Dell DL4000-Gerät
Benutzerhandbuch

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.

2015 - 12

Rev. A01

Inhaltsverzeichnis

1

Einführung in das Dell DL4000-Gerät

Dieses Kapitel ist eine Einführung in DL4000 und bietet außerdem eine Übersicht über das Gerät. Es beschreibt Merkmale, Funktionen und die Architektur und enthält die folgenden Themen:

- Kerntechnologien
- True Scale-Architektur
- Bereitstellungsarchitektur
- Produktmerkmale

Ihr Gerät setzt neue Standards beim einheitlichen Datenschutz, indem es Backup, Replikation und Wiederherstellung in einer Lösung kombiniert, die als schnellste und zuverlässigste Backuplösung zum Schutz virtueller Maschinen (VM) sowie physischer Maschinen und Cloud-Umgebungen konzipiert wurde.

Ihr Gerät kann Datengrößen bis Petabyte verarbeiten und verfügt über integrierte globale Deduplizierung, Komprimierung, Verschlüsselung sowie Replikation in jede beliebige private oder öffentliche Cloud-Infrastruktur. Server-Anwendungen und Daten können innerhalb von Minuten zur Datenaufbewahrung (Data Retention, DR) und Datenkonformität wiederhergestellt werden.

Ihr Gerät unterstützt Multi-Hypervisor-Umgebungen auf VMware vSphere und Microsoft Hyper-V für private und öffentliche Clouds.

Ihr Gerät kombiniert die folgenden Technologien:

- Live Recovery
- Verified Recovery
- Universal Recovery
- True Global Deduplication

Diese Technologien sind mit sicherer Integration für die Cloud-Notfallwiederherstellung ausgerüstet und bieten schnelle sowie zuverlässige Wiederherstellung. Mit seinem skalierbaren Objektspeicher ist Ihr Gerät das Einzige, welches Datengrößen bis Petabytes sehr schnell für integrierte globale Deduplizierung, Komprimierung, Verschlüsselung sowie Replikation in privaten oder öffentlichen Cloud-Infrastrukturen verarbeiten kann.

AppAssure befasst sich mit der Komplexität und Ineffizienz von Legacy-Tools mittels seiner Kerntechnologie und der Unterstützung von Hypervisor-Umgebungen, einschließlich Umgebungen auf VMware vSphere und Microsoft Hyper-V, die sowohl private als auch öffentliche Clouds umfassen. Mit AppAssure können Sie jedoch nicht nur diese technologischen Fortschritte nutzen, sondern auch die Kosten der IT-Verwaltung und Speicherung drastisch senken.

Kerntechnologien

Im Folgenden werden die Kerntechnologien von AppAssure ausführlich beschrieben.

Live Recovery

Live Recovery ist eine Technologie zur Sofortwiederherstellung für VMs oder Server, die nahezu ununterbrochenen Zugang zu Datenträgern auf virtuellen oder physischen Servern gewährt. Mit dieser Technologie können Sie einen kompletten Datenträger in gegen Null tendierenden RTO- und RPO-Zeiten wiederherstellen.

Die Backup- und Replikationstechnologie erstellt simultane Snapshots von mehreren VMs oder Servern und liefert dadurch nahezu sofortigen Daten- und Systemschutz. Sie können den Server direkt aus der Backupdatei wiederverwenden, ohne eine vollständige Wiederherstellung auf dem Produktionsspeicher abwarten zu müssen. Dadurch bleibt die Produktivität der Benutzer erhalten und die IT-Abteilungen können die Zahl der Wiederherstellungsfenster reduzieren, um die immer strengeren Leistungsverträge hinsichtlich Recovery Time Objective (RTO) und Recovery Point Objective (RPO) erfüllen zu können.

Verified Recovery

Verified Recovery ermöglicht Ihnen die Durchführung automatisierter Wiederherstellungstests und die Überprüfung von Backups. Die Technologie umfasst unter anderem Dateisysteme, Microsoft Exchange 2007, 2010 und 2013 sowie verschiedene Versionen von Microsoft SQL Server 2005, 2008, 2008 R2, 2012 und 2014. Verified Recovery ermöglicht die Wiederherstellbarkeit von Anwendungen und Backups in virtuellen und physischen Umgebungen und verfügt über einen umfassenden Algorithmus zur Integritätsprüfung, der auf 256-Bit SHA-Schlüsseln basiert. Diese Schlüssel prüfen während der Archivierungs-, Replikations- und Daten-Seeding-Vorgänge die Richtigkeit jedes Datenträgerblocks im Backup. Dadurch kann die Beschädigung von Daten rechtzeitig erkannt werden und es wird verhindert, dass beschädigte Datenblöcke erhalten oder während des Backups übertragen werden.

Universal Recovery

Dank der Universal Recovery-Technologie erhalten Sie uneingeschränkte Flexibilität bei der Maschinenwiederherstellung. Sie können Ihre Sicherungen auf folgenden Umgebungen wiederherstellen: von physischen Systeme 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 unterschiedlicher Hardware, z. B. P2V, V2V, V2P, P2P, P2C, V2C, C2P und C2V, durchführen.

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. Mit AppAssure können Sie außerdem von einer physischen oder einer virtuellen Umgebung auf eine Cloud-Umgebung wiederherstellen oder exportieren.

True Global Deduplication

Das Gerät bietet echte globale Deduplizierung, die die Anforderungen an die Kapazitäten des physischen Festplattenlaufwerks, dank Platzeinsparungsraten von über 50:1 bei gleichzeitiger Einhaltung der Datenspeicherungsanforderungen, reduziert. Die Inline-Komprimierung und Deduplizierung von AppAssure TrueScale auf Blockebene bei Verbindungsgeschwindigkeit und die vordefinierte Integritätsprüfung verhindern, dass die Backup- und Archivierungsvorgänge durch Datenbeschädigungen beeinträchtigt werden.

True Scale-Architektur

Ihr Gerät ist auf der AppAssure True Scale-Architektur aufgebaut. Es nutzt eine dynamische, aus mehreren Kernen bestehende Pipeline-Architektur, die so optimiert wurde, dass sie Ihren Unternehmensumgebungen eine solide Verbindungsgeschwindigkeit bereitstellt. True Scale wurde von Grund auf für lineare Skalierbarkeit, effiziente Speicherung und Verwaltung großer Datenmengen sowie für kurze RTOs und RPOs ohne Leistungseinbußen konzipiert. Die Technologie umfasst einen speziell erstellten Objekt- und Datenträger-Manager mit integrierter globaler Deduplizierung, Komprimierung, Verschlüsselung, Replikation und Aufbewahrung. Im folgenden Diagramm wird die AppAssure True Scale-Architektur beschrieben.

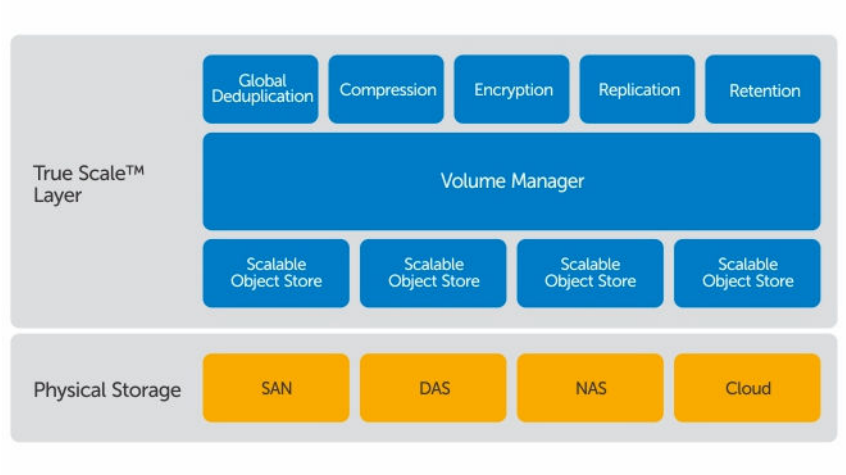


Abbildung 1. AppAssure True Scale-Architektur

Der AppAssure Volume-Manager und der skalierbare Objektspeicher bilden die Basis der AppAssure True Scale-Architektur. In den einzelnen skalierbaren Objektspeichern werden Blockebenen-Snapshots der virtuellen und physischen Server gespeichert. Der Volume-Manager verwaltet die zahlreichen Objektspeicher durch Bereitstellung eines gemeinsamen Repositorys oder durch bedarfsorientierte Speicherung der notwendigen Elemente. Der Objektspeicher unterstützt simultane Vorgänge mit asynchroner E/A, die hohen Durchsatz mit minimaler Latenz liefern und die Systemauslastung maximieren. Das Repository beruht auf unterschiedlichen Speichertechnologien wie Storage Area Network (SAN), Direct Attached Storage (DAS) oder Network Attached Storage (NAS).

Die Rolle des AppAssure Volume-Managers ähnelt der des Volume-Managers in einem Betriebssystem: Unter Verwendung der Stripeset- oder sequenziellen Zuweisungsrichtlinien fasst er verschiedene Speichergeräte mit unterschiedlicher Größe und unterschiedlichem Typ zu logischen Volumes zusammen. Der Objektspeicher kümmert sich um Speicherung, Abfrage, Verwaltung und anschließende Replizierung von Objekten, die von anwendungsbezogenen Snapshots abgeleitet wurden. Der Volume-Manager bietet eine skalierbare E/A-Leistung zusammen mit globaler Datendeduplizierung, Verschlüsslung sowie Aufbewahrungsverwaltung.

Bereitstellungsarchitektur

Das Gerät ist ein skalierbares Backup- und Wiederherstellungsprodukt, das flexibel im Unternehmen oder als von einem Anbieter verwalteter Dienst bereitgestellt wird. Der Typ der Bereitstellung hängt von der

Größe und den Anforderungen des Kunden ab. Bei der Planung einer Bereitstellung des Geräts sind die Planung des Netzwerks, die Speichertopologie, die Hardware- und Notfallwiederherstellungsinfrastruktur des Kerns sowie die Sicherheit einzubeziehen.

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

Darüber hinaus ist das Gerät mit Anwendungserkennung ausgestattet, da es die Fähigkeit besitzt, vorhandene Microsoft Exchange- und SQL-Anwendungen und ihre entsprechenden Datenbanken und Protokolldateien zu erkennen. Diese Datenträger werden anschließend nach Abhängigkeiten für umfassenden Schutz und effektive Wiederherstellung automatisch gruppiert. Damit wird sichergestellt, dass die Backups bei der Durchführung von Wiederherstellungen niemals unvollständig sind. Backups werden mithilfe anwendungsspezifischer Snapshots auf Blockebene durchgeführt. Das Gerät kann auch Vorgänge zum Abschneiden des Protokolls der geschützten Microsoft Exchange- und SQL-Server durchführen.

Das folgende Diagramm zeigt eine einfache Bereitstellung. In diesem Diagramm ist die AppAssure-Agentsoftware auf Maschinen wie Dateiserver, E-Mail-Server, Datenbankserver oder virtuelle Maschinen installiert. Sie sind mit einem einzigen Kern, der auch aus dem zentralen Repository besteht, verbunden und werden von ihm geschützt. Das Lizenzportal verwaltet Lizenzabonnements, Gruppen und Benutzer der geschützten Maschinen und Kerne in Ihrer Umgebung. Das Lizenzportal ermöglicht Benutzern, sich anzumelden, Kontos zu aktivieren, Software herunterzuladen und geschützte Maschinen und Kerne je nach Lizenz für Ihre Umgebung bereitzustellen.

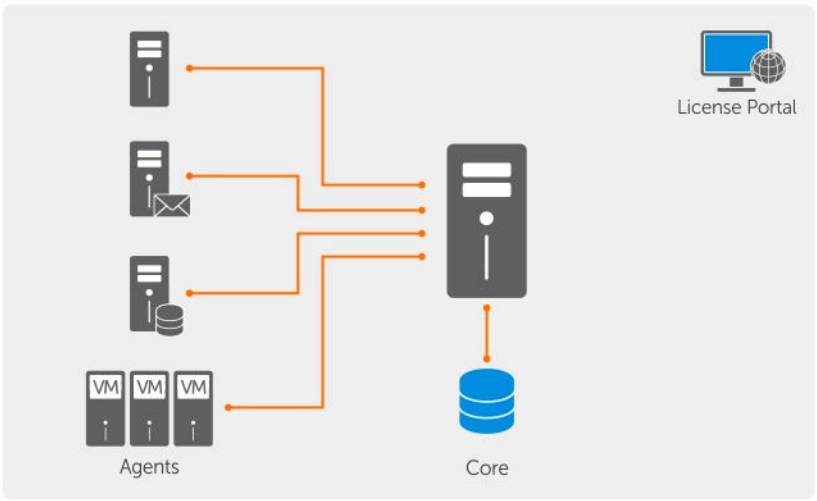


Abbildung 2. Grundlegende Bereitstellungsarchitektur

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

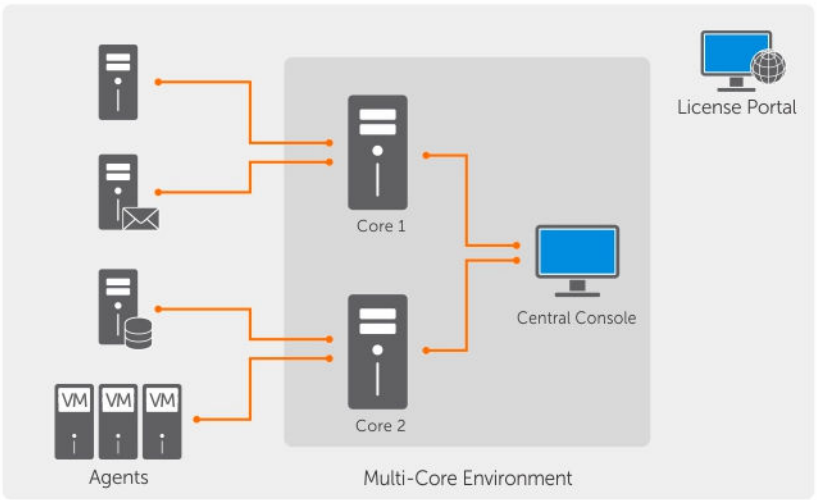


Abbildung 3. Multi-Kern-Bereitstellungsarchitektur

Smart Agent

Smart Agent überwacht die geänderten Blöcke auf dem Datenträger und erstellt ein Abbild der geänderten Blöcke in einem vordefiniertem Schutzintervall. Der Ansatz eines fortlaufenden inkrementellen Snapshots auf Blockebene verhindert das wiederholte Kopieren der gleichen Daten von der geschützten Maschine auf den Kern. Der Smart Agent ist auf den Maschinen installiert, die durch den Kern geschützt werden.

Der Smart Agent ist anwendungsbezogen und wechselt, wenn er nicht verwendet wird, in den Ruhezustand, mit nahezu null (0) Prozent CPU-Auslastung und weniger als 20 MB Speicheraufwand. Im aktiven Zustand nutzt der Smart Agent bis zu 2 bis 4 Prozent der Prozessor-Auslastung und weniger als 150 MB Speicher, worin bereits die Übertragung der Snapshots auf den Kern enthalten ist.

Der Smart Agent ist anwendungsbezogen und erkennt nicht nur den Typ der installierten Anwendung, sondern auch den Speicherort der Daten. Er gruppiert Datenträger automatisch nach Abhängigkeiten wie beispielsweise Datenbanken und protokolliert sie dann mit Blick auf einen effektiven Schutz und eine schnelle Wiederherstellung zusammen. Nachdem die AppAssure-Agentsoftware konfiguriert ist, verwendet er Smart-Technologie, um geänderte Blöcke auf geschützten Datenträgern nachzuverfolgen. Wenn der Snapshot bereit ist, wird er schnell mithilfe mehrinstanzenfähiger, socketbasierter Verbindungen auf den Kern übertragen. Um CPU-Bandbreite und Speicher auf den geschützten Maschinen einzusparen, verschlüsselt oder dedupliziert der Smart Agent die Daten an der Quelle nicht. Geschützte Maschinen werden zum Schutz mit einem Kern gepaart.

DL4000-Kern

Der Kern ist die zentrale Komponente der Bereitstellungsarchitektur. Der Kern speichert und verwaltet alle Maschinenbackups und bietet Kern-Services für Backup, Wiederherstellung und Aufbewahrung, Replikation, Archivierung sowie Verwaltung. Der Kern ist ein eigenständiger, über das Netzwerk adressierbarer Computer, der eine 64-Bit- des Microsoft Windows-Betriebssystems ausführt. Das Gerät führt die zielbasierte Inline-Komprimierung, Verschlüsselung und Deduplizierung der von der geschützten Maschine empfangenen Daten aus. Der Kern speichert dann die Snapshot-Backups in Repositorys wie Storage Area Network (SAN, Speicherbereichsnetzwerk), Direct Attached Storage (DAS, Direktverbundener Speicher).

Das Repository kann auch auf interner Speicherung im Kern beruhen. Der Kern wird durch den Zugriff auf die folgende URL von einem Webbrowser verwaltet: **https://CORENAME:8006/apprecovery/admin**. Intern sind alle Kern-Services über REST-APIs zugänglich. Auf die Kern-Services kann innerhalb des Kerns zugegriffen werden oder direkt über das Internet von jeder Anwendung aus, die eine HTTP/HTTPS-Anforderung senden und eine HTTP/HTTPS-Antwort empfangen kann. Alle API-Vorgänge werden über SSL durchgeführt und werden gegenseitig mithilfe von X.509 v3-Zertifikaten authentifiziert.

Kerne werden für die Replikation mit anderen Kernen gepaart.

Snapshot-Prozess

Als Snapshot wird der Vorgang bezeichnet, bei dem ein Basisabbild von einer geschützten Maschine auf den Kern übertragen wird. Dies ist der einzige Zeitpunkt, zu dem eine vollständige Kopie der Maschine bei Normalbetrieb über das Netzwerk transportiert wird, gefolgt von fortlaufenden inkrementellen Snapshots. Die AppAssure Agentsoftware für Windows verwendet den Microsoft Volume Shadow Copy Service (VSS) für das Einfrieren und Stilllegen von Anwendungsdaten auf Datenträgern, um ein dateisystemkonsistentes und anwendungskonsistentes Backup zu erfassen. Wenn ein Snapshot erstellt wird, verhindern VSS und der Generator auf dem Zielserver das Schreiben von Daten auf den Datenträger. Wenn das Schreiben von Inhalten auf den Datenträger angehalten wird, kommen alle E/A-Vorgänge des Datenträgers in eine Warteschlange und werden erst wieder fortgesetzt, nachdem der Snapshot fertiggestellt ist, alle derzeit ausgeführten Vorgänge abgeschlossen und alle geöffneten Dateien geschlossen worden sind. Der Prozess zum Erstellen einer Schattenkopie beeinträchtigt die Leistung des Produktionssystems nicht wesentlich.

AppAssure verwendet Microsoft VSS, da der Service über eine integrierte Unterstützung für alle Windows-internen Technologien wie NTFS, Registrierung, Active Directory usw. besitzt, um Daten vor dem Erstellen des Snapshots auf den Datenträger abzulegen. Zusätzlich verwenden andere Unternehmensanwendungen wie Microsoft Exchange und SQL die VSS-Generator-Plugins, um benachrichtigt zu werden, wenn ein Snapshot vorbereitet wird und wenn sie ihre geänderten Datenbankseiten auf dem Datenträger ablegen müssen, um die Datenbank in einen konsistenten Transaktionsstatus zu versetzen. Es muss unbedingt beachtet werden, dass VSS zur Stilllegung von System- und Anwendungsdaten auf dem Datenträger und nicht zum Erstellen des Snapshots verwendet wird. Die erfassten Daten werden umgehend auf den Kern übertragen und dort gespeichert. Wenn VSS für das Backup verwendet wird, wird der Anwendungsserver nicht für einen längeren Zeitraum in den Backupmodus versetzt, da die benötigte Zeit für eine Snapshot-Erstellung Sekunden und nicht Stunden beträgt. Ein weiterer Vorteil der Verwendung von VSS für Backups ist, dass es die AppAssure-Agentsoftware einen Snapshot großer Datenmengen aufzeichnen lässt, da der Snapshot auf Datenträgerebene funktioniert.

Replikation des Notfallwiederherstellungsstandorts oder Dienstanbieters

Für den Replikationsprozess benötigen Sie eine gekoppelte Quell-Ziel-Beziehung zwischen zwei Kernen. Der Quellkern kopiert die Wiederherstellungspunkte der geschützten Maschinen und überträgt diese asynchron und fortlaufend auf den Zielkern an einem Remote-Notfallwiederherstellungsstandort. 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 Workflows verwenden, über die Sie Verbindungen anfordern und automatische Rückmeldungen erhalten können. Für die erstmalige Übertragung der Daten können Sie Daten-Seeding mithilfe von externen Datenträgern durchführen. Dieses Verfahren eignet sich insbesondere für umfassende Datensätze oder Standorte mit langsamen Links.

Bei einem schwerwiegenden Ausfall unterstützt das Gerät Failover und Failback in replizierten Umgebungen. Im Fall eines globalen Ausfalls kann der Zielkern am sekundären Standort Instanzen aus replizierten geschützten Maschinen wiederherstellen und sofort den Schutz auf den Failed-over-Maschinen starten. Nachdem der primäre Standort wiederhergestellt ist, kann der replizierte Kern ein Failback der Daten aus den wiederhergestellten Instanzen zurück auf geschützte Maschinen am primären Standort ausführen.

Wiederherstellung

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

Produktmerkmale

Sie können den Schutz und die Wiederherstellung von kritischen Daten über folgende Funktionen und Funktionalitäten sicherstellen:

- Repository
- True Global Deduplication (Funktionen)
- Verschlüsselung
- Replikation
- Recovery-as-a-Service (RaaS)
- Aufbewahrung und Archivierung
- Virtualisieurng und die Cloud
- Benachrichtigungs- und Ereignisverwaltung
- Lizenzportal
- Webkonsole
- Serviceverwaltungs-APIs

Repository

Das Repository verwendet einen Deduplizierungs-Volume-Manager (DVM, Deduplication Volume Manager), um einen Volume-Manager zu implementieren, der Unterstützung für mehrere Volumes bietet. Jedes dieser Volumes kann auf einer anderen Speichertechnologie wie Speicherbereichsnetzwerk (SAN, Storage Area Network), direkt angeschlossener Speicherung (DAS, Direct Attached Storage), netzgebundener Speicherung (NAS, Network Attached Storage) oder Cloud-Speicherung beruhen. Jedes Volume besteht aus einem skalierbaren Objektspeicher mit Deduplizierung. Der skalierbare Objektspeicher verhält sich wie ein datensatzbasiertes Dateisystem, bei dem die Einheit der Speicherzuweisung ein Datenblock mit fester Größe ist, der Datensatz genannt wird. Mit dieser Architektur können Sie Unterstützung in Blockgröße zur Komprimierung und Deduplizierung konfigurieren. Rollup-Vorgänge werden von datenträgerintensiven Vorgängen zu Metadaten-Vorgängen reduziert, da beim Rollup keine Daten mehr verschoben werden, sondern nur noch die Datensätze.

Der DVM kann eine Reihe von Objektspeichern in einem Datenträger zusammenfassen. Diese können durch Erstellen zusätzlicher Dateisysteme erweitert werden. Die Objektspeicherdateien werden vorab zugewiesen und können bei Bedarf hinzugefügt werden, falls sich die Speicheranforderungen ändern. Auf einem einzigen Kern können bis zu 255 unabhängige Repositorys erstellt werden. Zusätzlich lässt sich ein Repository durch Hinzufügen neuer Dateierweiterungen weiter vergrößern. Ein erweitertes Repository

kann bis zu 4.096 Erweiterungen enthalten, die verschiedene Speichertechnologien umfassen. Die Maximalgröße eines Repositorys beträgt 32 Exabyte. Auf einem Kern können sich mehrere Repositorys befinden.

True Global Deduplication

True Global Deduplication (echte globale Deduplizierung) ist ein wirksames Verfahren zur Verringerung der Sicherungsspeicheranforderungen durch das Entfernen überflüssiger oder doppelter Daten. Deduplizierung ist wirksam, weil nur eine eindeutige Instanz der Daten über mehrere Sicherungen im Repository gespeichert wird. Die redundanten Daten werden zwar gespeichert, jedoch nicht physisch abgelegt, sondern einfach durch einen Verweis auf die eindeutige Dateninstanz im Repository ersetzt.

Bei herkömmlichen Backupanwendungen wurden jede Woche iterative Komplettbackups durchgeführt, Ihr Gerät hingegen führt inkrementelle Backups der Maschine auf Blockebene durch. Zusammen mit der Datendeduplizierung hilft dieser Ansatz eines fortlaufenden inkrementellen Backups (Incremental forever) dabei, die Gesamtmenge der an den Datenträger übergebenen Daten erheblich zu reduzieren.

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 gleichzeitig 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 4. Diagramm der Deduplizierung

Ihr Gerät führt zielbasierte Inline-Datendeduplizierungen durch. Das bedeutet, dass die Snapshot-Daten vor ihrer Deduplizierung auf den Kern übertragen werden. Bei der Inline-Datendeduplizierung werden die Daten dedupliziert, bevor sie an den Datenträger übergeben werden. Dieses Verfahren unterscheidet sich von der At-Source-Deduplizierung, bei der die Daten an der Quelle dedupliziert werden, bevor sie zur Speicherung auf das Ziel übertragen werden, und auch von der Postprocess-Deduplizierung, bei der die Daten als Rohdaten an das Ziel gesendet werden, wo sie nach der Übergabe an den Datenträger analysiert und dedupliziert werden. Bei der At-Source-Deduplizierung werden wertvolle Systemressourcen auf der Maschine gebunden, wohingegen sich für die Postprocess-

Datendeduplizierung alle notwendigen Daten auf dem Datenträger befinden müssen (d. h. ein höherer anfänglicher Kapazitätsaufwand), damit der Deduplizierungsprozess starten kann. Die Inline-Datendeduplizierung benötigt andererseits für den Deduplizierungsprozess keine zusätzlichen Datenträgerkapazitäten und CPU-Zyklen auf der Quelle oder auf dem Kern. Herkömmliche Backupanwendungen führen jede Woche iterative Komplettbackups durch, Ihr Gerät hingegen führt fortlaufende inkrementelle Backups der Maschine auf Blockebene durch. Zusammen mit der Datendeduplizierung trägt dieser Ansatz des fortlaufenden inkrementellen Backups (Incremental forever) dazu dabei, die Gesamtmenge der an den Datenträger übergebenen Daten erheblich zu reduzieren, und zwar in einem Verhältnis von bis zu 50:1.

Verschlüsselung

Das Gerät bietet eine integrierte Verschlüsselung, um Backups sowie gespeicherte Daten vor nicht autorisiertem Zugriff und unbefugter Nutzung zu schützen und gewährleistet damit Ihren Datenschutz. Nur ein Benutzer mit dem entsprechenden Verschlüsselungscode kann auf diese Daten zugreifen und sie entschlüsseln. Auf einem System können unbegrenzt viele Verschlüsselungscodes erstellt und gespeichert werden. Der DVM verwendet 256-Bit-AES-Verschlüsselung im CBC-Modus (Cipher Block Chaining) mit 256-Bit-Schlüsseln. Die Verschlüsselung wird inline auf Snapshot-Daten durchgeführt, bei Verbindungsgeschwindigkeiten und ohne die Leistung zu beeinträchtigen. Dies liegt daran, dass die DVM-Implementierung Multithread-fähig ist und Hardwarebeschleunigung verwendet, die für den Prozessor, auf dem sie bereitgestellt wird, spezifisch ist.

Die Verschlüsselung ist mehrinstanzenfähig. Die Deduplizierung wurde speziell auf Datensätze beschränkt, die mit dem gleichen Schlüssel verschlüsselt wurden. Zwei identische Datensätze, die mit unterschiedlichen Schlüsseln verschlüsselt wurden, werden nicht gegeneinander dedupliziert. Dank dieses Konzepts wird sichergestellt, dass mithilfe der Deduplizierung keine Daten zwischen unterschiedlichen Verschlüsselungsdomains weitergegeben werden können. Dies ist von Vorteil für Anbieter verwalteter Dienste, da replizierte Backups für mehrere Instanzen (Kunden) auf einem Kern gespeichert werden können, ohne dass eine der Instanzen die Daten einer der anderen Instanzen anzeigen oder darauf zugreifen kann. Jeder Verschlüsselungscode einer aktiven Instanz erstellt eine Verschlüsselungsdomain im Repository, in dem nur der Besitzer des Schlüssels die Daten anzeigen, darauf zugreifen oder sie verwenden kann. In einem Mehrinstanzenszenario werden Daten in den Verschlüsselungsdomains partitioniert und dedupliziert.

In Replikationsszenarien sichert das Gerät die Verbindung zwischen den zwei Kernen in einer Replikationstopologie mithilfe von SSL 3.0, um Abhören und Manipulation zu verhindern.

Replikation

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 zwecks der 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 eine Cloud, die 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.

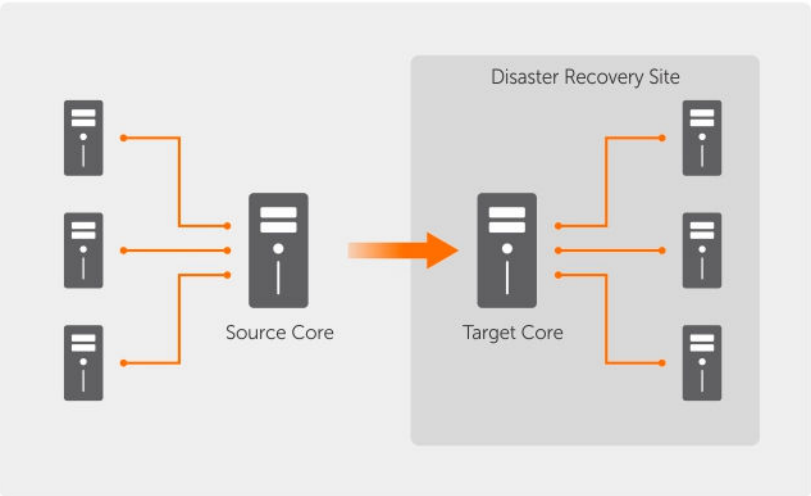


Abbildung 5. Grundlegende Replikationsarchitektur

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. „Seeding" ist die erste Übertragung deduplizierter Basisabbilder und inkrementeller Snapshots von geschützten Maschinen. Die Daten können sich auf Hunderte oder Tausende Gigabytes summieren. Die erste Replikation kann mithilfe externer Medien auf dem Zielkern platziert werden. Dies ist bei großen Datensätzen oder Standorten mit langsamer Verbindung nützlich. Die Daten im Seeding-Archiv sind komprimiert, verschlüsselt und dedupliziert. Wenn die Gesamtgröße des Archivs auf dem externen Datenträger den verfügbaren Speicherplatz überschreitet, kann sich das Archiv über mehrere Geräte erstrecken. Während des Seeding-Vorgangs werden die inkrementellen Wiederherstellungspunkte auf den Zielstandort repliziert. Nachdem die Daten auf den Zielkern übertragen wurden, werden die neu replizierten inkrementellen Wiederherstellungspunkte automatisch synchronisiert.

Recovery-as-a-Service (RaaS)

Anbieter von verwalteten Diensten (Managed Service Providers, MSPs) können das Gerät vollständig als Plattform für die Bereitstellung von Wiederherstellung als Service (RaaS, Recovery-as-a-Service) nutzen. RaaS ermöglicht eine vollständige Wiederherstellung in der Cloud (Recovery-in-the-Cloud), indem die physischen und virtuellen Server des Kunden zusammen mit deren Daten als virtuelle Maschinen zur Cloud des Dienstanbieters repliziert werden, um Wiederherstellungstests oder tatsächliche Wiederherstellungsvorgänge zu unterstützen. 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 Anbieter verwalteter Dienste unverzüglich virtuelle Maschinen für den Kunden bereitstellen.

MSPs können eine mehrinstanzenfähige AppAssure-basierte RaaS-Infrastruktur bereitstellen, die mehrere und eigenständige Organisationen oder Geschäftseinheiten (die Instanzen) hosten kann, die üblicherweise keine Sicherheit oder Daten auf einem einzelnen Server oder einer Gruppe von Servern gemeinsam nutzen. Die Daten jeder Instanz sind isoliert und vor anderen Instanzen und dem Dienstanbieter geschützt.

Aufbewahrung und Archivierung

In dem Gerät sind Backup- sowie Aufbewahrungsrichtlinien flexibel und können daher einfach konfiguriert werden. Die Möglichkeit zur Anpassung der Aufbewahrungsrichtlinien an die Bedürfnisse einer Organisation unterstützt Sie nicht nur bei der Einhaltung von Konformitätsanforderungen, sondern ermöglicht dies auch ohne Beeinträchtigung der RTO.

Aufbewahrungsrichtlinien erzwingen die Zeitdauer, für die Backups auf (schnellen und teuren) Datenträgern gespeichert werden. Mitunter machen geschäftliche und technische Anforderungen eine längere Aufbewahrung dieser Backups 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 unterstützt die längere Aufbewahrung von konformen und nicht-konformen Daten, und kann auch für das Seeding von Replikationsdaten auf einem Zielkern verwendet werden.

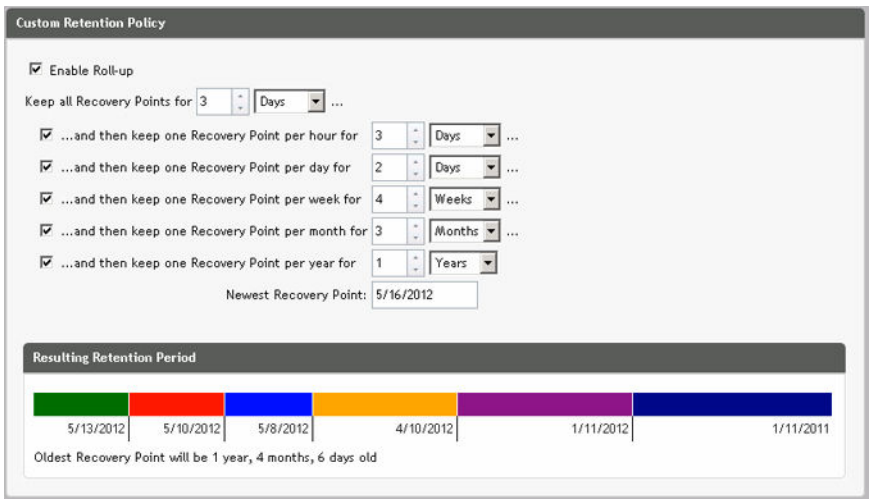


Abbildung 6. Benutzerdefinierte Aufbewahrungsrichtlinie

Aufbewahrungsrichtlinien können im Gerät benutzerdefiniert werden, um die Zeitspanne festzulegen, über die ein Backup-Wiederherstellungspunkt aufrecht erhalten wird. Wenn das Alter der Wiederherstellungspunkte das Ende der Aufbewahrungszeitspanne erreicht, läuft ihre Lebensdauer ab und die Backups werden aus dem Aufbewahrungspool entfernt. Normalerweise wird dieser Prozess ineffizient und schlägt schließlich fehl, da die Datenmenge und die Aufbewahrungsfrist schnell zu wachsen beginnen. Das Gerät löst dieses große Datenproblem, indem es die Aufbewahrung großer Datenmengen mithilfe komplexer Aufbewahrungsrichtlinien verwaltet und Rollup-Vorgänge für die Alterung von Daten mithilfe effizienter Metadatenvorgänge durchführt.

Backups können im Intervall weniger Minuten ausgeführt werden. Während diese Backups über Tage, Monate und Jahre altern, verwalten Aufbewahrungsrichtlinien die Alterung und das Löschen alter Backups. Der Alterungsprozess wird durch eine einfache Wasserfallmethode definiert. Die Stufen im Wasserfall werden in Minuten, Stunden und Tagen sowie Wochen, Monaten und Jahren definiert. Die Aufbewahrungsrichtlinie wird durch den nächtlichen Rollup-Prozess erzwungen.

Für Langzeitspeicherung ermöglicht das Gerät die Fähigkeit ein Archiv der Quelle oder des Zielkerns zu beliebigen Wechseldatenträgern zu erstellen. Das Archiv wird intern optimiert und alle Daten im 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. Außerdem kann das Archiv mit einer Passphrase gesperrt werden. Für die Wiederherstellung aus einem Archiv ist kein neuer Kern erforderlich. Jeder Kern kann das Archiv aufnehmen und Daten wiederherstellen, wenn der Administrator die Passphrase und den Verschlüsselungscode besitzt.

Virtualisierung und Cloud

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

Das Gerät kann beliebige geschützte oder replizierte Maschinen auf eine virtuelle Maschine exportieren, z. B. lizenzierte Versionen von VMware oder Hyper-V. Sie können einen einmaligen virtuellen Export durchführen, oder Sie können eine virtuelle Standby-VM festlegen, indem Sie einen kontinuierlichen virtuellen Export einrichten. Bei einem kontinuierlichen Export wird die virtuelle Maschine inkrementell nach jedem Snapshot aktualisiert. Die inkrementellen Aktualisierungen erfolgen sehr schnell und liefern Ihnen Standby-Klone, die mit einem Mausklick eingeschaltet werden können. Die unterstützten Exporttypen für virtuelle Maschinen sind VMware Workstation/Server in einen Ordner, direkter Export auf einen vSphere/VMware ESX(i)-Host, Export zu Oracle VirtualBox und Export in Microsoft Hyper-V-Server auf Windows Server 2008 (x64), 2008 R2, 2012 (x64) und 2012 R2 (mit Unterstützung für Hyper-V-VMs der 2. Generation).

Sie haben jetzt außerdem die Möglichkeit, Ihre Repository-Daten in der Cloud zu archivieren. Verwenden Sie dazu Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage oder einen anderen OpenStack-basierten Cloud-Dienst.

Benachrichtigungs- und Ereignisverwaltung

Neben der HTTP-REST-API umfasst das Gerät auch einen umfangreichen Satz an Funktionen für die Ereignisprotokollierung und Benachrichtigung mithilfe von E-Mails, Syslog oder Windows-Ereignisprotokollen. Über E-Mail-Benachrichtigungen können Benutzer oder Gruppen über Funktionszustand und Status unterschiedlicher Ereignisse als Reaktion auf eine Warnung benachrichtigt werden. Die Syslog- und Windows-Ereignisprotokoll-Methoden werden für die zentrale Protokollierung in ein Repository in Umgebungen mit mehreren Betriebssystemen verwendet. In reinen Windows-Umgebungen wird nur das Windows-Ereignisprotokoll verwendet.

Lizenzportal

Das Lizenzportal stellt einfach zu verwendende Tools für die Verwaltung der Lizenzberechtigungen bereit. Sie können Lizenzschlüssel herunterladen, aktivieren, anzeigen und verwalten sowie ein Unternehmensprofil zur Nachverfolgung Ihrer Lizenzbestände erstellen. Zusätzlich ermöglicht das Portal den Dienstanbietern und Wiederverkäufern, ihre Kundenlizenzen nachzuverfolgen und zu verwalten.

Webkonsole

Das Gerät beinhaltet eine neue webbasierte zentrale Konsole, die verteilte Kerne von einem zentralen Speicherort aus verwaltet. MSPs und Unternehmenskunden mit mehreren verteilten Kernen können die zentrale Konsole bereitstellen und so eine vereinheitlichte Ansicht für die zentrale Verwaltung erhalten. Die zentrale Konsole ermöglicht die Organisation der verwalteten Kerne in hierarchischen Organisationseinheiten. Diese Organisationseinheiten können Geschäftseinheiten, -standorte oder -kunden für MSPs mit rollenbasiertem Zugang darstellen. Außerdem kann die zentrale Konsole Berichte auf verwalteten Kernen ausführen.

Serviceverwaltungs-APIs

Das Gerät wird zusammen mit einer Serviceverwaltungs-API geliefert und bietet programmgesteuerten Zugriff auf alle Funktionen, die über die Central Management Console verfügbar sind. Die Serviceverwaltungs-API ist eine REST-API. Alle API-Vorgänge werden über SSL durchgeführt und werden gegenseitig mithilfe von X.509 v3-Zertifikaten authentifiziert. Auf den Verwaltungsservice kann innerhalb der Umgebung oder direkt über das Internet von jeder Anwendung aus zugegriffen werden, die HTTPS-Anforderungen und -Antworten senden und empfangen kann. Dieser Ansatz unterstützt eine einfache Integration in jede beliebige Webanwendung wie etwa RMM-Tools (Relationship Management Methodology) oder Abrechnungssysteme. Darüber hinaus ist ein SDK-Client für die PowerShell-Skripterstellung enthalten.

2

Arbeiten mit dem DL4000-Kern

Zugreifen auf die DL4000 Core Console

So erhalten Sie Zugang zur Core Console:

1. Aktualisieren Sie die vertrauenswürdigen Seiten in Ihrem Browser. Weitere Informationen finden Sie unter Aktualisieren von vertrauenswürdigen Seiten in Internet Explorer.
2. Konfigurieren Sie Ihre Browser für den Remotezugriff auf die Core Console. Weitere Informationen finden Sie unter Konfigurieren von Browsern für den Remotezugriff auf die Core Console.
3. Führen Sie für den Zugang zur Core Console einen der folgenden Schritte aus:
   - Melden Sie sich lokal bei Ihrem DL4000-Kernserver an, und doppelklicken Sie dann auf das Symbol der **Core Console**.
   - 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 Microsoft 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 **Add** (Hinzufügen).
8. Geben Sie in **Add this website to the zone**, (Diese Website zur Zone hinzufügen) Folgendes ein: **about:blank**.
9. Klicken Sie auf **Add** (Hinzufügen).
10. Klicken Sie auf **Close** (Schließen) und dann auf **OK**.

Konfigurieren von Browsern für den Remotezugriff auf die Core Console

Für den Zugriff auf die Core Console von einer Remote-Maschine müssen Sie Ihre Browser-Einstellungen anpassen.

ANMERKUNG: Melden Sie sich zum Ändern der Browser-Einstellungen als Administrator am System an.

ANMERKUNG: Google Chrome verwendet Microsoft Internet Explorer-Einstellungen, ändern Sie die Einstellungen für den Chrome-Browser über den Internet Explorer.

ANMERKUNG: Stellen Sie sicher, dass die Option **Internet Explorer Enhanced Security Configuration** (Verstärkte Sicherheitskonfiguration für Internet Explorer) eingeschaltet ist, wenn Sie entweder lokal oder remote auf die Core-Web-Konsole zugreifen. So schalten Sie die Option **Internet Explorer Enhanced Security Configuration** (Verstärkte Sicherheitskonfiguration für Internet Explorer) ein:

1. Öffnen Sie den **Server-Manager**.
2. Wählen Sie die Option **Local Server IE Enhanced Security Configuration** (Verstärkte Sicherheitskonfiguration für Internet Explorer für lokale Server) auf der rechten Seite aus. Stellen Sie sicher, dass sich die Option in der Position **On** (Ein) befindet.

Konfiguration der Browser-Einstellungen für Internet Explorer und Chrome:

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

1. Öffnen Sie Internet Explorer.
2. Wählen Sie im Menü **Tools** (Extras) die Option **Internet Options** (Internetoptionen) auf der Registerkarte **Security** (Sicherheit) aus.
3. Klicken Sie auf **Trusted Sites** (Vertrauenswürdige Seiten) und klicken Sie dann auf **Sites** (Seiten).
4. 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://<*Host-Name oder IP-Adresse des Geräteservers, der den AppAssure-Kern hostet*> zu **Trusted Sites** (Vertrauenswürdige Sites) hinzu.
5. Klicken sie auf **Close** (Schließen), wählen Sie **Trusted Sites** (Vertrauenswürdige Sites) aus und klicken Sie dann auf **Custom Level** (Benutzerdefinierte Stufe).
6. Scrollen Sie zu **Miscellaneous** → **Display Mixed Content** (Verschiedenes → Gemischten Inhalt anzeigen) und klicken Sie auf **Enable** (Aktivieren).
7. 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).
8. Klicken Sie auf **OK** und wählen Sie dann die Registerkarte **Advanced** (Erweitert).
9. Scrollen Sie zu **Multimedia** und wählen Sie **Play animations in webpages** (Auf Webseiten Animationen abspielen) aus.
10. Scrollen Sie zu **Security** (Sicherheit), markieren Sie **Enable Integrated Windows Authentication** (Integrierte Windows-Authentifizierung) und klicken Sie dann auf **OK**.

Konfiguration von Mozilla Firefox-Browser-Einstellungen

ANMERKUNG: Um die Mozilla Firefox-Browser-Einstellungen in den neuesten Versionen von Firefox zu ändern, muss der Schutz deaktiviert werden. Klicken Sie mit der rechten Maustaste auf die Schaltfläche „Site Identify" (Site identifizieren) (auf der linken Seite der URL), klicken Sie auf **Options** (Optionen) und dann auf **Disable protection for now** (Schutz vorübergehend deaktivieren).

So ändern Sie die Mozilla Firefox-Browser-Einstellungen:

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 Hostnamen oder die IP-Adresse des Gerätessystems, das den AppAssure-Kern hostet, durch ein Komma getrennt ein, zum Beispiel *IP-Adresse*, *Hostname*.

4. Starten Sie Firefox neu.

Ablaufplan für die Konfiguration des Kerns

Die Konfiguration umfasst verschiedene Aufgaben, wie etwa das Erstellen und Konfigurieren des Repositorys für die Speicherung von Sicherungs-Snapshots, das Definieren von Verschlüsselungsschlüsseln für die Sicherung geschützter Daten sowie das Einrichten von Warnungen und Benachrichtigungen. Sobald Sie die Konfiguration des Kerns abgeschlossen haben, können Sie Agenten schützen und Wiederherstellungen durchführen.

