschützte(n) Maschine(n) Wiederherstellungspunkte enthält, die Sie archivieren möchten.
6. Klicken Sie auf **Weiter**.
7. Geben Sie auf der Seite **Options** (Optionen) die in der folgenden Tabelle beschriebenen Informationen ein:

Textfeld	Beschreibung
Maximale Größe	Große Datenarchive können in mehrere Segmente unterteilt werden. Wählen Sie die maximale Menge an Speicherplatz aus, die Sie für die Erstellung des Archivs reservieren möchten. Führen Sie dazu einen der folgenden Schritte aus: • Wählen Sie „Entire Target“ (Gesamtes Ziel) aus, um den gesamten verfügbaren Speicherplatz im Pfad zu reservieren, der in Schritt 4 auf dem Ziel bereitgestellt wurde (wenn z. B. der Speicherort „D:\work\archive“ lautet, wird der gesamte verfügbare Speicherplatz auf Laufwerk D: reserviert). • Wählen Sie das leere Textfeld aus, verwenden Sie die Pfeile nach oben und unten, um eine Menge einzugeben, und wählen Sie dann eine Maßeinheit aus der Dropdown-Liste aus, um den maximalen Speicherplatz anzupassen, der reserviert werden soll. **ANMERKUNG:** Amazon-Cloud-Archive werden automatisch in 50-GB-Segmente unterteilt. Windows Azure Cloud-Archive werden automatisch in 200 GB-Segmente unterteilt.
Recycle action (Maßnahme wiederverwenden)	Wählen Sie eine der folgenden Recycling-Optionen aus: • **Do not reuse** (Nicht wiederverwenden) – Vorhandene Daten am Speicherort werden nicht überschrieben oder gelöscht. Wenn der Speicherort nicht leer ist, schlägt der Schreibvorgang in das Archiv fehl. • **Replace this core** (Diesen Kern ersetzen) – Alle bereits vorhandenen archivierten Daten auf diesem Kern werden überschrieben, die Daten für andere Kerne bleiben aber intakt. • **Erase Completely** (Vollständig löschen): Löscht alle archivierten Daten aus dem Verzeichnis, bevor das neue Archiv geschrieben wird. • **Incremental** (Inkrementell): Sie können Wiederherstellungspunkte zu einem vorhandenen Archiv hinzufügen. Die Wiederherstellungspunkte werden verglichen, um die Duplizierung von Daten zu verhindern, die bereits im Archiv vorhanden sind.

Textfeld	Beschreibung
Kommentar	Geben Sie alle zusätzlichen Informationen ein, die zur Erfassung für das Archiv notwendig sind. Der Kommentar wird angezeigt, wenn Sie das Archiv später importieren.
Use compatible format (Kompatibles Format verwenden)	Wählen Sie diese Option aus, um Ihre Daten in einem Format zu archivieren, das mit früheren Kernversionen kompatibel ist. ANMERKUNG: Das neue Format bietet eine bessere Leistung, es ist jedoch nicht kompatibel mit älteren Kerne.

8. Klicken Sie auf **Weiter**.
9. Geben Sie auf der Seite „Date Range" (Datumsbereich) das Start- und das Ablaufdatum der zu archivierenden Wiederherstellungspunkte ein.
   - Klicken Sie zum Eingeben einer Uhrzeit auf die angezeigte Zeit (der Standardwert ist 8:00 Uhr), um die Schieberegler für die Auswahl von Stunden und Minuten anzuzeigen.
   - Klicken Sie zum Eingeben eines Datums in das Textfeld, um den Kalender anzuzeigen, und klicken Sie dann auf den gewünschten Tag.
10. Klicken Sie auf **Finish** (Fertig stellen).

Archivierung in eine Cloud

Sie können Ihre Daten direkt über die Core Console durch Hochladen der Daten in die Clouds verschiedener Anbieter archivieren. Zu kompatiblen Clouds gehören Windows Azure, Amazon, Rackspace und alle OpenStack-basierten Anbieter.

So exportieren Sie ein Archiv in eine Cloud:

- Fügen Sie Ihr Cloud-Konto zur Core Console hinzu. Weitere Informationen finden Sie im Abschnitt zum Hinzufügen eines Cloud-Kontos im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**.
- Archivieren Sie Ihre Daten, und exportieren Sie sie in Ihr Cloud-Konto. Weitere Informationen finden Sie im Abschnitt zum Erstellen eines Archivs im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**.
- Rufen Sie archivierte Daten ab, indem Sie sie vom Cloud-Speicherort importieren. Weitere Informationen finden Sie im Abschnitt zum Importieren eines Archivs im DL1300-Benutzerhandbuch *Dell DL1300 Appliance User's Guide* unter **Dell.com/support/home**.

6

Wie Sie Hilfe bekommen

Ausfindig machen der Dokumentation und Software-Aktualisierungen

Direkte Links zur AppAssure- und DL1300 Appliance-Dokumentation und zu Software-Aktualisierungen finden Sie in der Core Console.

Dokumentation

So greifen Sie auf den Link für die Dokumentation zu:

1. Klicken Sie in der Core Console auf der Registerkarte **Appliance** (Gerät).
2. Öffnen Sie im linken Fensterbereich den Link unter **Appliance (Gerät)** → **Documentation (Dokumentation)**.

Software updates (Softwareaktualisierungen)

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

1. Klicken Sie in der Core Console auf der 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.