Für die Konfiguration des Kerns müssen Sie bestimmte Konzepte verstehen und zuerst die folgenden Vorgänge durchführen:

- Erstellen eines Repositorys
- Konfigurieren von Verschlüsselungsschlüsseln
- Konfigurieren von Ereignisbenachrichtigungen
- Konfigurieren von Aufbewahrungsrichtlinien
- Konfigurieren der SQL-Anfügbarkeit

ANMERKUNG: Wenn Sie ein Gerät verwenden, sollten Sie die Konfiguration des Kerns über die Registerkarte **Appliance** (Gerät) durchführen. Weitere Informationen zur Konfiguration des Kerns nach der anfänglichen Installation finden Sie im *Dell DL4000 Appliance Deployment Guide* (Bereitstellungshandbuch für das Dell DL4000-Gerät) unter **dell.com/support/home**.

Lizenzverwaltung

Sie können Ihre Lizenzen direkt über die Core Console verwalten. Über diese Konsole können Sie den Lizenzschlüssel ändern und den Lizenzserver kontaktieren. Sie können auch über die Seite „Lizenzierung" der Core Console auf das Lizenzportal zugreifen.

Die Lizenzierungsseite enthält folgende Informationen:

- Lizenztyp
- Lizenzstatus
- Lizenzbeschränkungen
- Anzahl von geschützten Maschinen
- Status der letzten Antwort vom Lizenzserver
- Zeitpunkt des letzten Kontaktes mit dem Lizenzserver
- Nächster geplanter Kontaktversuch mit dem Lizenzserver

Ändern eines Lizenzschlüssels

So ändern Sie einen Lizenzschlüssel:

1. Navigieren Sie zur Core Console.
2. Wählen Sie **Konfiguration** → **Lizenzierung** aus.
   Die Seite **Lizenzierung** wird angezeigt.

3. Klicken Sie im Abschnitt **Lizenzdetails** auf **Lizenz ändern**.

   Das Dialogfeld **Lizenz ändern** wird angezeigt.
4. Geben Sie im Dialogfeld **Lizenz ändern** den neuen Lizenzschlüssel ein, und klicken Sie auf **Fortfahren**.

Kontaktieren des Lizenzportalservers

Die Core Console kontaktiert regelmäßig den Portalserver, um bezüglich aller Änderungen, die im Lizenzportal durchgeführt wurden, auf dem neuesten Stand zu sein. In der Regel erfolgt die Kommunikation mit dem Portalserver automatisch in bestimmten Intervallen. Sie können die Kommunikation jedoch auch bei Bedarf initiieren.

So kontaktieren Sie den Portalserver:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Konfiguration → Lizenzierung**.
3. Klicken Sie in der Option **Lizenzserver** auf **etzt kontaktieren**.

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 `regdit`.
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 BS-Sprache während der Installation

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

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.

Verwalten von Kerneinstellungen

Mit den Kerneinstellungen werden verschiedene Einstellungen für Konfiguration und Leistung definiert. Die meisten Einstellungen werden für die optimale Nutzung konfiguriert. Sie können die folgenden Einstellungen aber auch nach Bedarf ändern:

- Allgemein
- Nightly Jobs (Nächtliche Aufgaben)
- Transfer Queue (Übertragungswarteschlange)
- Client Timeout Settings (Einstellungen für Client-Zeitüberschreitung)
- Deduplication Cache Configuration (Konfiguration des Deduplizierungscache)
- Database Connection Settings (Einstellungen für Datenbankverbindung)

Ändern des Anzeigenamens des Kerns

ANMERKUNG: Es wird empfohlen, dass Sie gleich bei der anfänglichen Konfiguration des Geräts einen permanenten Anzeigenamen auswählen. Wenn Sie ihn zu einem späteren Zeitpunkt ändern, müssen Sie mehrere Schritte manuell ausführen, um sicherzustellen, dass der neue Host-Name in Kraft tritt und das System richtig funktioniert. Weitere Informationen siehe Changing The Host Name Manually (Manuelles Ändern des Host-Namens).

So ändern Sie den Anzeigenamen des Kerns

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Konfiguration → Einstellungen**.
3. Klicken Sie im Bereich **Allgemein** auf **Ändern**.
   Das Dialogfeld **Allgemeine Einstellungen** wird angezeigt.
4. Geben Sie im Textfeld **Display Name** (Anzeigename) einen neuen Anzeigenamen für den Kern ein.
   Dies ist der Name, der in der Core Console angezeigt wird. Sie können bis zu 64 Zeichen eingeben.
5. Geben Sie in das Textfeld **Web Server-Port** eine Portnummer für den Web Server ein. Die Standardeinstellung ist 8006.
6. Geben Sie in das Feld **Service-Port** eine Portnummer für den Dienst ein. Die Standardeinstellung ist 8006.
7. Klicken Sie auf **OK**.

Anpassen der Uhrzeit für eine nächtliche Aufgabe

So passen Sie die Zeit für eine nächtliche Aufgabe an:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Konfiguration → Einstellungen**.
3. Klicken Sie im Bereich **Nightly Jobs** (Nächtliche Aufgaben) auf **Change** (Ändern).
   Das Dialogfeld **Nächtliche Aufgaben** wird angezeigt.
4. Geben Sie in das Textfeld **Nightly Jobs Time** (Uhrzeit für nächtliche Jobs) eine neue Uhrzeit zur Ausführung der nächtlichen Jobs ein.
5. Klicken Sie auf **OK**.

Ändern der Einstellungen für die Übertragungswarteschlange

Die Einstellungen für die Übertragungswarteschlange sind Einstellungen der Kernebene, die die maximale Anzahl gleichzeitiger Übertragungen und die maximale Anzahl der Wiederholungen für die Übertragung der Daten einrichtet.

So ändern Sie die Einstellungen für die Übertragungswarteschlange:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Konfiguration → Einstellungen**.
3. Klicken Sie im Bereich **Übertragungswarteschlange** auf **Ändern**.
   Das Dialogfeld **Übertragungswarteschlange** wird angezeigt.
4. Geben Sie im **Textfeld Maximum Concurrent** Transfers (Maximale Anzahl gleichzeitiger Übertragungen) einen Wert ein, um die Anzahl gleichzeitiger Übertragungen zu aktualisieren.
   Stellen Sie eine Nummer von 1 bis 60 ein. Je kleiner die Zahl, desto geringer ist die Last auf dem Netzwerk und auf anderen System-Ressourcen. Wenn sich die verarbeitete Kapazität erhöht, nimmt auch die Belastung des Systems zu.
5. Geben Sie im Textfeld **Maximum Retries** (Maximale Anzahl erneuter Versuche) einen Wert ein, um die maximale Anzahl an Wiederholungsversuchen zu aktualisieren.
6. Klicken Sie auf **OK**.

Anpassen der Client-Zeitüberschreitungseinstellungen

So stellen Sie die Client-Zeitüberschreitungseinstellungen ein:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Konfiguration → Einstellungen**.
3. Klicken Sie im Bereich **Client Timeout Settings Configuration** (Konfiguration der Client-Zeitüberschreitungseinstellungen) auf **Change** (Ändern).

   Das Dialogfeld **Client-Zeitüberschreitungseinstellungen** wird angezeigt.
4. Geben Sie im Textfeld **Connection Timeout** (Verbindungszeitüberschreitung) die Anzahl an Minuten und Sekunden ein, die vor einem Verbindungstimeout verstreichen müssen.
5. Geben Sie in das Textfeld **Verbindungszeitüberschreitung Benutzeroberfläche** die Anzahl der Minuten und Sekunden ein, die vor einer Verbindungszeitüberschreitung auf der Benutzeroberfläche verstreichen müssen.
6. Geben Sie im Textfeld **Lese-/Schreibzeitüberschreitung** die Anzahl an Minuten und Sekunden ein, die vor einem Timeout während eines Lese-/Schreibereignisses verstreichen müssen.
7. Geben Sie in das Textfeld **Lese-/Schreibzeitüberschreitung Benutzeroberfläche** die Anzahl der Minuten und Sekunden ein, die vor einer Zeitüberschreitung während eines Lese-/Schreibvorgangs auf der Benutzeroberfläche verstreichen müssen.
8. Klicken Sie auf **OK**.

Konfigurieren von Deduplizierungs-Cache-Einstellungen

So konfigurieren Sie Deduplizierungs-Cache-Einstellungen:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Konfiguration → Einstellungen**.
3. Klicken Sie im Bereich **Deduplication Cache Configuration** (Konfiguration der Deduplizierungs-Cache) auf **Change** (Ändern).

   Das Dialogfeld **Konfiguration des Deduplizierungs-Cache** wird angezeigt.
4. Geben Sie im Feld **Primary Cache Location** (Primärer Cache-Speicherort) einen aktualisierten Wert ein, um den primären Cache-Speicherort zu ändern.
5. Geben Sie im Feld **Secondary Cache Location** (Sekundärer Cache-Speicherort) einen aktualisierten Wert ein, um den sekundären Cache-Speicherort zu ändern.
6. Geben Sie im Feld **Metadata Cache Location** (Metadaten-Cache-Speicherort) einen aktualisierten Wert ein, um den Metadaten-Cache-Speicherort zu ändern.
7. Geben Sie in das Textfeld **Größe des Deduplizierungs-Cache** einen Wert ein, der dem Speicherplatz entspricht, den Sie für den Deduplizierungs-Cache zuweisen möchten.

   Wählen Sie als Maßeinheit für den Wert im Textfeld „Größe des Deduplizierungs-Cache“ im Drop-Down-Menü die Option GB (Gigabyte) oder TB (Terabyte) aus.
8. Klicken Sie auf **OK**.

   ANMERKUNG: Sie müssen den Kern-Service neu starten, damit die Änderungen wirksam werden.

Ändern von Moduleinstellungen

So ändern Sie die Moduleinstellungen:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Konfiguration → Einstellungen**.
3. Klicken Sie im Bereich **Replay-Modulkonfiguration** auf **Ändern**.
   Das Dialogfeld **Replay-Modulkonfiguration** wird angezeigt.
4. Geben Sie die nachfolgend beschriebenen Konfigurationsinformationen ein:

Textfeld	Beschreibung
IP-Adresse	• Um die bevorzugte IP-Adresse von Ihrem TCP/IP zu verwenden, klicken Sie auf **Automatisch bestimmt**. • Um eine IP-Adresse manuell einzugeben, klicken Sie auf **Spezifische Adresse verwenden**.
Preferable Port (Bevorzugter Port)	Geben Sie eine Portnummer ein, oder akzeptieren Sie die Standardeinstellungen. Der Standardport ist 8007. Der Port wird dazu verwendet, den Kommunikationskanal für das Modul festzulegen.
Verwendeter Port	Bezeichnet den Port, der für die Replay-Modulkonfiguration verwendet wird.
Automatische Portzuweisung zulassen	Klicken Sie hier, um den TCP-Port automatisch zuzuweisen.
Admin Group (Admin-Gruppe)	Geben Sie einen neuen Namen für die Verwaltungsgruppe ein. Der Standardname ist **BUILTIN\Administrators**.
Minimum Async I/O Length (Minimale Async-E/A-Länge)	Geben Sie einen Wert ein oder wählen Sie die Standardeinstellung. Beschreibt die minimale asynchrone Eingabe-/Ausgabelänge. Die Standardeinstellung ist 65536.
Receive Buffer Size (Größe Empfangspuffersp eicher)	Geben Sie eine Puffergröße für eingehende Daten ein oder akzeptieren Sie die Standardeinstellung. Die Standardeinstellung ist 8192.
Send Buffer Size (Größe Sendepufferspeic her)	Geben Sie eine Puffergröße für ausgehende Daten ein oder akzeptieren Sie die Standardeinstellung. Die Standardeinstellung ist 8192.
Read Timeout (Zeitüberschreitun g beim Lesen)	Geben Sie einen Wert für die Zeitüberschreitung beim Lesen ein oder wählen Sie die Standardeinstellung aus. Die Standardeinstellung ist 00:00:30.
Write Timeout (Zeitüberschreitun g beim Schreiben)	Geben Sie einen Wert für die Zeitüberschreitung beim Schreiben ein oder wählen Sie die Standardeinstellung aus. Die Standardeinstellung ist 00:00:30.

Textfeld	Beschreibung
Ohne Verzögerung	Es wird empfohlen, dieses Kontrollkästchen deaktiviert zu lassen, da eine Aktivierung Auswirkungen auf die Effizienz im Netzwerk hat. Wenn Sie zu dem Schluss kommen, dass Sie diese Einstellung ändern müssen, wenden Sie sich an den Dell Support, um Unterstützung zu erhalten.

5. Klicken Sie auf **OK**.

Ändern der Datenbankverbindungseinstellungen

So ändern Sie die Datenbankverbindungseinstellungen:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Konfiguration** → **Einstellungen**.
3. Führen Sie im Bereich **Datenbankverbindungseinstellungen** einen der folgenden Schritte aus:
   - Klicken Sie auf **Apply Default** (Standard übernehmen).
   - Klicken Sie auf **Change** (Ändern).

   Das Dialogfeld **Datenbankverbindungseinstellungen** wird angezeigt.
4. Geben Sie die nachfolgend beschriebenen Einstellungen für die Änderung der Datenbankverbindung ein.

Textfeld	Beschreibung
Host-Name	Geben Sie einen Hostnamen für die Datenbankverbindung ein.
Schnittstelle	Geben Sie eine Portnummer für die Datenbankverbindung ein.
Benutzername (optional)	Geben Sie einen Benutzernamen für den Zugriff auf und die Verwaltung der Datenbankverbindungseinstellungen ein. Er wird zur Festlegung von Anmeldeinformationen für den Zugriff auf die Datenbankverbindung verwendet.
Kennwort (optional)	Geben Sie ein Kennwort für den Zugriff auf und die Verwaltung der Datenbankverbindungseinstellungen ein.
Ereignis- und Aufgabenverlauf aufbewahren für (Dauer in Tagen)	Geben Sie die Anzahl an Tagen ein, die der Ereignis- und Aufgabenverlauf für die Datenbankverbindung aufbewahrt werden soll.
Max. Größe des Verbindungspools	Bestimmt die maximal zulässige Anzahl der im Cache gespeicherten Datenbankverbindungen für die dynamische Wiederverwendung. Die Standardeinstellung ist 100.
Min. Größe des Verbindungspools	Bestimmt die minimal zulässige Anzahl der im Cache gespeicherten Datenbankverbindungen für die dynamische Wiederverwendung. Die Standardeinstellung ist 0.

5. Klicken Sie auf **Test Connection** (Verbindung testen), um Ihre Einstellungen zu prüfen.
6. Klicken Sie auf **Speichern**.

Wissenswertes über Repositories

Ein Repository wird für die Speicherung der Snapshots verwendet, die von den geschützten Arbeitsstationen und Servern erfasst werden. Das Repository kann sich auf verschiedenen

Speichertechnologien wie Storage Area Network (SAN, Speicherbereichsnetzwerk), Direct Attached Storage (DAS, Direkt angeschlossene Speicherung) oder Network Attached Storage (NAS, Netzgebundene Speicherung) befinden.

Wenn Sie ein Repository erstellen, weist der Kern vorab den Speicherplatz zu, der für die Daten und Metadaten im angegebenen Speicherort erforderlich ist. Auf einem Kern können Sie bis zu 255 unabhängige Repositories erstellen, die verschiedene Speichertechnologien umfassen können. Darüber hinaus können Sie die Größe eines Repositorys zusätzlich erweitern, indem Sie neue Dateierweiterungen oder -spezifikationen hinzufügen. Ein erweitertes Repository kann bis zu 4096 Erweiterungen enthalten, die verschiedene Speichertechnologien umfassen.

Wichtige Repository-Konzepte und -Überlegungen sind u. a.:

- Das Repository basiert auf dem skalierbaren AppAssure-Objektdateisystem.
- Alle in einem Repository gespeicherten Daten sind global dedupliziert.
- Das skalierbare Objektdateisystem kann eine skalierbare E/A-Leistung zusammen mit globaler Datendeduplizierung, Verschlüsselung und Aufbewahrungsverwaltung bieten.

ANMERKUNG: DL4000-Repositorys werden auf primären Speichergeräten gespeichert. Archivspeichergeräte wie Data Domain werden aufgrund von Leistungsbeschränkungen nicht unterstützt. Gleichermaßen dürfen Repositorys nicht auf NAS-Dateispeichern gespeichert werden, die zur Cloud abgestuft werden, da diese Geräte zu Leistungsbeschränkungen neigen, wenn sie als primäre Speicher verwendet werden.

Ablaufplan für die Verwaltung eines Repositorys

Der Ablaufplan für die Verwaltung eines Repositorys deckt Aufgaben wie das Erstellen, Konfigurieren und Anzeigen eines Repositorys ab und umfasst folgende Themen:

- Zugreifen auf die Core Console
- Erstellen eines Repositorys
- Anzeigen von Details eines Repositorys
- Ändern der Repository-Einstellungen
- Hinzufügen eines Speicherorts zu einem vorhandenen Repository
- Prüfen eines Repositorys
- Löschen eines Repositorys
- Wiederherstellen eines Repositorys

ANMERKUNG: Es wird empfohlen, zur Konfiguration von Repositorys die Registerkarte **Gerät** zu verwenden.

Damit Sie das Gerät nutzen können, müssen Sie zuerst mindestens ein Repository auf dem Kernserver einrichten. Ein Repository speichert Ihre geschützten Daten, genauer gesagt, die Snapshots, die von den geschützten Servern in Ihrer Umgebung erstellt wurden.

Bei der Konfiguration eines Repositorys können Sie unterschiedliche Aufgaben ausführen, z. B. Festlegen des Speicherorts des Datenspeichers auf dem Kernserver, der Anzahl an Speicherorten, die zu jedem Repository hinzugefügt werden können, Festlegen des Repository-Namens und der Anzahl an aktuellen Abläufen, die Repositorys unterstützen.

Wenn Sie ein Repository erstellen, weist der Kern vorab den Platz zu, der für die Speicherung der Daten und Metadaten im angegebenen Speicherort erforderlich ist. Sie können auf einem Kern bis zu 255

unabhängige Repositorys erstellen. Um die Größe eines Repositorys weiter zu erhöhen, können Sie neue Speicherorte oder Volumes hinzufügen.

Sie können Repositorys zur Core Console hinzufügen bzw. darin bearbeiten.

Erstellen eines Repositorys

ANMERKUNG: Wenn Sie das Gerät als SAN verwenden, wird empfohlen, die Registerkarte **Appliance** (Gerät) zum Erstellen von Repositories zu verwenden. Siehe Breitstellung von ausgewählten Speichern.

Führen Sie die folgenden Schritte aus, um ein Repository manuell zu erstellen:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Configuration (Konfiguration)** → **Repositories** (Repositories).
3. Klicken Sie auf **Add new** (Neues hinzufügen).
   Das Dialogfeld **Add New Repository** (Neues Repository hinzufügen) wird angezeigt.
4. Geben Sie die in der folgenden Tabelle beschriebenen Informationen ein.

Textfeld	Beschreibung
Repository-Name	Geben Sie den Anzeigenamen des Repositorys ein. Dieses Textfeld enthält standardmäßig das Wort Repository sowie eine Indexnummer, die sequenziell dem neuen Repository eine Nummer hinzufügt, beginnend mit 1. Sie können den Namen bei Bedarf ändern und Sie können bis zu 150 Zeichen eingeben.
Gleichzeitige Vorgänge	Definieren Sie die Anzahl an gleichzeitigen Anforderungen, die Sie möchten, dass das Repository unterstützt. Der Standardwert lautet 64.
Bemerkungen	Geben Sie optional eine beschreibende Anmerkung zu diesem Repository ein.

5. Klicken Sie auf **Add Storage Location** (Speicherort hinzufügen), um den spezifischen Speicherort oder das Volume für das Repository zu definieren.

   VORSICHT: Wenn das AppAssure-Repository, das Sie in diesem Schritt erstellen, später entfernt wird, werden alle Ordner am Speicherort Ihres Repositorys gelöscht. Wenn Sie keinen dedizierten Ordner zum Speichern der Repository-Ordner definieren, werden diese Ordner in root gespeichert; wenn Sie das Repository löschen, löschen Sie auch den gesamten Inhalt von root, was zu verheerendem Datenverlust führt.

   ANMERKUNG: Repositories werden auf primären Speichergeräten gespeichert. Archivspeichergeräte wie Data Domain werden aufgrund von Leistungsbeschränkungen nicht unterstützt. Gleichermaßen dürfen Repositories nicht auf NAS-Dateispeichern gespeichert werden, die zur Cloud abgestuft werden, da diese Geräte zu Leistungsbeschränkungen neigen, wenn sie als primäre Speicher verwendet werden.

   Das Dialogfeld **Add Storage Location** (Speicherort hinzufügen) wird angezeigt.
6. Legen Sie fest, wie die Datei für den Speicherort hinzugefügt werden soll. Sie können auswählen, ob Sie die Datei auf lokalem Laufwerk oder auf CIFS-Freigabe hinzufügen.
   - Klicken Sie auf **Add file on local disk** (Datei auf lokalem Datenträger hinzufügen) und geben Sie dann die nachfolgend beschriebenen Informationen ein:

Textfeld	Beschreibung
Datenpfad	Geben Sie den Speicherort für die geschützten Daten ein; Geben Sie beispielsweise ein: **X:\Repository\Data**. Verwenden Sie bei der Angabe des Pfades nur alphanumerische Zeichen, den Bindestrich und den Punkt (nur zur Trennung von Hostnamen und Domänen). Bei den Buchstaben a bis z wird Groß-/Kleinschreibung nicht beachtet. Geben Sie keine Leerstellen ein. Keine anderen Symbole oder Satzzeichen sind zulässig.
Metadatenpfad	Geben Sie den Speicherort für die geschützten Metadaten ein; Geben Sie beispielsweise ein: **X:\Repository\Metadata**. Verwenden Sie bei der Angabe des Pfades nur alphanumerische Zeichen, den Bindestrich und den Punkt (nur zur Trennung von Hostnamen und Domänen). Bei den Buchstaben a bis z wird Groß-/Kleinschreibung nicht beachtet. Geben Sie keine Leerstellen ein. Keine anderen Symbole oder Satzzeichen sind zulässig.

- Oder klicken Sie auf **Add file on CIFS share** (Datei auf CIFS-Freigabe hinzufügen), und geben Sie dann die nachfolgend beschriebenen Informationen ein:

Textfeld	Beschreibung
UNC-Pfad	Geben Sie den Pfad für den Netzwerkfreigabe-Speicherort ein. Wenn sich dieser Speicherort auf root befindet, definieren Sie einen dedizierten Ordner (zum Beispiel: Repository). Der Pfad muss mit \\ beginnen. Verwenden Sie bei der Angabe des Pfades nur alphanumerische Zeichen, den Bindestrich und den Punkt (nur zur Trennung von Hostnamen und Domänen). Bei den Buchstaben a bis z wird Groß-/Kleinschreibung nicht beachtet. Geben Sie keine Leerstellen ein. Keine anderen Symbole oder Satzzeichen sind zulässig.
Benutzername	Geben Sie einen Benutzernamen für den Zugriff auf den Netzwerkfreigabe-Speicherort an.
Kennwort	Geben Sie ein Kennwort für den Zugriff auf den Netzwerkfreigabe-Speicherort an.

7. Klicken Sie im Fenster **Details** auf **Show/Hide Details** (Details anzeigen/ausblenden) und geben Sie dann die Einzelheiten für den Speicherort ein, wie unten beschrieben:

Textfeld	Beschreibung
Größe	Legen Sie die Größe oder Kapazität für den Speicherort fest. Die Standardeinstellung ist 250 MB. Sie können zwischen folgenden Optionen wählen: • MB • GB • TB **ANMERKUNG:** Die von Ihnen angegebene Größe darf nicht die Größe des Volumes überschreiten.

Textfeld	Beschreibung
	ANMERKUNG: Wenn dieser Speicherort ein Volume des New Technology File System (NTFS) ist, das Windows XP oder Windows 7 verwendet, beträgt die Größenbegrenzung 16 TB. Wenn der Speicherort ein NTFS-Volume ist, das Windows 8 oder Windows Server 2012 verwendet, dann ist die Dateigrößenbeschränkung 256 TB. **ANMERKUNG:** Damit das Betriebssystem validiert werden kann, muss Windows-Verwaltungs-Instrumentation (Windows Management Instrumentation, WMI) auf dem vorgesehenen Speicherort installiert sein.
Write Caching Policy (Schreib-Richtlinie zum Ablegen im Cache-Speicher)	Die Schreib-Richtlinie zum Ablegen im Cache-Speicher steuert, wie der Windows Cache-Manager im Repository verwendet wird, und hilft bei der Abstimmung des Repositorys für die optimale Leistung bei unterschiedlichen Konfigurationen. Setzen Sie den Wert auf eine der folgenden Optionen: • Ein • Aus • Sync Wenn der Wert auf Standardeinstellung „On" (Ein) eingestellt ist, steuert Windows das Ablegen im Cache-Speicher. **ANMERKUNG:** Die Festlegung der Schreib-Richtlinie zum Ablegen im Cache-Speicher auf „On" (Ein) kann zu schnellerer Leistung führen. Wenn Sie eine Version von Windows Server, die älter als Server 2012 ist verwenden, ist die empfohlene Einstellung **Off** (Aus). Wenn die Einstellung auf **Off** (Aus) gesetzt ist, wird das Ablegen im Cache-Speicher durch AppAssure gesteuert. Bei Auswahl von **Sync** steuert Windows das Ablegen im Cache-Speicher sowie die synchrone Eingabe/Ausgabe.
Bytes pro Sektor	Geben Sie die Anzahl an Bytes an, die jeder Sektor enthalten soll. Der Standardwert ist 512.
Durchschnittswert Byte pro Datensatz	Geben Sie die durchschnittliche Anzahl an Bytes pro Datensatz an. Der Standardwert ist 8192.

8. Klicken Sie auf **Save** (Speichern).
   Der Bildschirm **Repositories** (Repositorys) wird angezeigt, um den neu hinzugefügten Speicherort einzuschließen.
9. Wiederholen Sie Schritt 4 bis 7, um zusätzliche Speicherorte für das Repository hinzuzufügen.
10. Klicken Sie auf **Create** (Erstellen), um das Repository zu erstellen.
    Die **Repository**-Informationen werden in der Registerkarte **Konfiguration** angezeigt.

Anzeigen von Details zu einem Repository

So zeigen Sie die Details eines Repositorys an:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Configuration (Konfiguration)** → **Repositories** (Repositories).
3. Klicken Sie **>** neben der **Status**-Spalte des Repositorys, das Sie ändern möchten.
4. Sie können von der erweiterten Ansich aus folgenden Maßnahmen durchführen:
   - Einstellungen ändern
   - Einen Speicherort hinzufügen
   - Ein Repository überprüfen
   - Ein Repository löschen

   Details werden auch für das Repository angezeigt und schließen die Speicherorte und die Statistiken ein. Details für die Speicherorte schließen Metadatenpfad, Datenpfad, und die Größe ein. Statistische Informationen schließen Folgendes ein:
   - Deduplication (Deduplizierung) – Wird als die Anzahl der Deduplizierung-Hits auf einem Block, verpasste Deduplizierung auf einem Block, und Komprimierungsrate eines Blocks berichtet.
   - Record I/O (E/A aufzeichnen) – Besteht aus der Rate (MB/s), Leserate (MB/s), und Schreibschreiben (MB/s).
   - Storage Engine (Speicher Engine) – Schließt die Rate (MB/s) Leserate (MB/s), und Schreibschreiben (MB/s) ein.

Ändern von Repository-Einstellungen

Nachdem Sie ein Repository hinzugefügt haben, können Sie die Repository-Einstellungen wie die Beschreibung oder die maximale Anzahl gleichzeitiger Vorgänge ändern. Außerdem können Sie einen neuen Speicherort zum Repository hinzufügen.

So ändern Sie Repository-Einstellungen:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Configuration (Konfiguration)** → **Repositories** (Repositories).
3. Klicken Sie auf das Symbol für Einstellungen neben der Spalte „Komprimierungsgrad" unterhalb der Schaltfläche **Aktionen** und dann auf **Einstellungen**.

   Das Dialogfeld **Repository-Einstellungen** wird angezeigt.
4. Bearbeiten Sie beschriebenen die Repository-Informationen wie unten angezeigt

Feld	Beschreibung
Repository-Name	Stellt den Anzeigenamen des Repositorys dar. Dieses Textfeld enthält standardmäßig das Wort Repository sowie eine Indexnummer, die der Nummer des Repositorys entspricht. **ANMERKUNG:** Sie können den Repository-Namen nicht bearbeiten.
Beschreibung	Geben Sie optional eine beschreibende Anmerkung zum Repository ein.
Maximale Anzahl gleichzeitiger Vorgänge	Definieren Sie die Anzahl an gleichzeitigen Anforderungen, die vom Repository unterstützt werden sollen.

Feld	Beschreibung
Deduplizierung aktivieren	Löschen Sie dieses Kontrollkästchen, um Deduplizierung auszuschalten. Um Deduplizierung zu aktivieren, wählen Sie dieses Kontrollkästchen aus. ANMERKUNG: Das Ändern dieser Einstellung betrifft nur Backups, die nach der Erstellung dieser Einstellung erstellt wurden. Vorhandene Daten oder Daten, die von einem anderen Kern repliziert wurden oder von einem Archiv importiert wurden, behalten die Deduplikationswerte, die zu der Zeit vorhanden waren, als die Daten von den geschützten Maschinen erfasst wurden.
Komprimierung aktivieren	Löschen Sie dieses Kontrollkästchen, um Komprimierung auszuschalten. Um Komprimierung zu aktivieren, wählen Sie dieses Kontrollkästchen aus. ANMERKUNG: Diese Einstellung betrifft nur Backups, die nach der Erstellung dieser Einstellung erstellt wurden. Vorhandene Daten oder Daten, die von einem anderen Kern repliziert oder von einem Archiv importiert wurden, behalten die Komprimierungswerte, die zu der Zeit vorhanden waren, als die Daten von den geschützten Maschinen erfasst wurden.

5. Klicken Sie auf **Save** (Speichern).

Erweitern eines vorhandenen Repositorys

Wenn Sie dem Gerät ein weiteres MD1200 DAS hinzufügen, können Sie den verfügbaren Speicherplatz dazu verwenden, ein bestehendes Repository zu erweitern.

So erweitern Sie ein bestehendes Repository:

1. Nachdem Sie MD1200 DAS installiert haben, öffnen Sie die Core Console, wählen Sie die Registerkarte **Appliance** (Gerät) aus, und klicken Sie auf **Tasks**.
2. Klicken Sie auf dem Bildschirm **Tasks** neben dem neuen Speicher auf **Provision** (Bereitstellung).
3. Wählen Sie auf dem Bildschirm **Provisioning Storage** (Speicherbereitstellung) die Option **Expand the existing repository** (Aktuelles Repository erweitern), und wählen Sie dann das Repository aus, das Sie erweitern möchten
4. Klicken Sie auf **Provision** (Bereitstellung)

   Der Bildschirm **Tasks** zeigt die **Status Description** (Statusbeschreibung) neben dem Speichergerät als **Provisioned** (Bereitgestellt) an.

Hinzufügen eines Speicherorts zu einem vorhandenen Repository

Durch das Hinzufügen eines Speicherortes können Sie definieren, wo das Repository oder das Volume gespeichert werden soll.

So fügen Sie einen Speicherort zu einem vorhandenen Repository hinzu:

1. Klicken Sie auf **>** neben der **Status**-Spalte des Repositorys, dem Sie einen Speicherort hinzufügen möchten.
2. Klicken Sie auf **Add Storage Location** (Speicherort hinzufügen).

   Das Dialogfeld **Speicherort hinzufügen** wird angezeigt.
3. Legen Sie fest, wie die Datei für den Speicherort hinzugefügt werden soll. Sie können auswählen, ob Sie die Datei auf lokalem Laufwerk oder auf CIFS-Freigabe hinzufügen.

- Um eine lokale Maschine zu bestimmen, klicken Sie auf **Add file on local disk** (Datei auf lokale Festplatte hinzufügen), und geben Sie dann wie nachfolgend beschrieben die Informationen ein:

Textfeld	Beschreibung
Metadatenpfad	Geben Sie den Speicherort für die geschützten Metadaten ein.
Datenpfad	Geben Sie den Speicherort für die geschützten Daten ein.

- Um einen Speicherort der Netzwerkfreigabe zu bestimmen, klicken sie auf **Add file on CIFS share** (Datei auf CIFS-Freigabe hinzufügen) und geben Sie dann wie nachfolgend beschrieben die Informationen ein:

Textfeld	Beschreibung
UNC-Pfad	Geben Sie den Pfad für den Netzwerkfreigabe-Speicherort ein.
Benutzername	Geben Sie einen Benutzernamen für den Zugriff auf den Netzwerkfreigabe-Speicherort an.
Kennwort	Geben Sie ein Kennwort für den Zugriff auf den Netzwerkfreigabe-Speicherort an.

4. Klicken Sie im Abschnitt **Details** auf **Show/Hide Details** (Details anzeigen/ausblenden) und geben Sie dann die Einzelheiten für den Speicherort ein, wie in der folgenden Tabelle beschrieben.

Textfeld	Beschreibung
Größe	Legen Sie die Größe oder Kapazität für den Speicherort fest. Die standardmäßige Größe ist 250 MB. Sie können zwischen folgenden Optionen wählen: • MB • GB • TB **ANMERKUNG:** Die von Ihnen angegebene Größe darf nicht die Größe des Volumes überschreiten. **ANMERKUNG:** Wenn der Speicherort ein NTFS-Volume ist, das Windows XP oder Window 7 verwendet, dann ist die Dateigrößenbeschränkung 16 TB. Wenn der Speicherort ein NTFS-Volume ist, das Windows 8 oder Windows Server 2012 verwendet, dann ist die Dateigrößenbeschränkung 256 TB. **ANMERKUNG:** Damit das Betriebssystem validiert werden kann, muss WMI auf dem vorgesehenen Speicherort installiert sein.
Write Caching Policy (Schreib-Richtlinie zum Ablegen im Cache-Speicher)	Die Schreib-Richtlinie zum Ablegen im Cache-Speicher steuert, wie der Windows Cache-Manager im Repository verwendet wird, und hilft bei der Abstimmung des Repositorys für die optimale Leistung bei unterschiedlichen Konfigurationen. Setzen Sie den Wert auf eine der folgenden Optionen: • Ein • Aus • Sync Wenn Sie die Standardeinstellung **On** (Ein) ausgewählt haben, steuert Windows das Ablegen im Cache-Speicher.

Textfeld	Beschreibung
	ANMERKUNG: Die Festlegung der Schreib-Richtlinie zum Ablegen im Cache-Speicher auf **On** (Ein) kann zu schnellerer Leistung führen; die empfohlene Einstellung ist jedoch **Off** (Aus). Wenn die Einstellung auf **Aus** gesetzt ist, wird das Ablegen im Cache-Speicher durch AppAssure gesteuert. Bei Auswahl von **Sync** steuert Windows das Ablegen im Cache-Speicher sowie die synchrone Eingabe/Ausgabe.
Bytes pro Sektor	Geben Sie die Anzahl an Bytes an, die jeder Sektor enthalten soll. Der Standardwert ist 512.
Durchschnittswert Byte pro Datensatz	Geben Sie die durchschnittliche Anzahl an Bytes pro Datensatz an. Der Standardwert ist 8192.

5. Klicken Sie auf **Save** (Speichern).
   Der Bildschirm **Repositories** (Repositorys) wird angezeigt, um den neu hinzugefügten Speicherort einzuschließen.
6. Wiederholen Se die Schritte 4 bis 7, um weitere Speicher-Arrays für das Repository hinzuzufügen.
7. Klicken Sie auf **OK**.

Überprüfen eines Repositorys

Mit dem Gerät können Sie im Falle von Fehlern eine Diagnoseprüfung eines Repository-Datenträgers durchführen. Fehler am Kern können u. a. durch unsachgemäßes Ausschalten des Computers und Hardwarefehler verursacht werden.

ANMERKUNG: Dieser Vorgang darf nur zu diagnostischen Zwecken durchgeführt werden.

So überprüfen Sie ein Repository:

1. Klicken Sie auf der Registerkarte **Configuration** (Konfiguration) auf **Repositories** (Repositorys), wählen Sie **>** neben dem Repository aus, das Sie überprüfen möchten.
2. Klicken Sie im Fenster **Actions** (Maßnahmen) auf **Check** (Überprüfen).
   Das Dialogfeld **Repository überprüfen** wird angezeigt.
3. Klicken Sie im Dialogfeld **Check Repository** (Repository überprüfen) auf **Check** (Überprüfen).

   ANMERKUNG: Wenn die Prüfung fehlschlägt, stellen Sie das Repository aus einem Archiv wieder her.

Löschen eines Repositorys

So löschen Sie ein Repository:

1. Klicken Sie auf der Registerkarte **Configuration** (Konfiguration) auf **Repositories** (Repositorys), wählen Sie **>** neben dem Repository aus, das Sie löschen möchten.
2. Klicken Sie im Fenster **Actions** (Maßnahmen) auf **Delete** (Löschen).
3. Klicken Sie im Dialogfeld **Repository löschen** auf **Löschen**.

VORSICHT: Wenn ein Repository gelöscht wird, werden die Daten im Repository verworfen und können nicht wiederhergestellt werden.

Wenn Sie ein Repository löschen, müssen Sie über den OpenManage-Systemadministrator die virtuellen Laufwerke löschen, in der das Repository untergebracht war. Nach dem Löschen der virtuellen Laufwerke können Sie die Laufwerke erneut bereitstellen und das Repository neu erstellen.

Erneutes Bereitstellen von Volumes

So stellen Sie die Volumes erneut bereit:

1. Navigieren Sie zur Core Console.
2. **Gerät** → **Aufgaben**.
3. Klicken Sie auf **Remount Volumes** (Volumes erneut bereitstellen).
   Die Volumes werden erneut bereitgestellt.

Auflösen von fremden Volumes

Wenn ein bereitgestelltes MD1200 ausgeschaltet oder getrennt und dann später wieder eingeschaltet wurde, wird ein Ereignis auf der Core Console angezeigt und gemeldet, dass das MD1200 verbunden ist. Es werden jedoch keine Tasks auf der Registerkarte **Appliance** (Gerät) des Bildschirms **Tasks** angezeigt, die Ihnen eine Wiederherstellung ermöglichen würden. Der Bildschirm **Enclosures** (Gehäuse) meldet, dass sich das MD1200 in einem Fremdzustand befindet und die Repositorys auf den fremden virtuellen Laufwerken offline sind.

So lösen Sie fremde Volumes auf:

1. Wählen Sie auf der Core Console die Registerkarte **Gerät** aus, und klicken Sie dann auf **Volumes erneut bereitstellen**.
   Die Volumes werden erneut bereitgestellt.
2. Wählen Sie die Registerkarte **Configuration** (Konfiguration) aus und klicken Sie dann auf **Repositories** (Repositorys).
3. Wenn Sie auf **>** neben **Status** klicken, erweitern Sie das Repository mit der roten Statusanzeige.
4. Um die Integrität des Repository zu überprüfen, klicken Sie unter **Actions** (Maßnahmen) auf **Check** (Überprüfen).

Wiederherstellen eines Repositorys

Wenn das Gerät ein Repository nicht importieren kann, meldet es den Fehler auf dem Bildschirm **Tasks**, wobei der Task-Status durch einen roten Kreis gekennzeichnet wird und die Statusbeschreibung **Error, Completed — Exception** (Fehler, Abgeschlossen – Ausnahme) meldet. Um die Fehlerdetails auf dem Bildschirm **Tasks** anzuzeigen, erweitern Sie die Task-Details durch Klicken auf **>** neben der Spalte **Status**. In den **Status Details** (Statusdetails) wird gemeldet, dass der Status der Wiederherstellungs-Task eine Ausnahme ist, und die Spalte **Error Message** (Fehlermeldung) gibt zusätzliche Details zum Fehlerzustand an.

So stellen Sie ein Repository von einem fehlgeschlagenen Importstatus wieder her:

1. Navigieren Sie zur Core Console.
   Der Bildschirm **Repositories** zeigt das fehlgeschlagene Repository mit einer roten Statusanzeige an.
2. Klicken Sie auf **Configuration (Konfiguration)** → **Repositories** (Repositories).
3. Klicken Sie auf **>** neben **Status**, um das fehlgeschlagene Repository zu erweitern.
4. Klicken Sie im Abschnitt **Actions** (Maßnahmen) auf **Check** (Überprüfen) und klicken Sie dann auf **Yes** (Ja), um zu bestätigen, dass Sie die Überprüfung ausführen möchten.

Das Gerät stellt das Repository wieder her.

Verwalten von Sicherheit

Der Kern kann Snapshot-Daten einer geschützten Maschine im Repository verschlüsseln. Statt das gesamte Repository zu verschlüsseln, können Sie während beim Schutz der Maschine in einem Repository einen Verschlüsselungscode festlegen, sodass die Schlüssel für verschiedene geschützte Maschinen wiederverwendet werden können. Durch die Verschlüsselung wird die Leistung nicht beeinträchtigt, da jeder aktive Verschlüsselungscode eine Verschlüsselungsdomain erstellt. Somit kann ein einzelner Kern Mehrinstanzenfähigkeit unterstützen, indem er mehrere Verschlüsselungsdomains hostet. In einer Mehrinstanzumgebung werden Daten in den Verschlüsselungsdomains partitioniert und dedupliziert. Da Sie die Verschlüsselungscodes verwalten, können die Schlüssel nicht durch verlorene Datenträger kompromittiert werden. Berücksichtigen Sie folgende Sicherheitskonzepte für Schlüssel und Überlegungen:

- Die Verschlüsselung erfolgt mithilfe des 256-Bit-AES im CBS-Modus (Cipher Block Chaining), der mit SHA-3 kompatibel ist.
- Die Deduplizierung läuft zur Gewährleistung des Datenschutzes in einer Verschlüsselungsdomain ab.
- Durch die Verschlüsselung wird die Leistung nicht beeinträchtigt.
- Sie können die auf dem Kern konfigurierten Verschlüsselungscodes ergänzen, entfernen, importieren, exportieren, ändern und löschen.
- Sie können unbegrenzt viele Verschlüsselungsschlüssel auf dem Kern erstellen.

Hinzufügen eines Verschlüsselungscodes

So fügen Sie einen Verschlüsselungsschlüssel hinzu:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Konfiguration → Sicherheit**.
   Die Seite **Verschlüsselungscodes** wird angezeigt.
3. Klicken Sie auf **Actions** (Maßnahmen), und klicken Sie dann auf **Add Encryption Key** (Verschlüsselungsschlüssel hinzufügen).
   Das Dialogfeld **Create Encryption Key** (Verschlüsselungsschlüssel erstellen) wird angezeigt.
4. Geben Sie im Dialogfeld **Create Encryption Key** (Verschlüsselungsschlüssel erstellen) die unten beschriebenen Details für den Schlüssel ein.

Textfeld	Beschreibung
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein.
Beschreibung	Geben Sie eine Beschreibung 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.

5. Klicken Sie auf **OK**.

VORSICHT: Es wird empfohlen, dass Sie die Passphrase sicher aufbewahren. Wenn Sie Ihren Kennsatz verlieren oder vergessen, sind die Daten im virtuellen Laufwerk nicht mehr zugänglich.

Bearbeiten eines Verschlüsselungscodes

So bearbeiten Sie einen Verschlüsselungsschlüssel:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Konfiguration → Sicherheit**.

   Der Bildschirm **Encryption Keys** (Verschlüsselungsschlüssel) wird angezeigt.
3. Wählen Sie den Verschlüsselungscode aus, den Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.

   Das Dialogfeld **Verschlüsselungsschlüssel bearbeiten** wird angezeigt.
4. Bearbeiten Sie im Dialogfeld **Edit Encryption Key** (Verschlüsselungsschlüssel bearbeiten) den Namen, oder ändern Sie die Beschreibung für den Verschlüsselungsschlüssel.
5. Klicken Sie auf **OK**.

Ändern einer Verschlüsselungscode-Passphrase

So ändern Sie eine Verschlüsselungsschlüssel-Passphrase:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Konfiguration → Sicherheit**.

   Die Seite „Verschlüsselungscodes" wird angezeigt.
3. Wählen Sie den Verschlüsselungscode aus, den Sie ändern möchten, und klicken Sie dann auf **Passphrase ändern**.

   Das Dialogfeld **Passphrase ändern** wird angezeigt.
4. Geben Sie im Dialogfeld **Change Passphrase** (Passphrase ändern) die neue Passphrase für die Verschlüsselung ein, und wiederholen Sie die Passphrase, um Ihre Eingabe zu bestätigen.
5. Klicken Sie auf **OK**.

   VORSICHT: Es wird empfohlen, dass Sie die Passphrase sicher aufbewahren. Wenn Sie Ihre Passphrase verlieren, können Sie nicht auf die Datensätze auf dem System zugreifen.

Importieren eines Verschlüsselungscodes

So importieren Sie einen Verschlüsselungsschlüssel:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Konfiguration → Sicherheit**.
3. Klicken Sie auf das Drop-Down-Menü **Actions** (Maßnahmen) und dann auf **Settings** (Einstellungen).

   Das Dialogfeld **Schlüssel importieren** wird angezeigt.
4. Klicken Sie im Dialogfeld **Import Key** (Schlüssel importieren) auf **Browse** (Durchsuchen), um den the Verschlüsselungsschlüssel den Sie importieren möchten, zu finden, und klicken Sie dann auf **Open** (Öffnen).
5. Klicken Sie auf **OK**.

Exportieren eines Verschlüsselungscodes

So exportieren Sie einen Verschlüsselungsschlüssel:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Konfiguration** → **Sicherheit**.
3. Klicken Sie auf das Symbol der rechten spitzen Klammer **>** neben dem Namen des Verschlüsselungsschlüssels, den Sie exportieren möchten. Klicken Sie dann auf **Exportieren**.

   Das Dialogfeld **Schlüssel exportieren** wird angezeigt.
4. Klicken Sie im Dialogfeld **Export Key** (Schlüssel exportieren) auf **Download Key** (Schlüssel herunterladen), um die Verschlüsselungsschlüssel an einem sicheren Speicherort abzulegen und zu speichern.
5. Klicken Sie auf **OK**.

Entfernen eines Verschlüsselungsschlüssels

So entfernen Sie einen Verschlüsselungsschlüssel:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Konfiguration** → **Sicherheit**.
3. Klicken Sie auf das Symbol der rechten spitzen Klammer **>** neben dem Namen des Verschlüsselungsschlüssels, den Sie entfernen möchten. Klicken Sie dann auf **Entfernen**.

   Das Dialogfeld **Remove Key** (Schlüssel entfernen) wird angezeigt.
4. Klicken Sie im Dialogfeld **Remove Key** (Schlüssel entfernen) auf **OK**, um den Verschlüsselungsschlüssel zu entfernen.

   ANMERKUNG: Das Entfernen eines Verschlüsselungsschlüssels entschlüsselt die Daten nicht.

Verwalten von Cloud-Konten

Mit DL können Sie Ihre Daten durch das Erstellen eines Backup-Archivs mit Wiederherstellungspunkten in eine Cloud sichern. Mit DL können Sie Ihr Cloud-Konto über einen Cloud-Speicheranbieter erstellen, bearbeiten und verwalten. Sie können Ihre Daten über Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage oder andere OpenStack-basierte Cloud-Dienste in der Cloud archivieren. Weitere Informationen zur Verwaltung Ihrer Cloud-Konten finden Sie in den folgenden Themen:

- Hinzufügen eines Cloud-Kontos
- Bearbeiten eines Cloud-Kontos
- Konfigurieren von Cloud-Konto-Einstellungen
- Entfernen eines Cloud-Kontos

Hinzufügen eines Cloud-Kontos

Bevor Sie die archivierten Daten in eine Cloud exportieren können, müssen Sie das Konto für Ihren Cloud-Anbieter zur Core Console hinzufügen.

So fügen Sie ein Cloud-Konto hinzu:

1. Klicken Sie in der Core Console auf die Registerkarte **Tools** (Extras).
2. Klicken Sie im linken Menü auf **Clouds**.
3. Klicken Sie auf der Seite **Clouds** auf **Add New Account** (Neues Konto hinzufügen).

Daraufhin wird das Dialogfeld **Add New Account** (Neues Konto hinzufügen) geöffnet.

4. Wählen Sie einen kompatiblen Cloud-Anbieter über die Drop-Down-Liste **Cloud Type** (Cloud-Typ) aus.
5. Geben Sie die in der folgenden Tabelle beschriebenen Informationen auf der Grundlage des Cloud-Typs ein, den Sie in Schritt 4 ausgewählt haben.

Tabelle 1. Hinzufügen eines Cloud-Kontos

Cloud Type (Cloud-Typ)	Textfeld	Beschreibung
Microsoft Azure	Storage Account Name (Speicherkontoname)	Geben Sie den Namen Ihres Windows Azure-Kontos ein.
	Access Key (Zugriffsschlüssel)	Geben Sie den Zugriffsschlüssel für Ihr Konto ein.
	Anzeigename	Erstellen Sie einen Anzeigenamen für dieses Konto in AppAssure; Beispiel: Windows Azure 1.
Amazon S3	Access Key (Zugriffsschlüssel)	Geben Sie den Zugriffsschlüssel für Ihr Amazon-Konto ein.
	Secret Key (Geheimer Schlüssel)	Geben Sie den geheimen Schlüssel für dieses Konto ein.
	Anzeigename	Erstellen Sie einen Anzeigenamen für dieses Konto in AppAssure; Beispiel: Amazon 1.
Powered by OpenStack (Unterstützt durch OpenStack)	Benutzername	Geben Sie den Benutzernamen für Ihr OpenStack-basierten Cloud-Konto ein.
	API Key (API-Schlüssel)	Geben Sie den API-Schlüssel für Ihr Konto ein.
	Anzeigename	Erstellen Sie einen Anzeigenamen für dieses Konto in AppAssure; Beispiel: OpenStack 1.
	Tenant ID (Mandanten-ID)	Geben Sie die Mandanten-ID für dieses Konto an.
	Authentication URL (URL-Berechtigungsprüfung)	Geben Sie die URL für die Authentifizierung für dieses Konto an.
Rackspace Cloud Block Storage (Rackspace-Cloud-Blockspeicher)	Benutzername	Geben Sie den Benutzernamen für Ihr Rackspace-Cloud-Konto ein.
	API Key (API-Schlüssel)	Geben Sie den API-Schlüssel für dieses Konto ein.

Cloud Type (Cloud-Typ)	Textfeld	Beschreibung
	Anzeigename	Erstellen Sie einen Anzeigenamen für dieses Konto in AppAssure; Beispiel: Rackspace 1.

6. Klicken Sie auf **Hinzufügen**.

   Das Dialogfeld wird geschlossen, und das Konto wird auf der Seite **Clouds** der Core Console angezeigt.

Bearbeiten eines Cloud-Kontos

Führen Sie die folgenden Schritte zum Bearbeiten eines Cloud-Kontos aus:

1. Klicken Sie in der Core Console auf die Registerkarte **Tools** (Extras).
2. Klicken Sie im linken Menü auf **Clouds**.
3. Klicken Sie neben dem Cloud-Konto, das Sie bearbeiten möchten, auf das Drop-Down-Menü, und klicken Sie dann auf **Edit** (Bearbeiten).

   Das Fenster **Edit Account** (Konto bearbeiten) wird geöffnet.
4. Bearbeiten Sie die Informationen nach Bedarf, und klicken Sie dann auf **Save** (Speichern).

   ANMERKUNG: Cloud-Typen können nicht bearbeitet werden.

Konfigurieren von Cloud-Konto-Einstellungen

Mit den Cloud-Konfigurationseinstellungen können Sie ermitteln, wie oft AppAssure versuchen soll, eine Verbindung zu Ihrem Cloud-Konto herzustellen, außerdem können Sie die Anzahl der Versuche bis zur Zeitüberschreitung ermitteln.
So konfigurieren Sie die Verbindungseinstellungen für Ihr Cloud-Konto:

1. Klicken Sie in der Core Console auf die Registerkarte **Configuration** (Konfiguration).
2. Klicken Sie im linken Menü auf **Settings** (Einstellungen).
3. Führen Sie auf der Seite **Settings** (Einstellungen) einen Bildlauf zu **Cloud Configuration** (Cloud-Konfiguration) durch.
4. Klicken Sie auf das Drop-Down-Menü neben dem Cloud-Konto, das Sie konfigurieren möchten, und führen Sie dann eine der folgenden Aktionen aus:
   - Klicken Sie auf **Bearbeiten**.

     Das Dialogfeld **Cloud Configuration** (Cloud-Konfiguration) wird angezeigt.

     1. Verwenden Sie die Pfeil-nach-oben und -nach-unten-Tasten, um eine der folgenden Optionen zu bearbeiten:

        – **Request Timeout** (Anforderungszeitüberschreitung): Als Anzeige in Minuten und Sekunden bestimmt diese Option die Zeit, die AppAssure für einen Versuch aufwenden soll, bei einer Verzögerung eine Verbindung zum Cloud-Konto herzustellen. Die Verbindungsversuche werden nach der eingegebenen Dauer eingestellt.

        – **Retry Count** (Wiederholungsanzahl): Bestimmt die Anzahl der Versuche, die AppAssure ausführen soll, bevor entschieden wird, dass das Cloud-Konto nicht erreichbar ist.

        – **Write Buffer Size** (Schreibpuffergröße): Bestimmt die Puffergröße für das Schreiben von archivierten Daten in die Cloud.

- **Read Buffer Size** (Lesepuffergröße): Legt die Blockgröße fest, die für das Lesen archivierter Daten aus der Cloud reserviert ist.

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

- Klicken Sie auf **Reset** (Zurücksetzen). Mit dieser Option setzen Sie die Konfiguration auf die folgenden Standardeinstellungen zurück:
  - **Request Timeout:** (Anforderungszeitüberschreitung): 01:30 (Minuten und Sekunden)
  - **Retry Count:** (Anzahl der Versuche): 3 (Versuche)

Entfernen eines Cloud-Kontos

Sie können ein Cloud-Konto entfernen, um die Fortsetzung des Cloud-Service auszusetzen oder um die Verwendung dieses Kontos für einen bestimmten Kern anzuhalten.
So entfernen Sie ein Cloud-Konto:

1. Klicken Sie in der Core Console auf die Registerkarte **Tools** (Extras).
2. Klicken Sie im linken Menü auf **Clouds**.
3. Klicken Sie neben dem Cloud-Konto, das Sie bearbeiten möchten, auf das Drop-Down-Menü, und klicken Sie dann auf **Remove** (Entfernen).
4. Klicken Sie im Fenster **Delete Account** (Konto löschen) auf **Yes** (Ja) , um zu bestätigen, dass das Konto gelöscht werden soll.
5. Wenn das Cloud-Konto derzeit verwendet wird, werden Sie in einem zweiten Fenster gefragt, ob Sie die Datei trotzdem entfernen möchten. Klicken Sie auf **Yes** (Ja) , um den Vorgang zu bestätigen.

   ANMERKUNG: Das Entfernen eines Kontos, das derzeit verwendet wird, führt dazu, dass keine geplanten Archivierungs-Jobs für dieses Konto ausgeführt werden.

Grundlegendes zur Replikation

Wissenswertes über den Schutz von Workstations und Servern

Um Ihre Daten zu schützen, müssen Sie die Workstations und Server, die Sie schützen möchten, zur Core Console hinzufügen; zum Beispiel Ihren Exchange-Server, SQL-Server, oder Ihren Linux-Server.

ANMERKUNG: In diesem Abschnitt bezieht sich das Wort *Maschine* im Allgemeinen auch auf die AppAssure-Agentsoftware, die auf dieser Maschine installiert ist.

In der Core Console können Sie die Maschine bestimmen, auf der die AppAssure-Agentsoftware installiert wird, und angeben, welche Datenträger geschützt werden sollen, die Zeitpläne für den Schutz definieren, weitere Sicherheitsmaßnahmen hinzufügen (z. B. Verschlüsselung) und vieles mehr. Weitere Informationen über den Zugriff auf die Core Console für den Schutz von Arbeitsstationen und Servern siehe Protecting A Machine (Schützen einer Maschine).

Wissenswertes über die Replikation

Replikation ist der Prozess des Kopierens von Wiederherstellungspunkten und des Übertragens dieser Punkte auf einen sekundären Speicherort, um sie im Falle einer Notfallwiederherstellung verwenden zu können. Für diesen Prozess benötigen Sie eine gekoppelte Quell-Ziel-Beziehung zwischen zwei Kernen. Der Quellkern kopiert die Wiederherstellungspunkte der geschützten Maschinen 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 Folgendes:

- **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 geschützten Maschinen 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.

  ANMERKUNG: In diesem Szenario haben Kunden nur Zugriff auf ihre eigenen Daten.

Mögliche Replikationskonfigurationen sind:

- **Punkt zu Punkt**. Eine einzelne geschützte Maschine von einem einzelnen Quellkern wird auf einen einzelnen Zielkern repliziert.

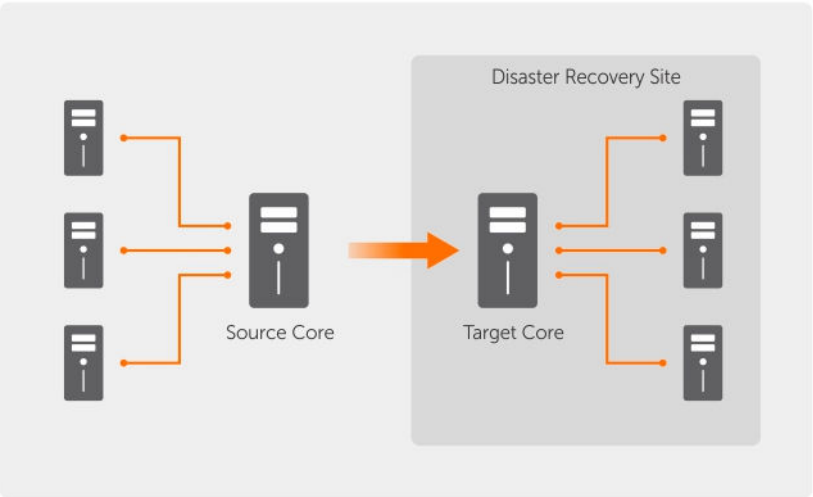


Abbildung 7. Einfaches Replikationsarchitektur-Diagramm

- **Multi-Punkt-zu-Punkt**. Repliziert mehrere Quellkerne auf einen einzelnen Zielkern.

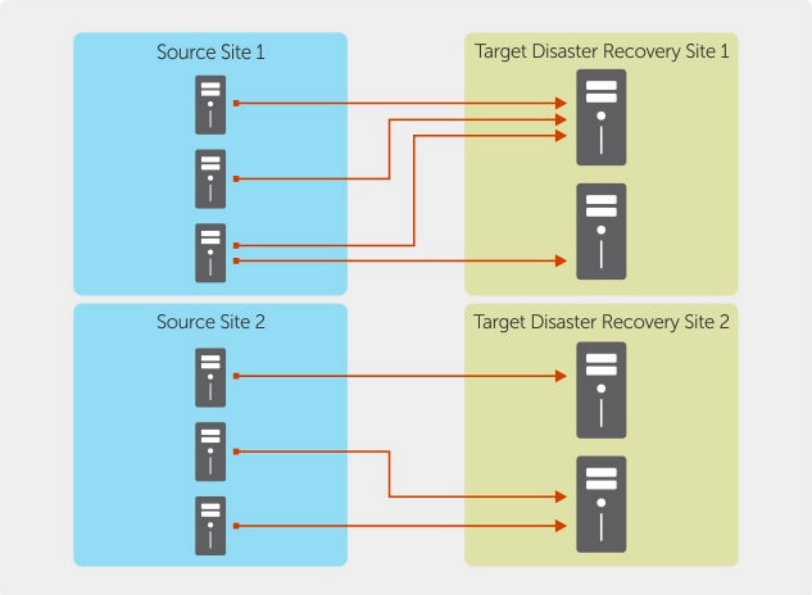


Abbildung 8. Multi-Punkt Replikationsarchitektur-Diagramm

Wissenswertes über Seed-Routing

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 Datenträger auf dem Zielkern platziert werden, um die ersten Daten auf den Zielkern zu übertragen. Üblicherweise ist das bei umfassenden Datensätzen oder Standorten mit langsamer Verbindung nützlich.

ANMERKUNG: Es ist zwar möglich, das Seeding der Basisdaten über eine Netzwerkverbindung durchzuführen, dies wird jedoch nicht empfohlen. Das erste Seeding ist mit sehr großen Datenmengen verbunden, die eine normale WAN-Verbindung überlasten könnten. Wenn die Seed-Daten zum Beispiel 10 GB in Anspruch nehmen und die WAN-Verbindung 24 MBit/s überträgt, dann kann die Übertragung bis zum Abschluss mehr als 40 Tage in Anspruch nehmen.

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.

Seeding ist ein zweiteiliger Vorgang (auch bezeichnet als copy-consume):

- Der erste Teil umfasst das Kopieren; die ursprünglichen replizierten Daten werden auf einen Quell-Wechseldatenträger geschrieben. Beim „copying" (Kopieren) werden alle vorhandenen Wiederherstellungspunkte vom Zielkern auf einen lokalen Wechseldatenträger, wie z. B. ein USB-Laufwerk, dupliziert. Nachdem das Kopieren abgeschlossen wurde, müssen Sie den Datenträger dann vom Standort des Quellkerns zum Standort des Remote-Zielkerns transportieren.
- Der zweite Teil besteht im Konsumieren und erfolgt, wenn ein Zielkern das transportierte Laufwerk erhält und die replizierten Daten auf das Repository kopiert. Der Zielkern konsumiert die Wiederherstellungspunkte und verwendet sie, um replizierte geschützte Maschinen zu erstellen.

ANMERKUNG: Während die Replikation von inkrementellen Snapshots zwischen Quell- und Zielkernen erfolgen kann, bevor das Seeding abgeschlossen ist, bleiben die replizierten Snapshots, die von der Quelle auf das Ziel übertragen werden, solange „verwaist", bis die ursprünglichen Daten konsumiert sind und die Snapshots mit den replizierten Basisabbildern kombiniert werden.

Da große Datenmengen auf den Wechseldatenträger kopiert werden müssen, wird eine eSATA-, USB 3.0- oder eine andere Hochgeschwindigkeitsverbindung zum Wechseldatenträger empfohlen.

Wissenswertes über Failover und Failback

Im Falle eines schwerwiegenden Systemausfalls, bei dem der Quellkern und die geschützten Maschinen ausfallen, unterstützt das DL-Gerät Failover und Failback in replizierten Umgebungen. Failover bedeutet das Wechseln auf einen redundanten oder im Standby-Modus befindlichen Zielkern bei einem Systemfehler oder einer anormalen Beendigung eines Quellkerns und der geschützten Maschine. Das Hauptziel des Failovers ist das Starten eines neuen Agenten, der mit dem ausgefallenen Agenten identisch ist, welcher durch den ausgefallenen Zielkern geschützt war. Das zweite Ziel besteht darin, den Zielkern in einen neuen Modus zu schalten, sodass der Zielkern den Failover-Agenten genauso schützt, wie der Quellkern den ursprünglichen Agenten vor dem Ausfall geschützt hat. Der Zielkern kann am sekundären Standort Instanzen aus replizierten Agenten wiederherstellen und sofort den Schutz auf den Maschinen starten, die das Failover durchgeführt haben.

Failback bezeichnet das Wiederherstellen einer geschützten Maschine und eines Kerns zurück in ihren ursprünglichen Zustand (vor dem Ausfall). Das Hauptziel des Failbacks besteht darin, die geschützte Maschine (in den meisten Fällen eine neue Maschine, die den ausgefallenen Agenten ersetzt) in solch einen Zustand wiederherzustellen, dass er identisch mit dem letzten Zustand des neuen, temporären Agenten ist. Nach seiner Wiederherstellung wird der Agent durch einen wiederhergestellten Quellkern geschützt. Die Replikation wird ebenfalls wiederhergestellt und der Zielkern agiert wieder als Replikationsziel.

Wissenswertes über die Replikation und verschlüsselte Wiederherstellungspunkte

Während das Seed-Laufwerk keine Sicherungen der Kern-Registrierung und -Zertifikate enthält, so enthält es jedoch Verschlüsselungsschlüssel vom Quellkern, wenn die Wiederherstellungspunkte, die von der Quelle auf das Ziel repliziert werden, verschlüsselt sind. Die replizierten Wiederherstellungspunkte bleiben verschlüsselt, nachdem sie auf den Zielkern übertragen worden sind. Die Besitzer oder Administratoren des Zielkerns brauchen die Passphrase, um die verschlüsselten Daten wiederherzustellen.

Wissenswertes über Aufbewahrungsrichtlinien für die Replikation

Die Aufbewahrungsrichtlinien auf dem Quellkern bestimmen die Aufbewahrungsrichtlinien für die auf den Zielkern replizierten Daten. Dies liegt an der Replikationsaufgabe, die die zusammengeführten Wiederherstellungspunkte aus einem Rollup oder einem Ad-hoc-Löschen überträgt.

ANMERKUNG: Der Zielkern kann kein Rollup und kein Ad-hoc-Löschen von Wiederherstellungspunkten durchführen. Diese Maßnahmen können nur vom Quellkern durchgeführt werden.

Überlegungen zur Leistung bei der replizierten Datenübertragung

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 muss nur einmal vorgenommen werden, da er die Grundlage für eine regelmäßige, geplante Replikation legt.

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 geschützter Maschinen Es ist wichtig, die Anzahl der geschützten Maschinen in Betracht zu ziehen, die pro Quellkern geschützt werden sollen, und wie viele Sie davon auf das Ziel replizieren möchten. Mit AppAssure können Sie die Replikation pro geschützten Server so durchführen, dass Sie auswählen können, ob Sie bestimmte Server replizieren möchten. Wenn alle geschützten Server repliziert werden müssen, beeinflusst dies die Änderungsrate stark, insbesondere, 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.

In der nachfolgenden Tabelle finden Sie Beispiele für die notwendige Bandbreite pro Gigabyte für eine angemessene Änderungsrate.

> **ANMERKUNG:** Für optimale Ergebnisse befolgen Sie bitte die Empfehlungen aus der nachfolgenden Tabelle.

Maximale Änderungsrate für WAN-Verbindungstypen

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	838 GB pro Stunde

Im Falle eines Verbindungsausfalls während der Datenübertragung wird die Replikation vom letzten Wiederherstellungspunkt der Übertragung wieder aufgenommen, wenn die Verbindungsfunktionalität wiederhergestellt ist.

Ablaufplan zur Durchführung von Replikationen

Um Daten mit AppAssure zu replizieren, müssen Sie die Quell- und Zielkerne für die Replikation konfigurieren. Wenn Sie die Replikation konfiguriert haben, können Sie Daten der geschützten Maschine replizieren, die Replikation überwachen und verwalten und Wiederherstellungen durchführen.

Zur Durchführung von Replikationen in AppAssure müssen Sie die folgenden Vorgänge ausführen:

- Selbstverwaltende Replikation konfigurieren. Weitere Informationen über die Replikation auf einen selbstverwaltenden Zielkern finden Sie unter Replizieren auf einen selbstverwalteten Kern.
- Drittanbieter-Replikation konfigurieren. Weitere Informationen über die Replikation auf einen Zielkern eines Drittanbieters finden Sie unter Replizieren auf einen von einem Drittanbieter verwalteten Kern.
- Replizieren einer an den Quellkern angebundenen neuen geschützten Maschine. Weitere Informationen zur Replikation einer geschützten Maschine siehe Replicating A New Protected Machine (Eine neue geschützte Maschine replizieren).
- Eine bestehende geschützte Maschine replizieren. Weitere Informationen über die Konfiguration eines Agenten für Replikation siehe Replicating Agent Data On A Machine (Replizieren von Agentendaten auf einer Maschine).
- Die Replikationspriorität für einen Agenten einstellen. Weitere Informationen über die Priorisierung der Replikation eines Agenten finden Sie unter Festlegen der Replikationspriorität für einen Agenten.
- Die Replikation nach Bedarf überwachen. Weitere Informationen über die Überwachung einer Replikation finden Sie unter Monitoring Replication (Überwachen der Replikation).
- Die Replikationseinstellungen nach Bedarf verwalten. Weitere Informationen über die Verwaltung von Replikationseinstellungen finden Sie unter Verwalten der Replikationseinstellungen.
- Replizierte Daten im Notfall oder bei Datenverlust wiederherstellen. Weitere Informationen über die Wiederherstellung replizierter Daten finden Sie unter Wiederherstellen replizierter Daten .

Replizieren auf einen selbstverwalteten Kern

Ein selbstverwalteter Kern ist ein Kern, auf den Sie Zugriff haben, oft weil er von Ihrer Firma an einem externen Standort verwaltet wird. Replikation kann vollständig auf dem Quellkern ausgeführt werden, außer wenn Sie Ihre Daten „seeden“ wollen. „Seeden“ erfordert, dass Sie das Seed-Laufwerk auf dem Zielkern konsumieren, nachdem Sie die Replikation auf dem Quellkern konfiguriert haben.

ANMERKUNG: Diese Konfiguration betrifft die Replikation zu einem externen Standort und gegenseitige Replikation. Der Kern muss auf allen Quell- und Zielmaschinen installiert sein. Wenn Sie Ihr System für Multi-Punkt-zu-Punkt-Replikation konfigurieren, müssen Sie diese Aufgabe auf allen Quellkernen und auf dem einen Zielkern ausführen.

Konfiguration des Quellkerns, um zu einem selbstverwaltenden Zielkern zu replizieren

So konfigurieren Sie den Quellkern, um zu einem selbstverwaltenden Zielkern zu replizieren:

1. Klicken Sie im Kern auf die Registerkarte **Replication** (Replikation).
2. Klicken Sie auf **Add Target Core** (Zielkern hinzufügen).

   Der Assistent für **Replication** (Replikation) wird angezeigt.
3. Wählen Sie **I have my own Target Core** (Ich verfüge über einen eigenen Zielkern), und geben Sie die Informationen gemäß der folgenden Tabelle ein:

Textfeld	Beschreibung
Host-Name	Geben Sie den Hostnamen oder die IP-Adresse der Kern-Maschine ein, auf die Sie replizieren.
Schnittstelle	Geben Sie die Portnummer ein, über die der AppAssure-Kern mit der Maschine kommuniziert. Die Standardportnummer ist 8006.
Benutzername	Geben Sie den Benutzernamen für den Zugriff auf die Maschine ein, z. B. **Administrator**.
Kennwort	Geben Sie das Kennwort für den Zugriff auf die Maschine ein.

   Wenn der Kern, den Sie hinzufügen möchten, zuvor mit diesem Quellkern gepaart wurde, führen Sie die folgenden Schritte aus:

   a. Wählen Sie die Option **Use an existing target core** (Vorhandenen Zielkern auswählen) aus.
   b. Wählen Sie den Zielkern aus der Dropdown-Liste aus.
   c. Klicken Sie auf **Weiter**.
   d. Fahren Sie mit Schritt 7 fort.
4. Klicken Sie auf **Weiter**.
5. Geben Sie auf der Seite **Details** einen Namen für diese Replikationskonfiguration ein, z. B. „SourceCore1“. Wenn Sie eine vorherige Replikationskonfiguration erneut initiieren oder reparieren möchten, wählen Sie **My Core has been migrated and I would like to repair replication** (Mein Kern wurde migriert, und ich möchte die Replikation reparieren.) aus.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie auf der Seite **Agents** (Agenten) die Agenten aus, die Sie replizieren möchten, und verwenden Sie dann die Drop-Down-Listen in der Spalte **Repository**, um ein Repository für jeden Agenten auszuwählen.
8. Wenn Sie den Seeding-Vorgang zur Übertragung der Basisdaten durchführen möchten, führen Sie die folgenden Schritte aus:

   ANMERKUNG: Da große Datenmengen auf den Wechseldatenträger kopiert werden müssen, wird eine eSATA-, USB 3.0- oder eine andere Hochgeschwindigkeitsverbindung zum Wechseldatenträger empfohlen.

   a. Wählen Sie auf der Seite **Agents** (Agenten) die Option **Use a seed drive to perform initial transfer** (Seed-Laufwerk zum Ausführen einer erstmaligen Übertragung verwenden) aus. Wenn Sie derzeit über einen oder mehrere Maschinen verfügen, die eine Replikation auf einem Zielkern durchführen, können Sie diese geschützten Maschinen dem Seed-Laufwerk hinzufügen, indem Sie die Option **With already replicated** (Mit bereits repliziert) auswählen.

b. Klicken Sie auf **Weiter**.
c. Verwenden Sie auf der Seite **Seed Drive Location** (Speicherort des Seed-Laufwerks) die Drop-Down-Liste **Location Type** (Speicherorttyp), um eine der folgenden Optionen auszuwählen:
   - Local (Lokal): Geben Sie in das Textfeld **Location** (Speicherort) ein, wo Sie das Seed-Laufwerk speichern möchten, z. B. „D:\work\archive“.
   - Network (Netzwerk): Geben Sie in das Textfeld **Location** (Speicherort) ein, wo Sie das Seed-Laufwerk speichern möchten und geben Sie dann Ihre Anmeldeinformationen für die Netzwerkfreigabe in die Textfelder **User Name** (Benutzername) und **Password** (Kennwort) ein.
   - Cloud: Wählen Sie im Textfeld **Account** (Konto) das Konto aus. Um ein Cloud-Konto auswählen zu können, müssen Sie es zuerst in der Cloud-Konsole hinzugefügt haben. Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos. Wählen Sie den Ihrem Konto zugewiesenen **Container** aus. Wählen Sie den **Ordnernamen** aus, in dem die archivierten Daten gespeichert werden sollen.
d. Klicken Sie auf **Next** (Weiter).

9. Geben Sie im Dialogfeld **Seed Drive Option** (Seed-Laufwerk-Option) die nachfolgend beschriebenen Informationen ein.

Textfeld	Beschreibung
Maximale Größe	Große Datenarchive können in mehrere Segmente unterteilt werden. Wählen Sie die maximale Größe des Segments ein, das Sie für die Erstellung des Seed-Laufwerks reservieren möchten. Führen Sie dazu einen der folgenden Schritte aus: • Wählen Sie **Entire Target** (Gesamtes Ziel) aus, um den gesamten verfügbaren Speicherplatz zu reservieren, der auf der Seite „Seed Drive Location“ (Speicherort des Seed-Laufwerks) für die künftige Verwendung bereitgestellt wurde (wenn z. B. der Speicherort „D:\work\archive“ lautet, wird der gesamte Speicherplatz auf Laufwerk D: reserviert, wenn dieser zum Kopieren des Seed-Laufwerks benötigt wird, er wird jedoch nicht unmittelbar nach dem Start des Kopiervorgangs reserviert). • Wählen Sie das leere Textfeld aus, geben Sie eine Menge ein, und wählen Sie dann eine Maßeinheit aus der Dropdown-Liste aus, um den maximalen Speicherplatz anzupassen, der reserviert werden soll.
Customer ID (Kunden-ID, optional)	Geben Sie optional die Kunden-ID ein, die Sie vom Dienstanbieter erhalten haben.
Recycle action (Maßnahme wiederverwenden)	Falls der Pfad bereits ein Seed-Laufwerk enthält, wählen Sie eine der folgenden 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 auf das Seed-Laufwerk fehl. • **Replace this core** (Diesen Kern ersetzen) – Alle bereits vorhandenen Daten auf diesem Kern werden überschrieben, die Daten für andere Kerne bleiben aber intakt. • **Erase completely** (Vollständig löschen) – Alle Daten werden aus dem Verzeichnis gelöscht, bevor auf das Seed-Laufwerk geschrieben wird.
Kommentar	Geben Sie eine Anmerkung oder eine Beschreibung des Archivs ein.

Textfeld	Beschreibung
Add all Agents to Seed Drive (Alle Agenten dem Seed-Laufwerk hinzufügen)	Wählen Sie die Agenten aus, die Sie mithilfe des Seed-Laufwerks replizieren möchten.
Build RP chains (fix orphans) (Wiederherstellungspunkt-Ketten aufbauen (Waisen beheben))	Wählen Sie diese Option aus, um die gesamte Wiederherstellungspunkt-Kette auf das Seed-Laufwerk zu replizieren. Diese Option ist standardmäßig aktiviert. Durch das typische Seed-Routing in AppAssure wird nur der neueste Wiederherstellungspunkt auf das Seed-Laufwerk repliziert, wodurch die Dauer und der Speicherplatz für die Erstellung eines Seed-Laufwerks reduziert wird. Wenn Sie sich für das Erstellen von Wiederherstellungspunkten auf den Seed-Laufwerken entscheiden, muss genügend Speicherplatz auf dem Seed-Laufwerken vorhanden sein, um die neuesten Wiederherstellungspunkte von den Agenten zu speichern. Dieser Schritt kann zusätzliche Zeit in Anspruch nehmen.
Use compatible format (Kompatibles Format verwenden)	Wählen Sie diese Option aus, um das Seed-Laufwerk in einem Format zu erstellen, dass mit den neuen und alten Versionen des AppAssure-Kerns kompatibel ist.

10. Wählen Sie auf der Seite **Agents** (Agenten) die Agenten aus, die Sie über das Seed-Laufwerk auf den Zielkern replizieren möchten.
11. Klicken Sie auf **Fertigstellen**.
12. Wenn Sie ein Seed-Laufwerk erstellt haben, senden Sie es an Ihren Zielkern.

    Die Verknüpfung des Quellkerns mit dem Zielkern ist abgeschlossen. Die Replikation beginnt, sie erstellt jedoch auch verwaiste Wiederherstellungspunkte auf dem Zielkern, bis das Seed-Laufwerk belegt ist und stellt die erforderlichen Basisabbilder bereit.

Konsumieren des Seed-Laufwerks auf einem Zielkern

Dieses Verfahren ist nur erforderlich, wenn Sie ein Seed-Laufwerk erstellt haben, während Sie die Replikation für einen selbstverwalteten Kern konfiguriert haben.
So konsumieren Sie das Seed-Laufwerk auf einem Zielkern:

1. Wenn das Seed-Laufwerk auf einen Wechseldatenträger, wie z. B. ein USB-Laufwerk, gespeichert wurde, verbinden Sie das Laufwerk mit dem Zielkern.
2. Wählen Sie aus der Kernkonsole auf dem Quellkern die Registerkarte **Replication** (Replikation).
3. Wählen Sie in **Incoming Replication** (Eingehende Replikation), unter Verwendung des Drop-Down-Menüs den korrekten Quellkern aus, und klicken Sie dann auf **Consume** (Konsumieren).

   Die Fenster „Consume" (Konsumieren) wird angezeigt.
4. Wählen Sie für **Location Type** (Speicherorttyp) eine der folgenden Optionen aus der Drop-Down-Liste aus:
   - Lokal
   - Netzwerk
   - Cloud
5. Geben Sie bei Bedarf folgenden Informationen ein:

Textfeld	Beschreibung
Standort	Geben Sie den Pfad zum Speicherort des Laufwerks an, z. B. ein USB-Laufwerk oder eine Netzwerkfreigabe (z. B.: D:\).
Benutzername	Geben Sie den Benutzernamen für das freigegebene Laufwerk oder den Ordner ein. Der Benutzername ist nur für einen Netzwerkpfad erforderlich.
Kennwort	Geben Sie das Kennwort für das freigegebene Laufwerk oder den Ordner ein. Das Kennwort ist nur für einen Netzwerkpfad erforderlich.
Account (Konto)	Wählen Sie ein Konto aus der Drop-Down-Liste aus. Um ein Cloud-Konto auszuwählen, müssen Sie es zunächst in der Kernkonsole hinzugefügt haben.
Container	Wählen Sie einen Container, der mit Ihrem Konto verknüpft ist, aus dem Drop-Down-Menü aus.
Ordnername	Geben Sie den Namen des Ordners ein, in dem die archivierten Daten gespeichert sind; z.B. -Archiv – [ERSTELLUNGSDATUM] – [ERSTELLUNGSZEIT]

6. Klicken Sie auf **Check File** (Datei prüfen).

   Nachdem der Kern die Datei geprüft hat, bestückt er automatisch das Feld **Date Range** (Datumsbereich) mit den Daten der ältesten und neuesten Wiederherstellungspunkte, die im Seed-Laufwerk enthalten sind. Er importiert auch alle Kommentare, die im Rahmen der Konfiguration der Replikation für einen selbstverwalteten Kern eingegeben wurden.

7. Wählen Sie unter **Agent Names** (Agentennamen) im Fenster **Consume** (Konsumieren) die Maschinen aus, für die Sie Daten konsumieren möchten, und klicken Sie dann auf **Consume** (Konsumieren).

   ANMERKUNG: Um den Fortschritt der Datenkonsumierung zu überprüfen, wählen Sie die Registerkarte **Events** (Ereignisse) aus.

Aufgeben eines ausstehenden Seed-Laufwerks

Wenn Sie ein Seed-Laufwerk mit der Absicht erstellen, es zum Zielkern zu konsumieren, aber Sie entschließen sich, es nicht auf den Remote-Standort zu schicken, bleibt ein Link für das ausstehende Seed-Laufwerk auf der Registerkarte **Replication** (Replikation) des Quellkerns. Möglicherweise möchten Sie das ausstehende Seed-Laufwerk zugunsten von andern oder aktuelleren Seed-Daten aufgeben.

ANMERKUNG: Dieser Vorgang entfernt den Link zu dem ausstehenden Seed-Laufwerk aus der Core Console auf dem Quellkern. Es entfernt das Laufwerk nicht aus dem Speicherort, an dem es gespeichert ist.

So geben Sie ein ausstehendes Seed-Laufwerk auf:

1. Wählen Sie aus der Core Console auf dem Quellkern die Registerkarte **Replication** (Replikation).
2. Klicken Sie auf **Outstanding Seed Drive (#)** (Ausstehendes Seed-Laufwerk (#))

   Der Abschnitt **Ausstehende Seed-Laufwerke** wird angezeigt. Er schließt den Namen des Remote-Zielkerns, das Datum und die Uhrzeit, an dem das Seed-Laufwerk erstellt wurde und den Datenbereich der Wiederherstellungspunkte ein, die im Seed-Laufwerk eingeschlossen sind.
3. Klicken Sie auf das Drop-Down-Menü für das Laufwerk, das Sie aufgeben möchten, und wählen Sie dann **Abandon** (Aufgeben).

   Das Fenster **Ausstehendes Seed-Laufwerk** wird angezeigt.
4. Klicken Sie auf **Yes** (Ja), um die Auswahl zu bestätigen.

   Das Seed-Laufwerk wird entfernt. Wenn keine anderen Seed-Laufwerke auf dem Quellkern bestehen, dann wird beim nächsten Öffnen der Registerkarte **Replikation**, der Link **Ausstehendes Seed-Laufwerk (#)** und der Abschnitt **Ausstehende Seed-Laufwerke** nicht angezeigt.

Replizieren auf einen von einem Drittanbieter verwalteten Kern

Ein Zielkern eines Drittanbieters ist ein Zielkern der von einem MSP verwaltet und gewartet wird. Replikation auf einen von einem Drittanbieter verwalteten Kern erfordert nicht, dass Sie Zugriff auf den Zielkern haben. Nachdem ein Kunde die Replikation auf dem Zielkern oder -Kernen konfiguriert, stellt MSP die Konfiguration auf dem Zielkern fertig.

ANMERKUNG: Diese Konfiguration betrifft gehostete und Cloud-Replikationen. Der AppAssure-Kern muss auf allen Quell-Kernmaschinen installiert sein.

Konfigurieren der Replikation zu einem von einem Dritten verwalteten Zielkern

ANMERKUNG: Diese Konfiguration betrifft die gehostete Replikation und die Cloud-Replikation. Wenn Sie AppAssure für die Multi-Punkt-zu-Punkt Replikation konfigurieren, müssen Sie diese Aufgaben auf allen Quellkernen ausführen.

So konfigurieren Sie die Replikation für einen von einem Drittanbieter verwalteten Kern:

1. Wechseln Sie zur Core Console, und klicken Sie auf die Registerkarte **Replikation**.
2. Klicken Sie im Drop-Down-Menü **Actions** (Maßnahmen) auf **Add Remote Core** (Remote-Kern hinzufügen).
3. Wählen Sie im Dialogfeld **Select Replication Type** (Replikationstyp auswählen) die Option **I have a subscription to a third-party providing off-site backup and disaster recovery services, and wish to replicate my backups to that service** (Ich habe ein Abonnement eines Drittanbieters, der eine externe Sicherung sowie Notfallwiederherstellungsdienste bereitstellt, und möchte meine Sicherungen in diesen Service replizieren) aus und geben Sie anschließend die nachfolgend beschriebenen Informationen ein.

Textfeld	Beschreibung
Host-Name	Geben Sie den Hostnamen, die IP-Adresse oder FQDN für die Remote-Kern-Maschine ein.
Schnittstelle	Geben Sie die Portnummer ein, die Sie vom Dritt-Dienstanbieter erhalten haben. Die Standardportnummer ist 8006.

4. Klicken Sie auf **Continue** (Weiter).
5. Verfahren Sie im Dialogfeld **Add Remote Core** (Remote-Kern hinzufügen) wie folgt:
   a. Wählen Sie die geschützten Maschinen aus, die repliziert werden sollen.
   b. Wählen Sie ein Repository für jede geschützte Maschine aus.
   c. Geben Sie Ihre Abonnement-E-Mail-Adresse und Kunden-ID ein, die Sie vom Dienstanbieter erhalten haben.
6. Wenn Sie den Seeding-Vorgang zur Übertragung der Basisdaten durchführen möchten, wählen Sie die Option **Use a seed drive to perform initial transfer** (Seed-Laufwerk für Erstübertragung verwenden).
7. Klicken Sie auf **Submit Request** (Anfrage senden).

   ANMERKUNG: Falls Sie die Option **Use a seed drive to perform initial transfer** (Seed-Laufwerk für Erstübertragung verwenden) ausgewählt haben, wird das Dialogfeld **Copy to Seed Drive** (Auf Seed-Laufwerk kopieren) angezeigt.
8. Geben Sie im Dialogfeld **Auf Seed-Laufwerk kopieren** die in der folgenden Tabelle beschriebenen Informationen für das Seed-Laufwerk ein.

Textfeld	Beschreibung
Standort	Geben Sie den Pfad zum Laufwerk an, auf dem Sie die Ursprungsdaten speichern möchten, wie z. B. ein lokales USB-Laufwerk.
Benutzername	Geben Sie den Benutzernamen zum Verbinden mit dem Laufwerk ein. ANMERKUNG: Dies ist erforderlich, wenn sich das Seed-Laufwerk in einer Netzwerkfreigabe befindet.
Kennwort	Geben Sie das Kennwort zum Verbinden mit dem Laufwerk ein. ANMERKUNG: Dies ist erforderlich, wenn sich das Seed-Laufwerk in einer Netzwerkfreigabe befindet.
Maximale Größe	Wählen Sie eine der folgenden Optionen: • Das gesamte Ziel • Ein Anteil des verfügbaren Laufwerkspeicherplatzes. So legen Sie einen Anteil des Laufwerks fest: a. Geben Sie die gewünschte Menge an Speicherplatz im Textfeld ein. b. Wählen Sie die Maßeinheit aus.
Recycle action (Maßnahme wiederverwenden)	Falls der Pfad bereits ein Seed-Laufwerk enthält, wählen Sie eine der folgenden 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 auf das Seed-Laufwerk fehl. • **Replace this core** (Diesen Kern ersetzen) – Alle bereits vorhandenen Daten auf diesem Kern werden überschrieben, die Daten für andere Kerne bleiben aber intakt. • **Erase completely** (Vollständig löschen) – Alle Daten werden aus dem Verzeichnis gelöscht, bevor auf das Seed-Laufwerk geschrieben wird.
Kommentar	Geben Sie eine Anmerkung oder eine Beschreibung des Archivs ein.
Agenten	Wählen Sie die Agenten aus, die Sie mithilfe des Seed-Laufwerks replizieren möchten.

ANMERKUNG: Da große Datenmengen auf den Wechseldatenträger kopiert werden müssen, wird eine eSATA-, USB 3.0- oder eine andere Hochgeschwindigkeitsverbindung zum Wechseldatenträger empfohlen.

9. Klicken Sie auf **Start**, um das Seed-Laufwerk auf den ausgewählten Pfad zu schreiben.
10. Senden Sie das Seed-Laufwerk, wie vom Dritt-Dienstanbieter angewiesen.

Überprüfen einer Replikationsanfrage

Eine Replikationsanfrage wird vom Quellkern zum Zielkern des Dritten gesendet. Als Dritter können Sie die Anfrage anzeigen, ihr anschließend zustimmen, um die Replikation für Ihren Kunden zu starten, oder Sie können sie verweigern, um die Durchführung der Replikation zu verhindern.

So zeigen Sie eine Replikationsanfrage auf einem Kern eines Drittanbieters an:

1. Öffnen Sie die Core Console auf dem Zielkern, und klicken Sie auf die Registerkarte **Replikation**.
2. Klicken Sie auf **Pending Requests (#)** (Ausstehende Anfragen (Nr.)).

   Der Abschnitt **Pending Replication Requests** (Ausstehende Replikationsanfragen) wird angezeigt.
3. Wählen Sie neben den Anfragen, die Sie anzeigen möchten, **Review** (Anzeigen) aus dem Dropdown-Menü aus.

   Das Fenster **Replikationsanfragen überprüfen** wird angezeigt.

   ANMERKUNG: Die vom Kunden gestellte Anfrage bestimmt, welche Informationen im Abschnitt **Quellkernidentität** angezeigt werden.
4. Führen Sei im Fenster „Review Replication Request" (Replikationsanfrage überprüfen) einen der folgenden Vorgänge aus:
   - Klicken Sie zum Ablehnen der Anfrage auf **Deny** (Ablehnen).
   - So genehmigen Sie die Anfrage:

     1. – Wählen Sie **Vorhandenen replizierten Kern ersetzen** aus, und wählen Sie dann einen Kern aus der Dropdown-Liste aus.
        – Wählen Sie **Neuen Quellkern erstellen** aus. Überprüfen Sie **Kernname**, **E-Mail-Adresse** des Kunden und **Kunden-ID**, und bearbeiten Sie die Informationen bei Bedarf.
     2. Wählen Sie unter **Agenten** die Maschinen aus, für die die Zustimmung gilt, und wählen Sie dann das entsprechende Repository für jede Maschine aus, indem Sie die Dropdown-Liste verwenden.
     3. Geben Sie optional die Anmerkungen ein, die Sie im Kästchen **Comment** (Anmerkungen) anzeigen möchten.
     4. Klicken Sie auf **Send Response** (Antwort senden).

        Die Replikation wird angenommen.

Ignorieren einer Replikationsanfrage

Als Dritt-Dienstanbieter eines Zielkerns haben Sie die Option, eine Anfrage auf Durchführung einer Replikation, die von einem Kunden gesendet wurde, zu ignorieren. Diese Option kann verwendet werden, wenn ein Kunde versehentlich eine Anfrage sendet oder wenn Sie eine Anfrage ablehnen wollen, ohne sie zuerst zu überprüfen.

So ignorieren Sie eine Replikation:

1. Wählen Sie aus der Kernkonsole auf dem Quellkern die Registerkarte **Replication** (Replikation).
2. Klicken sie auf der Registerkarte „Replication" (Replikation) auf **Pending Requests (#)** (Ausstehende Anfragen (Nr.)).

   Der Abschnitt **Pending Replication Requests** (Ausstehende Replikationsanfragen) wird angezeigt.
3. Wählen Sie neben der Anfrage, die Sie ignorieren möchten, aus dem Drop-Down-Menü **Ignore** (Ignorieren) aus.

   Der Zielkern sendet eine Meldung an den Quellkern, dass die Anfrage ignoriert wurde.

Überwachen der Replikation

Wenn die Replikation eingerichtet ist, können Sie den Status der Replikationsaufgaben für Quell- und Zielkerne überwachen. Sie können die Statusinformationen aktualisieren, Replikationsdetails anzeigen usw.

So überwachen Sie die Replikation:

1. Klicken Sie in der Core Console auf die Registerkarte **Replication** (Replikation).
2. In dieser Registerkarte können Sie Informationen zum Status der Replikationsaufgaben abrufen und sie überwachen, wie nachfolgend beschrieben.

Tabelle 3. Überwachen der Replikation

Abschnitt	Beschreibung	Verfügbare Maßnahmen
Pending Replication Requests (Replikationsanfragen ausstehend)	Ihre Kunden-ID, E-Mail-Adresse und der Hostname sind aufgelistet, wenn eine Replikationsanfrage an einen Drittanbieter (MSP) gesendet wurde. Diese Daten werden so lange hier angezeigt, bis die Anfrage vom MSP angenommen wird.	Klicken Sie im Drop-Down-Menü auf **Ignore** (Ignorieren), um die Anfrage zu ignorieren oder zurückzuweisen.
Outstanding Seed Drives (Seed-Laufwerke ausstehend)	Seed-Laufwerke sind aufgelistet, die bereits beschrieben, aber noch nicht vom Zielkern konsumiert wurden. Der Remote-Kernname, sein Erstellungsdatum und der Datumsbereich werden angezeigt.	Klicken Sie im Drop-Down-Menü auf **Abandon** (Aufgeben), um den Seed-Vorgang aufzugeben oder abzubrechen.
Outgoing Replication (Ausgehende Replikation)	Listet alle Zielkerne auf, auf die der Quellkern repliziert. Der Remote-Kernname, der Zustand, die Anzahl der geschützten Maschinen, die repliziert werden, und der Fortschritt einer Replikationsübertragung werden angezeigt.	Auf einem Quellkern im Drop-Down-Menü können Sie die folgenden Optionen auswählen: • **Details** (Einzelheiten) – ID, URI, Anzeigename, Zustand, Kunden-ID, E-Mail-Adresse und Anmerkungen zum replizierten Kern anzeigen. • **Change Settings** (Einstellungen ändern) – Anzeigename anzeigen und Host und Port für den Zielkern bearbeiten. • **Add Agents** (Agenten hinzufügen) – Ermöglicht die Auswahl eines Hosts aus einer Drop-Down-Liste, die Auswahl geschützter Maschinen zur Replikation und die Erstellung eines Seed-Laufwerks für die Erstübertragung der neuen geschützten Maschine.

Abschnitt	Beschreibung	Verfügbare Maßnahmen
Incoming Replication (Eingehende Replikation)	Alle Quellmaschinen werden aufgelistet, von denen das Ziel replizierte Daten empfängt. Remote-Kernname, Status, Maschinen und Fortschritt werden angezeigt.	Auf einem Zielkern im Drop-Down-Menü können Sie die folgenden Optionen auswählen: • **Details** (Einzelheiten) – ID, Hostname, Kunden-ID, E-Mail-Adresse und Anmerkungen zum replizierten Kern anzeigen. • **Consume** (Konsumieren) – Konsumiert die ursprünglichen Daten vom Seed-Laufwerk und speichert sie auf dem lokalen Repository.

3. Klicken Sie auf die Schaltfläche **Refresh** (Aktualisieren), um die Abschnitte dieser Registerkarte auf die neuesten Informationen zu aktualisieren.

Verwalten der Replikationseinstellungen

Sie können eine Reihe von Einstellungen so anpassen, wie die Replikation auf den Quell- und Zielkernen ausgeführt werden soll.

So verwalten Sie Replikationseinstellungen:

1. Klicken Sie in der Core Console auf die Registerkarte **Replication** (Replikation).
2. Klicken Sie im Drop-Down-Menü **Actions** (Maßnahmen) auf **Settings** (Einstellungen).
3. Bearbeiten Sie im Fenster **Replication Settings** (Replikationseinstellungen) die Replikationseinstellungen wie nachfolgend beschrieben.

Option	Beschreibung
Cache lifetime (Cache-Lebensdauer)	Geben Sie den Zeitraum zwischen zwei Zielkern-Statusabfragen durch den Quellkern an.
Volume image session timeout (Zeitüberschreitung für Volume-Abbild-Sitzung)	Geben Sie die Dauer an, während der der Quellkern versucht, ein Volume-Abbild auf den Zielkern zu übertragen.
Max. concurrent replication jobs (Max. Anzahl gleichzeitiger Replikationsaufgaben)	Geben Sie die Anzahl an geschützten Maschinen an, die gleichzeitig auf den Zielkern replizieren dürfen.
Max. parallel streams (Max. Anzahl paralleler Streams)	Geben Sie die Anzahl an Netzwerkverbindungen an, die eine einzelne geschützte Maschine zur Replikation ihrer Daten gleichzeitig verwenden darf.

4. Klicken Sie auf **Save** (Speichern).

Entfernen der Replikation

Sie können die Replikation abbrechen und geschützte Maschinen aus der Replikation auf verschiedene Arten entfernen. Mögliche Optionen sind:

- Einen Agenten aus der Replikation auf dem Quellkern entfernen
- Einen Agenten auf dem Zielkern entfernen
- Einen Zielkern aus der Replikation entfernen
- Einen Quellkern aus der Replikation entfernen

ANMERKUNG: Durch Entfernen eines Quellkerns werden alle replizierten Maschinen entfernt, die von diesem Kern geschützt werden.

Entfernen einer geschützten Maschine aus der Replikation auf dem Quellkern

So entfernen Sie eine geschützte Maschine aus der Replikation auf dem Quellkern:

1. Öffnen Sie im Quellkern die Core Console, und klicken Sie auf die Registerkarte **Replication** (Replikation).
2. Vergrößern Sie den Abschnitt **Outgoing Replication** (Ausgehende Replikation).
3. Klicken Sie im Dropdown-Menü der geschützten Maschine, die Sie aus der Replikation entfernen möchten, auf **Delete** (Löschen).
4. Klicken Sie im Dialogfeld **Outgoing Replication** (Ausgehende Replikation) auf **Yes** (Ja), um das Löschen zu bestätigen.

Entfernen einer geschützten Maschine aus dem Zielkern

So entfernen Sie eine geschützte Maschine aus dem Zielkern:

1. Öffnen Sie im Zielkern die Core Console, und klicken Sie auf die Registerkarte **Replication** (Replikation).
2. Vergrößern Sie den Abschnitt **Incoming Replication** (Eingehende Replikation).
3. Klicken Sie im Dropdown-Menü der geschützten Maschine, die Sie aus der Replikation entfernen möchten, auf **Delete** (Löschen), und wählen Sie dann eine der folgenden Optionen aus.

Option	Beschreibung
Relationship Only (Nur Beziehung)	Die geschützte Maschine wird aus der Replikation entfernt, die replizierten Wiederherstellungspunkte werden jedoch beibehalten.
Mit Wiederherstellungspunkt	Die geschützte Maschine wird aus der Replikation entfernt und alle von dieser Maschine empfangenen replizierten Wiederherstellungspunkte werden gelöscht.

Einen Zielkern aus der Replikation entfernen

So entfernen Sie einen Zielkern aus der Replikation:

1. Öffnen Sie im Quellkern die Core Console, und klicken Sie auf die Registerkarte **Replication** (Replikation).
2. Klicken Sie unter **Ausgehende Replikation** auf das Drop-Down-Menü neben dem Remote-Kern, den Sie löschen möchten, und klicken Sie auf **Löschen**.

3. Klicken Sie im Dialogfeld **Outgoing Replication** (Ausgehende Replikation) auf **Yes** (Ja), um das Löschen zu bestätigen.

Einen Quellkern aus der Replikation entfernen

ANMERKUNG: Das Entfernen eines Quellkerns führt zur Entfernung aller replizierten Agenten, die von diesem Kern geschützt werden.

So entfernen Sie einen Quellkern aus der Replikation:

1. Öffnen Sie im Zielkern die Core Console, und klicken Sie auf die Registerkarte **Replication** (Replikation).
2. Klicken Sie unter **Incoming Replication** (Eingehende Replikation) im Drop-Down-Menü auf **Delete** (Löschen) und wählen Sie dann eine der folgenden Optionen aus.

Option	Beschreibung
Relationship Only (Nur Beziehung)	Der Quellkern wird aus der Replikation entfernt, die replizierten Wiederherstellungspunkte werden aber beibehalten.
With Recovery Points (Mit Wiederherstellungspunkten)	Der Quellkern wird aus der Replikation entfernt und alle von dieser Maschine empfangenen replizierten Wiederherstellungspunkte werden gelöscht.

3. Klicken Sie im Dialogfeld **Incoming Replication** (Eingehende Replikation) auf **Yes** (Ja), um das Löschen zu bestätigen.

Wiederherstellen von replizierten Daten

Die Funktion der „Tag-für-Tag"-Replikation bleibt auf dem Quellkern erhalten, während jedoch nur der Zielkern die zur Notfallwiederherstellung notwendigen Funktionen abschließen kann.

Zur Notfallwiederherstellung kann der Zielkern die replizierten Wiederherstellungspunkte zur Wiederherstellung der geschützten Agenten und des Kerns verwenden.

Sie können die folgenden Wiederherstellungsoptionen vom Zielkern aus durchführen:

- Wiederherstellungspunkte laden.
- Rollback auf Wiederherstellungspunkten durchführen.
- Export einer virtuellen Maschine (VM) durchführen.
- Bare-Metal-Wiederherstellung (BMR) durchführen.
- Failback durchführen (falls Sie eine Failover/Failback-Replikationsumgebung eingerichtet haben).

Ablaufplan für Failover und Failback

Wenn Sie mit einer Notfallsituation konfrontiert sind, in der Ihr Quellkern und die zugeordnete geschützte Maschine ausgefallen sind, können Sie in AppAssure die Failover-Funktion aktivieren, um den Schutz auf Ihren identischen Failover-Kern (Zielkern) umzuschalten und einen neuen (replizierten) Agenten zu starten, der mit dem ausgefallen Agenten identisch ist. Nachdem Ihr Quellkern und Ihre Agenten repariert wurden, können Sie ein Failback durchführen, um die Daten vom Failover-Kern und -Agenten auf dem Quellkern und -agenten wiederherzustellen. In AppAssure bestehen Failover und Failback aus folgenden Verfahren.

- Einrichten Ihrer Umgebung für ein Failover.

- Durchführen des Failovers für Zielkern und verknüpfte Agenten.
- Wiederherstellen des Quellkerns durch Ausführen eines Failbacks.

Einrichten einer Failover-Umgebung

Für das Einrichten Ihrer Failover-Umgebung ist es erforderlich, dass Sie zuvor einen Quell- und einen Zielkern sowie einen verknüpften Agenten für die Replikation eingerichtet haben. Führen Sie die Schritte in diesem Verfahren durch, um die Replikation für ein Failover einzurichten.

So richten Sie eine Umgebung für ein Failover ein

1. Installieren Sie einen Kern für die Quelle und einen Kern für das Ziel.
2. Installieren Sie einen AppAssure-Agenten, der vom Quellkern geschützt wird.
3. Erstellen Sie ein Repository auf dem Quellkern und eines auf dem Zielkern.

   Weitere Informationen finden Sie unter Erstellen eines Repositorys.
4. Fügen Sie den zu schützenden Agenten unter dem Quellkern hinzu.

   Weitere Informationen finden Sie unter Schützen einer Maschine.
5. Richten Sie Replikation vom Quell- auf den Zielkern ein und replizieren Sie den geschützten Agenten mit allen Wiederherstellungspunkten.

   Führen Sie die Schritte aus, die unter Replizieren auf einen selbstverwalteten Kern beschrieben sind, um den Zielkern hinzuzufügen, zu dem Sie replizieren möchten.

Durchführen eines Failovers auf dem Zielkern

Wenn Sie mit einer Notfallsituation konfrontiert sind, in der Ihr Quellkern und die zugeordnete geschützte Maschinen ausgefallen sind, können Sie die Failover-Funktion aktivieren, um den Schutz auf Ihren identischen Failover-Kern (Zielkern) umzuschalten. Der Zielkern wird zum einzigen Kern, der die Daten in Ihrer Umgebung schützt. Starten Sie dann einen neuen Agenten, um den ausgefallenen Agenten vorübergehend zu ersetzen.

So führen Sie ein Failover auf dem Zielkern durch:

1. Navigieren Sie zur Core Console auf dem Zielkern, und klicken Sie auf die Registerkarte **Replication** (Replikation).
2. Wählen Sie unter **Incoming Replication** (Eingehende Replikation) den Quellcode aus, und erweitern Sie dann die Details unter dem individuellen Agenten.
3. Klicken Sie im Menü **Actions** (Maßnahmen) für diesen Kern auf **Failover.**

   Der in dieser Tabelle angezeigte Status für diese Maschine ändert sich in **Failover**.
4. Klicken Sie auf die Registerkarte **Machines** (Maschinen) und wählen Sie dann die Maschine aus, die über den verknüpften AppAssure-Agenten mit Wiederherstellungspunkten verfügt.
5. Exportieren Sie die Sicherungsinformationen über den Wiederherstellungspunkt auf dem Agenten zu einer virtuellen Maschine.
6. Fahren Sie die Maschine herunter, auf der sich der AppAssure-Agent befindet.
7. Starten Sie die virtuelle Maschine, auf der sich nun die exportierten Sicherheitsinformationen befinden.

   Sie müssen warten, bis die Gerätetreibersoftware installiert ist.
8. Starten Sie die virtuelle Maschine neu und warten Sie darauf, dass der Agent-Service gestartet wird.
9. Gehen Sie zurück zur Core Console für den Zielkern und überprüfen Sie, ob der neue Agent in der Registerkarte **Machines** (Maschinen) unter **Protected Machine**s (Geschützte Maschinen) und in der Registerkarte **Replication** (Replikation) unter **Incoming Replication** (Eingehende Replikation) angezeigt wird.

10. Erzwingen Sie mehrere Snapshots und überprüfen Sie, ob diese korrekt abgeschlossen werden.

    Weitere Informationen finden Sie unter Erzwingen eines Snapshots.
11. Sie können nun mit dem Failback weitermachen.

    Weitere Informationen finden Sie unter Durchführen eines Failbacks.

Durchführen eines Failbacks

Nachdem Sie den fehlerhaften Originalquellkern oder die geschützte Maschinen repariert oder ersetzt haben, müssen Sie die Daten von Ihren Failed-over-Maschinen verschieben, um die Quellmaschinen wiederherstellen zu können.

So führen Sie ein Failback aus:

1. Navigieren Sie zur Core Console auf dem Zielkern, und klicken Sie auf die Registerkarte **Replication** (Replikation).
2. Wählen Sie unter **Incoming Replication** (Eingehende Replikation) den Failover-Agenten aus und vergrößern Sie die Detail-Ansicht.
3. Klicken Sie im Menü **Actions** (Maßnahmen) auf **Failback**.

   Das Dialogfeld **Failback Warnings** (Failback-Warnungen) öffnet sich und zeigt Ihnen die Schritte an, die Sie ausführen müssen, bevor Sie auf die Schaltfläche **Start Failback** (Failback starten) klicken können.
4. Klicken Sie auf **Cancel** (Abbrechen).
5. Wenn die fehlgeschlagene Maschine auf Microsoft SQL Server oder Microsoft Exchange Server ausgeführt wird, halten Sie diese Dienste an.
6. Klicken Sie in der Core Console des Zielkerns auf die Registerkarte **Tools** (Extras).
7. Erstellen Sie ein Archiv auf dem Failed-over-Agenten und geben Sie es auf ein Laufwerk oder einen Speicherort in der Netzwerkfreigabe aus.
8. Nachdem Sie das Archiv erstellt haben, navigieren Sie zur Core Console im neu reparierten Quell-Kern und klicken Sie auf die Registerkarte **Tools** (Extras).
9. Importieren Sie das Archiv, das Sie soeben unter Schritt 7 erstellt haben.
10. Gehen Sie zur Core Console auf dem Zielkern zurück und klicken Sie auf die Registerkarte **Replication** (Replikation).
11. Wählen Sie unter **Incoming Replication** (Eingehende Replikation) den Failover-Agenten aus und vergrößern Sie die Detail-Ansicht.
12. Klicken Sie im Menü **Actions** (Maßnahmen) auf **Failback**.
13. Klicken Sie im Dialogfeld **Failback Warnings** (Failback-Warnungen) auf **Start Failback** (Failback starten).
14. Schalten Sie die Maschine aus, die den exportierten, während des Failovers erstellten Agenten enthält.
15. Führen Sie eine Bare-Metal-Wiederherstellung (BMR) für den Quellkern und -agenten durch.

    ANMERKUNG: Wenn Sie die Wiederherstellung starten, müssen Sie die Wiederherstellungspunkte verwenden, die vom Zielkern in den Agenten auf der virtuellen Maschine importiert wurden.
16. Warten Sie auf den BMR-Neustart und auf den Start des Agent-Service. Lassen Sie sich dann die Netzwerkverbindungseinzelheiten der Maschine anzeigen und notieren Sie sie.
17. Navigieren Sie zur Core Console auf dem Quellkern und modifizieren Sie in der Registerkarte **Machines** (Maschinen) die Einstellungen des Maschinenschutzes, um die neuen Netzwerkverbindungseinzelheiten hinzuzufügen.

18. Navigieren Sie zur Core Console auf dem Zielkern und löschen Sie dort den Agenten aus der Registerkarte **Replication** (Replikation).
19. Richten Sie in der Core Console des Quellkerns erneut die Replikation zwischen Quelle und Ziel ein, indem Sie auf die Registerkarte **Replication** (Replikation) klicken und dann den Zielkern für die Replikation hinzufügen.

Verwalten von Ereignissen

Durch die Verwaltung von Kernereignissen wird die Überwachung des Funktionszustands und der Verwendung des Kerns unterstützt. Der Kern umfasst vordefinierte Sätze von Ereignissen, mit denen Administratoren über entscheidende Probleme auf dem Kern oder bei Sicherungsaufgaben benachrichtigt werden können.

Über die Registerkarte **Ereignisse** können Sie Benachrichtigungsgruppen, E-Mail-SMTP-Einstellungen, die Wiederholungsreduzierung und die Ereignisaufbewahrung verwalten. Die Option „Benachrichtigungsgruppen“ ermöglicht Ihnen die Verwaltung von Benachrichtigungsgruppen, über die Sie folgende Aufgaben ausführen können:

- Festlegen eines Ereignisses für das Sie eine Benachrichtigung für folgende Bedingungen generieren:
  - Cluster
  - Attachability (Anfügbarkeit)
  - Jobs
  - Lizenzierung
  - Log Truncation (Abschneiden des Protokolls)
  - Archivieren
  - Kern-Service
  - Exportieren
  - Protection (Schutz)
  - Replikation
  - Rollback
  - SMTP-Server-Einstellungen
  - Aktivierte Protokolle der Ablaufverfolgung
  - Cloud-Konfiguration
- Festlegen des Benachrichtigungstyps (Fehler, Warnung und Zur Information).
- Festlegen des Absenders und des Sendeorts der Benachrichtigung. Mögliche Optionen sind:
  - E-Mail-Adresse
  - Windows-Ereignisprotokolle
  - Syslog-Server
- Festlegen einer Zeitgrenze für die Wiederholung.
- Festlegen der Aufbewahrungsdauer für alle Ereignisse.

Konfigurieren von Benachrichtigungsgruppen

So konfigurieren Sie Benachrichtigungsgruppen:

1. Wählen Sie im Kern die Registerkarte **Configuration** (Konfiguration) aus.
2. Klicken Sie unter **Manage** (Verwalten) auf die Option **Events** (Ereignisse).

3. Klicken Sie auf **Add Group** (Gruppe hinzufügen).

   Das Dialogfeld **Benachrichtigungsgruppe hinzufügen** wird geöffnet. Es enthält die folgenden drei Bereiche:

   - **Allgemein**
   - **Enable Events (Ereignisse aktivieren)**
   - **Notification Options (Benachrichtigungsoptionen)**

4. Geben Sie im Bereich **Allgemein** die grundlegenden Informationen für die Benachrichtigungsgruppe wie folgt ein:

Textfeld	Beschreibung
Name	Geben Sie zur Identifizierung der Ereignisbenachrichtigungsgruppe einen Namen für die Ereignisbenachrichtigungsgruppe ein.
Beschreibung	Geben Sie zur Beschreibung des Zwecks der Ereignisbenachrichtigungsgruppe eine Beschreibung für die Ereignisbenachrichtigungsgruppe ein.

5. Wählen Sie im Bereich **Enable Events** (Ereignisse aktivieren) die Bedingungen aus, für die Ereignisprotokolle (Benachrichtigungen) erstellt und gemeldet werden.

   Sie können Benachrichtigungen für folgende Situationen erstellen:

   - **All Events (Alle Ereignisse)**
   - **Appliance Events (Geräte-Ereignisse)**
   - **Boot CD (Start-CD)**
   - **Sicherheit**
   - **DatabaseRetention**
   - **LocalMount**
   - **Cluster**
   - **Notification (Benachrichtigung)**
   - **Power Shell Scripting (Power Shell-Skripts)**
   - **Push Install (Push-Installation)**
   - **Nightly Jobs (Nächtliche Aufgaben)**
   - **Attachability (Anfügbarkeit)**
   - **Jobs**
   - **Lizenzierung**
   - **Log Truncation (Abschneiden des Protokolls)**
   - **Archivieren**
   - **Kern-Service**
   - **Exportieren**
   - **Protection (Schutz)**
   - **Replikation**
   - **Repository**
   - **Rollback**
   - **Rollup**

6. Im Bereich **Notification Options** (Benachrichtigungsoptionen) geben Sie an, wie der Benachrichtigungsprozess erfolgen soll.

   Die Benachrichtigungsoptionen sind:

Textfeld	Beschreibung
Per E-Mail benachrichtigen	Geben Sie die Empfänger der Benachrichtigung per E-Mail an. Sie können entweder separate mehrfache E-Mail-Adressen angeben oder auch Blindkopien und Kopien. Die folgenden Optionen stehen zur Auswahl: • **in:** • **Cc:** • **Bcc:**
Notify by Windows Event Log (Über Windows-Ereignisprotokoll benachrichtigen)	Wählen Sie diese Option, wenn Benachrichtigungen durch das Windows-Ereignisprotokoll gemeldet werden sollen. Diese Option wird zur Angabe verwendet, ob Benachrichtigungen durch das Windows-Ereignisprotokoll gemeldet werden sollen.
Notify by sys logd (Durch sys logd benachrichtigen).	Wählen Sie diese Option, wenn Benachrichtigungen durch sys logd gemeldet werden sollen. Geben Sie die Details für sys logd in den folgenden Textfeldern an: • **Hostname** • **Port 1**

7. Klicken Sie auf **OK**.

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 ebenfalls die Benachrichtigungsgruppen-Einstellungen einschließlich der Option **Notify by email** (Per E-Mail benachrichtigen) konfigurieren, bevor E-Mail-Benachrichtigungen gesendet werden. Weitere Informationen zum Festlegen von Ereignissen zum Empfangen von E-Mail-Warnungen siehe „Configuring Notification Groups For System Events" (Konfigurieren von Benachrichtigungsgruppen für Systemereignisse) im *Dell DL4000 Appliance User's Guide* (Benutzerhandbuch für das Dell DL4000-Gerät).

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 **Email Notification Configuration** (Konfiguration der E-Mail-Benachrichtigung) 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

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

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

Konfigurieren der Wiederholungsreduzierung

So konfigurieren Sie die Wiederholungsreduzierung:

1. Klicken Sie im Kern auf die Registerkarte **Konfiguration**.
2. Klicken Sie unter **Manage** (Verwalten) auf die Option **Events** (Ereignisse).
3. Klicken Sie im Bereich **Repetition Reduction** (Wiederholungsreduzierung) auf **Change** (Ändern).
   Das Dialogfeld „Wiederholungsreduzierung" wird angezeigt.
4. Wählen Sie **Enable Repetition Reduction** (Wiederholungsreduzierung aktivieren) aus.
5. Geben Sie im Textfeld **Store events for X minutes** (Ereignisse X Minuten speichern) die Anzahl an Minuten ein, die die Ereignisse für die Wiederholungsreduzierung gespeichert werden sollen.
6. Klicken Sie auf **OK**.

Konfigurieren der Ereignisaufbewahrung

So konfigurieren Sie die Ereignisaufbewahrung:

1. Klicken Sie im Kern auf die Registerkarte **Konfiguration**.
2. Klicken Sie unter **Manage** (Verwalten) auf die Option **Events** (Ereignisse).
3. Klicken Sie unter **Database Connection Settings** (Datenbankverbindungseinstellungen) auf **change** (Ändern).

   Das Dialogfeld **Datenbankverbindungseinstellungen** wird angezeigt.
4. Geben Sie im Textfeld **Retain event and job history for** (Ereignis- und Aufgabenverlauf aufbewahren) die Anzahl der Tage ein, für die Sie die Informationen über Ereignisse aufbewahren möchten.

   Sie können zum Beispiel 30 Tage (Standard) auswählen.
5. Klicken Sie auf **Speichern**.

Verwalten der Wiederherstellung

Der Kern kann Daten sofort wiederherstellen oder von den Wiederherstellungspunkten aus eine Wiederherstellung von Maschinen auf physischen oder virtuellen Maschinen durchführen. Die Wiederherstellungspunkte enthalten Agenten-Volume-Snapshots, die auf Blockebene erstellt wurden. Diese Snapshots sind anwendungsbezogen, d. h. alle offenen Transaktionen und laufenden Transaktionsprotokolle werden abgeschlossen und die Cache-Speicher werden auf dem Datenträger abgelegt, bevor der Snapshot erstellt wird. Bei Verwendung dieser Art von Snapshots zusammen mit Verified Recovery kann der Kern verschiedene Typen von Wiederherstellungen durchführen, darunter:

- Wiederherstellung von Dateien und Ordnern
- Wiederherstellung von Datenvolumes mithilfe von Live Recovery
- Wiederherstellung von Datenvolumes für Microsoft Exchange Server und Microsoft SQL Server mithilfe von Live Recovery
- Bare-Metal-Wiederherstellung mithilfe von Universal Recovery
- Bare-Metal-Wiederherstellung auf unterschiedlicher Hardware mithilfe von Universal Recovery
- Ad-hoc- und fortlaufender Export auf virtuelle Maschinen

Wissenswertes über Systeminformationen

Dank AppAssure können Sie Informationen über den Kern, wie z. B. Systeminformationen, lokale und bereitgestellte Volumes, sowie AppAssure-Modulverbindungen anzeigen.

Wenn Sie die Bereitstellung einzelner oder aller Wiederherstellungspunkte, die lokal auf einem Kern bereitgestellt wurden, entfernen möchten, können Sie dies über die Option **Bereitstellen** unter der Registerkarte **Extras** durchführen.

Anzeigen von Systeminformationen

So zeigen Sie Systeminformationen an:

1. Wechseln Sie zum Kern, und wählen Sie dann die Registerkarte **Extras** aus.
2. Klicken Sie unter **Tools** (Extras) auf die Option **System Info** (Systeminformationen).

Herunterladen von Installationsprogrammen

Sie haben die Möglichkeit, Installationsprogramme vom Kern herunterzuladen. Über die Registerkarte **Extras** können Sie das Agenten-Installationsprogramm oder das Programm für die lokale Bereitstellung Local Mount Utility herunterladen.

ANMERKUNG: Informationen zum Aufrufen des Agenten-Installationsprogramms finden Sie im Abschnitt zum Herunterladen und Installieren des Agenten-Installationsprogramms. Informationen zum Bereitstellen des Agenten-Installationsprogramms finden Sie im Bereitstellungshandbuch für das Dell DL4300-Gerät *Dell DL4000 Appliance Deployment Guide*, das unter **Dell.com/support/home** verfügbar ist. Informationen zum Aufrufen des Local Mount Utility-Installationsprogramms finden Sie unter Informationen zu Local Mount Utility (Programm für lokale Bereitstellung). Weitere Informationen zu Local Mount Utility finden Sie unter Herunterladen und Installieren von Local Mount Utility.

Informationen zum Agenten-Installationsprogramm

Das Agenten-Installationsprogramm wird verwendet, um die AppAssure-Agentenanwendung auf Maschinen zu installieren, die über den Kern geschützt werden sollen. Wenn Sie feststellen, dass Sie über eine Maschine verfügen, für die das Agenten-Installationsprogramm benötigt wird, können Sie das Web-Installationsprogramm über die Registerkarte **Extras** des Kerns herunterladen.

ANMERKUNG: Das Herunterladen des Kerns erfolgt über das Lizenzportal. Weitere Informationen zum Herunterladen des Kern-Installationsprogramms finden Sie unter **https://licenseportal.com**.

Herunterladen und Installieren des Agenteninstallationsprogramms

Sie können das Installationsprogramm für den Agenten auf alle Maschinen herunterladen und dort bereitstellen, die über den Kern geschützt werden.

So laden Sie das Agenteninstallationsprogramm herunter und installieren Sie es:

1. Laden Sie die Installationsdatei für den Agenten vom Lizenzportal oder vom Kern herunter.
   Zum Beispiel: **Agent-X64-5.3.x.xxxxx.exe**
2. Klicken Sie auf **Save File** (Datei speichern).
   Weitere Informationen zum Installieren der Agenten finden Sie im Bereitstellungshandbuch für das Dell DL4300-Gerät *Dell DL4000 Appliance Deployment Guide*, das unter **Dell.com/support/home** verfügbar ist.

Wissenswertes über Local Mount Utility

Local Mount Utility (LMU) ist eine Anwendung zum Herunterladen, mit der Sie einen Wiederherstellungspunkt auf einem Remote-Kern von jeder Maschine aus bereitstellen können. Das leichte Programm umfasst die Treiber `aavdisk` und `aavstor`, wird aber nicht als Dienst ausgeführt. Wenn Sie das Programm installieren, wird es standardmäßig im Verzeichnis **C:\Programme\AppRecovery\Local Mount Utility** installiert, und es wird eine Verknüpfung auf dem Desktop der Maschine angezeigt.

LMU wurde zwar für den Remotezugriff auf Kerne entworfen, Sie können das Programm aber auch auf einem Kern installieren. Wenn es auf einem Kern ausgeführt wird, erkennt es alle Bereitstellungen von

diesem Kern und zeigt sie an, einschließlich der Bereitstellungen durch die Core Console. Umgekehrt werden auch Bereitstellungen, die durch LMU durchgeführt wurden, in der Konsole angezeigt.

Herunterladen und Installieren von Local Mount Utility

So laden Sie Local Mount Utility herunter und installieren es:

1. Greifen Sie von der Maschine, auf der Sie LMU installieren möchten, auf die Core Console zu, indem Sie die Konsolen-URL in Ihren Browser eingeben und sich mit Ihrem Benutzernamen und Kennwort anmelden.
2. Wählen Sie in der Core Console die Registerkarte **Extras** aus.
3. Klicken Sie in der Registerkarte **Tools** (Extras) auf **Downloads**.
4. Klicken Sie unter **Local Mount Utility** (Programm für lokale Bereitstellung) auf den Link **Download web installer** (Webinstallationsprogramm herunterladen).
5. Klicken Sie im Fenster **Opening LocalMountUtility-Web.exe** (LocalMountUtility-Web.exe wird geöffnet) auf **Save File** (Datei speichern).

   Die Datei wird im lokalen Ordner „Downloads“ gespeichert. In manchen Browsern öffnet sich der Ordner automatisch.
6. Klicken Sie im Ordner **Downloads** mit der rechten Maustaste auf **LocalMountUtility-Web** executable und klicken Sie auf **Open** (Öffnen).

   Je nach Konfiguration Ihrer Maschine wird eventuell das Fenster **User Account Control** (Benutzerkontensteuerung) angezeigt.
7. Wenn das Fenster **User Account Control** (Benutzerkontensteuerung) angezeigt wird, klicken Sie auf **Yes** (Ja), um dem Programm zu erlauben, Änderungen auf der Maschine vorzunehmen.

   Der Installationsassistent von **AppAssure Local Mount Utility** wird gestartet.
8. Klicken Sie auf dem **Willkommen**sbildschirm des Installationsassistenten von **AppAssure Local Mount Utility** auf **Next** (Weiter), um zur Seite **License Agreement** (Lizenzvereinbarung) zu gelangen.
9. Wählen Sie auf der Seite mit der **Lizenzvereinbarung** die Option **I accept the terms in the license agreement** (Ich stimme den Bedingungen der Lizenzvereinbarung zu) aus, und klicken Sie dann auf **Next** (Weiter), um zur Seite **Prerequisites** (Erforderliche Komponenten) zu gelangen.
10. Installieren Sie auf der Seite **Prerequisites** (Erforderliche Komponenten) alle erforderlichen Komponenten und klicken Sie auf **Next** (Weiter), um auf die Seite **Installation Options** (Installationsoptionen) zu gelangen.
11. Führen Sie auf der Seite **Installation Options** (Installationsoptionen) die folgenden Aufgaben durch:
    a. Wählen Sie einen Zielordner für das LMU aus, indem Sie auf die Schaltfläche **Ändern** klicken.

       ANMERKUNG: Der Standardzielordner ist C:\Program Files\AppRecovery\LocalMountUtility.
    b. Wählen Sie aus, ob Sie der Option **Allow Local Mount Utility** (Local Mount Utility erlauben) erlauben, automatisch Diagnose- und Nutzungsinformationen an AppAssure Software, Inc zu senden.
    c. Klicken Sie auf **Next** (Weiter), um zur Seite **Progress** (Fortschritt) zu gelangen und die Anwendung herunterzuladen. Die Anwendung wird in den Zielordner heruntergeladen, wobei der Fortschritt in der Fortschrittsanzeige angezeigt wird. Wenn der Download abgeschlossen ist, geht der Assistent automatisch zur Seite **Completed** (Abgeschlossen) über.
12. Klicken Sie auf **Finish** (Fertigstellen), um den Assistenten zu schließen.

Hinzufügen eines Kerns zu Local Mount Utility

Um einen Wiederherstellungspunkt bereitzustellen, müssen Sie einen Kern zum LMU hinzufügen. Es gibt keine Obergrenze dafür, wie viele Kerne Sie hinzufügen können.

So fügen Sie einen Kern zum Local Mount Utility hinzu:

1. Auf der Maschine, auf der das LMU installiert ist, starten Sie LMU durch Doppelklicken auf das Desktop-Symbol.
2. Wenn das Fenster **User Account Control** (Benutzerkontensteuerung) angezeigt wird, klicken Sie auf **Yes** (Ja), um dem Programm zu erlauben, Änderungen auf der Maschine vorzunehmen.
3. Klicken Sie in der oberen linken Ecke des Fensters „AppAssure Local Mount Utility" auf **Add core** (Kern hinzufügen).
4. Geben Sie im Fenster **Add Core** (Kern hinzufügen) die erforderlichen Anmeldeinformationen wie nachfolgend beschrieben ein:

Textfeld	Beschreibung
Host-Name	Der Name des Kerns, von dem aus Sie Wiederherstellungspunkte bereitstellen möchten. ANMERKUNG: Wenn Sie das LMU auf einem Kern installieren, fügt LMU automatisch die Localhost-Maschine hinzu.
Schnittstelle	Die Portnummer, die zur Kommunikation mit dem Kern verwendet wird. Die Standardportnummer ist 8006.
Use my Windows user credentials (Windows-Benutzer-Anmeldeinformationen verwenden)	Wählen Sie diese Option aus, wenn die Anmeldeinformationen, mit denen Sie auf den Kern zugreifen, die gleichen wie Ihre Windows-Anmeldeinformationen sind.
Use specific credentials (Besondere Anmeldeinformationen verwenden)	Wählen Sie diese Option aus, wenn die Anmeldeinformationen, mit denen Sie auf den Kern zugreifen, sich von Ihren Windows-Anmeldeinformationen unterscheiden.
Benutzername	Der Benutzername, der zum Zugriff auf die Kernmaschine verwendet wird. ANMERKUNG: Diese Option ist nur verfügbar, wenn Sie spezifische Anmeldeinformationen auswählen.
Kennwort	Das Kennwort, das für den Zugriff auf die Kernmaschine verwendet wird. ANMERKUNG: Diese Option ist nur verfügbar, wenn Sie spezifische Anmeldeinformationen auswählen.

5. Klicken Sie auf **Verbinden**.
6. Wenn Sie mehrere Kerne hinzufügen möchten, wiederholen Sie die Schritte 3 - 5 so oft wie erforderlich.

Untersuchen eines bereitgestellten Wiederherstellungspunktes mithilfe von Local Mount Utility

ANMERKUNG: Das Verfahren ist nicht erforderlich, wenn Sie einen Wiederherstellungspunkt direkt nach seiner Bereitstellung untersuchen, da sich der Ordner, in dem sich der Wiederherstellungspunkt befindet, nach Abschluss des Bereitstellungsvorgangs automatisch öffnet.

So untersuchen Sie einen Wiederherstellungspunkt mithilfe vom Local Mount Utility:

1. Auf der Maschine, auf der LMU installiert ist, starten Sie LMU durch Doppelklicken auf das Desktop-Symbol.
2. Klicken Sie im Hauptfenster von **Local Mount Recovery** (Lokale Bereitstellungswiederherstellung) auf **Active mounts** (Aktive Bereitstellungen).

   Das Fenster **Active Mounts** (Aktive Bereitstellungen) öffnet sich und zeigt alle bereitgestellten Wiederherstellungspunkte an.
3. Klicken Sie neben dem Bereitstellungspunkt, über den die Wiederherstellung erfolgen soll, auf **Explore** (Untersuchen), um den Ordner mit deduplizierten Volumes zu öffnen.

Bereitstellen eines Wiederherstellungspunkts mithilfe von Local Mount Utility

Vor dem Bereitstellen eines Wiederherstellungspunkts muss LMU eine Verbindung zu dem Kern herstellen, auf dem der Wiederherstellungspunkt gespeichert ist. Wie in Hinzufügen eines Kerns zu Local Mount Utility beschrieben, kann eine unbegrenzte Anzahl von Kernen zu LMU hinzugefügt werden. Die Anwendung kann jedoch immer nur mit einem Kern gleichzeitig eine Verbindung herstellen. Wenn Sie zum Beispiel einen Wiederherstellungspunkt eines Agenten bereitstellen, der von einem Kern geschützt wird, und dann einen Wiederherstellungspunkt eines Agenten bereitstellen, der von einem anderen Kern geschützt wird, wird LMU automatisch vom ersten Kern getrennt, um eine Verbindung zum zweiten Kern aufzubauen.

So stellen Sie einen Wiederherstellungspunkt mithilfe von Local Mount Utility bereit:

1. Auf der Maschine, auf der das LMU installiert ist, starten Sie LMU durch Doppelklicken auf das Desktop-Symbol.
2. Vergrößern Sie im Hauptfenster des **AppAssure Local Mount Utility** den gewünschten Kern in der Navigationsstruktur, um die geschützten Agenten anzuzeigen.
3. Wählen Sie aus der Navigationsstruktur den gewünschten Agenten aus.

   Die Wiederherstellungspunkte werden im Hauptbereich angezeigt.
4. Erweitern Sie den Wiederherstellungspunkt, den Sie bereitstellen möchten, um einzelne Datenträgervolumes oder Datenbanken anzuzeigen.
5. Klicken Sie mit der rechten Maustaste auf den Wiederherstellungspunkt, den Sie bereitstellen möchten, und wählen Sie eine der folgenden Optionen aus:
   - Mount (Bereitstellen)
   - Mount writable (Beschreibbar bereitstellen)
   - Mount with previous writes (Bereitstellen mit früheren Schreibvorgängen)
   - Advanced mount (Erweitertes Bereitstellen)
6. Führen Sie im Fenster **Advanced Mount** (Erweitertes Bereitstellen) die nachfolgend beschriebenen Optionen aus.

Textfeld	Beschreibung
Mount point path (Pfad für Bereitstellungspunkt)	Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), um einen Pfad für die Wiederherstellungspunkte auszuwählen, der nicht dem Standardpfad zum Bereitstellungspunkt entspricht.
Mount type (Bereitstellungstyp)	Wählen Sie eine der folgenden Optionen: • Mount read-only (Schreibgeschützt bereitstellen) • Mount writable (Beschreibbar bereitstellen)

Textfeld	Beschreibung
	• Mount read-only with previous writes (Schreibgeschützt bereitstellen mit vorherigen Schreibvorgängen)

7. Klicken Sie auf **Mount** (Bereitstellen).

LMU öffnet automatisch den Ordner, in dem sich der bereitgestellte Wiederherstellungspunkt befindet.

ANMERKUNG: Wenn Sie einen Wiederherstellungspunkt auswählen, der bereits bereitgestellt ist, werden Sie vom Dialogfeld **Bereitstellung** gefragt, ob Sie die Bereitstellung des Wiederherstellungspunktes entfernen möchten.

Aufheben der Bereitstellung eines Wiederherstellungspunkts mithilfe von Local Mount Utility

So entfernen Sie die Bereitstellung eines Wiederherstellungspunkts mithilfe von Local Mount Utility:

1. Auf der Maschine, auf der das LMU installiert ist, starten Sie LMU durch Doppelklicken auf das Desktop-Symbol.
2. Klicken Sie im Hauptfenster von **Local Mount Recovery** (Lokale Bereitstellungswiederherstellung) auf **Active mounts** (Aktive Bereitstellungen).

   Das Fenster **Active Mounts** (Aktive Bereitstellungen) öffnet sich und zeigt alle bereitgestellten Wiederherstellungspunkte an.
3. Wählen Sie eine der in der nachfolgend Tabelle beschriebenen Optionen aus, um die Bereitstellung von Wiederherstellungspunkten zu entfernen.

Option	Beschreibung
Dismount (Bereitstellung entfernen)	Nur der angrenzende Wiederherstellungspunkt wird entfernt. a. Klicken Sie auf **Dismount** (Bereitstellung entfernen) neben dem ausgewählten Wiederherstellungspunkt. b. Schließen Sie das Fenster.
Dismount all (Alle Bereitstellungen entfernen)	Alle bereitgestellten Wiederherstellungspunkte werden entfernt. a. Klicken Sie auf **Dismount all** (Alle Bereitstellungen entfernen). b. Klicken Sie im Fenster **Dismount All** (Alle Bereitstellungen entfernen) zur Bestätigung auf **Yes** (Ja). c. Schließen Sie das Fenster.

Informationen zum Taskleistenmenü von Local Mount Utility

Das Taskleistenmenü des LMU befindet sich in der Taskleiste auf Ihrem Desktop. Klicken Sie mit der rechten Maustaste auf das Symbol, um die folgenden Optionen anzuzeigen:

Browse Recovery Points (Wiederherstellungspunkte durchsuchen)	Öffnet den LMU-Hauptbildschirm.

Active Mounts (Aktive Bereitstellungen)	Öffnet den Bildschirm der aktiven Bereitstellungen.
Optionen	Öffnet den Bildschirm der Optionen, in dem Sie das **Default Mount Point Directory** (Standardverzeichnis für einen Bereitstellungspunkt), die **Default Core Credentials** (Standardanmeldeinformationen eines Kerns) und die **Language** (Sprache) für die LMU-Benutzeroberfläche ändern können.
Info	Öffnet den Begrüßungsbildschirm mit den Lizenzinformationen.
Beenden	Schließt die Anwendung.

ANMERKUNG: Mit dem „X" in der oberen Ecke des Hauptbildschirms wird die Anwendung auf die Taskleiste minimiert.

Verwenden von Kern- und Agentenoptionen

Wenn Sie mit der rechten Maustaste auf den Kern oder den Agenten im Haupt-LMU-Bildschirm klicken, können Sie verschiedene Optionen verwenden. Dazu gehören:

- Localhost-Optionen
- Remote-Kern-Optionen
- Agenten-Optionen

Aufrufen von Localhost-Optionen

Um auf Localhost-Optionen zuzugreifen, klicken Sie mit der rechten Maustaste auf den Kern oder Agenten, und klicken Sie anschließend auf **Verbindung zum Kern erneut herstellen**. Die Informationen zum Kern werden aktualisiert, z. B. kürzlich hinzugefügte Agenten.

Aufrufen von Optionen für den Remote-Kern

Klicken Sie zum Aufrufen von Optionen für den Remote-Kern mit der rechten Maustaste auf den Kern oder Agenten, und wählen Sie dann eine der nachfolgend beschriebenen Remote-Kern-Optionen aus:

Option	Beschreibung
Reconnect to core (Verbindung zu Kern erneut herstellen)	Aktualisiert die Informationen zum Kern, wie z. B. kürzlich hinzugefügte Agenten.
Remove core (Kern entfernen)	Entfernt den Kern aus dem **Local Mount Utility** (Programm für lokale Bereitstellung)
Edit core (Kern bearbeiten)	Öffnet das Fenster **Edit Core** (Kern bearbeiten), in dem Sie Hostnamen, Port und Anmeldeinformationen ändern können.

Zugreifen auf Agentenoptionen

Um Zugang zu den Agentenoptionen zu erhalten, klicken Sie mit der rechten Maustaste auf den Kern oder den Agenten, und klicken Sie dann auf **Wiederherstellungspunkte aktualisieren**. Die Liste der Wiederherstellungspunkte für den ausgewählten Agenten wird aktualisiert.

Verwalten von Aufbewahrungsrichtlinien

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 unterstützt. Weitere Informationen über die Konfiguration von Aufbewahrungsrichtlinien finden Sie unter Anpassen der Einstellungen von Aufbewahrungsrichtlinien.

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 unter Adding A Cloud Account (Hinzufügen eines Cloud-Kontos).
- Archivieren Sie Ihre Daten, und exportieren Sie sie in Ihr Cloud-Konto.
- Rufen Sie archivierte Daten aus der Cloud ab, indem Sie diese vom Cloud-Speicherort importieren.

Wissenswertes über die Archivierung

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 die Registerkarte **Configuration** (Konfiguration).
2. Klicken Sie unter **Manage** (Verwalten) auf die Option **Archive** (Archivieren) aus.

   Das Dialogfeld **Archiv erstellen** wird angezeigt.
3. Geben Sie im Dialogfeld **Create Archive** (Archiv erstellen) die im Folgenden beschriebenen Details für das Archiv ein:

Textfeld	Beschreibung
Date range (Datumsbereich)	Um den Datumsbereich anzugeben, wählen Sie das Datum für und von.

Textfeld	Beschreibung
Archive password (Archivierungskennwort)	Geben Sie ein Kennwort für das Archiv ein, das zur Festlegung der Anmeldeinformationen zwecks Sicherung des Archivs verwendet wird.
Confirm (Bestätigen)	Geben Sie das Kennwort erneut ein, um das Archiv zu sichern. Die erneute Eingabe dient der Validierung der in das Textfeld **Archivkennwort** eingegebenen Informationen.
Output Location (Ausgabespeicherort)	Geben Sie zur Definition des Pfads, auf dem sich das Archiv befindet, den Speicherort für die Ausgabe ein. Hierbei kann es sich um einen lokalen Datenträger oder eine Netzwerkfreigabe handeln. Zum Beispiel: **d:\work \archive** oder **\\servername\sharename** für Netzwerkpfade. **ANMERKUNG:** Wenn der Ausgabespeicherort eine Netzwerkfreigabe ist, geben Sie einen Benutzernamen und ein Kennwort für die Verbindung mit der Freigabe ein.
Benutzername	Geben Sie zur Festlegung von Anmeldeinformationen für die Netzwerkfreigabe einen Benutzernamen ein.
Kennwort	Geben Sie zur Festlegung von Anmeldeinformationen für die Netzwerkfreigabe ein Kennwort für den Netzwerkpfad ein.
Maximale Größe	Geben Sie an, wie viel Speicherplatz für das Archiv verwendet werden soll. Sie haben die Auswahl zwischen: • Gesamtes Ziel • Bestimmte Größe in MB oder GB
Recycle action (Maßnahme wiederverwenden)	Wählen Sie die entsprechende wiederzuverwendende Maßnahme aus.
Kommentar	Geben Sie alle zusätzlichen Informationen ein, die zur Erfassung für das Archiv notwendig sind.

4. Klicken Sie auf **Archive** (Archivieren).

Festlegen einer geplanten Archivierung

Mit der Funktion „Geplante Archivierung" können Sie den Zeitpunkt festlegen, zu dem ein Archiv einer ausgewählten Maschine automatisch erstellt und am angegebenen Speicherort gespeichert werden soll. Dies bietet sich an, wenn Sie relativ häufig Archive einer Maschine speichern möchten, ohne die Archive manuell erstellen zu müssen. Führen Sie die Schritte im folgenden Verfahren aus, um die automatische Archivierung zu planen.
So legen Sie eine geplante Archivierung fest:

1. Klicken Sie in der Core Console auf die Registerkarte **Extras**.
2. Klicken Sie bei der Option **Archiv** auf **Geplant**.
3. Klicken Sie auf der Seite „Geplante Archivierung" auf **Hinzufügen**.
   Daraufhin wird das Dialogfeld **Assistent zum Hinzufügen eines Archivs** angezeigt.
4. Wählen Sie auf der Seite **Speicherort** des **Assistenten zum Hinzufügen von Archiven** eine der folgenden Optionen aus der Drop-Down-Liste **Speicherorttyp** aus:

- Lokal: Ausgabespeicherort – Geben Sie den Speicherort für die Ausgabe ein. Er definiert den Pfad, unter dem das Archiv abgelegt werden soll.
- Netzwerk
  - Ausgabespeicherort: Geben Sie den Speicherort für die Ausgabe ein. Er definiert den Pfad, unter dem das Archiv abgelegt werden soll.
  - Benutzername: Geben Sie einen Benutzernamen ein. Dieser wird für die Anmeldeinformationen für die Netzwerkfreigabe verwendet.
  - Kennwort: Geben Sie ein Kennwort für den Netzwerkpfad ein. Dieses wird für die Anmeldeinformationen für die Netzwerkfreigabe verwendet.
- Cloud
  - Konto: Wählen Sie ein Konto aus der Drop-Down-Liste aus. Damit ein Cloud-Konto ausgewählt werden kann, müssen Sie es zuvor in der Core Console hinzugefügt haben.
  - Container: Wählen Sie einen Container, der mit Ihrem Konto verknüpft ist, aus dem Drop-Down-Menü aus.
  - Ordnername: Geben Sie einen Namen für den Ordner ein, in dem die archivierten Daten gespeichert werden sollen. Der Standardname ist „AppAssure-5-Archiv-[ERSTELLT AM]-[ERSTELLT UM]".

5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Maschinen** des Assistenten aus, welche geschützten Maschinen die Wiederherstellungspunkte enthalten, die Sie archivieren möchten.
7. Klicken Sie auf **Weiter.**
8. Wählen Sie auf der Seite **Optionen** eine der folgenden Aktionen für die Wiederverwendung aus der Drop-Down-Liste aus:
   - **Diesen Kern ersetzen** – Alle bereits vorhandenen archivierten Daten auf diesem Kern werden überschrieben, die Daten für andere Kerne bleiben aber intakt.
   - **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.
9. Wählen Sie auf der Seite **Zeitplan** eine der folgenden Optionen für die Häufigkeit der Datensendung aus:
   - Täglich: Zu dieser Uhrzeit – Wählen Sie die Stunde aus, zu der täglich das Archiv erstellt werden soll.
   - Weekly (Wöchentlich)
     - An diesem Wochentag: Wählen Sie den Wochentag aus, an dem das Archiv automatisch erstellt werden soll.
     - Zu dieser Uhrzeit: Wählen Sie die Stunde aus, zu der täglich das Archiv erstellt werden soll.
   - Monthly (Monatlich)
     - An diesem Tag des Monats: Wählen Sie den Tag des Monats aus, an dem das Archiv automatisch erstellt werden soll.
     - Zu dieser Uhrzeit: Wählen Sie die Stunde aus, zu der täglich das Archiv erstellt werden soll.
10. Um die Archivierung anzuhalten, um sie später wiederaufzunehmen, wählen Sie **Erste Pause Archivierung** aus.

    Sie können beispielsweise die geplanten Archivierung unterbrechen, wenn Sie Zeit für die Vorbereitung des Zielspeicherorts benötigen, und dann die Archivierung wiederaufnehmen. Wenn Sie diese Option nicht aktivieren, beginnt die Archivierung zu der geplanten Uhrzeit.
11. Klicken Sie auf **Fertigstellen**.

Anhalten und Wiederaufnehmen einer geplanten Archivierung

Wenn Sie sich beim Festlegen einer geplanten Archivierung für das Anhalten der Archivierung entschieden haben, können Sie die geplante Archivierung zu einem späteren Zeitpunkt wieder aufnehmen.
So können Sie eine geplante Archivierung anhalten oder wieder aufnehmen:

1. Wechseln Sie zur **Core Console**, und klicken Sie auf die Registerkarte **Extras**.
2. Klicken Sie bei der Option **Archiv** auf **Geplant**.
3. Wählen Sie auf der Seite **Geplante Archivierung** eine der folgenden Vorgehensweisen:
   - Wählen Sie das bevorzugte Archiv aus, und klicken Sie dann auf eine der folgenden Aktionen:
     - Pause
     - Wiederaufnehmen
   - Klicken Sie neben dem bevorzugten Archiv auf das Drop-Down-Menü und dann auf eine der folgenden Aktionen:
     - Pause
     - Wiederaufnehmen

   Der Status des Archivs wird in der Spalte **Zeitplan** angezeigt.

Bearbeiten einer geplanten Archivierung

1. Klicken Sie in der Core Console auf die Registerkarte **Extras**.
2. Klicken Sie bei der Option **Archivierung** auf **Geplant**.
3. Klicken Sie auf der Seite „Geplante Archivierung" auf das Drop-Down-Menü neben dem Archiv, das Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.

   Daraufhin wird das Dialogfeld **Assistent zum Hinzufügen eines Archivs** angezeigt.
4. Wählen Sie auf der Seite **Speicherort** des **Assistenten zum Hinzufügen von Archiven** eine der folgenden Optionen aus der Drop-Down-Liste **Speicherorttyp** aus:
   - Lokal: Ausgabespeicherort – Geben Sie den Speicherort für die Ausgabe ein. Er definiert den Pfad, unter dem das Archiv abgelegt werden soll.
   - Netzwerk
     - Ausgabespeicherort: Geben Sie den Speicherort für die Ausgabe ein. Er definiert den Pfad, unter dem das Archiv abgelegt werden soll.
     - Benutzername: Geben Sie einen Benutzernamen ein. Dieser wird für die Anmeldeinformationen für die Netzwerkfreigabe verwendet.
     - Kennwort: Geben Sie ein Kennwort für den Netzwerkpfad ein. Dieses wird für die Anmeldeinformationen für die Netzwerkfreigabe verwendet.
   - Cloud
     - Konto: Wählen Sie ein Konto aus der Drop-Down-Liste aus. Damit ein Cloud-Konto ausgewählt werden kann, müssen Sie es zuvor in der Core Console hinzugefügt haben.
     - Container: Wählen Sie einen Container, der mit Ihrem Konto verknüpft ist, aus dem Drop-Down-Menü aus.
     - Ordnername: Geben Sie einen Namen für den Ordner ein, in dem die archivierten Daten gespeichert werden sollen. Der Standardname ist „AppAssure-5-Archiv-[ERSTELLT AM]-[ERSTELLT UM]".

5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Maschinen** des Assistenten aus, welche geschützten Maschinen die Wiederherstellungspunkte enthalten, die Sie archivieren möchten.
7. Klicken Sie auf **Weiter.**
8. Wählen Sie auf der Seite **Zeitplan** eine der folgenden Optionen für die Häufigkeit der Datensendung aus:
   - Täglich: Zu dieser Uhrzeit – Wählen Sie die Stunde aus, zu der täglich das Archiv erstellt werden soll.
   - Weekly (Wöchentlich)
     - An diesem Wochentag: Wählen Sie den Wochentag aus, an dem das Archiv automatisch erstellt werden soll.
     - Zu dieser Uhrzeit: Wählen Sie die Stunde aus, zu der täglich das Archiv erstellt werden soll.
   - Monthly (Monatlich)
     - An diesem Tag des Monats: Wählen Sie den Tag des Monats aus, an dem das Archiv automatisch erstellt werden soll.
     - Zu dieser Uhrzeit: Wählen Sie die Stunde aus, zu der täglich das Archiv erstellt werden soll.
9. Um die Archivierung anzuhalten, um sie später wiederaufzunehmen, wählen Sie **Erste Pause Archivierung** aus.

   Sie können beispielsweise die geplanten Archivierung unterbrechen, wenn Sie Zeit für die Vorbereitung des Zielspeicherorts benötigen, und dann die Archivierung wiederaufnehmen. Wenn Sie diese Option nicht aktivieren, beginnt die Archivierung zu der geplanten Uhrzeit.
10. Klicken Sie auf **Fertigstellen**.

Überprüfen eines Archivs

Sie können ein Archiv auf seine strukturelle Integrität überprüfen, indem Sie eine Archivüberprüfung durchführen. Dabei wird überprüft, ob alle erforderlichen Dateien im Archiv vorhanden sind. Um ein Archiv zu überprüfen, führen Sie die Schritte des folgenden Verfahrens aus:

1. Klicken Sie in der Core Console auf die Registerkarte **Extras**.
2. Klicken Sie bei der Option **Archiv** auf **Archiv überprüfen**.

   Das Dialogfeld **Archiv überprüfen** wird angezeigt.
3. Wählen Sie eine der folgenden Optionen aus der Drop-Down-Liste aus:
   - Lokal: Ausgabespeicherort – Geben Sie den Speicherort für die Ausgabe ein. Er definiert den Pfad, unter dem das Archiv abgelegt werden soll.
   - Netzwerk
     - Ausgabespeicherort: Geben Sie den Speicherort für die Ausgabe ein. Er definiert den Pfad, unter dem das Archiv abgelegt werden soll.
     - Benutzername: Geben Sie einen Benutzernamen ein. Dieser wird für die Anmeldeinformationen für die Netzwerkfreigabe verwendet.
     - Kennwort: Geben Sie ein Kennwort für den Netzwerkpfad ein. Dieses wird für die Anmeldeinformationen für die Netzwerkfreigabe verwendet.
   - Cloud
     - Konto: Wählen Sie ein Konto aus der Drop-Down-Liste aus. Damit ein Cloud-Konto ausgewählt werden kann, müssen Sie es zuvor in der Core Console hinzugefügt haben.
     - Container: Wählen Sie einen Container, der mit Ihrem Konto verknüpft ist, aus dem Drop-Down-Menü aus.

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

4. Wenn Sie zudem eine strukturelle Integritätsüberprüfung durchführen möchten, klicken Sie auf **Strukturelle Integrität**.
5. Klicken Sie auf **Datei überprüfen**.

Importieren eines Archivs

So importieren Sie ein Archiv:

1. Wählen Sie in der Core Console die Registerkarte **Configuration** (Konfiguration).
2. Klicken Sie unter **Manage** auf die Option **Archive** (Archivieren) und dann **Import** (Importieren).

   Das Dialogfeld **Archiv importieren** wird angezeigt.
3. Geben Sie im Dialogfeld **Import Archive** (Archiv importieren) die im Folgenden beschriebenen Details zum Importieren des Archivs ein.

Textfeld	Beschreibung
Input Location (Eingabespeicherort)	Wählen Sie den Speicherort zum Importieren des Archivs aus.
Benutzername	Geben Sie die Anmeldeinformationen ein, um einen Zugriff zur Sicherung des Archivs aufzubauen.
Kennwort	Geben Sie ein Kennwort für den Zugriff auf das Archiv ein.

4. Klicken Sie auf **Check File** (Datei prüfen), um zu prüfen, ob das zu importierende Archiv vorhanden ist.

   Das Dialogfeld **Wiederherstellung** wird angezeigt.
5. Prüfen Sie im Dialogfeld **Restore** (Wiederherstellung) den Namen des Quellkerns.
6. Wählen Sie die Agenten aus, die aus dem Archiv importiert werden sollen.
7. Wählen Sie das Repository.
8. Klicken Sie auf **Restore** (Wiederherstellung), um das Archiv zu importieren.

Verwalten der SQL-Anfügbarkeit

Mithilfe der Konfiguration der SQL-Anfügbarkeit kann der Kern unter Verwendung einer lokalen Instanz des Microsoft SQL-Servers Anfügungen an die SQL-Datenbank und die Protokolldateien in einem Snapshot eines SQL-Servers vornehmen. Durch den Test der Anfügbarkeit kann der Kern die Konsistenz der SQL-Datenbanken prüfen und sicherstellen, dass alle Datendateien (MDF- und LDF-Dateien) im Sicherungs-Snapshot verfügbar sind. Anfügbarkeitsprüfungen können bei Bedarf für bestimmte Wiederherstellungspunkte oder als Teil eines nächtlichen Jobs ausgeführt werden.

Anfügbarkeit erfordert eine lokale Instanz des Microsoft SQL-Servers auf der AppAssure-Kernmaschine. Diese Instanz muss eine vollständig lizenzierte Version des SQL-Servers sein, die von Microsoft oder durch einen lizenzierten Händler erworben wurde. Unter Microsoft ist es nicht möglich, passive SQL-Lizenzen zu verwenden.

Anfügbarkeit wird für SQL-Server 2005, 2008, 2008 R2, 2012 und 2014 unterstützt. Dem für den Test verwendeten Konto muss auf der SQL-Serverinstanz die Sysadmin-Rolle erteilt werden.

Das SQL-Server-On-Disk-Speicherformat ist in den 64-Bit- und 32-Bit-Umgebungen identisch, und die Anfügbarkeit funktioniert in beiden Versionen. Eine Datenbank, die von einer in einer Umgebung laufenden Serverinstanz getrennt wurde, kann an eine in einer anderen Umgebung ausgeführte Serverinstanz angefügt werden.

VORSICHT: Die Version des SQL-Servers auf dem Kern muss gleichwertig oder höher als die SQL Server-Version auf allen Agenten mit installiertem SQL-Server sein.

Konfigurieren der SQL-Anfügbarkeitseinstellungen

Bevor Sie Anfügbarkeitsprüfungen auf geschützten SQL-Datenbanken ausführen, wählen Sie eine lokale Instanz des SQL-Servers auf der Kernmaschine, die dazu verwendet wird, die Prüfungen gegen die Agentenmaschine auszuführen.

ANMERKUNG: Anfügbarkeit erfordert eine lokale Instanz des Microsoft SQL-Servers auf der AppAssure-Kernmaschine. Diese Instanz muss eine vollständig lizenzierte Version des SQL-Servers sein, die von Microsoft oder durch einen lizenzierten Händler erworben wurde. Unter Microsoft ist es nicht möglich, passive SQL-Lizenzen zu verwenden.

So konfigurieren Sie die SQL-Anfügbarkeitseinstellungen:

1. Navigieren Sie zur Core Console.
2. Klicken Sie auf **Konfiguration → Einstellungen**.
3. Klicken Sie im Bereich „Nächtliche Jobs“ auf **Ändern**.

   Das Dialogfeld **Nächtliche Jobs** wird angezeigt.
4. Wählen Sie die Option **Job für das Durchführen der Anfügbarkeitsprüfung** aus, und klicken Sie dann auf **Einstellungen**.
5. Wählen Sie mithilfe des Drop-Down-Menüs die Instanz von SQL Server aus, die auf dem Kern installiert ist.

   Folgende Optionen stehen zur Auswahl:
   - **SQL Server 2005**
   - **SQL Server 2008**
   - **SQL Server 2008 R2**
   - **SQL Server 2012**
   - **SQL Server 2014**
6. Wählen Sie den Typ der Anmeldeinformationen aus.

   Folgende Optionen stehen zur Auswahl:
   - **Windows**
   - **SQL**
7. Geben Sie die Anmeldeinformationen mit Administratorberechtigungen für die Windows- oder SQL-Server-Instanzen ein, wie nachfolgend beschrieben.

Textfeld	Beschreibung
Benutzername	Geben Sie einen Benutzernamen für die Anmeldeberechtigung beim SQL-Server ein.
Kennwort	Geben Sie ein Kennwort für die SQL-Anfügbarkeit ein. Es wird zur Steuerung der Anmeldeaktivität verwendet.

8. Klicken Sie auf **Test Connection** (Verbindung testen).

ANMERKUNG: Wenn Sie die Anmeldeinformationen falsch eingegeben haben, wird eine Meldung angezeigt, die Sie darauf hinweist, dass das Testen der Anmeldeinformationen fehlgeschlagen ist. Korrigieren Sie die Anmeldeinformationen und führen Sie den Verbindungstest erneut durch.

9. Klicken Sie auf **Speichern**.

   Anfügbarkeitsprüfungen stehen nun zur Durchführung auf den geschützten SQL-Serverdatenbanken zur Verfügung.

10. Klicken Sie im Fenster „Nächtliche Jobs" auf **OK**.

    Die Anfügbarkeitsprüfungen werden nun planmäßig im Rahmen der nächtlichen Jobs durchgeführt.

Konfigurieren von nächtlichen SQL-Anfügbarkeitsprüfungen und Abschneiden des Protokolls

So konfigurieren Sie nächtliche SQL-Anfügbarkeitsprüfungen und das Abschneiden des Protokolls

1. Wählen Sie im linken Navigationsbereich des Kerns die Maschine aus, auf der nächtliche Anfügbarkeitsprüfungen und Abschneiden des Protokolls durchgeführt werden sollen, und klicken Sie auf **SQL-Server-Einstellungen**.
2. Navigieren Sie zur Core Console.
3. Klicken Sie auf **Konfiguration → Einstellungen**.
4. Klicken Sie im Bereich **Nightly Jobs** (Nächtliche Aufgaben) auf **Change** (Ändern).
5. Wählen Sie die folgenden SQL-Server-Einstellungen aus oder löschen Sie sie, je nach Bedarf Ihrer Organisation:
   - **Job für das Durchführen der Anfügbarkeitsprüfung**
   - **Job für das Abschneiden des Protokolls (nur einfaches Wiederherstellungsmodell)**
6. Klicken Sie auf **OK**.

   Die Einstellungen für Anfügbarkeit und Abschneiden des Protokolls werden für den geschützten SQL-Server wirksam.

Verwalten von Überprüfungen der Bereitstellungsfähigkeit und Abschneiden des Protokolls bei Exchange-Datenbanken

Wenn Sie AppAssure zur Sicherung von Microsoft Exchange-Servern verwenden, können Überprüfungen der Bereitstellungsfähigkeit auf allen Exchange-Datenbanken nach jedem Snapshot durchgeführt werden. Diese Funktion zur Beschädigungsermittlung weist die Administratoren auf mögliche Fehler hin und stellt sicher, dass alle Daten auf den Exchange-Servern bei einem Ausfall erfolgreich wiederhergestellt werden.

ANMERKUNG: Die Funktionen zur Überprüfung der Bereitstellungsfähigkeit und zum Abschneiden des Protokolls gelten nur für Microsoft Exchange 2007, 2010 und 2013. Außerdem muss dem Konto des AppAssure Agent-Services die Rolle des organisatorischen Administrators in Exchange zugewiesen werden.

Konfigurieren von Bereitstellungsfähigkeit und Abschneiden des Protokolls von Exchange-Datenbanken

Sie können Exchange-Datenbank-Servereinstellungen anzeigen, aktivieren oder deaktivieren, einschließlich automatischer Überprüfung der Bereitstellungsfähigkeit, nächtliche Prüfsummen-Überprüfung, oder nächtliches Abschneiden des Protokolls.

So konfigurieren Sie Bereitstellungsfähigkeit und Abschneiden des Protokolls bei Exchange-Datenbanken:

1. Wählen Sie im linken Navigationsbereich der Core Console die Maschine aus, für die Sie die Überprüfung der Bereitstellungsfähigkeit und das Abschneiden des Protokolls konfigurieren möchten.

   Die Registerkarte **Summary** (Zusammenfassung) wird für die ausgewählte Maschine angezeigt.
2. Klicken Sie auf **Exchange Server Settings** (Exchange-Server-Einstellungen).

   Das Dialogfeld **Exchange Server Settings** (Exchange-Server-Einstellungen) wird angezeigt.
3. Wählen Sie die folgenden Exchange-Server-Einstellungen aus oder löschen Sie sie, je nach Bedarf Ihrer Organisation:
   - **Enable automatic mountability check (Automatische Überprüfung der Bereitstellungsfähigkeit aktivieren)**
   - **Enable nightly checksum check (Nächtliche Prüfsummen-Überprüfung aktivieren)**
   - **Enable nightly log truncation (Nächtliches Abschneiden des Protokolls aktivieren)**
4. Klicken Sie auf **OK**.

   Die Einstellungen für Bereitstellungsfähigkeit und Abschneiden des Protokolls werden für den geschützten Exchange-Server wirksam.

   ANMERKUNG: Weitere Informationen zum Erzwingen des Abschneidens von Protokollen finden Sie unter Erzwingen des Abschneidens des Protokolls.

Erzwingen einer Überprüfung der Bereitstellungsfähigkeit

So erzwingen Sie eine Überprüfung der Bereitstellungsfähigkeit:

1. Wählen Sie im linken Navigationsbereich der Core Console die Maschine aus, für die Sie die Überprüfung der Bereitstellungsfähigkeit erzwingen möchten, und klicken Sie dann auf die Registerkarte **Wiederherstellungspunkte**.
2. Klicken Sie auf **>** neben einem Wiederherstellungspunkt in der Liste, um die Ansicht zu erweitern.
3. Klicken Sie auf **Force Mountability Check** (Überprüfung der Bereitstellungsfähigkeit erzwingen).

   Sie werden durch eine Meldung um Erzwingen der Überprüfung der Bereitstellungsfähigkeit aufgefordert.
4. Klicken Sie auf **Ja**.

   ANMERKUNG: Anweisungen zum Anzeigen des Status der Überprüfung der Bereitstellungsfähigkeit finden Sie unter Anzeigen von Ereignissen und Benachrichtigungen.

   Das System führt die Überprüfung der Bereitstellungsfähigkeit durch.

Erzwingen von Prüfsummen-Überprüfungen

So erzwingen Sie eine Überprüfung der Prüfsumme

1. Wählen Sie im linken Navigationsbereich der Core Console die Maschine aus, für die Sie die Prüfsummen-Überprüfung erzwingen möchten, und klicken Sie dann auf die Registerkarte **Wiederherstellungspunkte**.
2. Klicken Sie auf **>** neben einem Wiederherstellungspunkt in der Liste, um die Ansicht zu erweitern.
3. Klicken Sie auf **Force Checksum Check** (Prüfsummen-Überprüfung erzwingen).

   Das Fenster **Force Attachability Check** (Anfügbarkeitsprüfung erzwingen) wird angezeigt, um Sie darauf hinzuweisen, dass Sie eine Prüfsummen-Überprüfung erzwingen möchten.
4. Klicken Sie auf **Ja**.

Das System führt die Prüfsummen-Überprüfung durch.

ANMERKUNG: Informationen zum Anzeigen des Status der Prüfsummen-Überprüfung finden Sie unter Anzeigen von Ereignissen und Benachrichtigungen.

Erzwingen des Abschneidens des Protokolls

ANMERKUNG: Diese Option steht nur für Exchange- oder SQL-Maschinen zur Verfügung.

So erzwingen Sie das Abschneiden des Protokolls:

1. Wechseln Sie zur Core Console, und klicken Sie dann auf die Registerkarte **Maschinen**.
2. Führen Sie auf der Registerkarte **Machines** (Maschinen) einen der folgenden Schritte aus:
   - Klicken Sie auf den Hyperlink für die Maschine, für die Sie das Protokoll abschneiden möchten.
   - Oder wählen Sie im Navigationsbereich die Maschine aus, für die Sie das Protokoll abschneiden möchten.
3. Klicken Sie im Drop-Down-Menü **Actions** (Maßnahmen) für diese Maschine auf **Force Log Truncation** (Abschneiden des Protokolls erzwingen).
4. Bestätigen Sie, ob Sie mit dem Erzwingen des Protokoll-Abschneidens fortfahren möchten.

Statusanzeigen eines Wiederherstellungspunkts

Nachdem ein Wiederherstellungspunkt auf einem geschützten SQL- oder Exchange-Server erstellt wurde, zeigt die Anwendung den Status in der entsprechenden Farbe in der Tabelle der **Recovery Points** (Wiederherstellungspunkte) an. Die angezeigte Farbe basiert auf den Überprüfungseinstellungen für die geschützte Maschine und dem Erfolg bzw. Fehlschlagen dieser Überprüfungen, wie in den folgenden Tabellen beschrieben.

ANMERKUNG: Weitere Informationen zum Anzeigen von Wiederherstellungspunkten finden Sie unter Anzeigen von Wiederherstellungspunkten.

Die folgende Tabelle listet die Statusanzeigen auf, die bei SQL-Datenbanken angezeigt werden.

Statusfarbe des Wiederherstellungspunkts bei SQL-Datenbanken

Statusfarbe	Beschreibung
Weiß	Zeigt an, das eines der folgenden Probleme besteht: • Eine SQL-Datenbank war nicht vorhanden. • Anfügbarkeitsprüfungen wurden nicht aktiviert. • Anfügbarkeitsprüfungen wurden noch nicht durchgeführt.
Gelb	Zeigt an, dass die SQL-Datenbank offline und eine Überprüfung nicht möglich war.
Rot	Zeigt an, dass die Anfügbarkeitsprüfung fehlgeschlagen ist.
Grün	Zeigt an, dass die Anfügbarkeitsprüfung erfolgreich war.

Die folgende Tabelle listet die Statusanzeigen auf, die bei Exchange-Datenbanken angezeigt werden.

Statusfarbe des Wiederherstellungspunkts bei Exchange-Datenbanken

Begriff Überschrift	Beschreibung Überschrift
Weiß	Zeigt an, das eines der folgenden Probleme besteht: • Eine Exchange-Datenbank war nicht vorhanden. • Überprüfungen der Bereitstellungsfähigkeit wurden nicht aktiviert. **ANMERKUNG:** Dies kann für bestimmte Volumes innerhalb eines Wiederherstellungspunktes gelten.
Gelb	Zeigt an, dass die Überprüfungen der Bereitstellungsfähigkeit der Exchange-Datenbank aktiviert sind, die Überprüfungen aber noch nicht durchgeführt wurden.
Rot	Zeigt an, dass entweder die Überprüfungen der Bereitstellungsfähigkeit oder die Prüfsummen-Überprüfungen in mindestens einer Datenbank fehlgeschlagen sind.
Grün	Zeigt an, dass die Überprüfung der Bereitstellungsfähigkeit bzw. die Prüfsummen-Überprüfung erfolgreich war.

ANMERKUNG: Wiederherstellungspunkte, mit denen keine Exchange- oder SQL-Datenbank verbunden ist, werden mit einer weißen Statusanzeige angezeigt. In Situationen, in denen es für den Wiederherstellungspunkt sowohl eine Exchange- als auch eine SQL-Datenbank gibt, wird die schwerwiegendste Statusanzeige für den Wiederherstellungspunkt angezeigt.

3

Verwalten des Geräts

Die Core Console enthält eine Registerkarte mit der Bezeichnung **Gerät**, die Sie dazu verwenden können, Speicherplatz zur Verfügung zu stellen, den Funktionszustand des Geräts zu überwachen, und auf Verwaltungstools zuzugreifen.

Überwachung des Gerätestatus

Sie können den Status der Geräte-Subsysteme über die Registerkarte **Appliance** (Gerät) auf der Seite **Overall Status** (Allgemeiner Status) überwachen. Die Seite **Overall Status** (Allgemeiner Status) zeigt eine Statusanzeige neben jedem Subsystem und eine Statusbeschreibung an, die den Funktionszustand des Subsystems anzeigt.

Die Seite „Allgemeiner Status" stellt ferner Links für Hilfsprogramme bereit, die weiter in die Tiefe gehen und weitere Details zu den einzelnen Untersystemen enthalten, die für Fehlerbehebungs-Warnmeldungen oder Fehler hilfreich sein können. Der Link **Systemadministrator**, der für die Untersysteme „Geräte-Hardware" und „Speicher-Hardware" verfügbar ist, fordert Sie dazu auf, sich bei der Anwendung „Systemadministrator", die für die Hardwareverwaltung verwendet wird, anzumelden. Weitere Informationen über diese Anwendung finden Sie im OpenManage Server-Administratorhandbuch *OpenManage Server Administrator User's Guide* unter **dell.com/support/home**. Der Link **Status der Bereitstellung**, der für das Untersystem „Speicherbereitstellung" verfügbar ist, öffnet den Bildschirm **Aufgaben**, der den Status der Bereitstellung dieses Untersystems anzeigt. Wenn Speicherplatz für die Bereitstellung zur Verfügung steht, wird neben der Bereitstellungsaufgabe ein Link für die **Bereitstellung** unter **Aktionen** angezeigt.

Speicherbereitstellung

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

- AppAssure-Repositories

  ANMERKUNG: Wenn Fibre Channel-HBA konfiguriert ist, ist das Erstellen der Repositorys ein manueller Prozess. AppAssure erstellt kein Repository automatisch im Stammverzeichnis. Weitere Informationen siehe *Dell DL4000Appliance Deployment Guide* (Bereitstellungshandbuch für das Dell DL4300-Gerät).

- Virtuelles Standby der geschützten Maschinen

ANMERKUNG: MD1400s mit 1TB-, 2TB-, 4TB-, oder 6TB-Laufwerken (für hohe Kapazitäten), die mit dem H830-Controller verbunden sind, werden unterstützt. Bis zu vier MD1400s werden unterstützt.

ANMERKUNG: Die DL4000-Konfiguration mit hoher Kapazität unterstützt entweder H810-PERC-SAS-Adapter oder zwei Fibre Channel-HBAs. Weitere Informationen zur Konfiguration von Fibre Channel-HBAs finden Sie im entsprechenden Whitepaper zur FC-Implementierung *DL4xxx – Fibre Channel Implementation* unter **dell.com/support/home**.

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

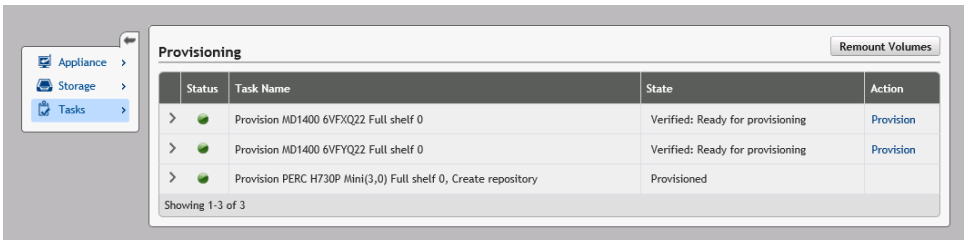
Basierend auf einer mittelgroßen Umgebung die keine virtuellen Standby-Maschinen braucht, können Sie den ganzen Speicher dazu verwenden eine erhebliche Anzahl von Agenten zu sichern. Wenn Sie jedoch weitere Ressourcen für virtuelle Standby-Maschinen benötigen und eine kleinere Anzahl von Agentenmaschinen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

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

So schließen Sie die Laufwerksbereitstellung für alle verfügbaren Speicher ab:

1. Klicken Sie in der Registerkarte **Appliance** (Gerät) auf **Tasks** → **Provisioning (Bereitstellung)**.
   Der Bildschirm **Provisioning** (Bereitstellung) zeigt die erwartete Kapazität der Speicherzuweisung an. Diese Kapazität wird dazu verwendet, ein neues AppAssure-Repository zu erstellen.

   VORSICHT: Bevor Sie fortfahren, stellen Sie sicher, dass Sie Schritt 2 bis 4 dieses Verfahrens ausgeführt haben.
2. Öffnen Sie das Fenster **Speicherbereitstellung**, indem Sie in der Aktionsspalte neben dem Speicher, den Sie bereitstellen möchten, auf **Bereitstellung** klicken.
3. Markieren Sie im Abschnitt **Optionale Speicherreserve** das Kontrollkästchen **Einen Teil des Speichers zuweisen, der für virtuelle Standby-Maschinen und andere Zwecke bereitgestellt wird**, und geben Sie einen Prozentsatz des zuzuweisenden Speichers an. Andernfalls wird der Prozentsatz des Speichers, der im Abschnitt **Optionale Speicherreserve** angegeben ist, von allen angeschlossenen Festplatten entnommen.
4. Klicken Sie auf **Provision** (Bereitstellung)



Breitstellung von ausgewählten Speichern

So stellen Sie ausgewählte Speicher bereit:

1. Klicken Sie in der Registerkarte **Appliance** (Gerät) auf **Tasks** → **Provisioning (Speicherzuweisung)**.

Der Bildschirm **Provisioning** (Speicherzuweisung) zeigt die erwartete Kapazität der Speicherzuweisung an. Diese Kapazität wird dazu verwendet, ein neues AppAssure-Repository zu erstellen.

2. Um nur einen Teil des verfügbaren Speichers bereitzustellen, klicken Sie auf **Provision** (Bereitstellung) unter **Action** (Maßnahme) neben dem Speicherplatz, den Sie bereitstellen möchten.
   - Um ein neues Repository zu erstellen, wählen Sie **Create a new repository**, (Ein neues Repository erstellen) und geben Sie einen Namen für das Repository ein.

     Standardmäßig wird Repository 1 im neuen Repository-Namen angezeigt. Sie können sich dazu entscheiden, den Namen zu überschreiben.
   - Wählen Sie **Expand the existing repository** (Aktuelles Repository erweitern) und das entsprechende Repository in der Liste **Existing Repositories** (Aktuelle Repositories) aus, um einem vorhandenen Repository Kapazität hinzuzufügen.

   ANMERKUNG: Um Kapazität hinzuzufügen wird empfohlen, dass sie ein aktuelles Repository erweitern, anstatt ein weiteres Repository hinzuzufügen. Speicherplatz wird von separaten Repositories nicht gleichermaßen effizient genutzt, weil eine Deduplizierung nicht über separate Repositories hinweg durchgeführt werden kann.
3. Wählen Sie unter **Optional Storage Reserve** (Optionale Speicherreserve) die Option **Allocate a portion of the storage being provisioned for Standby Virtual Machines or other purposes** (Einen Teil des Speichers zuweisen, der für virtuelle Standby-Maschinen und andere Zwecke bereitgestellt wird) aus, und geben Sie dann den Prozentsatz des Speichers an, der für die VMs bereitgestellt werden soll.
4. Klicken Sie auf **Provision** (Bereitstellung)

   Die Laufwerksbereitstellung beginnt, und im Bereich **Status** des Bildschirms **Tasks** wird der Status der AppAssure-Repository-Erstellung angezeigt. Als **State** (Zustand) wird **Provisioned** (Bereitgestellt) angezeigt.
5. Um die Details anzuzeigen nachdem die Laufwerksbereitstellung fertiggestellt wird, klicken Sie auf **>** neben der Statusanzeige.

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

Löschen der Speicherplatzzuweisung für ein virtuelles Laufwerk

Bevor Sie diesen Vorgang starten, stellen Sie fest, welches virtuelle Laufwerk Sie löschen möchten. Wählen Sie in der Core Console die Registerkarte **Appliance** (Gerät) aus, klicken Sie auf **Tasks**, und erweitern Sie dann das Repository, das die virtuellen Laufwerke enthält, um die Details zu den virtuellen Laufwerken anzuzeigen.
So löschen Sie die Speicherplatzzuweisung für ein virtuelles Laufwerk:

1. Erweitern Sie **Storage** (Speicher) aus der Anwendung OpenManage Server Administrator.
2. Erweitern Sie den Controller, der das virtuelle Laufwerk enthält und wählen Sie dann **Virtual Disks** (Virtuelle Laufwerke) aus.
3. Wählen Sie das virtuelle Laufwerk, das Sie entfernen möchten und wählen Sie dann **Delete** (Löschen) aus dem Drop-Down-Menü **Tasks** aus.
4. Nachdem Sie den Löschvorgang bestätigt haben, wird der Speicherplatz in der Core Console auf der Registerkarte **Gerät** im Bildschirm **Aufgaben** als zur Bereitstellung verfügbar angezeigt.

Auflösen fehlgeschlagener Aufgaben

AppAssure meldet fehlgeschlagene Überprüfungs-, Bereitstellungs- und Recovery-Aufgaben in Form von Ereignissen auf der Startseite der Core Console sowie in der Registerkarte **Gerät** des Bildschirms **Aufgaben**.

Um zu verstehen, wie ein fehlgeschlagener Task aufgelöst wird, wählen Sie die Registerkarte **Appliance** (Gerät) aus und klicken Sie dann auf **Tasks**. Zur Erweiterung des fehlgeschlagenen Tasks klicken Sie auf das Symbol **>** neben **Status**, und überprüfen Sie die Fehlermeldung und die vorgeschlagene Maßnahme.

Upgrade des Geräts

So führen Sie ein Upgrade des Geräts aus:

1. Laden Sie **Recovery and Update Utility** (Dienstprogramm zur Wiederherstellung und Aktualisierung) von **dell.com/support** auf DL4000 Backup to Disk-Gerät herunter.
2. Kopieren Sie das Dienstprogramm auf den Geräte-Desktop und extrahieren Sie die Dateien.
3. Doppelklicken Sie auf das Symbol **launchRUU** (RUU starten).
4. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Yes** (Ja), um zu bestätigen, dass Sie keinen der aufgelisteten Vorgänge ausführen.
5. Klicken Sie auf **Start**, wenn der Bildschirm **Dienstprogramm zur Wiederherstellung und Aktualisierung** angezeigt wird.
6. Wenn Sie dazu aufgefordert werden, fortzufahren, klicken Sie auf **OK**.

   Die Windows Server-Rollen und -Funktionen, ASP .NET MVC3, LSI-Provider, DL-Anwendungen, OpenManage Server Administrator und AppAssure-Kern-Software sind als Teil des Dienstprogramms zur Wiederherstellung und Aktualisierung installiert. Desweiteren aktualisiert das Dienstprogramm zur Wiederherstellung und Aktualisierung den RASR-Inhalt.

   ANMERKUNG: Als Teil des AppAssure Core Software Erweiterungsprozesses informiert Sie das Dienstprogramm zur Wiederherstellung und Erweiterung über die aktuell installierten Versionen von AppAssure und fordert Sie dazu auf, zu bestätigen, dass Sie die Kern-Software auf die Version, die mit dem Dienstprogramm gebündelt ist, erweitern möchten. AppAssure Core-Software-Herabstufungen werden nicht unterstützt.
7. Starten Sie das System neu, wenn Sie dazu aufgefordert werden.
8. Nachdem alle Dienste und Anwendungen installiert wurden, klicken Sie auf **Proceed** (Fortfahren).

   Die Core Console startet.

Reparieren des Geräts

So reparieren Sie das Gerät:

1. Laden Sie **Recovery and Update Utility** (Dienstprogramm zur Wiederherstellung und Aktualisierung) über **dell.com/support** auf Ihr Gerät.
2. Kopieren Sie das Dienstprogramm auf den Geräte-Desktop und extrahieren Sie die Dateien.
3. Doppelklicken Sie auf das Symbol **launchRUU** (RUU starten).
4. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Yes** (Ja), um zu bestätigen, dass Sie keinen der aufgelisteten Vorgänge ausführen.
5. Klicken Sie auf **Start**, wenn der Bildschirm „Recovery and Update Utility“ (Dienstprogramm zur Wiederherstellung und Aktualisierung) angezeigt wird.

6. Wenn Sie dazu aufgefordert werden, fortzufahren, klicken Sie auf **OK**.

   Die aktualisierten Versionen von den Windows Server Rollen und Funktionen, ASP .NET MVC3, LSI Provider, DL-Anwendungen, OpenManage Server Administrator und AppAssure-Kern-Software werden als Teil vom „Recovery and Update Utility" (Dienstprogramm zur Wiederherstellung und Aktualisierung) installiert.
7. Wenn die gebündelte Version im Dienstprogramm dieselbe ist als die installierte Version, fordert Sie das Dienstprogramm zur Wiederherstellung und Aktualisierung dazu auf, zu bestätigen, dass Sie eine Reparaturinstallation ausführen möchten. Dieser Schritt kann übergangen werden, wenn eine Reparaturinstallation auf dem AppAssure-Kern nicht notwendig ist.
8. Wenn die gebündelte Version im Dienstprogramm höher ist als die installierte Version, fordert Sie das Dienstprogramm zur Wiederherstellung und Aktualisierung dazu auf, zu bestätigen, dass Sie die AppAssure-Kern-Software aktualisieren möchten.

   ANMERKUNG: Zurückstufungen für die AppAssure-Kern-Software werden nicht unterstützt.
9. Starten Sie das System neu, wenn Sie dazu aufgefordert werden.
10. Nachdem alle Dienste und Anwendungen installiert wurden, klicken Sie auf **Proceed** (Fortfahren).

    Der AppAssure-Gerätekonfigurationsassistent wird gestartet, wenn das System nach der Reparatur erneut konfiguriert werden muss, andernfalls wird Core Console gestartet.

4

Schutz von Arbeitsstationen und Servern

Wissenswertes über den Schutz von Workstations und Servern

Um Ihre Daten zu schützen, müssen Sie die Workstations und Server, die Sie schützen möchten, zur Core Console hinzufügen; zum Beispiel Ihren Exchange-Server, SQL-Server, oder Ihren Linux-Server.

ANMERKUNG: In diesem Abschnitt bezieht sich das Wort *Maschine* im Allgemeinen auch auf die AppAssure-Agentsoftware, die auf dieser Maschine installiert ist.

In der Core Console können Sie die Maschine bestimmen, auf der die AppAssure-Agentsoftware installiert wird, und angeben, welche Datenträger geschützt werden sollen, die Zeitpläne für den Schutz definieren, weitere Sicherheitsmaßnahmen hinzufügen (z. B. Verschlüsselung) und vieles mehr. Weitere Informationen über den Zugriff auf die Core Console für den Schutz von Arbeitsstationen und Servern siehe Protecting A Machine (Schützen einer Maschine).

Konfigurieren von Maschineneinstellungen

Nachdem Sie Schutz für die Maschinen in AppAssure hinzugefügt haben, können Sie grundlegende Konfigurationseinstellungen für die Maschinen (Name, Hostname usw.), Schutzeinstellungen (Schutzzeitplan für Volumes auf der Maschine ändern, Volumes hinzufügen oder entfernen und/oder den Schutz anhalten) und vieles mehr ändern.

Anzeigen und Ändern von Konfigurationseinstellungen

So können Sie Konfigurationseinstellungen anzeigen und ändern:

1. Nachdem Sie eine geschützte Maschine hinzugefügt haben, führen Sie einen der folgenden Schritte aus:
   - Klicken Sie in der Core Console auf die Registerkarte **Maschinen** und dann auf den Hyperlink für die Maschine, deren Einstellungen Sie ändern möchten.
   - Wählen Sie im Bereich **Navigation** die Maschine aus, die Sie ändern möchten.
2. Klicken Sie auf das Register **Configuration** (Konfiguration).

   Die Seite **Settings** (Einstellungen) wird angezeigt.
3. Klicken Sie auf **Edit** (Bearbeiten), um die in der folgenden Tabelle beschriebenen Maschinen-Einstellungen zu bearbeiten.

Textfeld	Beschreibung
Anzeigename	Geben Sie einen Anzeigenamen für die Maschine ein. Ein Name für die Maschine, der in der Core Console angezeigt werden soll. Standardmäßig ist das der Hostname der Maschine. Nach Wunsch können Sie

Textfeld	Beschreibung
	den Anzeigenamen jedoch auch in einen benutzerfreundlicheren Namen ändern.
Host-Name	Geben Sie einen Hostnamen für die Maschine ein.
Schnittstelle	Geben Sie eine Schnittstellennummer für die Maschine ein. Der Kern verwendet die Schnittstelle, um mit dieser Maschine zu kommunizieren.
Repository	Wählen Sie ein Repository für die Wiederherstellungspunkte aus. Zeigt das Repository auf dem Kern an, in dem die Daten für diese Maschine gespeichert werden sollen. ANMERKUNG: Die Einstellung kann nur dann geändert werden, falls keine Wiederherstellungspunkte vorhanden sind oder ein vorheriges Repository fehlt.
Verschlüsselungsschlüssel	Bearbeiten Sie den Verschlüsselungsschlüssel bei Bedarf. Gibt an, ob Verschlüsselung auf die Daten jedes Volumes auf dieser Maschine angewendet wird, die in dem Repository gespeichert wird.

Anzeigen von Systeminformationen für eine Maschine

Die Core Console zeigt alle geschützten Maschinen über eine Liste an, in der die Maschinen zusammen mit ihrem Status aufgeführt werden.

So zeigen Sie die Systeminformationen für eine Maschine an:

1. Wählen Sie in der Core Console unter **Geschützte Maschinen** die Maschine aus, für die Sie detaillierte Systeminformationen anzeigen möchten.
2. Klicken Sie auf die Registerkarte **Extras** der betreffenden Maschine.

   Die Informationen über die Maschine werden auf der Seite **System Information** (Systeminformationen) angezeigt. Es werden unter anderem folgende Details angezeigt:

   - Host-Name
   - Betriebssystemversion
   - OS Architecture (Betriebssystemarchitektur)
   - Speicher (physisch)
   - Anzeigename
   - Fully Qualified Domain Name (Vollqualifizierter Domainname)
   - Virtual Machine Type (Typ der virtuellen Maschine, falls vorhanden)

   Ausführliche Informationen über die Volumes auf dieser Maschine enthalten:

   - Name
   - Geräte-ID
   - Dateisystem
   - Capacity (Kapazität, einschließlich Raw, formatiert und benutzt)
   - Prozessoren
   - Prozessortypen

- Netzwerkadapter
- Mit dieser Maschine verknüpfte IP-Adressen

Konfigurieren von Benachrichtigungsgruppen für Systemereignisse

Durch Erstellen von Benachrichtigungsgruppen können Sie in AppAssure konfigurieren, wie Systemereignisse für Ihre Maschine gemeldet werden. Solche Ereignisse können Systemwarnungen, Fehler usw. einschließen.

So konfigurieren Sie Benachrichtigungsgruppen für Systemereignisse:

1. Klicken Sie in der Core Console auf die Registerkarte **Machines** (Maschinen).
2. Führen Sie auf der Registerkarte **Machines** (Maschinen) einen der folgenden Schritte aus:
   - Klicken Sie auf den Hyperlink für die Maschine, die Sie ändern möchten.
   - Oder wählen Sie im Navigationsbereich die Maschine aus, die Sie ändern möchten.

   Die Registerkarte **Zusammenfassung** wird angezeigt.
3. Klicken Sie auf die Registerkarte **Configuration** (Konfiguration), und klicken Sie dann auf **Events** (Ereignisse).

   Die Seite **Benachrichtigungsgruppen** wird angezeigt.
4. Klicken Sie auf **Use custom alert settings** (Benutzerdefinierte Benachrichtigungseinstellungen verwenden) und anschließend auf **Apply** (Übernehmen).

   Der Bildschirm **Benutzerdefinierte Benachrichtigungsgruppen** wird angezeigt.
5. Klicken Sie auf **Add Group** (Gruppe hinzufügen), um eine neue Benachrichtigungsgruppe für den Versand einer Liste der Systemereignisse hinzuzufügen.

   Das Dialogfeld **Add Notification Group** (Benachrichtigungsgruppe hinzufügen) wird angezeigt.

   ANMERKUNG: Um die Standard-Benachrichtigungseinstellungen zu benutzen, wählen Sie die Option **Use Core alert settings** (Kern-Benachrichtigungseinstellungen verwenden) aus.
6. Fügen Sie die in der folgenden Tabelle beschriebenen Benachrichtigungsoptionen hinzu.

Textfeld	Beschreibung
Name	Geben Sie einen Namen für die Benachrichtigungsgruppe ein.
Beschreibung	Geben Sie eine Beschreibung für die Benachrichtigungsgruppe ein.
Enable Events (Ereignisse aktivieren)	Wählen Sie aus, welche Ereignisse Sie für die Benachrichtigungsgruppe freigeben möchten. Sie können entweder **All** (Alle) oder eine Untergruppe von Ereignissen auswählen, um Folgendes einzuschließen: • **BootCd** • **LocalMount** • **Metadaten** • **Cluster** • **Notification (Benachrichtigung)** • **PowerShellScripting** • **PushInstall (Push-Installation)** • **Attachability (Anfügbarkeit)** • **Jobs** • **Lizenzierung** • **Log Truncation (Abschneiden des Protokolls)**

Textfeld	Beschreibung
	• **Archivieren** • **Kern-Service** • **Exportieren** • **Protection (Schutz)** • **Replikation** • **Rollback** • **Rollup** Sie können Ihre Auswahl auch nach Typ vornehmen: • **Info** • **Warnung** • **Fehler** ANMERKUNG: Wenn Sie sich für die Auswahl nach Typ entscheiden, werden standardmäßig die entsprechenden Ereignisse automatisch aktiviert. Bei Auswahl von Warning (WARNUNG) werden beispielsweise die folgenden Ereignisse aktiviert: „Attachability" (Anfügbarkeit), „Jobs" (Aufgaben), „Licensing" (Lizenzierung), „Archive" (Archivierung), „CoreService" (Kern-Service), „Export", „Protection" (Schutz), „Replication" (Replikation) und „Rollback".
Notification Options (Benachrichtigungsoptionen)	Wählen Sie das Verfahren aus, wie Benachrichtigungen behandelt werden, die Sie aus den folgenden Optionen auswählen können: • **Per E-Mail benachrichtigen** – Geben Sie in den Textfeldern „An", „Kopie" und „Blindkopie" die E-Mail-Adressen an, an die die Ereignisse gesendet werden sollen. ANMERKUNG: Um E-Mails zu empfangen, muss SMTP vorher konfiguriert sein. • **Notify by Windows Event log** (Über Windows-Ereignisprotokoll benachrichtigen) – Das Windows-Ereignisprotokoll steuert die Benachrichtigung. • **Notify by syslogd** (Durch syslogd benachrichtigen) – Geben Sie den Hostnamen und Anschluss ein, an den die Ereignisse gesendet werden sollen. – **Host** – Geben Sie den Hostnamen für den Server ein. – **Port** (Anschluss) – Geben Sie eine Portnummer zur Kommunikation mit dem Server ein.

7. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.
8. Um eine vorhandene Benachrichtigungsgruppe zu bearbeiten, klicken Sie auf **Edit** (Bearbeiten) neben der zu bearbeitenden Benachrichtigungsgruppe.

   Das Dialogfeld **Edit Notification Group** (Benachrichtigungsgruppe bearbeiten) wird angezeigt, in dem Sie die Einstellungen bearbeiten können.

Bearbeiten von Benachrichtigungsgruppen für Systemereignisse

So konfigurieren Sie Benachrichtigungsgruppen für Systemereignisse:

1. Wechseln Sie zur Core Console, und klicken Sie dann auf die Registerkarte **Maschinen**.
2. Führen Sie auf der Registerkarte **Machines** (Maschinen) einen der folgenden Schritte aus:
   - Klicken Sie auf den Hyperlink für die Maschine, die Sie ändern möchten.
   - Oder wählen Sie im Navigationsbereich die Maschine aus, die Sie ändern möchten.

   Die Registerkarte **Zusammenfassung** wird angezeigt.
3. Klicken Sie auf die Registerkarte **Configuration** (Konfiguration), und klicken Sie dann auf **Events** (Ereignisse).
4. Klicken Sie auf **Use custom alert settings** (Benutzerdefinierte Benachrichtigungseinstellungen verwenden) und anschließend auf **Apply** (Übernehmen).

   Der Bildschirm **Benutzerdefinierte Benachrichtigungsgruppen** wird angezeigt.
5. Klicken Sie auf das Symbol **Edit** (Bearbeiten) unter der Spalte **Action** (Maßnahme).

   Das Dialogfeld **Benachrichtigungsgruppe bearbeiten** wird angezeigt.
6. Bearbeiten Sie die in der folgenden Tabelle beschriebenen Benachrichtigungsoptionen.

Textfeld	Beschreibung
Name	Stellt den Namen der Benachrichtigungsgruppe dar. ANMERKUNG: Sie können den Namen der Benachrichtigungsgruppe nicht bearbeiten.
Beschreibung	Geben Sie eine Beschreibung für die Benachrichtigungsgruppe ein.
Enable Events (Ereignisse aktivieren)	Wählen Sie aus, welche Ereignisse Sie für die Benachrichtigungsgruppe freigeben möchten. Sie können entweder **All** (Alle) oder eine Untergruppe von Ereignissen auswählen, um Folgendes einzuschließen: • **BootCd** • **LocalMount** • **Metadaten** • **Cluster** • **Notification (Benachrichtigung)** • **PowerShellScripting** • **PushInstall (Push-Installation)** • **Attachability (Anfügbarkeit)** • **Jobs** • **Lizenzierung** • **Log Truncation (Abschneiden des Protokolls)** • **Archivieren** • **Kern-Service** • **Exportieren** • **Protection (Schutz)** • **Replikation** • **Rollback**

Textfeld	Beschreibung
	• **Rollup** Sie können Ihre Auswahl auch nach Typ vornehmen: • **Info** • **Warnung** • **Fehler** **ANMERKUNG:** Wenn Sie sich für die Auswahl nach Typ entscheiden, werden standardmäßig die entsprechenden Ereignisse automatisch aktiviert. Bei Auswahl von Warning (WARNUNG) werden beispielsweise die folgenden Ereignisse aktiviert: „Attachability“ (Anfügbarkeit), „Jobs“ (Aufgaben), „Licensing“ (Lizenzierung), „Archive“ (Archivierung), „CoreService“ (Kern-Service), „Export“, „Protection“ (Schutz), „Replication“ (Replikation) und „Rollback“.
Notification Options (Benachrichtigungsoptionen)	Wählen Sie das Verfahren aus, wie Benachrichtigungen behandelt werden, die Sie aus den folgenden Optionen auswählen können: • **Notify by Email** (Per E-Mail benachrichtigen) – Geben Sie in den Textfeldern „To“ (An), „CC“ (Cc) und „BCC“ (Bcc) die E-Mail-Adressen an, an die die Ereignisse gesendet werden sollen. **ANMERKUNG:** Um E-Mails zu erhalten, muss SMTP vorher konfiguriert sein. • **Notify by Windows Event log** (Über Windows-Ereignisprotokoll benachrichtigen) – Das Windows-Ereignisprotokoll steuert die Benachrichtigung. • **Notify by syslogd** (Durch syslogd benachrichtigen) – Sie müssen den Hostnamen und Anschluss eingeben, an den die Ereignisse gesendet werden sollen. – **Host** – Geben Sie den Hostnamen für den Server ein. – **Port** (Anschluss) – Geben Sie eine Portnummer zur Kommunikation mit dem Server ein.

7. Klicken Sie auf **OK**.

Anpassen der Einstellungen von Aufbewahrungsrichtlinien

Die Aufbewahrungsrichtlinie für eine Maschine gibt an, wie lange die Wiederherstellungspunkte für eine Agentenmaschine im Repository gespeichert werden. 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 Rollup-Prozess umgesetzt, der Sie beim Bestimmen der Fälligkeit und beim Löschen alter Sicherungen unterstützt. Diese Aufgabe ist auch ein Schritt im Vorgang des Änderns der Einstellungen für Cluster-Knoten.

So passen Sie die Einstellungen von Aufbewahrungsrichtlinien an

1. Klicken Sie in der Core Console auf die Registerkarte **Machines** (Maschinen).
2. Führen Sie auf der Registerkarte **Machines** (Maschinen) einen der folgenden Schritte aus:
   - Klicken Sie auf den Hyperlink für die Maschine, die Sie ändern möchten.
   - Oder wählen Sie im Navigationsbereich die Maschine aus, die Sie ändern möchten.

Die Registerkarte **Zusammenfassung** wird angezeigt.

3. Klicken Sie auf die Registerkarte **Configuration** (Konfiguration), und klicken Sie dann auf **Retention Policy** (Aufbewahrungsrichtlinie).

   ANMERKUNG: Wenn Sie die für den Kern konfigurierte Standard-Aufbewahrungsrichtlinie verwenden möchten, müssen Sie sicherstellen, dass die Option „Use Core default retention policy" (Standard-Aufbewahrungsrichtlinie für Kern verwenden) ausgewählt ist.

   Der Bildschirm **Aufbewahrungsrichtlinie** wird angezeigt.

4. Um die benutzerdefinierten Richtlinien zu erstellen, klicken Sie auf **Use custom retention policy** (Benutzerdefinierte Aufbewahrungsrichtlinie verwenden).

   Der Bildschirm **Benutzerdefinierte Aufbewahrungsrichtlinie** wird angezeigt.

5. Aktivieren Sie das Kontrollkästchen **Enable Rollup** (Rollup aktivieren), und geben Sie dann die erforderlichen Zeitintervalle für die Aufbewahrung der Sicherungsdaten an. Die Optionen für die Aufbewahrungsrichtlinie werden nachfolgend beschrieben.

Textfeld	Beschreibung
Keep all Recovery Points for n [retention time period] (Alle Wiederherstellungspunkte beibehalten für n [Aufbewahrungsdauer])	Gibt die Aufbewahrungsdauer für die Wiederherstellungspunkte an. Geben Sie eine Zahl für die Aufbewahrungsdauer an, und wählen Sie dann eine Zeitdauer aus. Die Standardeinstellung ist **3**. Folgende Optionen stehen zur Auswahl: • **Tage** • **Wochen** • **Monate** • **Jahre**
...and then keep one recovery point per hour for n [retention time period] (...und dann einen Wiederherstellungspunkt pro Stunde beibehalten für n [Aufbewahrungsdauer])	Gibt eine genauere Aufbewahrungsstufe an. Diese Option wird zusammen mit der primären Einstellung als Baustein zur weiteren Definition dafür verwendet, wie lange Wiederherstellungspunkte beibehalten werden sollen. Geben Sie eine Zahl für die Aufbewahrungsdauer an, und wählen Sie dann eine Zeitdauer aus. Die Standardeinstellung ist 2. Folgende Optionen stehen zur Auswahl: • **Tage** • **Wochen** • **Monate** • **Jahre**
...and then keep one Recovery Point per day for n [retention time period] (...und dann einen Wiederherstellungspunkt pro Tag beibehalten für n	Gibt eine genauere Aufbewahrungsstufe an. Diese Option wird zusammen mit der primären Einstellung als Baustein zur weiteren Definition dafür verwendet, wie lange Wiederherstellungspunkte beibehalten werden sollen. Geben Sie eine Zahl für die Aufbewahrungsdauer an, und wählen Sie dann eine Zeitdauer aus. Die Standardeinstellung ist 4. Folgende Optionen stehen zur Auswahl: • **Tage** • **Wochen** • **Monate**

Textfeld	Beschreibung
[Aufbewahrungsdauer])	• **Jahre**
...and then keep one Recovery Point per week for n [retention time period] (...und dann einen Wiederherstellungspunkt pro Woche beibehalten für n [Aufbewahrungsdauer])	Gibt eine genauere Aufbewahrungsstufe an. Diese Option wird zusammen mit der primären Einstellung als Baustein zur weiteren Definition dafür verwendet, wie lange Wiederherstellungspunkte beibehalten werden sollen. Geben Sie eine Zahl für die Aufbewahrungsdauer an, und wählen Sie dann eine Zeitdauer aus. Die Standardeinstellung ist 3. Folgende Optionen stehen zur Auswahl: • **Wochen** • **Monate** • **Jahre**
...and then keep one Recovery Point per month for n [retention time period] (...und dann einen Wiederherstellungspunkt pro Monat beibehalten für n [Aufbewahrungsdauer])	Gibt eine genauere Aufbewahrungsstufe an. Diese Option wird zusammen mit der primären Einstellung als Baustein zur weiteren Definition dafür verwendet, wie lange Wiederherstellungspunkte beibehalten werden sollen. Geben Sie eine Zahl für die Aufbewahrungsdauer an, und wählen Sie dann eine Zeitdauer aus. Die Standardeinstellung ist 2. Folgende Optionen stehen zur Auswahl: • **Monate** • **Jahre**
...and then keep one Recovery Point per year for n [retention time period] (...und dann einen Wiederherstellungspunkt pro Jahr beibehalten für n [Aufbewahrungsdauer])	Geben Sie eine Zahl für die Aufbewahrungsdauer an, und wählen Sie dann eine Zeitdauer aus.

Das Textfeld Newest Recovery Point (Neuester Wiederherstellungspunkt) zeigt den aktuellsten Wiederherstellungspunkt an. Die Einstellungen von Aufbewahrungsrichtlinien bestimmen den ältesten Wiederherstellungspunkt.

Im folgenden Beispiel wird die Berechnung der Aufbewahrungsdauer dargestellt.

Alle Wiederherstellungspunkte beibehalten für 3 Tage.

...und dann einen Wiederherstellungspunkt pro Stunde beibehalten für 3 Tage

...und dann einen Wiederherstellungspunkt pro Tag beibehalten für 4 Tage

...und dann einen Wiederherstellungspunkt pro Woche beibehalten für 3 Wochen

...und dann einen Wiederherstellungspunkt pro Monat beibehalten für 2 Monate

...und dann einen Wiederherstellungspunkt pro Monat beibehalten für 1 Jahr

Der neueste Wiederherstellungspunkt wird auf den aktuellen Tag,den aktuellen Monat und das aktuelle Jahr festgelegt.

In diesem Beispiel wäre der älteste Wiederherstellungspunkt demzufolge ein Jahr, vier Monate und sechs Tage alt.

6. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.
7. Wählen Sie **Force Rollup** (Rollup erzwingen) aus, um ein Rollup basierend auf der aktuellen Aufbewahrungsrichtlinie für die Maschine durchzuführen oder lassen Sie zu, dass die von Ihnen festgelegte Aufbewahrungsrichtlinie während des nächtlichen Rollup-Prozesses übernommen wird.

Anzeigen von Lizenzinformationen

Sie können aktuelle Lizenzstatusinformationen für die auf einer Maschine installierte AppAssure-Agentensoftware anzeigen.

So zeigen Sie Lizenzinformationen an:

1. Klicken Sie in der Core Console auf die Registerkarte **Machines** (Maschinen).
2. Führen Sie auf der Registerkarte **Machines** (Maschinen) einen der folgenden Schritte aus:
   - Klicken Sie auf den Hyperlink für die Maschine, die Sie anzeigen möchten.
   - Oder wählen Sie im Navigationsbereich die Maschine aus, die Sie anzeigen möchten.
3. Klicken Sie auf die Registerkarte **Configuration** (Konfiguration), und klicken Sie dann auf **Licensing** (Lizenzierung).

   Der **Status**-Bildschirm zeigt die Einzelheiten über die Produktlizenzierung an.

Ändern von Schutzzeitplänen

In AppAssure können Sie die Schutzzeitpläne für bestimmte Volumes auf einer Maschine ändern.

So ändern Sie Schutzzeitpläne:

1. Klicken Sie in der Core Console auf die Registerkarte **Machines** (Maschinen).
2. Führen Sie auf der Registerkarte **Machines** (Maschinen) einen der folgenden Schritte aus:
   - Klicken Sie auf den Hyperlink für die Maschine, die Sie ändern möchten.
   - Oder wählen Sie im Navigationsbereich die Maschine aus, die Sie ändern möchten.
3. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie auf der Registerkarte **Summary** (Zusammenfassung) der Maschine in der Tabelle **Volumes** auf den Hyperlink für den Schutzzeitplan des Volumes, das Sie anpassen möchten.
   - Klicken Sie auf die Registerkarte **Configuration** (Konfiguration) und dann auf **Protection Settings** (Schutzeinstellungen). Klicken Sie in der Liste der Volumes neben dem Volume, das Sie anpassen möchten, auf das Symbol für **Edit** (Bearbeiten).

   Das Dialogfeld **Protection Schedule** (Schutzzeitplan) wird angezeigt.
4. Bearbeiten Sie im Dialogfeld **Protection Schedule** (Schutzzeitplan) die folgenden Zeitplanoptionen, wie zum Schutz Ihrer Daten erforderlich. Die Optionen werden in der folgenden Tabelle beschrieben.

Option	Beschreibung
Intervall	**Wochentag** – Um Daten entsprechend einem bestimmten Zeitintervall (z. B. alle 15 Minuten) zu schützen, wählen Sie **Interval** (Intervall) und dann Folgendes aus: • Wenn Sie anpassen möchten, wann Daten während Spitzenauslastungszeiten geschützt werden sollen, können Sie eine **Startzeit,** eine **Endzeit** sowie ein **Intervall** in den Drop-Down-Menüs auswählen. • Um Daten während Nebenzeiten zu schützen, aktivieren Sie das Kontrollkästchen **Protection interval during off-peak times** (Schutzintervall während Nebenzeiten), und wählen Sie dann ein Intervall für den Schutz im Drop-Down-Menü aus. **Wochenenden** – Wenn Daten an den Wochenenden geschützt werden sollen, aktivieren Sie das Kontrollkästchen **Protection interval during weekends** (Schutzintervall an Wochenenden), und wählen Sie dann ein Intervall im Drop-Down-Menü aus. ANMERKUNG: Falls sich SQL- oder Exchange-Datenbanken und -Protokolle auf verschiedenen Volumes befinden, müssen die Volumes zu einer Schutzgruppe gehören.
Täglich	Wenn die Daten täglich geschützt werden sollen, wählen Sie die Option **Daily** (Täglich) und dann im Drop-Down-Menü **Protection Time** (Schutzzeit) eine Zeit aus, zu der der Schutz der Daten gestartet werden soll.
No Protection (Kein Schutz)	Um den Schutz für dieses Volume zu entfernen, wählen Sie die Option **No Protection** (Kein Schutz) aus.

Wenn Sie diese benutzerdefinierten Einstellungen auf alle Volumes auf dieser Maschine anwenden möchten, wählen Sie **Apply to All Volumes** (Auf alle Volumes anwenden).

5. Nachdem Sie alle notwendigen Änderungen vorgenommen haben, klicken Sie auf **OK**.

Ändern von Übertragungseinstellungen

Sie können die Einstellungen zum Verwalten des Datenübertragungsprozesses für eine geschützte Maschine ändern. Die Übertragungseinstellungen, die in diesem Abschnitt beschrieben werden, sind Einstellungen auf Agentenebene. Um Übertragungen auf Kernebene zu bewirken, lesen Sie den Abschnitt Ändern der Einstellungen für die Übertragungswarteschlange.

VORSICHT: Das Ändern der Übertragungseinstellungen kann drastische Auswirkungen auf Ihre Umgebung haben. Bevor Sie die Einstellungswerte für Übertragungen ändern, lesen Sie das Handbuch zur Leistungssteigerung von Übertragungen mit dem Titel „Tansfer Performance Tuning Guide“ in der Dell AppAssure-Wissensdatenbank unter https://support.software.dell.com/appassure/kb.

Es gibt drei Arten von Übertragungen:

Snapshots	Die Übertragung, bei der die Daten auf Ihrer geschützten Maschine gesichert werden.
VM-Export	Ein Übertragungstyp, bei dem eine virtuelle Maschine mit allen Sicherungsinformationen und Parametern erstellt wird, wie durch den für den Schutz der Maschine definierten Zeitplan angegeben.

Rollback	Ein Vorgang, der Sicherungsinformationen auf einer geschützten Maschine wiederherstellt.

Die Datenübertragung beinhaltet die Übertragung einer Datenmenge über ein Netzwerk von Agentenmaschinen zum Kern. Bei der Replikation kann die Übertragung auch vom Ursprungs- bzw. Quellkern zum Zielkern stattfinden.

Datenübertragung kann durch bestimmte Einstellungen der Leistungsoptionen für Ihr System optimiert werden. Diese Einstellungen steuern die Nutzung der Datenbandbreite während des Sicherungsvorgangs der Agentenmaschinen, der Ausführung von VM-Exporten oder der Durchführung eines Rollbacks. Einige Faktoren, die die Datenübertragungsrate beeinflussen, sind:

- Anzahl der gleichzeitigen Agent-Datenübertragungen
- Anzahl der gleichzeitigen Agent-Datenflüsse
- Menge der Datenänderungen auf dem Laufwerk
- Verfügbare Netzwerkbandbreite
- Leistung des Repository-Laufwerkssubsystems
- Die Menge an Speicher, die für Datenpuffer verfügbar ist

Sie können die Leistungsoptionen für die beste Unterstützung Ihrer Geschäftsanforderungen einstellen, und die Leistung, basierend auf Ihre Umgebung, feinabstimmen.

So ändern Sie Übertragungseinstellungen:

1. Führen Sie in der Core Console eine der folgenden Maßnahmen aus:
   - Klicken Sie auf die Registerkarte **Machines** (Maschinen), und klicken Sie dann auf den Hyperlink für die Maschine, deren Einstellungen Sie ändern möchten.
   - Klicken Sie im Navigationsbereich auf die Maschine, die Sie ändern möchten.
2. Führen Sie auf der Registerkarte **Machines** (Maschinen) einen der folgenden Schritte aus:
   - Klicken Sie auf den Hyperlink für die Maschine, die Sie ändern möchten.
   - Oder wählen Sie im Navigationsbereich die Maschine aus, die Sie ändern möchten.
3. Klicken Sie auf die Registerkarte **Configuration** (Konfiguration) und dann auf **Transfer Settings** (Übertragungseinstellungen).

   Die aktuellen Übertragungseinstellungen werden angezeigt.
4. Klicken sie auf der Seite **Transfer Settings** (Übertragungseinstellungen) auf **Change** (Ändern).

   Das Dialogfeld **Übertragungseinstellungen** wird angezeigt.
5. Geben Sie die Optionen **Transfer Settings** (Übertragungseinstellungen) für die Maschine ein, wie in der folgenden Tabelle beschrieben.

Textfeld	Beschreibung
Priorität	Legt die Übertragungspriorität zwischen geschützten Maschinen fest. Ermöglicht es Ihnen, Priorität durch einen Vergleich mit anderen geschützten Maschinen zuzuweisen. Wählen Sie eine Zahl von 1 bis 10, wobei 1 die höchste Priorität darstellt. Die Standardeinstellung ist eine Priorität von 5. **ANMERKUNG:** Priorität wird auf Übertragungen angewendet, die sich in der Warteschlange befinden.

Textfeld	Beschreibung
Maximum Concurrent Streams (Maximale Anzahl gleichzeitiger Streams)	Legt die maximale Anzahl der TCP-Links fest, die zur parallelen Verarbeitung pro Agent an den Kern gesandt werden. ANMERKUNG: Dell empfiehlt, diesen Wert auf 8 einzustellen. Wenn abgeworfene Pakete auftreten, versuchen Sie, diese Einstellung zu erhöhen.
Maximum Concurrent Writes (Maximale Anzahl gleichzeitiger Schreibvorgänge)	Legt die maximale Anzahl an gleichzeitigen Laufwerksschreibaktionen pro Agent-Verbindung fest. ANMERKUNG: Dell empfiehlt, diesen Wert auf denselben Wert einzustellen, den Sie für Maximum Concurrent Streams (Maximale Anzahl gleichzeitiger Streams) ausgewählt haben. Wenn ein Paketverlust auftritt, stellen Sie diesen Wert etwas niedriger. Wenn zum Beispiel Maximum Current Streams auf 8 eingestellt ist, stellen Sie diese Option auf 7 ein.
Maximum Retries (Maximale Anzahl der Wiederholungen)	Legt die maximale Anzahl an Wiederholungsversuchen für jede geschützte Maschine fest, falls einige der Vorgänge nicht abgeschlossen werden können.
Maximum Segment Size (Maximale Segmentgröße)	Gibt die größte Anzahl an Daten (in Byte) an, die ein Computer in einem einzelnen TCP-Segment empfangen kann. Die Standardeinstellung ist 4194304. **VORSICHT: Ändern Sie diese Option nicht von der Standardeinstellung.**
Maximum Transfer Queue Depth (Maximale Tiefe der Übertragungswarteschlange)	Gibt die Anzahl der Befehle an, die gleichzeitig gesendet werden können.Sie können diese Option auf eine höhere Zahl einstellen, wenn Ihr System eine höhere Nummer von gleichzeitigen Eingabe / Ausgabe-Operationen besitzt.
Ausstehende Lesevorgänge pro Stream	Gibt an, wie viele Leseoperationen in der Warteschlange am hinteren Ende gespeichert werden. Diese Einstellung hilft, die in einer Warteschlange eingereihten Agenten zu steuern. ANMERKUNG: Dell empfiehlt, diesen Wert auf 24 einzustellen.
Excluded Writers (Ausgeschlossene Writer)	Wählen Sie einen Writer aus, den Sie ausschließen möchten. Da die Writer, die in der Liste angezeigt werden, für die Maschine die Sie konfigurieren spezifisch sind, können Sie eventuell nicht alle aufgeführten Writer sehen. Einige Writer, die Sie sehen, könnten diese einschließen: • ASR Writer (ASR-Generator) • BITS Writer (BITS-Generator) • COM+ REGDB Writer (COM+REGDB-Generator) • Performance Counters Writer (Leistungsindikatoren-Generator) • Registry Writer (Registrierungsgenerator)

Textfeld	Beschreibung
	• Shadow Copy Optimization Writer (Generator zur Optimierung der Schattenkopie) • SQLServerWriter • System Writer (Systemgenerator) • Task Scheduler Writer (Aufgabenplanungsgenerator) • VSS Metadata Store Writer (VSS-Metadaten-Speichergenerator) • WMI Writer (WMI-Generator)
Transfer Data Server Port (Übertragungsdaten-Serverport)	Geben Sie die Schnittstelle für die Übertragungen ein. Die Standardeinstellung ist 8009.
Transfer Timeout (Zeitüberschreitung für Übertragungen)	Gibt die Zeitspanne in Minuten und Sekunden an, in der ein Paket statisch und ohne Übertragung bleiben kann.
Snapshot-Zeitüberschreitung	Gibt die maximale Zeitspanne in Minuten und Sekunden an, die gewartet werden soll, um einen Snapshot zu erstellen.
Network Read Timeout (Zeitüberschreitung für Netzwerk-Lesevorgänge)	Gibt die maximale Zeitspanne der Wartezeit in Minuten und Sekunden an, bis eine Verbindung für einen Lesevorgang erstellt wird. Wenn der Lesevorgang im Netzwerk innerhalb dieses Zeitraums nicht ausgeführt wurde, wird der Vorgang wiederholt.
Network Write Timeout (Zeitüberschreitung für Netzwerk-Schreibvorgänge)	Gibt die maximale Zeitspanne der Wartezeit in Sekunden an, bis eine Verbindung für einen Schreibvorgang erstellt wird. Wenn der Schreibvorgang im Netzwerk innerhalb dieses Zeitraums nicht ausgeführt wurde, wird der Vorgang wiederholt.

6. Klicken Sie auf **OK**.

Neustarten eines Services

So starten Sie einen Service neu:

1. Klicken Sie in der Core Console auf die Registerkarte **Machines** (Maschinen).
2. Führen Sie auf der Registerkarte **Machines** (Maschinen) einen der folgenden Schritte aus:
   - Klicken Sie auf den Hyperlink für die Maschine, die Sie neu starten möchten.
   - Oder wählen Sie im im Bereich **Navigation** die Maschine aus, die Sie neu starten möchten.
3. Klicken Sie auf die Registerkarte **Tools** (Extras), und klicken Sie dann auf **Diagnostics** (Diagnose).
4. Wählen Sie die Option **Restart Service** (Service neu starten) aus, und klicken Sie dann auf die Schaltfläche **Restart Service** (Service neu starten).

Anzeigen von Maschinenprotokollen

Wenn Fehler oder Probleme mit der Maschine auftreten, überprüfen Sie die Protokolle, um das Problem zu beheben.

So zeigen Sie Maschinenprotokolle an:

1. Klicken Sie in der Core Console auf die Registerkarte **Machines** (Maschinen).
2. Führen Sie auf der Registerkarte **Machines** (Maschinen) einen der folgenden Schritte aus:
   - Klicken Sie auf den Hyperlink für die Maschine, die die Protokolle enthalten, die Sie anzeigen möchten.
   - Wählen Sie im Bereich **Navigation** die Maschine aus, die die Protokolle enthalten, die Sie anzeigen möchten.
3. Klicken Sie auf die Registerkarte **Tools** (Extras), und klicken Sie dann auf **Diagnostics** (Diagnose).
4. Klicken Sie auf den Link **View Log** (Protokoll anzeigen).

Schützen einer Maschine

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

ANMERKUNG: Damit die Maschine geschützt wird, muss auf ihr die Agentensoftware installiert sein. Sie haben die Wahl, die Agentensoftware vor diesem Vorgang zu installieren, alternativ können Sie die Software auf dem Agenten bereitstellen, wenn Sie im Dialogfeld **Verbindung** den Schutz definieren. Wenn Sie die Agentensoftware während des Schützens einer Maschine installieren möchten, lesen Sie die spezifischen Anweisungen unter Bereitstellen der Agentensoftware beim Schutz eines Agenten.

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 zur selben Zeit finden Sie unter Schützen von mehreren Maschinen.

So schützen Sie eine Maschine:

1. Falls Sie dies nicht nach der Installation der Agentensoftware getan haben, starten Sie die Maschine, auf der die Agentensoftware installiert ist, neu.
2. Führen Sie in der Core Console auf der Kernmaschine eine der folgenden Maßnahmen aus:
   - Klicken Sie von der Registerkarte **Home** (Begrüßung) unter **Protected machines** (Geschützte Maschinen) auf **Protect Machine** (Maschine schützen).
   - Wählen Sie die Registerkarte **Machines** (Maschinen) aus, und klicken sie im Drop-Down-Menü **Actions** (Maßnahmen) auf **Protect Machine** (Maschine schützen).

   Das Dialogfeld **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.

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

Textfeld	Beschreibung
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 **Connect** (Verbinden), um eine Verbindung mit dieser Maschine herzustellen.

   ANMERKUNG: Wenn die Agentensoftware noch nicht auf der von Ihnen angegebenen Maschine installiert ist, folgen Sie dem Verfahren unter Bereitstellen der Agent Software beim Schutz eines Agenten. Starten Sie die Agentenmaschine nach der Bereitstellung der Agentensoftware neu, und fahren Sie dann mit dem nächsten Schritt fort.

5. Bearbeiten Sie im Dialogfeld **Protect** (Schützen) nach Bedarf die in der folgenden Tabellen näher beschriebenen Einstellungen.

Feld	Beschreibung
Anzeigename	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. ANMERKUNG: Sie können den Anzeigenamen für eine bestehende Maschine auch später durch Zugriff auf die Registerkarte **Configuration** (Konfiguration) ändern.
Repository	Wählen Sie das Repository auf dem Kern aus, in dem die Daten dieser Maschine gespeichert werden sollen.
Verschlüsselungsschlüssel	Geben Sie an, ob Verschlüsselung auf die Daten von jedem Volume auf dieser Maschine angewendet wird, die in dem Repository gespeichert wird. ANMERKUNG: Die Verschlüsselungseinstellungen für ein Repository werden auf der Registerkarte **Configuration** (Konfiguration) in der Core Console definiert.
Initially Pause Protection (Schutz anfänglich anhalten)	Nachdem Sie eine zu schützende Maschine hinzugefügt haben, beginnt AppAssure automatisch mit der Erstellung eines Basis-Snapshots mit Daten. Aktivieren Sie dieses Kontrollkästchen, um den Schutz anfänglich anzuhalten. Anschließend müssen Sie einen manuellen Snapshot erzwingen, wenn Sie bereit sind, den Schutz Ihrer Daten zu starten. Weitere Informationen über das manuelle Erzwingen eines Snapshots finden Sie unter Erzwingen eines Snapshots.
Volumegruppen	Unter „Volumegruppen“ können Sie definieren, welche Volumes Sie schützen möchten, und Sie können einen Schutzzeitplan erstellen. Um einen Standard-Schutzzeitplan von allen 60 Minuten für alle Volumes auf der Maschine einzustellen, klicken Sie auf **Apply Default** (Standard übernehmen).

Feld	Beschreibung
	Sie können auch ein Volume auf der Maschine auswählen und dessen Schutzparameter definieren. Die ursprünglichen Einstellungen wenden einen Standardschutzzeitplan von allen 60 Minuten an. Um den Zeitplan für ein Volume zu ändern, klicken Sie auf **Edit** (Bearbeiten) für das Volume. Sie können dann den Intervall zwischen Snapshots weiter definieren (einschließlich eines getrennten Zeitplans für das Wochenende) oder Sie können eine tägliche Zeit angeben, um einen Snapshot zu beginnen. Weitere Informationen zum Bearbeiten eines Schutzzeitplans für ein ausgewähltes Volume finden Sie unter Erstellen von benutzerdefinierten Zeitplänen für Volumes.

6. Klicken Sie auf **Protect** (Schützen).

   Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, beginnt ein Basisabbild (welches ein Snapshot aller Daten der geschützten Volumes ist) sofort mit der Übertragung zum Repository auf dem Kern, es sei denn, Sie haben angegeben, anfänglich den Schutz anzuhalten.

   VORSICHT: Wenn Sie eine Linux Maschine geschützt haben, dürfen Sie die Bereitstellung eines geschützten Volumes nicht manuell aufheben. Falls Sie dies tun müssen, müssen Sie vor der Aufhebung der Bereitstellung des Volumes den folgenden Befehl ausführen: bsctl -d [path_to_volume]. In diesem Befehl bezieht sich <path to volume> nicht auf den Bereitstellungspunkt des Volumes, sondern er bezieht sich auf den Beschreiber der Datei oder auf das Volume, das in einer ähnlichen Form wie dieses Beispiel sein muss: /dev/sda1.

Bereitstellen der Agentensoftware beim Schutz eines Agenten

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

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

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

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

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

   Das Dialogfeld **Deploy Agent** (Agenten bereitstellen) wird angezeigt.
3. 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) – Legt den Namen für die Maschine fest, die auf der Core Console angezeigt wird. Der Anzeigename kann der gleiche wie der Hostname sein.
- **Protect machine after install** (Maschine nach dem Installieren schützen) – Bei Auswahl dieser Option kann AppAssure, automatisch einen Basis-Snapshot erstellen, nachdem Sie die Maschine zum Schutz hinzugefügt haben. Diese Option ist per Standardeinstellung ausgewählt. Wenn Sie diese Option aufheben, müssen Sie manuell einen Snapshot erzwingen, wenn Sie bereit sind, den Datenschutz zu starten. Weitere Informationen über das manuelle Erzwingen eines Snapshots siehe „Forcing A Snapshot" (Erzwingen eines Snapshots) im *Dell DL4000 Appliance User's Guide* (Benutzerhandbuch für das Dell DL4000-Gerät).
- **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.

4. 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.

Erstellen von benutzerdefinierten Zeitplänen für Volumes

So erstellen Sie benutzerdefinierte Zeitpläne für Volumes

1. Wählen Sie im Dialogfeld **Maschine schützen** (Informationen zum Aufrufen dieses Dialogfelds finden Sie im Abschnitt Schützen einer Maschine) unter dem Eintrag **Volume-Gruppen** ein Volume für den Schutz aus, und klicken Sie anschließend auf **Bearbeiten**.

   Das Dialogfeld **Schutzzeitplan** wird angezeigt.
2. Wählen Sie im Dialogfeld **Protection Schedule** (Schutzzeitplan) eine der folgenden in der Tabelle beschriebenen Zeitplanoptionen für den Schutz Ihrer Daten aus.

Textfeld	Beschreibung
Intervall	Folgende Optionen stehen zur Auswahl: • **Wochentag** – Um Daten in einem bestimmten Intervall zu schützen, wählen Sie **Interval** (Intervall) und dann Folgendes aus: – Wenn Sie anpassen möchten, wann Daten während Spitzenauslastungszeiten geschützt werden sollen, können Sie eine **Startzeit,** eine **Endzeit** sowie ein **Intervall** in den Drop-Down-Menüs angeben. – Um Daten während Nebenzeiten zu schützen, aktivieren Sie das Kontrollkästchen **Protection interval during off-peak times** (Schutzintervall während Nebenzeiten), und wählen Sie dann ein Intervall für den Schutz im **Time** (Zeit) Drop-Down-Menü aus. • **Wochenenden** – Wenn Daten auch an den Wochenenden geschützt werden sollen, wählen Sie **Protect interval during weekends**

Textfeld	Beschreibung
	(Schutzintervall an Wochenenden), und wählen Sie dann ein **Intervall** im Drop-Down-Menü aus.
Täglich	Wenn die Daten täglich geschützt werden sollen, wählen Sie die Option **Daily protection** (Täglicher Schutz) und dann im Drop-Down-Menü **Time** (Zeit) eine Zeit aus, zu der der Schutz der Daten gestartet werden soll.
No Protection (Kein Schutz)	Um den Schutz für dieses Volume zu entfernen, wählen Sie die Option **No Protection** (Kein Schutz) aus.

Wenn Sie diese benutzerdefinierten Einstellungen auf alle Volumes auf dieser Maschine anwenden möchten, wählen Sie **Apply to All Volumes** (Auf alle Volumes anwenden).

3. Nachdem Sie alle notwendigen Änderungen vorgenommen haben, klicken Sie auf **OK**.
4. Wiederholen Sie die Schritte 2 und 3 für jedes weitere Volume, das Sie anpassen möchten.
5. Klicken Sie im Dialogfeld **Protect Machine** (Maschine schützen) auf **Protect** (Schützen).

Ändern von Exchange-Server-Einstellungen

Wenn Sie Daten auf einem Microsoft Exchange-Server schützen möchten, müssen Sie zusätzliche Einstellungen in der Core Console konfigurieren.

So ändern Sie Exchange-Server-Einstellungen:

1. Nachdem Sie die Exchange Server-Maschine für den Schutz hinzugefügt haben, wählen Sie die Maschine im Fensterbereich **Navigation** aus.

   Die Registerkarte **Zusammenfassung)** wird für die Maschine angezeigt.
2. Klicken Sie auf der Registerkarte **Summary** (Zusammenfassung) auf den Link **Exchange Server Settings** (Exchange-Server-Einstellungen).

   Das Dialogfeld **Exchange-Server-Einstellungen** wird angezeigt.
3. Im Dialogfeld **Exchange Server Settings** (Exchange-Server-Einstellungen) können Sie die folgenden Einstellungen aktivieren oder deaktivieren.
   - „Automatische Überprüfung der Bereitstellungsfähigkeit aktivieren".
   - „Enable nightly checksum check" (Nächtliche Prüfsummen-Überprüfung aktivieren). Sie können durch Auswahl der folgenden Optionen weitere Anpassungen vornehmen:
     - Automatically truncate Exchange logs after successful checksum check (Exchange-Protokolle nach erfolgreicher Prüfsummen-Überprüfung automatisch abschneiden)
     - „Truncate log before checksum check completes" (Protokoll vor Abschluss der Prüfsummen-Überprüfung abschneiden)
4. Sie können außerdem die Anmeldeinformationen für Ihren Exchange-Server ändern. Dabei müssen Sie nach unten zum Bereich mit den **Exchange Server-Informationen** scrollen und dann auf **Change Credentials** (Anmeldeinformationen ändern) klicken.

   Das Dialogfeld **Exchange-Anmeldeinformationen festlegen** wird angezeigt.
5. Geben Sie Ihre neuen Anmeldeinformationen ein. Klicken Sie dann auf **OK.**

Ändern von SQL-Server-Einstellungen

Wenn Sie Daten von Microsoft SQL Server schützen möchten, müssen Sie zusätzliche Einstellungen in der Core Console konfigurieren.

So ändern Sie SQL-Server-Einstellungen:

1. Nachdem Sie die SQL-Server-Maschine für den Schutz hinzugefügt haben, wählen Sie die Maschine im Fensterbereich **Navigation** der Core-Konsole aus.

   Die Registerkarte **Zusammenfassung)** wird für die Maschine angezeigt.
2. Klicken Sie auf der Registerkarte **Summary** (Zusammenfassung) auf den Link SQL Server Settings (SQL-Server-Einstellungen).

   Das Dialogfeld **SQL-Server-Einstellungen** wird angezeigt.
3. Im Dialogfeld **SQL Server Settings** (SQL Server-Einstellungen) können Sie ggf. die folgenden Einstellungen bearbeiten:
   - Enable nightly attachability check (Nächtliche Anfügbarkeitsprüfung aktivieren)
   - Truncate log after successful attachability check (simple recovery model only) (Protokoll nach erfolgreicher Anfügbarkeitsprüfung abschneiden (nur einfaches Wiederherstellungsmodell))
4. Sie können außerdem die Anmeldeinformationen für SQL-Server ändern. In diesem Fall müssen Sie nach unten zum Bereich mit der **SQL-Server-Informationen**-Tabelle scrollen und dann auf **Change Credentials** (Anmeldeinformationen ändern) klicken.

   Das Dialogfeld **SQL-Server-Anmeldeinformationen festlegen** wird angezeigt.
5. Geben Sie Ihre neuen Anmeldeinformationen ein. Klicken Sie dann auf **OK.**

Bereitstellen eines Agenten (Push-Installation)

AppAssure erfordert Microsoft.net für die Installation des Agenten. Microsoft.net muss auf jeder Client-Maschine installiert sein, bevor der Agent über einen manuellen Installationsprozess oder einen Push-Installationsvorgang installiert wird.
Mit AppAssure können Sie das Installationsprogramm des AppAssure-Agenten zum Schutz auf einzelnen Windows-Maschinen bereitstellen. Führen Sie die erforderlichen Schritte in den folgenden Verfahren aus, um das Installationsprogramm mit einer Push-Installation mit dem Agenten zu verbinden. Um mehrere Maschinen gleichzeitig bereitzustellen, lesen Sie Bereitstellen auf mehreren Maschinen.

ANMERKUNG: Agenten müssen mit einer Sicherheitsrichtlinie konfiguriert werden, um eine Remote-Installation zu ermöglichen.

So stellen Sie einen Agenten bereit:

1. Wählen Sie in der Core Console die Registerkarte **Machines** (Maschinen) aus.
2. Klicken Sie im Drop-down-Menü **Actions** (Maßnahmen) auf **Deploy Agent** (Agenten bereitstellen).

   Das Dialogfeld **Deploy Agent** (Agenten bereitstellen) wird angezeigt.
3. Geben Sie im Dialogfeld **Deploy Agent** (Agenten bereitstellen) die in der folgenden Tabelle beschriebenen Anmeldeeinstellungen ein.

Textfeld	Beschreibung
Maschine	Geben Sie den Hostnamen oder die IP-Adresse der Maschine ein, die Sie bereitstellen möchten.
Benutzername	Geben Sie den Benutzernamen ein, der für die Verbindung mit dieser Maschine verwendet wird, z. B. Administrator.
Kennwort	Geben Sie das Kennwort ein, um eine Verbindung mit dieser Maschine herzustellen.

Textfeld	Beschreibung
Automatic reboot after install (Automatischer Neustart nach Installation)	Wählen Sie diese Option aus, um anzugeben, ob der Kern nach Abschluss der Bereitstellung und Installation des AppAssure-Agenteninstallationsprogramms gestartet werden soll.

4. Klicken Sie auf **Verify** (Überprüfen), um die Anmeldeinformationen zu validieren, die Sie eingegeben haben.

   Das Dialogfeld **Deploy Agent** (Agenten bereitstellen) zeigt die Meldung an, dass die Validierung durchgeführt wird.
5. Klicken Sie zum Abbrechen des Überprüfungsvorgangs auf **Abort** (Abbrechen).

   Sobald der Überprüfungsvorgang abgeschlossen wurde, wird die Meldung angezeigt, dass die Überprüfung abgeschlossen ist.
6. Klicken Sie auf **Deploy** (Bereitstellen).

   Es wird die Meldung angezeigt, dass die Bereitstellung gestartet wurde. Sie können den Fortschritt in der Registerkarte **Ereignisse** beobachten.
7. Klicken Sie auf **Show details** (Details anzeigen), um weitere Informationen zum Status der Agenten-Bereitstellung anzuzeigen.
8. Klicken Sie auf **OK**.

Replizieren eines neuen Agenten

Wenn Sie einen AppAssure-Agenten zum Schutz auf einen Quellkern hinzufügen, bietet Ihnen AppAssure die Möglichkeit, den neuen Agenten auf einen vorhandenen Zielkern zu replizieren.

So replizieren Sie einen neuen Agenten:

1. Wechseln Sie zur Core Console und klicken Sie dann auf die Registerkarte **Machines** (Maschinen).
2. Klicken Sie im Drop-Down-Menü **Actions** (Maßnahmen) auf **Protect Machine** (Maschine schützen).
3. Geben Sie im Dialogfeld **Protect Machine** (Maschine schützen) die in der folgenden Tabelle beschriebenen Informationen ein.

Textfeld	Beschreibung
Host	Geben Sie den Hostnamen oder die IP-Adresse der Maschine ein, die Sie schützen möchten.
Schnittstelle	Geben Sie die Portnummer ein, die der AppAssure-Kern verwenden sollte, um mit dem Agenten auf dieser Maschine zu kommunizieren.
Benutzername	Geben Sie den Benutzernamen ein, der für die Verbindung mit dieser Maschine verwendet wird, z. B. Administrator.
Kennwort	Geben Sie das Kennwort ein, um eine Verbindung mit dieser Maschine herzustellen.

4. Klicken Sie auf **Connect** (Verbinden), um eine Verbindung mit dieser Maschine herzustellen.
5. Klicken Sie auf **Show Advanced Options** (Erweiterte Optionen anzeigen) und bearbeiten Sie bei Bedarf folgende Einstellungen.

Textfeld	Beschreibung
Anzeigename	Geben Sie einen Namen für die Maschine ein, die in der Core Console angezeigt werden soll.
Repository	Wählen Sie das Repository auf dem AppAssure-Kern aus, in dem die Daten für diese Maschine gespeichert werden.
Verschlüsselungsschlüssel	Geben Sie an, ob Verschlüsselung auf die Daten von jedem Volume auf dieser Maschine angewendet wird, die in dem Repository gespeichert wird. ANMERKUNG: Die Verschlüsselungseinstellungen für ein Repository werden auf der Registerkarte **Configuration** (Konfiguration) in der Core Console definiert.
Remote-Kern	Geben Sie den Zielkern an, auf den Sie den Agenten replizieren möchten.
Remote-Repository	Der Name des gewünschten Repositorys auf dem Zielkern, in dem die replizierten Daten von dieser Maschine gespeichert werden.
Pause	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Replikation anhalten möchten; z. B. wenn Sie sie anhalten möchten, bis AppAssure ein Basisabbild des neuen Agenten gemacht hat.
Zeitplan	Wählen Sie eine der folgenden Optionen: • Protect all volumes with default schedule (Alle Volumes gemäß Standardzeitplan schützen) • Protect specific volumes with custom schedule (Alle Volumes gemäß benutzerdefiniertem Zeitplan schützen) ANMERKUNG: Der Standardzeitplan ist alle 15 Minuten.
Initially pause protection (Schutz anfänglich anhalten)	Aktivieren Sie dieses Kontrollkästchen, wenn Sie den Schutz anhalten möchten; z. B. um AppAssure daran zu hindern, ein Basisabbild während der Spitzenauslastungszeiten zu erstellen.

6. Klicken Sie auf **Protect** (Schützen).

Verwalten von Maschinen

In diesem Abschnitt werden verschiedene Aufgaben beschrieben, die Sie beim Verwalten Ihrer Maschinen ausführen können, z. B. Entfernen einer Maschine aus Ihrer AppAssure-Umgebung, Einrichten der Replikation, Erzwingen des Abschneidens des Protokolls, Abbrechen von Vorgängen und mehr.

Entfernen einer Maschine

1. Wechseln Sie zur Core Console, und klicken Sie dann auf die Registerkarte **Maschinen**.
2. Führen Sie auf der Registerkarte **Machines** (Maschinen) einen der folgenden Schritte aus:
   - Klicken Sie auf den Hyperlink für die Maschine, die Sie entfernen möchten.
   - Oder wählen Sie im Navigationsbereich die Maschine aus, die Sie entfernen möchten.
3. Klicken Sie im Drop-Down-Menü **Actions** (Maßnahmen) mit der rechten Maustaste auf **Remove Machines** (Maschinen entfernen), und wählen Sie dann eine der in der folgenden Tabelle beschriebenen Optionen aus.

Option	Beschreibung
Relationship Only (Nur Beziehung)	Der Quellkern wird aus der Replikation entfernt, die replizierten Wiederherstellungspunkte werden aber beibehalten.
With Recovery Points (Mit Wiederherstellungspunkten)	Der Quellkern wird aus der Replikation entfernt und alle von dieser Maschine empfangenen replizierten Wiederherstellungspunkte werden gelöscht.

Replizieren von Agentendaten auf einer Maschine

Replikation ist die Beziehung zwischen den Ziel- und Quell-Kernen am gleichen Standort oder zwischen zwei Standorten mit langsamer Verbindung für jeden einzelnen Agenten. Wenn eine Replikation zwischen zwei Kernen eingerichtet ist, überträgt der Quellkern die inkrementellen Snapshot-Daten von ausgewählten Agenten asynchron auf den Ziel- oder Quellkern. Eine ausgehende Replikation kann für eine Übertragung zu einem Anbieter verwalteter Dienste, der eine externe Sicherung sowie einen Notfallwiederherstellungsdienst bereitstellt, oder auf einen selbst verwalteten Kern konfiguriert werden. So replizieren Sie Agentendaten auf einer Maschine:

1. Wählen Sie in der Core Console die Registerkarte **Machines** (Maschinen) aus.
2. Wählen Sie die Maschine aus, die Sie replizieren möchten.
3. Klicken Sie im Drop-Down-Menü **Actions** (Aktionen) auf **Replikation** und schließen Sie dann eine der folgenden Optionen ab:
   - Wenn Sie Replikation einrichten, klicken Sie auf **Enable** (Aktivieren).
   - Falls Sie bereits eine vorhandene Replikation eingerichtet haben, klicken Sie auf **Copy** (Kopieren).

   Das Dialogfeld **Replikationen aktivieren** wird angezeigt.
4. Geben Sie im Textfeld **Host** einen Hostnamen ein.
5. Wählen Sie unter **Agents** (Agenten) die Maschine aus, auf denen sich der Agent und die Daten befinden, die Sie replizieren möchten.
6. Aktivieren Sie bei Bedarf das Kontrollkästchen **Use a seed drive to perform initial transfer** (Seed-Laufwerk für Erstübertragung verwenden).
7. Klicken Sie auf **Add** (Hinzufügen).
8. Um die Replikation anzuhalten oder fortzusetzen, klicken Sie im Drop-Down-Menü **Actions** (Maßnahmen) auf **Replication** (Replikation) und anschließend je nach Bedarf auf **Pause** (Anhalten) oder **Resume** (Fortsetzen).

Replikationspriorität für einen Agenten einstellen

So stellen Sie die Replikationspriorität für einen Agenten ein:

1. Navigieren Sie in der Core Console zur geschützten Maschine, für die Sie die Replikationspriorität einstellen möchten, und klicken Sie auf die Registerkarte **Configuration** (Konfiguration).
2. Klicken Sie auf **Select Transfer Settings** (Übertragungseinstellungen auswählen) und wählen Sie dann aus der Drop-Down-Liste **Priority** (Priorität) eine der folgenden Optionen aus.
   - **Standardeinstellung**
   - **Höchster Wert**
   - **Niedrigster Wert**
   - **1**
   - **2**

- **3**
- **4**

ANMERKUNG: Die Standardpriorität ist 5. Wenn ein Agent die Priorität 1 erhält und ein anderer Agent die Priorität „Highest" (Höchster Wert), dann wird der Agent mit der Priorität „Highest" vor dem Agenten mit der Priorität 1 repliziert.

3. Klicken Sie auf **OK**.

Abbrechen von Vorgängen auf einer Maschine

Sie können aktuell ausgeführte Vorgänge für eine Maschine abbrechen. Dabei können Sie angeben, ob Sie nur einen aktuellen Snapshot oder alle aktuellen Vorgänge (d. h. einschließlich Exporten, Replikationen usw.) abbrechen möchten.

So brechen Sie Vorgänge auf einer Maschine ab:

1. Wählen Sie in der Core Console die Registerkarte **Machines** (Maschinen) aus.
2. Wählen Sie die Maschine aus, für die Sie Vorgänge abbrechen möchten.
3. Klicken Sie im Drop-Down-Menü **Actions** (Aktionen) auf **Cancel** (Abbrechen), und wählen Sie eine der untenstehend beschriebenen Optionen aus:

Textfeld	Beschreibung
All Operations (Alle Vorgänge)	Bricht alle aktiven Vorgänge für diese Maschine ab.
Snapshot	Bricht den derzeit in Bearbeitung befindlichen Snapshot ab.

Anzeigen des Maschinenstatus und anderer Details

So zeigen Sie den Maschinenstatus und andere Details an:

1. Führen Sie im Navigationsfenster der Core Console eine der folgenden Maßnahmen aus:
   - Wählen Sie die Registerkarte **Machines** (Maschinen) aus. Klicken Sie dann auf den Hyperlink für die Maschine, deren Einstellungen Sie anzeigen möchten
   - Klicken Sie im Navigationsbereich auf die Maschine, die Sie anzeigen möchten.

Die Registerkarte **Summary** (Zusammenfassung) wird angezeigt.

Die Informationen über die Maschine werden auf der Seite **Summary** (Zusammenfassung) angezeigt. Es werden unter anderem folgende Details angezeigt:

- Host-Name
- Last Snapshot taken (Letzter Snapshot erstellt)
- Next Snapshot scheduled (Nächster Snapshot geplant)
- Encryption status (Verschlüsselungsstatus)
- Version number (Versionsnummer)
- Mountability Check status (Status der Überprüfung der Bereitstellungsfähigkeit)
- Checksum Check status (Prüfsummen-Überprüfungsstatus)
- Last Log Truncation performed (Letzte durchgeführte Abschneidung des Protokolls)

Ausführliche Informationen über die Volumes auf dieser Maschine werden ebenfalls angezeigt und enthalten:

- Total size (Gesamtgröße)
- Used Space (Belegte Speicherkapazität)
- Free Space (Freier Speicherplatz)

Wenn SQL Server auf der Maschine installiert ist, werden auch detaillierte Informationen über den Server angezeigt. Diese Informationen schließen Folgendes ein:

- Name
- Install Path (Installierungspfad)
- Version
- Version number (Versionsnummer)
- Database Name (Name der Datenbank)
- Online-Status

Wenn Exchange Server auf der Maschine installiert ist, werden auch detaillierte Informationen über den Server und die Postspeicher angezeigt. Diese Informationen schließen Folgendes ein:

- Name
- Install Path (Installierungspfad)
- Datenpfad
- Name Exchange Databases Path (Name des Exchange-Datenbanken-Pfads)
- Log File Path (Protokolldatei-Pfad)
- Log Prefix (Protokoll-Präfix)
- System Path (Systempfad)
- MailStore Type (Postspeicher-Typ)

Verwalten von mehreren Maschinen

Dieses Thema beschreibt die Aufgaben, die Administratoren durchführen müssen, um die Agentensoftware auf mehreren Windows-Maschinen gleichzeitig bereitzustellen.

Zum Bereitstellen und Schützen mehrerer Agenten müssen Sie die folgenden Aufgaben durchführen:

1. Stellen Sie AppAssure auf mehreren Maschinen bereit.
   Siehe Bereitstellen auf mehreren Maschinen.
2. Überwachen Sie die Aktivität der Batch-Bereitstellung.
   Siehe Überwachen der Bereitstellung auf mehreren Maschinen.
3. Schützen Sie mehrere Maschinen.
   Lesen Sie den Abschnitt unter Schützen mehrerer Maschinen.

   ANMERKUNG: Dieser Schritt kann übersprungen werden, wenn Sie während der Bereitstellung die Option „Protect Machine After Install“ (Maschine nach der Installierung schützen) gewählt haben.
4. Überwachen Sie die Aktivität des Batch-Schutzes
   Lesen Sie den Abschnitt unter Überwachen des Schutzes für mehrere Maschinen.

Bereitstellen auf mehreren Maschinen

Die können den Task der Bereitstellung der AppAssure Agent-Software auf mehrere Windows-Maschinen durch Verwendung der Bulk Deploy (Massenbereitstellung)-Funktion von AppAssure vereinfachen. Sie können die Massenbereitstellung für folgende Maschinen verwenden:

- Maschinen auf einem virtuellen vCenter/ESXi-Host
- Maschinen auf einem Active Directory-Domain
- Maschinen auf jedem anderen Host

Die Massenbereitstellungsfunktion ermittlet automatisch die Maschinen auf einem Host und ermöglicht es Ihnen, die Maschinen, die Sie bereitstellen möchten, auszuwählen. Als Alternative können Sie die Host- und Maschineninformationen manuell eingeben.

ANMERKUNG: Die bereitzustellenden Maschinen müssen Internetzugang haben, um Bits herunterzuladen und zu installieren, da AppAssure die Webversion des AppAssure-Agenten-Installationsprogramms zur Bereitstellung der Installationskomponenten nutzt. Wenn kein Internetzugang verfügbar ist, laden Sie das AppAssure-Agenten-Installationsprogramm von der Kernmaschine. Weitere Informationen über das Verschieben des Agenten-Installationsprogramms von der Kernmaschine finden Sie unter Verschieben des Agenten-Installationsprogramms von der Kernmaschine. Sie können Kern- und Agentenaktualisierungen vom Lizenzportal herunterladen.

Verschieben des Agenten-Installationsprogramms von der Kernmaschine

Wenn die bereitgestellten Server über keinen Internetzugang verfügen, können Sie die tatsächliche Agenten-Installationsdatei von der Kernmaschine laden. Im Gerät sind die Agenten-Installationsprogrammdateien bereits enthalten.

ANMERKUNG: Laden Sie Kern- und Agentenaktualisierungen vom Lizenzportal herunter.

So verschieben Sie das Agenten-Installationsprogramm von der Kernmaschine:

1. Kopieren Sie die Agenten-Installationsdatei **Agent-X64–5.x.x.xxxxx.exe** von der Kernmaschine auf das Verzeichnis **C:\Program Files\apprecovery\core\installers**.
2. Wählen Sie in der Core Console die Registerkarte **Konfiguration** aus, und klicken Sie dann auf **Einstellungen**.
3. Bearbeiten Sie im Abschnitt **Deploy Settings** (Einstellungen bereitstellen) den **Agent Installer Name** (Namen des Agenten-Installer).

Bereitstellen für Maschinen auf einer Active Directory Domain

Bevor Sie diesen Vorgang starten, müssen Sie über die Domänen-Informationen und die Anmeldeinformationen für den Active Directory-Server verfügen.

So stellen Sie den Agenten auf mehreren Maschinen auf einer Active Directory-Domäne bereit:

1. Wechseln Sie zur Core Console, klicken Sie auf die Registerkarte **Extras** und dann auf **Massenbereitstellung**.
2. Klicken Sie im Fenster **Deploy Agent on Machines** (Agent auf Maschinen bereitstellen) auf **Active Directory**.
3. Geben Sie im Dialogfeld **Connect to Active Directory** (Mit Active Directory verbinden) die Domänen-Informationen und die Anmeldeinformationen ein, wie in der folgenden Tabelle beschrieben:

Textfeld	Beschreibung
Domäne	Domänenname oder IP-Adresse der Active Directory-Domäne.
Benutzername	Der Benutzername, der für die Verbindung mit dieser Domäne verwendet wird, z. B. Administrator.
Kennwort	Das sichere Kennwort, das für die Verbindung mit dieser Domäne verwendet wird.

4. Klicken Sie auf **Verbinden**.
5. Wählen Sie im Dialogfeld **Maschinen aus Active Directory hinzufügen** die Maschinen aus, für die Sie den AppAssure-Agenten bereitstellen möchten, und klicken Sie dann auf **Hinzufügen**.

   Die Maschinen, die Sie hinzugefügt haben, erscheinen im Fenster **Deploy Agent on Machines** (Agenten auf Maschinen bereitstellen).
6. Um das Kennwort für die Maschine einzugeben, wählen Sie ein Repository, fügen Sie einen Verschlüsselungsschlüssel hinzu, oder bearbeiten Sie andere Einstellungen für eine Maschine. Klicken Sie auf den Link **Bearbeiten)** für diese Maschine und führen Sie dann Folgendes aus.
   a. Geben Sie im Dialogfeld **Edit Settings** (Einstellungen bearbeiten) die Einstellungen, wie in der folgenden Tabelle beschrieben, ein:

Textfeld	Beschreibung
Host-Name	In Schritt 3 automatisch angegeben.
Anzeigename	Automatisch zugewiesen, basierend auf dem Hostnamen, der in Schritt 3 angegeben wurde.
Schnittstelle	Die Schnittstellennummer, über die der Kern mit dem Agenten auf der Maschine kommuniziert.
Benutzername	In Schritt 3 automatisch angegeben.
Kennwort	Geben Sie das Kennwort für die Maschine ein.
Automatic reboot after install (Automatischer Neustart nach Installation)	Geben Sie an, ob die Maschine nach Abschluss der Bereitstellung automatisch neu starten soll. ANMERKUNG: Diese Option ist obligatorisch, wenn sie die Maschine nach der Bereitstellung automatisch durch aktivierung des Kontrollkästchens **Protect Machine After Install** (Maschine nach dem Installieren schützen) schützen wollen.
Protect Machine After Install (Maschine nach dem Installieren schützen)	Geben Sie an, ob Sie die Maschine nach der Bereitstellung automatisch schützen wollen. Dadurch können Sie die Option **Protecting Multiple Machines** (Schützen von mehreren Maschinen) überspringen.
Repository	Verwenden Sie die Drop-Down-Liste, um das Repository auf dem Kern auszuwählen, in dem die Daten der Maschine gespeichert werden sollen. Das Repository, das Sie ausgewählt haben, wird für alle geschützten Maschinen verwendet. ANMERKUNG: Diese Option ist nur verfügbar, wenn Sie **Protect machine after install** (Maschine nach dem Installieren schützen) auswählen.
Verschlüsselungsschlüssel	(Optional) Verwenden Sie die Drop-Down-Liste, um anzugeben, ob Verschlüsselung auf die Daten auf dieser Maschine angewendet wird, die in dem Repository gespeichert werden soll. Der Verschlüsselungsschlüssel wird allen Maschinen zugewiesen, die geschützt sind.

Textfeld	Beschreibung

ANMERKUNG: Diese Option ist nur verfügbar, wenn Sie **Protect machine after install** (Maschine nach dem Installieren schützen) auswählen.

b. Klicken Sie auf **Speichern**.

7. Überprüfen Sie, ob sich AppAssure mit jeder Maschine verbinden kann. Wählen Sie dazu jede Maschine im Fenster **Agent auf Maschinen bereitstellen** aus, und klicken Sie dann auf **Überprüfen**.
8. Das Fenster **Deploy Agent on Machines** (Agent auf Maschinen bereitstellen) zeigt ein Symbol neben jeder Maschine an, das die Einsatzbereitschaft der Maschine wie folgt repräsentiert:

Textfeld	Beschreibung
Grünes Symbol	AppAssure kann sich mit der Maschine verbinden und kann bereitgestellt werden.
Gelbes Symbol	AppAssure kann sich mit der Maschine verbinden, allerdings ist der Agent bereits mit einer Kernmaschine gekoppelt.
Rotes Symbol	AppAssure kann sich nicht mit der Maschine verbinden. Möglicherweise sind die Anmeldeinformationen ungültig, die Maschine ist ausgeschaltet, die Firewall blockiert den Datenverkehr oder es liegt ein anderes Problem vor. Zur Behebung klicken Sie auf **Einstellungen bearbeiten** in der Symbolleiste oder auf den Link **Bearbeiten** neben der Maschine.

9. Nachdem die Maschinen erfolgreich überprüft wurden, wählen Sie die einzelnen Maschinen aus, auf denen Sie den AppAssure-Agenten bereitstellen möchten, und klicken Sie dann auf **Bereitstellen**.
10. Wenn Sie die Option **Protect machine after install** (Maschine nach dem Installieren schützen) auswählen, werden die Maschinen automatisch neu gestartet und der Schutz wird aktiviert.

Bereitstellen für Maschinen auf einem virtuellen VMware vCenter- oder ESXi-Host

Bevor Sie diesen Vorgang starten, müssen Sie die Speicherinformationen für den Host und die Anmeldeinformationen für den virtuellen VMware vCenter/ESXi-Host bereitstellen.

ANMERKUNG: Auf allen virtuellen Maschinen muss VM Tools installiert sein, damit AppAssure den Hostnamen der virtuellen Maschine erkennen kann, auf der bereitgestellt werden soll. Anstelle des Hostnamens verwendet AppAssure den Namen der virtuellen Maschine, was jedoch zu Problemen führen kann, wenn sich der Hostname vom Namen der virtuellen Maschine unterscheidet.

Bereitstellen auf mehrere Maschinen auf einem virtuellen vCenter/ESXi-Host:

1. Wechseln Sie zur Core Console, klicken Sie auf die Registerkarte **Extras** und dann auf **Massenbereitstellung**.
2. Klicken Sie im Fenster **Deploy Agent on Machines** (Agent auf Maschinen bereitstellen) auf **vCenter/ ESXi**.
3. Geben Sie im Dialogfeld **Connect to VMware vCenter Server/ESXi** (Mit VMware vCenter Server/ESX verbinden) die Hostinformationen und Anmeldeinformationen wie folgt ein und klicken sie auf **OK**.

Textfeld	Beschreibung
Host	Geben Sie den Hostnamen oder die IP-Adresse des virtuellen Hosts des VMware vCenter Server/ESX(i) ein.

Benutzername	Geben Sie den Benutzernamen, der für die Verbindung mit diesem virtuellen Host verwendet wird ein; z. B. Administrator.
Kennwort	Geben Sie das sichere Kennwort ein, der für die Verbindung mit diesem virtuellen Host verwendet wird

4. Aktivieren Sie im Dialogfeld **Maschinen vom VMware vCenter-Server/ESXi hinzufügen** das Kontrollkästchen neben den Maschinen, auf denen Sie den AppAssure-Agenten bereitstellen möchten, und klicken Sie auf **Hinzufügen**.
5. Im Fenster **Agent auf Maschinen bereitstellen** können Sie die Maschinen, die Sie angegeben haben, anzeigen. Wenn Sie ein Repository, einen Verschlüsselungsschlüssel oder andere Einstellungen einer Maschine auswählen möchten, aktivieren Sie das Kontrollkästchen neben der Maschine und klicken Sie auf **Einstellungen bearbeiten**.

   Weitere Informationen zu den Einstellungen finden Sie unter Bereitstellen für Maschinen auf einer Active Directory Domain.
6. Überprüfen Sie, ob sich AppAssure mit jeder Maschine verbinden kann. Wählen Sie dazu die einzelnen Maschinen im Fenster **Agent auf Maschinen bereitstellen** aus, und klicken Sie dann auf **Überprüfen**.
7. Das Fenster **Deploy Agent on Machines** (Agent auf Maschinen bereitstellen) zeigt ein Symbol neben jeder Maschine an, das die Einsatzbereitschaft der Maschine wie folgt repräsentiert:

Textfeld	Beschreibung
Grünes Symbol	AppAssure kann sich mit der Maschine verbinden und kann bereitgestellt werden.
Gelbes Symbol	AppAssure kann sich mit der Maschine verbinden, allerdings ist der Agent bereits mit einer Kernmaschine gekoppelt.
Rotes Symbol	AppAssure kann sich nicht mit der Maschine verbinden. Möglicherweise sind die Anmeldeinformationen ungültig, die Maschine ist ausgeschaltet, die Firewall blockiert den Datenverkehr oder es liegt ein anderes Problem vor. Zur Behebung klicken Sie auf **Einstellungen bearbeiten** in der Symbolleiste oder auf den Link **Bearbeiten** neben der Maschine.

8. Nachdem die Maschinen erfolgreich überprüft wurden, wählen Sie jede Maschine aus und klicken Sie auf **Deploy** (Bereitstellen).
9. Wenn Sie die Option **Protect machine after install** (Maschine nach dem Installieren schützen) auswählen, werden die Maschinen automatisch neu gestartet und der Schutz wird aktiviert.

Bereitstellen für Maschinen auf allen anderen Hosts

So stellen Sie mehrere Maschinen auf allen anderen Hosts bereit:

1. Wechseln Sie zur Core Console, klicken Sie auf die Registerkarte **Extras** und dann auf **Massenbereitstellung**.
2. Führen Sie im Fenster **Deploy Agent on Machines** (Bereitstellung eines Agenten auf Maschinen) einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Neu**, um mehrere Maschinen unter Verwendung des Dialogfelds **Maschine hinzufügen** anzugeben. Dieses ermöglicht Ihnen, einen neuen Host für Maschinen, Anmeldeinformationen, Repository, Verschlüsselungsschlüssel und andere Informationen einzugeben. Weitere Einzelheiten zu den verschiedenen Einstellungen finden Sie unter Bereitstellen für Maschinen auf einer Active Directory Domain.

Nachdem Sie diese Informationen eingegeben haben, klicken Sie auf **OK**, um sie der Liste **Deploy Agent on Machines** (Agent auf Maschinen bereitstellen) hinzuzufügen oder klicken Sie auf **OK & New** (OK und Neu), um noch eine Maschine hinzuzufügen.

ANMERKUNG: Wenn Sie nach der Betriebssystembereitstellung die Maschine automatisch schützen lassen möchten, aktivieren Sie das Kontrollkästchen **Maschine nach dem Installieren schützen**. Wenn Sie das Kontrollkästchen auswählen, wird der Computer automatisch neu gestartet, bevor der Schutz aktiviert wird.

- Klicken Sie auf **Manually** (Manuell), um mehrere Maschinen in einer Liste festzulegen. Jede Zeile stellt eine Maschine dar, auf der bereitgestellt werden kann. Geben Sie im Dialogfeld **Add Machines Manually** (Maschinen manuell hinzufügen) die IP-Adresse oder den Namen der Maschine, den Benutzernamen, das Kennwort; getrennt durch einen doppelten Doppelpunkt und die Schnittstelle wie folgt an:

  ```
  hostname::username::password::port For example:
  10.255.255.255::administrator::&11@yYz90z::8006 abc-
  host-00-1::administrator::99!zU$o83r::168
  ```

3. Im Fenster **Agent auf Maschinen bereitstellen** können Sie die Maschinen, die Sie angegeben haben, sehen. Wenn Sie ein Repository, einen Verschlüsselungsschlüssel oder andere Einstellungen einer Maschine auswählen möchten, aktivieren Sie das Kontrollkästchen neben der Maschine und klicken Sie auf **Einstellungen bearbeiten**.

   Weitere Informationen zu den Einstellungen finden Sie unter Bereitstellen für Maschinen auf einer Active Directory Domain.

4. Überprüfen Sie, ob sich AppAssure mit jeder Maschine verbinden kann. Wählen Sie dazu die einzelnen Maschinen im Fenster **Agent auf Maschinen bereitstellen** aus, und klicken Sie dann auf **Überprüfen**.

   Das Fenster **Deploy Agent on Machines** (Agent auf Maschinen bereitstellen) zeigt ein Symbol neben jeder Maschine an, das die Einsatzbereitschaft der Maschine wie folgt repräsentiert:

Textfeld	Beschreibung
Grünes Symbol	AppAssure kann sich mit der Maschine verbinden und kann bereitgestellt werden.
Gelbes Symbol	AppAssure kann sich mit der Maschine verbinden, allerdings ist der Agent bereits mit einer Kernmaschine gekoppelt.
Rotes Symbol	AppAssure kann sich nicht mit der Maschine verbinden. Möglicherweise sind die Anmeldeinformationen ungültig, die Maschine ist ausgeschaltet, die Firewall blockiert den Datenverkehr oder es liegt ein anderes Problem vor. Zur Behebung klicken Sie auf **Einstellungen bearbeiten** in der Symbolleiste oder auf den Link **Bearbeiten** neben der Maschine.

5. Nachdem die Maschinen erfolgreich überprüft wurden, aktivieren Sie das Kontrollkästchen neben den Maschinen und klicken Sie auf **Deploy** (Bereitstellen).
6. Wenn Sie die Option **Protect machine after install** (Maschine nach dem Installieren schützen) auswählen, werden die Maschinen automatisch neu gestartet und der Schutz wird aktiviert.

Überwachen der Bereitstellung von mehreren Maschinen

Sie können den Bereitstellungsfortschritt der AppAssure-Agentensoftware auf den Maschinen anzeigen lassen.

So überwachen Sie die Bereitstellung mehrerer Maschinen:

1. Klicken Sie in der Core Console auf die Registerkarte **Ereignisse**, machen Sie den Bereitstellungsjob in der Liste ausfindig, und klicken Sie auf die Schaltfläche in der Spalte **Details**.

Das Fenster **Monitor Active Task** (Aktive Aufgabe überwachen) zeigt die Einzelheiten der Bereitstellung an.

Es werden sowohl allgemeine Informationen zum Fortschritt als auch der Status jeder einzelnen Bereitstellung angezeigt. Die angezeigten Details umfassen:

- Startzeit
- Endzeit
- Verstrichene Zeit
- Time Remaining (Verbleibende Zeit)
- Fortschritt
- Phase

2. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Open in New window** (In einem neuen Fenster öffnen), um ein neues Fenster zur Ansicht des Bereitstellungsfortschritts zu öffnen.
   - Oder klicken Sie auf **Close** (Schließen), und die Bereitstellungsaufgabe wird im Hintergrund weiter ausgeführt.

Schützen mehrerer Maschinen

Nach der Massenbereitstellung der Agentensoftware auf den Maschinen müssen Sie diese nun schützen, damit die Daten geschützt werden. Wenn Sie die Option **Maschine nach dem Installieren schützen** ausgewählt haben, als Sie den Agenten bereitgestellt haben, können Sie dieses Verfahren überspringen.

ANMERKUNG: Agenten-Maschinen müssen mit einer Sicherheitsrichtlinie konfiguriert werden, um eine Remote-Installation zu ermöglichen.

So schützen Sie mehrere Maschinen:

1. Wechseln Sie zur Core Console, klicken Sie auf die Registerkarte **Extras** und dann auf **Massenschutz**.

   Das Fenster **Maschinen schützen** wird angezeigt.
2. Fügen Sie die Maschinen, die Sie schützen möchten durch Anklicken einer der folgenden Optionen hinzu.

   Weitere Informationen zum Durchführen der einzelnen Optionen finden Sie unter Bereitstellen auf mehreren Maschinen.
   - Klicken Sie auf **Active Directory**, um Maschinen auf einer Active Directory-Domäne anzugeben.
   - Klicken Sie auf **vCenter/ESXi**, um virtuelle Maschinen auf einem vCenter/ESXi virtuellem Host anzugeben.
   - Klicken Sie auf **New** (Neu), um mehrere Maschinen durch Verwendung des Dialogfelds „Add Machine“ (Maschine hinzufügen) anzugeben.
   - Klicken Sie auf **Manually** (Manuell), um mehrere Maschinen in einer Liste durch Eingeben des Hostnamen und der Anmeldeinformationen anzugeben.
3. Im Fenster **Maschinen schützen**, können Sie die Maschinen, die Sie hinzugefügt haben, anzeigen. Wenn Sie ein Repository, einen Verschlüsselungsschlüssel oder andere erweiterte Einstellungen einer Maschine auswählen möchten, aktivieren Sie das Kontrollkästchen neben der Maschine, und klicken Sie auf **Einstellungen bearbeiten**.
4. Legen Sie die Einstellungen wie folgt fest und klicken Sie auf **OK**.

Textfeld	Beschreibung
Benutzername	Geben Sie den Benutzernamen ein, der für die Verbindung mit dieser Maschine verwendet wird, z. B. Administrator.

Textfeld	Beschreibung
Kennwort	Geben Sie das sichere Kennwort ein, um eine Verbindung mit dieser Maschine herzustellen.
Schnittstelle	Geben Sie die Portnummer an, über die der Kern mit dem Agenten auf der Maschine kommuniziert.
Repository	Wählen Sie das Repository auf dem Kern aus, in dem die Daten für diese Maschinen gespeichert werden. Das von Ihnen ausgewählte Repository wird für alle geschützten Maschinen verwendet.
Verschlüsselungsschlüssel	Gibt an, ob Verschlüsselung auf den Agenten auf den Maschinen angewendet wird, die im Repository gespeichert sind. Der Verschlüsselungsschlüssel wird allen Maschinen zugewiesen, die geschützt sind.
Protection Schedule (Schutzzeitplan)	Geben Sie den Zeitplan an, nach dem der Schutz der Maschinen durchgeführt wird. Der Standardzeitplan beträgt alle 60 Minuten zur Hauptzeit und alle 60 Minuten am Wochenende. Klicken Sie zum Bearbeiten des Zeitplans zur Anpassung an Ihr Unternehmen auf **Edit** (Bearbeiten). **ANMERKUNG:** Weitere Informationen finden Sie unter Ändern von Schutzzeitplänen.
Initially Pause Protection (Schutz anfänglich anhalten)	Optional können Sie den Schutz beim ersten Durchführen anhalten; das bedeutet, dass der Kern keine Snapshots von den Maschinen erstellt, bis Sie den Schutz manuell wieder aufnehmen.

5. Überprüfen Sie, ob sich AppAssure mit jeder Maschine verbinden kann. Führen Sie dazu folgende Schritte durch: Markieren Sie das Kontrollkästchen neben der jeweiligen Maschine im Fenster **Maschinen schützen**, und klicken Sie auf **Überprüfen**.
6. Das Fenster **Protect Machines** (Maschinen schützen) zeigt ein Symbol neben jeder Maschine an, welches deren Einsatzbereitschaft wie folgt repräsentiert:

Symbol	Beschreibung
Grünes Symbol	AppAssure kann sich mit der Maschine verbinden und die Maschine kann geschützt werden.
Gelbes Symbol	AppAssure kann sich mit der Maschine verbinden, allerdings ist der Agent bereits mit einer Kernmaschine gekoppelt.
Rotes Symbol	AppAssure kann sich nicht mit der Maschine verbinden. Möglicherweise sind die Anmeldeinformationen ungültig, die Maschine ist ausgeschaltet, die Firewall blockiert den Datenverkehr oder es liegt ein anderes Problem vor. Zur Behebung klicken Sie auf **Einstellungen bearbeiten** in der Symbolleiste oder auf den Link **Bearbeiten** neben der Maschine.

7. Nachdem die Maschinen erfolgreich überprüft wurden, aktivieren Sie das Kontrollkästchen neben den Maschinen und klicken Sie auf **Schützen**.

Überwachen des Schutzes von mehreren Maschinen

Sie können den Fortschritt überwachen, während AppAssure die Schutzrichtlinien und Zeitpläne auf den Maschinen anwendet.

So überwachen Sie den Schutz mehrerer Maschinen:

1. Klicken Sie auf die Registerkarte **Machines** (Maschinen), um Status und Fortschritt des Schutzes anzuzeigen.

   Die Seite **Geschützte Maschinen** wird angezeigt.
2. Klicken Sie die Registerkarte **Events** (Ereignisse), um verwandte Aufgaben, Ereignisse und Benachrichtigungen anzuzeigen.

   Die Seite **Tasks** wird angezeigt.

Textfeld	Beschreibung
So zeigen Sie Informationen zu Aufgaben an	Wenn die Volumes übertragen werden, wird im Fensterbereich **Tasks** (Aufgaben) ihr Status sowie Start- und Endzeiten angezeigt. Klicken Sie auf **Details** (Einzelheiten), um nähere Informationen zur Aufgabe zu erhalten.
So zeigen Sie Benachrichtigungsinformationen an	Beim Hinzufügen jeder geschützten Maschine wird eine Benachrichtigung protokolliert, die genau festhält, ob der Vorgang erfolgreich war oder ob Fehler berichtet wurden. Die Warnstufe wird zusammen mit dem Übertragungsdatum und der Meldung angezeigt. Wenn Sie alle Warnmeldungen von der Seite löschen möchten, klicken Sie auf **Dismiss All** (Alle schließen).
So zeigen Sie Ereignisinformationen an	Einzelheiten zur Maschine und zu den übertragenen Daten werden im Fensterbereich **Ereignisse** angezeigt. Die Ereignisstufe, das Transaktionsdatum und die Zeitmeldung werden angezeigt.

Verwalten von Snapshots und Wiederherstellungspunkten

Ein Wiederherstellungspunkt ist eine Sammlung von Snapshots, die auf individuellen Datenträgervolumes erstellt werden und im Repository gespeichert werden. Snapshots erfassen und speichern den Status eines Datenträgervolumes zu einem bestimmten Zeitpunkt, während die Anwendungen, die diese Daten generieren, noch ausgeführt werden. In AppAssure können Sie einen Snapshot erzwingen, Snapshots vorübergehend anhalten, eine Liste von aktuellen Wiederherstellungspunkten im Repository anzeigen, und sie auch, wenn notwendig, löschen. Wiederherstellungspunkte werden dazu verwendet, geschützte Maschinen wiederherzustellen oder ein lokales Dateisystem bereitzustellen.

Die von AppAssure erfassten Snapshots werden auf Blockebene erstellt und sind anwendungsspezifisch. Dies bedeutet, dass alle offenen Transaktionen und laufenden Transaktionsprotokolle abgeschlossen und die Cache-Speicher auf dem Datenträger abgelegt werden, bevor der Snapshot erstellt wird.

AppAssure verwendet einen Low-Level-Volume-Filtertreiber, der an die bereitgestellten Volumes angefügt wird und dann alle Änderungen auf Blockebene für den nächsten bevorstehenden Snapshot nachverfolgt. Mithilfe der Microsoft Volume Shadow Services (VSS) (Microsoft Volumeschatten-Dienste (VSS)) werden anwendungsausfallbeständige Snapshots ermöglicht.

Anzeigen von Wiederherstellungspunkten

So zeigen Sie Wiederherstellungspunkte an:

1. Wählen Sie im linken Navigationsbereich der Core Console die Maschine aus, für die Sie Wiederherstellungspunkte anzeigen möchten, und klicken Sie dann auf die Registerkarte **Recovery Points** (Wiederherstellungspunkte).

Sie können die in der folgenden Tabelle beschriebenen Informationen über die Wiederherstellungspunkte für die Maschine anzeigen:

Info	Beschreibung
Status	Zeigt den aktuellen Status des Wiederherstellungspunkts an.
Verschlüsselt	Zeigt an, ob der Wiederherstellungspunkt verschlüsselt ist.
Inhalt	Zeigt eine Liste der im Wiederherstellungspunkt eingeschlossenen Volumes an.
Typ	Definiert den Typ des Wiederherstellungspunkts entweder als Base oder Differenzial.
Erstellungsdatum	Zeigt das Datum an, an dem der Wiederherstellungspunkt erstellt wurde.
Größe	Zeigt die Speicherplatzmenge an, die der Wiederherstellungspunkt in dem Repository belegt.

Anzeigen eines bestimmten Wiederherstellungspunkts

So zeigen Sie einen bestimmten Wiederherstellungspunkt an

1. Wählen Sie im linken Navigationsbereich der Core Console die Maschine aus, für die Sie Wiederherstellungspunkte anzeigen möchten, und wählen Sie dann die Registerkarte **Wiederherstellungspunkte** aus.
2. Klicken Sie auf **>** neben einem Wiederherstellungspunkt in der Liste, um die Ansicht zu erweitern.
   Sie können ausführlichere Informationen über den Inhalt des Wiederherstellungspunkts für die ausgewählte Maschine anzeigen, sowie Zugriff auf verschiedene Vorgänge erhalten, die auf dem Wiederherstellungspunkt durchgeführt werden können, wie in der folgenden Tabelle beschrieben:

Info	Beschreibung
Maßnahmen	Das Menü **Actions(Maßnahmen)** schließt die folgenden Vorgänge ein, die sie auf dem ausgewählten Wiederherstellungspunkt ausführen können: **Mount** (Bereitstellen) – Wählen Sie diese Option aus, um den ausgewählten Wiederherstellungspunkt bereitzustellen. Weitere Informationen zum Bereitstellen eines ausgewählten Wiederherstellungspunktes finden Sie unter Bereitstellen eines Wiederherstellungspunktes für eine Windows-Maschine. **Exportieren** – Mithilfe der Exportoption können Sie den ausgewählten Wiederherstellungspunkt in ESXi, auf eine VMWare Workstation oder in HyperV exportieren. Weitere Informationen zum Exportieren eines ausgewählten Wiederherstellungspunkts finden Sie unter Exportieren von Sicherungsinformationen für Ihre Windows-Maschine auf eine virtuelle Maschine. **Rollback** – Wählen Sie diese Option aus, um eine Wiederherstellung von dem ausgewählten Wiederherstellungspunkt auf ein von Ihnen angegebenes Volume durchzuführen. Weitere Informationen zum Ausführen von Wiederherstellungen von ausgewählten Wiederherstellungspunkten finden Sie unter Starten eines Wiederherstellungsvorgangs vom AppAssure-Kern.

3. Klicken Sie auf **>** neben einem Wiederherstellungspunkt in der Liste, um die Ansicht zu erweitern.

Sie können die in der folgenden Tabelle beschriebenen Informationen über die erweiterten Wiederherstellungspunkte für die ausgewählten Volumes anzeigen.

Textfeld	Beschreibung
Titel	Zeigt das spezifische Volume im Wiederherstellungspunkt an.
Raw Capacity (Roh-Kapazität)	Zeigt die Menge des zur Verfügung stehenden rohen Speicherplatzes auf dem ganzen Volume an.
Formatierte Kapazität	Zeigt die Menge des zur Verfügung stehenden Speicherplatzes auf dem Volume an, das für Daten verfügbar ist, nachdem das Volume formatiert wurde.
Verwendete Kapazität	Zeigt die Menge des zur Verfügung stehenden Speicherplatzes an, der aktuell auf dem Volume verwendet wird.

Bereitstellen eines Wiederherstellungspunkts für eine Windows-Maschine

In AppAssure können Sie einen Wiederherstellungspunkt für eine Windows-Maschine bereitstellen, um über ein lokales Dateisystem auf gespeicherte Daten zuzugreifen.

So stellen Sie einen Wiederherstellungspunkt für eine Windows-Maschine bereit:

1. Führen Sie in der Core Console eine der folgenden Maßnahmen aus:
   - Wählen Sie die Registerkarte **Machines** (Maschinen) aus.

     a. Wählen Sie im Drop-Down-Menü neben der Maschine oder dem Cluster mit dem Wiederherstellungspunkt, den Sie bereitstellen möchten, von der Registerkarte **Actions** (Maßnahmen) **Mount** (Bereitstellen) aus.
     b. Wählen Sie aus der Liste im Dialogfeld **Mount Recovery Point** (Wiederherstellungspunkt bereitstellen) einen Wiederherstellungspunkt aus, und klicken Sie dann auf **Next** (Weiter).

     Das Dialogfeld **Wiederherstellungspunkte bereitstellen** wird angezeigt.
   - Wählen Sie in der Core Console die Maschine aus, die Sie auf einem lokalen Dateisystem bereitstellen möchten.

     Die Registerkarte **Summary** (Zusammenfassung) wird für die ausgewählte Maschine angezeigt.

     a. Wählen Sie die Registerkarte **Recovery Points** (Wiederherstellungspunkte) aus.
     b. Erweitern Sie in der Liste der Wiederherstellungspunkte den Wiederherstellungspunkt, den Sie bereitstellen möchten.
     c. Klicken Sie in den erweiterten Details für diesen Wiederherstellungspunkt auf **Mount** (Bereitstellen).

     Das Dialogfeld **Wiederherstellungspunkte bereitstellen** wird angezeigt.
2. Bearbeiten Sie im Dialogfeld **Mount** (Bereitstellen) die Textfelder für die Bereitstellung eines Wiederherstellungspunkts, wie in der folgenden Tabelle beschrieben:

Textfeld	Beschreibung
Mount Location: Local Folder (Bereitstellungsort: lokaler Ordner)	Gibt den Pfad an, der für den Zugriff auf den bereitgestellten Wiederherstellungspunkt verwendet wird.

Textfeld	Beschreibung
Volume Images (Volume-Abbilder)	Geben Sie die Volume-Abbilder an, die Sie bereitstellen möchten.
Mount Type (Bereitstellungstyp)	Gibt an, wie auf Daten für den bereitgestellten Wiederherstellungspunkt zugegriffen werden kann: • Mount Read-only (Schreibgeschützt bereitstellen). • Mount Read-only with previous writes (Schreibgeschützt mit vorherigen Schreibvorgängen bereitstellen). • Mount Writable (Mit Schreibzugriff bereitstellen).
Erstellen Sie eine Windows-Freigabe für diese Bereitstellung	(Optional) Aktivieren Sie das Kontrollkästchen, um festzulegen, ob der bereitgestellte Wiederherstellungspunkt freigegeben wird, und legen Sie dann Zugriffsrechte dafür fest, einschließlich Freigabename und Zugriffsgruppen.

3. Klicken Sie auf **Mount** (Bereitstellen), um den Wiederherstellungspunkt bereitzustellen.

Entfernen der Bereitstellung ausgewählter Wiederherstellungspunkte

Sie können die Bereitstellung ausgewählter Wiederherstellungspunkte entfernen, die lokal auf dem Kern bereitgestellt sind.

So entfernen Sie die Bereitstellung ausgewählter Wiederherstellungspunkte

1. Wählen Sie in der Core Console die Registerkarte **Extras** aus.
2. Klicken Sie unter **Tools** (Extras) auf die Option **System Info** (Systeminformationen).
3. Suchen und wählen Sie die bereitgestellte Anzeige für den Wiederherstellungspunkt, dessen Bereitstellung Sie entfernen möchten, und klicken Sie dann auf **Dismount** (Bereitstellung entfernen).

Entfernen der Bereitstellung aller Wiederherstellungspunkte

Sie können die Bereitstellung aller Wiederherstellungspunkte entfernen, die lokal auf dem Kern bereitgestellt sind.

So entfernen Sie die Bereitstellung aller Wiederherstellungspunkte:

1. Wählen Sie in der Core Console die Registerkarte **Extras** aus.
2. Klicken Sie unter **Tools** (Extras) auf die Option **System Info** (Systeminformationen).
3. Klicken Sie im Bereich **Local Mounts** (Lokale Bereitstellungen) auf **Dismount All** (Alle Bereitstellungen entfernen).

Bereitstellen eines Wiederherstellungspunkts für eine Linux-Maschine

1. Erstellen Sie ein neues Verzeichnis für die Bereitstellung eines Wiederherstellungspunkts (Sie können zum Beistpiel den Befehl `mkdir` verwenden).
2. Versichern Sie sich, dass das Verzeichnis vorhanden ist (Sie können zum Beispiel den Befehl `ls` verwenden).
3. Führen Sie das Dienstprogramm AppAssure **aamount** als Stamm oder als Superbenutzer aus, wie zum Beispiel:

   ```
   sudo aamount
   ```

4. Geben Sie den folgenden Befehl bei der AppAssure Bereitstellungsaufforderung ein, um die geschützten Maschinen aufzulisten.

   `lm`

5. Wenn Sie dazu aufgefordert werden, geben Sie die IP-Adresse oder den Hostnamen Ihres AppAssure-Kernservers an.
6. Geben Sie die Anmeldeinformationen für den Kernserver ein, das heißt, den Benutzernamen und das Kennwort.

   Eine Liste wird angezeigt, welche die von diesem AppAssure-Server geschützten Maschinen anzeigt. Sie listet die gefundenen Maschinen mit deren Zeilenobjektnummer, Host/IP-Adresse und einer ID-Nummer für die Maschine auf. (Beispiel: `293cc667-44b4-48ab-91d8-44bc74252a4f`).

7. Geben Sie den folgenden Befehl ein, um die aktuell bereitgestellten Wiederherstellungspunkte für eine bestimmte Maschine aufzulisten:

   `lr <line_number_of_machine>`

   ANMERKUNG: MIt diesem Befehl können Sie auch die ID-Nummer anstatt der Zeilenobjektnummer der Maschine eingeben.

   Eine Liste, die die grundlegenden und inkrementellen Wiederherstellungspunkte für diese Maschine anzeigt, wird angezeigt. Diese Liste schließt die Zeilenobjektnummer, den Datum/Zeitstempel, den Speicherort des Volumes, die Größe des Wiederherstellungspunkts und eine ID-Nummer für das Volume ein, das am Ende eine Sequenznummer einschließt (zum Beispiel, `293cc667-44b4-48ab-91d8-44bc74252a4f:2`), welche den Wiederherstellungspunkt identifiziert.

8. Geben Sie den folgenden Befehl ein, um den bestimmten Wiederherstellungspunkt am angegebenen Pfad für den Bereitstellungspunkt auszuwählen und bereitzustellen.

   `m <volume_recovery_point_ID_number> <path>`

   ANMERKUNG: Um den Wiederherstellungspunkt zu identifizieren, können Sie in dem Befehl auch eine Zeilennummer anstatt der ID-Nummer des Wiederherstellungspunkts festlegen. Verwenden Sie in diesem Fall die Zeilennummer des Agenten/der Maschine (von der Im Ausgabe), gefolgt von der Zeilennummer des Wiederherstellungspunkts und des Buchstabens des Volumes, gefolgt vom Pfad, wie, `m <machine_line_number> <recovery_point_line_number> <volume_letter> <path>`. Wenn zum Beispiel die Ausgabe `lm` drei Agentenmaschinen auflistet und Sie den Befehl `lr` für Nummer 2 eingeben und das Volume B mit 23 Wiederherstellungspunkten auf **/tmp/mount_dir** bereitstellen, dann heißt der Befehl: `m 2 23 b /tmp/mount_dir`.

   VORSICHT: Sie dürfen die Bereitstellung für ein geschütztes Linux-Volume nicht manuell aufheben. Falls Sie dies tun müssen, müssen Sie vor der Aufhebung der Bereitstellung des Volumes den folgenden Befehl ausführen: `bsctl -d <path to volume>`. In diesem Befehl bezieht sich `<path to volume>` nicht auf den Bereitstellungspunkt des Volumes, sondern er bezieht sich auf den Beschreiber der Datei oder des Volumes; welches in einer ähnlichen Form wie dieses Beispiel sein muss: /dev/sda1.

Entfernen von Wiederherstellungspunkten

Sie können Wiederherstellungspunkte für eine bestimmte Maschine einfach aus dem Repository entfernen. Beim Löschen von Wiederherstellungspunkten in AppAssure können Sie eine der folgenden Optionen angeben:

Textfeld	Beschreibung
Delete All Recovery Points(Alle Wiederherstellungspunkte löschen)	Entfernt alle Wiederherstellungspunkte für die ausgewählte Agentenmaschine aus dem Repository.
Delete a Range of Recovery Points (Einen Bereich an Wiederherstellungspunkten löschen)	Entfernt alle Wiederherstellungspunkte in einem angegebenen Bereich vor dem aktuellen, bis hin zum und einschließlich des aktuellen Basisabbilds, das alle Daten auf der Maschine umfasst, sowie alle Wiederherstellungspunkte nach dem aktuellen bis hin zum nächsten Basisabbild.

ANMERKUNG: Die von Ihnen gelöschten Wiederherstellungspunkte können nicht wiederhergestellt werden.

So entfernen Sie Wiederherstellungspunkte:

1. Wählen Sie im linken Navigationsbereich der Core Console die Maschine aus, für die Sie Wiederherstellungspunkte anzeigen möchten, und klicken Sie dann auf die Registerkarte **Recovery Points** (Wiederherstellungspunkte).
2. Klicken Sie auf das Menü **Actions** (Maßnahmen).
3. Wählen Sie eine der folgenden Optionen:
   - Um alle derzeit gespeicherten Wiederherstellungspunkte zu löschen, klicken Sie auf **Delete All** (Alle löschen).
   - Zum Löschen eines Satzes von Wiederherstellungspunkten in einem bestimmten Datenbereich klicken Sie auf **Bereich löschen**. Das Dialogfeld **Löschen** wird angezeigt. Geben Sie im Dialogfeld **Bereich löschen** den Bereich von Wiederherstellungspunkten an, den Sie löschen möchten. Legen Sie dazu ein Startdatum und eine Startzeit sowie ein Enddatum und eine Endzeit fest, und klicken Sie dann auf **Löschen**.

Löschen einer verwaisten Wiederherstellungspunkt-Kette

Ein verwaister Wiederherstellungspunkt ist ein inkrementeller Snapshot, der keinem Basisabbild zugeordnet ist. Nachfolgende Schnapshots werden weiterhin auf diesem Wiederherstellungspunkt erstellt. Ohne das Basisabbild sind die resultierenden Wiederherstellungspunkte unvollständig und es ist unwahrscheinlich, dass sie die erforderlichen Daten für die Durchführung einer Wiederherstellung enthalten. Diese Wiederherstellungspunkte werden als Teil der verwaisten Wiederherstellungspunkt-Kette angesehen. Wenn diese Situation eintritt, besteht die beste Lösung in der Löschung der Kette und der Erstellung eines neuen Basisabbilds.

ANMERKUNG: Die Fähigkeit zum Löschen einer verwaisten Wiederherstellungspunkt-Kette ist für replizierte Wiederherstellungspunkte auf einem Zielkern nicht verfügbar.

So löschen Sie eine verwaiste Wiederherstellungspunkt-Kette:

1. Wählen Sie auf der Core Console die geschützte Maschine aus, für die Sie die Kette mit verwaisten Wiederherstellungspunkten löschen möchten.
2. Klicken Sie auf die Registerkarte **Recovery Points** (Wiederherstellungspunkte).
3. Erweitern Sie unter **Recovery Points** (Wiederherstellungspunkte) den verwaisten Wiederherstellungspunkt.

   Dieser Wiederherstellungspunkt wird in der Spalte **Type** (Typ) als **Incremental Orphaned** (Inkrementell verwaist) bezeichnet.
4. Klicken Sie neben **Actions** (Maßnahmen) auf **Settings** (Einstellungen).

   Das Fenster **Wiederherstellungspunkte löschen** wird angezeigt.

5. Klicken Sie im Fenster **Delete Recovery Points** (Wiederherstellungspunkte löschen) auf **Yes** (Ja).

   VORSICHT: Wenn Sie diesen Wiederherstellungspunkt löschen, wird die ganze Kette der Wiederherstellungspunkte, einschließlich aller inkrementeller Wiederherstellungspunkte, die vorher oder nachher auftreten, bis zum letzten Basisabbild gelöscht. Dieser Vorgang kann nicht rückgängig gemacht werden.

   Die verwaiste Wiederherstellungspunkt-Kette ist gelöscht.

Erzwingen eines Snapshots

Durch das Erzwingen eines Snapshots können Sie eine Datenübertragung für die aktuelle geschützte Maschine erzwingen. Wenn Sie einen Snapshot erzwingen, wird die Übertragung entweder sofort gestartet oder zur Warteschlange hinzugefügt. Dabei werden nur die Daten übertragen, die seit einem vorherigen Wiederherstellungspunkt geändert wurden. Wenn kein früherer Wiederherstellungspunkt verfügbar ist, werden alle Daten auf den geschützten Volumes übertragen. Dies wird auch als Basisimage bezeichnet.

So erzwingen Sie einen Snapshot

1. Klicken Sie in der Core Console auf die Registerkarte **Maschinen**, und wählen Sie dann in der Liste der geschützten Maschinen die Maschine oder den Cluster mit dem Wiederherstellungspunkt aus, für die/den Sie Snapshots erzwingen möchten.
2. Klicken Sie auf das Drop-Down-Menü **Actions** (Maßnahmen) für diese Maschine und anschließend klicken Sie auf **Force Snapshot** (Snapshot erzwingen), und wählen Sie dann eine der in der unten beschriebenen Optionen aus.
   - **Force Snapshot** (Snapshot erzwingen) – Erstellt einen inkrementellen Snapshot der Daten, die seit der Erstellung des letzten Snapshots aktualisiert wurden.
   - **Force Base Image** (Basisabbild erzwingen) – Erstellt einen kompletten Snapshot der Daten auf den Volumes der Maschine.
3. Wenn die Benachrichtigung in Dialogfeldfenster **Transfer Status** (Übertragungsstatus) angezeigt wird, dass der Snapshot in die Warteschlange gestellt wurde, klicken Sie auf **OK**.

   Auf der Registerkarte **Machinen** erscheint neben der Maschine eine Fortschrittsanzeige, um den Fortschritt des Snapshots anzuzeigen.

Anhalten und Wiederaufnehmen des Schutzes

Wenn Sie den Schutz anhalten, unterbrechen Sie vorübergehend alle Übertragungen der Daten von der aktuellen Maschine.

So halten Sie den Schutz an und setzen Sie ihn fort:

1. Klicken Sie in der Core Console auf die Registerkarte **Machines** (Maschinen).
2. Wählen Sie die Maschine aus, für die Sie den Schutz anhalten möchten.

   Die Registerkarte **Zusammenfassung** wird für diese Maschine angezeigt.
3. Klicken Sie im Drop-Down-Menü **Actions** (Maßnahmen) für diese Maschine auf **Pause** (Anhalten).
4. Um den Schutz fortzusetzen, klicken Sie im Menü **Actions** (Maßnahmen) auf **Resume** (Fortsetzen).

Wiederherstellen von Daten

Sie können Daten umgehend auf Ihren physischen Maschinen (Windows- oder Linux-Maschinen) oder, im Falle von Windows-Maschinen, auf virtuellen Maschinen anhand von gespeicherten Wiederherstellungspunkten wiederherstellen. Die in diesem Abschnitt behandelten Themen beschreiben,

wie Sie einen spezifischen Wiederherstellungspunkt für Windows-Maschinen auf eine virtuelle Maschine exportieren oder ein Rollback von einer Maschine auf einen früheren Wiederherstellungspunkt durchführen.

Wenn Sie zwischen zwei Kernen (Quelle und Ziel) die Replikation eingerichtet haben, können sie Daten erst vom Zielkern exportieren, nachdem die erste Replikation abgeschlossen ist. Weitere Details finden Sie unter Replizieren von Agentendaten auf einer Maschine.

ANMERKUNG: Windows 8- und Windows Server 2012-Betriebssysteme, die von FAT32-EFI-Partitionen gestartet werden, sind für Schutz oder Wiederherstellung nicht verfügbar; das gleiche gilt für ReFS-Volumes (Resilient File System).

Backup

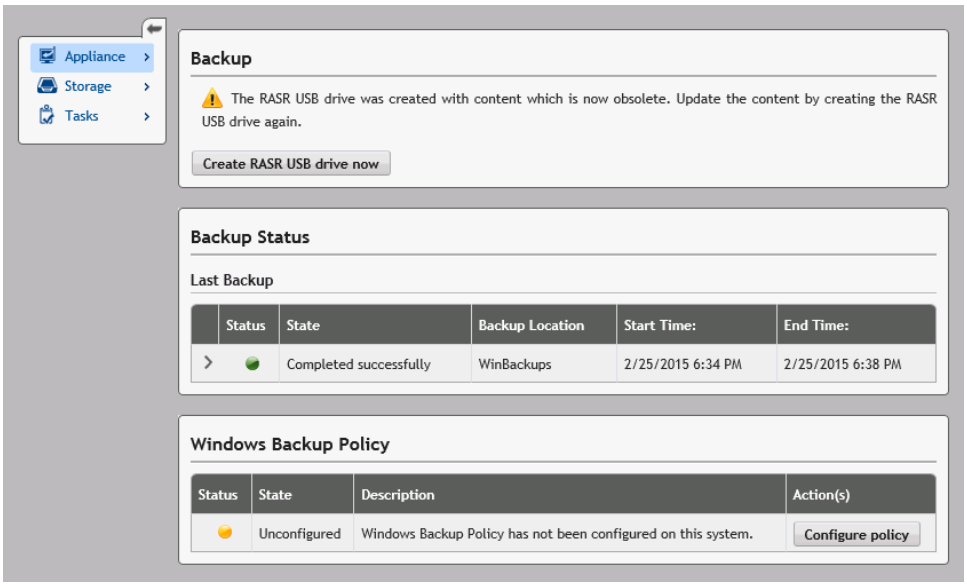
Mit der Backup-Registerkarte können Sie die Backup-Richtlinie konfigurieren und das System über den RASR USB-Schlüssel oder IDSDM wiederherstellen. Um diese Funktion zu verwenden, muss das Windows-Backup der virtuellen Festplatte vorhanden sein. Das Windows-Backup der virtuellen Festplatte wird während des **AppAssure Appliance Configuration Wizard** (AppAssure-Gerätekonfigurationsassistent) ausgeführt. Weitere Informationen finden Sie unter „Rapid Appliance Self Recovery" (Geräte-Schnellselbstwiederherstellung) im *Dell DL43000 Appliance Deployment Guide* (Dell DL43000 Gerät-Bereitstellungshandbuch). Ohne Windows-Backup der virtuellen Festplatte können Sie keine Richtlinie ändern oder Windows-Backups erstellen.

Backup-Status

Der Backup-Status von Microsoft Windows ist in der Registerkarte **Last Backup** (Letztes Backup) verfügbar. Wenn derzeit ein Backup ausgeführt wird, werden die Informationen in der Registerkarte **Current Backup** (Aktuelles Backup) angezeigt. Führen Sie die folgenden Schritte aus, um das letzte Backup anzuzeigen:

1. Navigieren Sie in Core Console zur Registerkarte **Appliance (Gerät)** → **Backup**.
2. Klicken Sie auf den Pfeil neben der Schaltfläche **Status**, um den Status des Backups anzuzeigen.
3. Das Fenster **Last Backup** (Letztes Backup) zeigt die folgenden Informationen an:
   - Status
   - Zustand
   - Backup-Speicherort
   - Startzeit
   - Endzeit
   - Fehlerbeschreibung
   - Gesicherte Elemente

   ANMERKUNG: Die oben genannten Informationen werden angezeigt, ob die Windows Backup-Richtlinie ausgeführt wird oder nicht.



Wenn ein Backup ausgeführt wird, werden **Current Backup Progress** (Aktueller Backup-Fortschritt) und **Start Time** (Startzeit) angezeigt.

Windows-Backup-Richtlinie

Führen Sie zum Konfigurieren einer Windows-Backup-Richtlinie folgende Schritte aus:

1. Navigieren Sie in Core Console zu **Appliance (Gerät)** → **Backup**.
2. Klicken Sie auf die Schaltfläche **Configure Policy** (Richtlinie konfigurieren).
   Das Fenster **Windows Backup Policy** (Windows-Backup-Richtlinie) wird angezeigt.
3. Geben Sie die Parameter wie nachfolgend beschrieben ein:

Textfeld	Beschreibung
Folgende Elemente werden gesichert:	• OS(C:) • WIEDERHERSTELLUNG • Bare-Metal-Wiederherstellung • Systemzustand Alle oben genannten Optionen sind per Standardeinstellung ausgewählt.
Wählen Sie den Zeitpunkt für das Backup aus:	Geben Sie den Zeitpunkt für das Backup ein:

4. Klicken Sie auf **Configure** (Konfigurieren).
   Nach der Konfiguration stehen Ihnen folgende Optionen zur Verfügung: **Backup now** (Jetzt sichern) **Delete policy** (Richtlinie löschen) oder **View policy** (Richtlinie anzeigen), die Sie im Fenster **Windows Backup Policy** (Windows-Backup-Richtlinie) auswählen können.

Über das Exportieren geschützter Daten von Windows-Maschinen auf virtuelle Maschinen

AppAssure unterstützt einen einmaligen oder einen dauerhaften Export (um virtuellen Standby zu unterstützen) 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 und dann eine Wiederherstellung ausführen.

Das folgende Diagramm zeigt eine typische Bereitstellung für das Exportieren von Daten auf eine virtuelle Maschine.

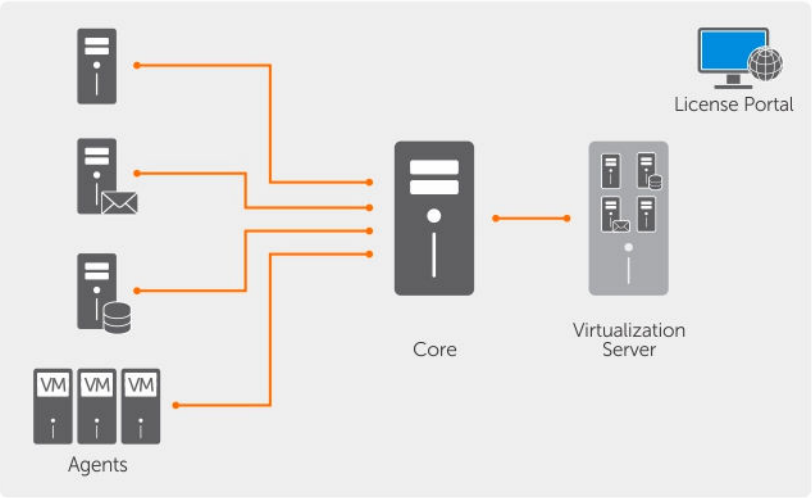


Abbildung 9. Exportieren von Daten auf eine virtuelle Maschine

Sie können einen virtuellen Standby durch das fortlaufende Exportieren geschützter Daten von Ihrer Windows-Maschine auf eine virtuelle Maschine erstellen. Wenn Sie auf eine virtuelle Maschine exportieren, werden alle Backupdaten von einem Wiederherstellungspunkt, als auch die Parameter, die für den Schutzzeitplan für die Maschine definiert wurden, exportiert.

Sie können einen virtuellen Export der Wiederherstellungspunkte der geschützten Windows- oder Linuxmaschinen nach VMware, ESXi, Hyper-V und Oracle VirtualBox durchführen.

ANMERKUNG: Die Registerkarte „Appliance“ (Gerät) zeigt alle virtuellen Maschinen an, unterstützt aber nur die Verwaltung von Hyper-V und virtuellen ESXi-Maschinen. Verwenden Sie die Hypervisor-Management-Tools, um die anderen virtuellen Maschinen zu verwalten.

ANMERKUNG: Die virtuelle Maschine, auf die Sie exportieren, muss eine lizenzierte Version von ESXi, VMWare Workstation, oder Hyper-V sein, und keine Test- oder Gratisversion.

Einschränkungen der Unterstützung von dynamischen Volumes und Basisvolumes

AppAssure unterstützt das Erstellen von Snapshots auf allen dynamischen Volumes und Basisvolumes. AppAssure unterstützt außerdem das Exportieren von einfachen dynamischen Volumes, die auf einem einzigen physischen Laufwerk vorhanden sind. Wie ihr Name bereits sagt, sind einfache dynamische Volumes weder gestriped, noch gespiegelt oder verteilt. Nicht einfache dynamische Volumes haben

willkürliche Festplattengeometrien, die nicht vollständig interpretiert und daher nicht exportiert werden können. AppAssure kann komplexe oder nicht einfache dynamische Volumes exportieren.

AppAssure Version 5.3.1.60393 hat in der Benutzerschnittstelle ein Kontrollkästchen hinzugefügt, das Sie darüber informiert, dass Exporte auf einfache dynamische Volumes beschränkt sind. Bevor die Benutzerschnittstelle mit dieser Version geändert wurde, erschien die Option des Exportieren von komplexen oder nicht-einfachen dynamischen Datenträgern als ob sie eine Option wäre. Wenn Sie versucht hätten, auf diese Platten zu exportieren, wäre der Export-Job fehlgeschlagen.

Exportieren von Backupinformationen von der Microsoft Windows-Maschine auf eine virtuelle Maschine

In AppAssure können Sie Daten von Ihren Microsoft Windows-Maschinen auf eine virtuelle Maschine (VMware, ESXi, Hyper-V und Oracle VirtualBox) exportieren, indem Sie alle Backupinformationen aus einem Wiederherstellungspunkt sowie die für den Schutzzeitplan für Ihre Maschine definierten Parameter exportieren.

So exportieren Sie Windows-Sicherungsinformationen in eine virtuelle Maschine:

1. Klicken Sie in der Core Console auf die Registerkarte **Machines** (Maschinen).
2. Wählen Sie in der Liste der geschützten Maschinen die Maschine oder den Cluster mit dem Wiederherstellungspunkt aus, die Sie exportieren möchten.
3. Klicken Sie im Drop-Down-Menü **Actions** (Maßnahmen) für diese Maschine auf **Export** (Exportieren), und wählen Sie dann die Art des Exports aus, den Sie durchführen möchten. Folgende Optionen stehen zur Auswahl:
   - ESXi-Export
   - VMWare Workstation-Export
   - Hyper-V-Export
   - Oracle VirtualBox-Export

   Daraufhin wird das Dialogfeld **Exporttyp auswählen** angezeigt.

Exportieren von Windows-Daten über die Option „ESXi Export“ (ESXi-Export)

In AppAssure können Sie wählen, Daten über die Option „ESXi Export“ (ESXi-Export) zu exportieren, indem Sie einen einmaligen oder dauerhaften Export ausführen.

Durchführen eines einmaligen ESXi-Exports

So führen Sie einen einmaligen ESXi-Export aus:

1. Klicken Sie im Dialogfeld **Select Export Type** (Exporttyp auswählen) auf **One-time export** (Einmaliger Export).
2. Klicken Sie auf **Weiter**.

   Das Dialogfeld **ESXi-Export – Wiederherstellungspunkt auswählen** wird angezeigt.
3. Wählen Sie einen Wiederherstellungspunkt zum Exportieren aus und klicken Sie dann auf **Next** (Weiter).

   Das Dialogfeld **Virtueller Standby-Wiederherstellungspunkt auf VMware vCenter Server/ESXi** wird angezeigt.

Definieren von Informationen für virtuelle Maschinen zum Durchführen eines ESXi-Exports

So definieren Sie Informationen für virtuelle Maschinen zum Ausführen eines ESXi-Exports:

1. Geben Sie über das Dialogfeld **Virtual Standby Recovery Point to VMware vCenter Server/ESXi** (Virtueller Standby-Wiederherstellungspunkt auf VMware vCenter Server/ESXi) die Parameter für den Zugriff auf die virtuelle Maschine gemäß der folgenden Tabelle ein.

Textfeld	Beschreibung
Host-Name	Geben Sie einen Hostnamen für die Maschine ein.
Schnittstelle	Geben Sie die Schnittstelle für die Host-Maschine ein. Die Standardschnittstellennummer ist 443.
Benutzername	Geben Sie die Anmeldeinformationen für die Host-Maschine ein.
Kennwort	Geben Sie die Anmeldeinformationen für die Host-Maschine ein.

2. Klicken Sie auf **Verbinden**.

Ausführen eines dauerhaften ESXi-Exports (virtueller Standby)

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

1. Klicken Sie im Dialogfeld **Select Export Type** (Exporttyp auswählen) auf **Continuous (Virtual Standby)** (Dauerhaft (Virtueller Standby)).
2. Klicken Sie auf **Weiter**.

   Daraufhin wird das Dialogfeld **Virtual Standby Recovery Point to VMware vCenter Server/ESXi** (Virtueller Standby-Wiederherstellungspunkt auf VMware vCenter Server/ESXi) angezeigt.
3. Geben Sie die Parameter zum Zugriff auf die virtuelle Maschine wie nachfolgend beschrieben ein.

Textfeld	Beschreibung
Host-Name	Geben Sie einen Hostnamen für die Maschine ein.
Schnittstelle	Geben Sie die Schnittstelle für die Host-Maschine ein. Die Standardschnittstellennummer ist 443.
Benutzername	Geben Sie die Anmeldeinformationen für die Host-Maschine ein.
Kennwort	Geben Sie die Anmeldeinformationen für die Host-Maschine ein.

4. Klicken Sie auf Verbinden.
5. Geben Sie auf der Registerkarte **Options** (Optionen) die Informationen für die virtuelle Maschine wie beschrieben ein.

Textfeld	Beschreibung
Virtual Machine Name (Name der virtuellen Maschine)	Geben Sie den Namen für die zu erstellende virtuelle Maschine ein, z. B. VM-0A1B2C3D4. ANMERKUNG: Es wird empfohlen, einen Namen zu verwenden, der vom Agentennamen abgeleitet ist oder mit dem Namen des Agenten übereinstimmt. Sie können auch einen Namen erstellen, der von dem Hypervisor-Typ, der IP-Adresse oder dem DNS-Namen abgeleitet ist.

Textfeld	Beschreibung
Speicher	Geben Sie die Speichernutzung an. Folgende Optionen stehen zur Auswahl: • Gleiche RAM-Größe verwenden wie Quellmaschine • Klicken Sie auf **Use a specific amount of RAM** (Eine bestimmte RAM-Größe verwenden), um anzugeben, wie viel RAM verwendet werden soll. Zum Beispiel: 4096 MB. Die kleinste zulässige Größe ist 512 MB. Die maximale Größe wird durch das Fassungsvermögen und die Begrenzungen der Host-Maschinen bestimmt. (Empfohlen)
ESXi Datacenter (ESXi-Rechenzentrum)	Geben Sie den Namen für das ESXi-Rechenzentrum ein.
ESXi Host (ESXi-Host)	Geben Sie die Anmeldeinformationen für den ESXi-Host ein.
Data Store (Datenspeicher)	Geben Sie die Details für den Datenspeicher ein.
Version	Wählen Sie die Version der virtuellen Maschine aus. ANMERKUNG: Um den vSphere-Client zur Verwaltung von virtuellen Maschinen zu verwenden, wählen Sie die Version 8 oder früher.
Resource Pool (Ressourcenpool)	Geben Sie den Namen für den Ressourcenpool ein.

6. Klicken Sie auf **Start Export** (Export starten).

Exportieren von Windows-Daten über die Option „VMware Workstation Export“ (VMware Workstation-Export)

In AppAssure können Sie wählen, Daten über die Option „VMware Workstation Export“ (VMware Workstation-Export) zu exportieren, indem Sie einen einmaligen oder dauerhaften Export ausführen. Führen Sie die Schritte in den folgenden Verfahren aus, um einen Export über die Option „VMware Workstation Export“ (VMware Workstation-Export) für den entsprechenden Exporttyp durchzuführen.

Ausführen eines einmaligen VMware Workstation-Exports

So führen Sie einen einmaligen VMware Workstation-Export aus:

1. Klicken Sie im Dialogfeld **Select Export Type** (Exporttyp auswählen) auf **One-time export** (Einmaliger Export).
2. Klicken Sie auf **Next** (Weiter).

   Das Dialogfeld **VM Export - Select Recovery Point** (VM-Export – Wiederherstellungspunkt auswählen) wird angezeigt.
3. Wählen Sie einen Wiederherstellungspunkt zum Exportieren aus und klicken Sie dann auf **Next** (Weiter).

   Das Dialogfeld **Virtual Standby Recovery Point to VMware Workstation/Server** (Virtueller Standby-Wiederherstellungspunkt auf VMware Workstation/Server) wird angezeigt.

Definieren von einmaligen Einstellungen für das Ausführen eines VMware Workstation-Exports

So definieren Sie die einmaligen Einstellungen für das Ausführen eines VMware Workstation-Exports:

1. Geben Sie über das Dialogfeld **Virtual Standby Recovery Point to VMware Workstation/Server** (Virtueller Standby-Wiederherstellungspunkt auf VMware Server/Server) die Parameter für den Zugriff auf die virtuelle Maschine wie nachfolgend beschrieben ein.

Textfeld	Beschreibung
Target Path (Zielpfad)	Geben Sie den Pfad des lokalen Ordners oder der Netzwerkfreigabe an, auf dem/der die virtuelle Maschine erstellt werden soll. ANMERKUNG: Wenn Sie einen Netzwerkfreigabepfad angegeben haben, geben Sie gültige Anmeldeinformationen für ein Konto ein, das auf der Zielmaschine registriert ist. Das Konto muss über Lese- und Schreibberechtigungen auf die Netzwerkfreigabe verfügen.
Benutzername	Geben Sie die Anmeldeinformationen für die virtuelle Maschine ein. • Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie einen gültigen Benutzernamen für ein Konto eingeben, der auf der Zielmaschine registriert ist. • Wenn Sie einen lokalen Pfad angegeben haben, ist kein Benutzername erforderlich.
Kennwort	Geben Sie die Anmeldeinformationen für die virtuelle Maschine ein. • Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie ein gültiges Kennwort für ein Konto eingeben, der auf der Zielmaschine registriert ist. • Wenn Sie einen lokalen Pfad angegeben haben, ist kein Kennwort erforderlich.

2. Wählen Sie im Fensterbereich **Export Volumes** (Volumes exportieren) die zu exportierenden Volumes aus, z. B. C:\ und D:\.
3. Geben Sie im Fensterbereich „Options" (Optionen) die Informationen für die virtuelle Maschine und die Speichernutzung gemäß der folgenden Tabelle ein:

Textfeld	Beschreibung
Virtual Machine (Virtuelle Maschine)	Geben Sie den Namen für die zu erstellende virtuelle Maschine ein, z. B. VM-0A1B2C3D4. ANMERKUNG: Es wird empfohlen, einen Namen zu verwenden, der vom Agentennamen abgeleitet ist oder mit dem Namen des Agenten übereinstimmt. Sie können auch einen Namen erstellen, der von dem Hypervisor-Typ, der IP-Adresse oder dem DNS-Namen abgeleitet ist.
Speicher	Geben Sie den Speicher der virtuellen Maschine an. • Klicken Sie auf **Use the same amount of RAM as the source machine** (Die gleiche RAM-Größe wie die Quellmaschine verwenden), um anzugeben, dass die RAM-Konfiguration die gleiche wie auf der Quellmaschine sein soll.

Textfeld	Beschreibung
	• Klicken Sie auf **Use a specific amount of RAM** (Eine bestimmte RAM-Größe verwenden), um anzugeben, wie viel RAM verwendet werden soll. Zum Beispiel: 4096 MB. Die kleinste zulässige Größe ist 512 MB. Die maximale Größe wird durch das Fassungsvermögen und die Begrenzungen der Host-Maschine bestimmt. (Empfohlen)

4. Klicken Sie auf **Export** (Exportieren)

Ausführen eines dauerhaften VMware Workstation-Exports (virtueller Standby)

So führen Sie einen dauerhaften VMware Workstation-Export aus (virtueller Standby):

1. Klicken Sie im Dialogfeld **Select Export Type** (Exporttyp auswählen) zunächst auf **Continuous (Virtual Standby)** (Dauerhaft (virtueller Standby)) und dann auf **Next** (Weiter).

   Das Dialogfeld **VM-Export – Wiederherstellungspunkt auswählen** wird angezeigt.
2. Wählen Sie einen Wiederherstellungspunkt zum Exportieren aus und klicken Sie dann auf **Next** (Weiter).

   Das Dialogfeld **Virtueller Standby-Wiederherstellungspunkt auf VMware Workstation/Server** wird angezeigt.
3. Geben Sie die Parameter zum Zugriff auf die virtuelle Maschine wie nachfolgend beschrieben ein.

Textfeld	Beschreibung
Target Path (Zielpfad)	Geben Sie den Pfad des lokalen Ordners oder der Netzwerkfreigabe an, auf dem/der die virtuelle Maschine erstellt werden soll. ANMERKUNG: Wenn Sie einen Netzwerkfreigabepfad angegeben haben, geben Sie gültige Anmeldeinformationen für ein Konto ein, das auf der Zielmaschine registriert ist. Das Konto muss über Lese- und Schreibberechtigungen auf die Netzwerkfreigabe verfügen.
Benutzername	Geben Sie die Anmeldeinformationen für die virtuelle Maschine ein. • Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie einen gültigen Benutzernamen für ein Konto eingeben, der auf der Zielmaschine registriert ist. • Wenn Sie einen lokalen Pfad angegeben haben, ist kein Benutzername erforderlich.
Kennwort	Geben Sie die Anmeldeinformationen für die virtuelle Maschine ein. • Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie ein gültiges Kennwort für ein Konto eingeben, der auf der Zielmaschine registriert ist. • Wenn Sie einen lokalen Pfad angegeben haben, ist kein Kennwort erforderlich.

4. Wählen Sie im Fensterbereich **Export Volumes** (Volumes exportieren) die zu exportierenden Volumes aus, z. B. C:\ und D:\.
5. Geben Sie im Fensterbereich **Options** (Optionen) die Informationen für die virtuelle Maschine und die Speichernutzung gemäß der folgenden Tabelle ein:

Textfeld	Beschreibung
Virtual Machine (Virtuelle Maschine)	Geben Sie den Namen für die zu erstellende virtuelle Maschine ein, z. B. `VM-0A1B2C3D4`. **ANMERKUNG:** Es wird empfohlen, einen Namen zu verwenden, der vom Agentennamen abgeleitet ist oder mit dem Namen des Agenten übereinstimmt. Sie können auch einen Namen erstellen, der von dem Hypervisor-Typ, der IP-Adresse oder dem DNS-Namen abgeleitet ist.
Speicher	Geben Sie den Speicher der virtuellen Maschine an. • Klicken Sie auf **Use the same amount of RAM as the source machine** (Die gleiche RAM-Größe wie die Quellmaschine verwenden), um anzugeben, dass die RAM-Konfiguration die gleiche wie auf der Quellmaschine sein soll. • Klicken Sie auf **Use a specific amount of RAM** (Eine bestimmte RAM-Größe verwenden), um anzugeben, wie viel RAM verwendet werden soll, zum Beispiel: 4096 MB. Die kleinste zulässige Größe ist 512 MB. Die maximale Größe wird durch das Fassungsvermögen und die Begrenzungen der Host-Maschine bestimmt. (Empfohlen)

6. Klicken Sie zum Testen des Exports der Daten auf **Perform initial ad-hoc export** (Anfänglichen Ad-hoc-Export ausführen).
7. Klicken Sie auf **Speichern**.

Exportieren von Windows-Daten mit Hyper-V-Export

Sie haben die Möglichkeit, Daten über die Option „Hyper-V-Export“ u exportieren, indem Sie einen einmaligen oder dauerhaften Export ausführen. Führen Sie die Schritte in den folgenden Verfahren aus, um einen Export unter Verwendung der Option „Hyper-V-Export“ für den entsprechenden Exporttyp durchzuführen.
Ihr DL-Gerät unterstützt die erste Generation der Hyper-V-Exportfunktion auf folgende Hosts:

- Windows 8
- Windows 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Ihr DL-Gerät unterstützt die zweite Generation der Hyper-V-Exportfunktion auf folgende Hosts:

- Windows 8.1
- Windows Server 2012 R2

ANMERKUNG: Nicht alle geschützten Maschinen können auf Hyper-V-Hosts der zweiten Generation exportiert werden.

Nur geschützte Maschinen mit den folgenden UEFI-Betriebssystemen (Unified Extensible Firmware Interface) unterstützen den virtuellen Export auf Hyper-V-Hosts der zweiten Generation:

- Windows 8 (UEFI)
- Windows 8.1 (UEFI)

- Windows Server 2012 UEFI
- Windows Server 2012 R2 (UEFI)

ANMERKUNG: Der Hyper-V-Export auf eine VM der zweiten Generation kann fehlschlagen, wenn der Hyper-V-Host nicht über ausreichend Arbeitsspeicher verfügt, um den Export durchzuführen.

Führen Sie die Schritte in den folgenden Verfahren für den entsprechenden Exporttyp durch.

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. 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: Lediglich die DL1000-Konfiguration von 3 TB mit 2 VMs unterstützt einmaligen und dauerhaften Export und damit virtuelle Standby-Funktionen.

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.

Textfeld	Beschreibung
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.

Exportieren von Microsoft Windows-Daten mit Oracle VirtualBox-Export

In AppAssure können Sie mit Oracle VirtualBox-Export einen einmaligen oder einen dauerhaften Export (für virtuelles Standby) ausführen.

Führen Sie die Schritte in den folgenden Verfahren für den entsprechenden Exporttyp durch.

ANMERKUNG: Für diese Art von Export müssen Sie Oracle VirtualBox auf der Kernmaschine installieren. VirtualBox Version 4.2.18 oder höher wird von Windows-Hosts unterstützt.

Ausführen eines einmaligen Oracle VirtualBox-Exports

Führen Sie die Schritte in diesem Verfahren aus, um einen einmaligen Export auf Oracle VirtualBox auszuführen.

So führen Sie einen einmaligen Oracle VirtualBox-Export aus

1. Führen Sie in AppAssure Core Console eine der folgenden Maßnahmen aus:
   - Klicken Sie in der Schaltflächenleiste auf **Export** (Exportieren), um den Export-Assistenten zu starten, und führen Sie die folgenden Schritte aus:
     1. Klicken Sie auf der Seite **Select Export Type** (Exporttyp auswählen) auf **One-time export** (Einmaliger Export) und dann auf **Next** (Weiter).
     2. Wählen Sie auf der Seite **Protected Machines** (Geschützte Maschinen) die auf eine virtuelle Maschine zu exportierende geschützte Maschine aus, und klicken Sie dann auf **Next** (Weiter).
   - Navigieren Sie zu der Maschine, die Sie exportieren möchten, und klicken Sie dann auf der Registerkarte **Summary** (Zusammenfassung) im Dropdown-Menü **Actions** (Maßnahmen) dieser Maschine auf **Export** (Exportieren) > **One-time** (Einmalig).

   Der Export Wizard (Assistent für den Export) wird auf der Seite **Recovery Points** (Wiederherstellungspunkte) angezeigt.
2. Wählen Sie auf der Seite **Recovery Points** (Wiederherstellungspunkte) den Wiederherstellungspunkt des AppAssure-Kerns aus, den Sie exportieren möchten, und klicken Sie dann auf **Next** (Weiter).
3. Wählen Sie auf der Seite **Destination** (Ziel) im Export Wizard (Assistenten für den Export) im Dropdown-Menü **Recover to Virtual machine** (Auf virtuelle Maschine wiederherstellen) die Option **VirtualBox** aus, und klicken Sie dann auf **Next** (Weiter).
4. Wählen Sie auf der Seite **Virtual Machine Options** (Optionen für die virtuelle Maschine) die Option **Use Windows machine** (Windows-Maschine verwenden) aus.
5. Geben Sie die Parameter zum Zugriff auf die virtuelle Maschine wie in der folgenden Tabelle beschrieben ein.

Option	Beschreibung
Virtual Machine Name (Name der virtuellen Maschine)	Geben Sie einen Namen für die zu erstellende virtuelle Maschine ein. ANMERKUNG: Der Standardname entspricht dem Namen der Quellmaschine.
Target Path (Zielpfad)	Geben Sie einen lokalen oder Remote-Ziel-Pfad für die Erstellung der virtuellen Maschine an. ANMERKUNG: Der Zielpfad sollte kein Stammverzeichnis sein.

Option	Beschreibung
	Wenn Sie einen Netzwerkfreigabepfad angeben, müssen Sie gültige Anmeldeinformationen (Benutzername und Kennwort) für ein Konto eingeben, das auf der Zielmaschine registriert ist. Das Konto muss über Lese- und Schreibberechtigungen auf die Netzwerkfreigabe verfügen.
Speicher	Geben Sie die Speichernutzung für die virtuelle Maschine ein, indem Sie auf eine der folgenden Optionen klicken: • Klicken Sie auf **Use the same amount of RAM as the source machine** (Die gleiche RAM-Größe wie die Quellmaschine verwenden), um anzugeben, dass die RAM-Konfiguration die gleiche wie auf der Quellmaschine sein soll. • Klicken Sie auf **Use a specific amount of RAM** (Eine bestimmte RAM-Größe verwenden), um anzugeben, wie viel RAM verwendet werden soll, zum Beispiel: 4096 MB. Die kleinste zulässige Größe ist 512 MB. Die maximale Größe wird durch das Fassungsvermögen und die Begrenzungen der Host-Maschine bestimmt. (Empfohlen)

6. Um ein Benutzerkonto für die virtuelle Maschine anzugeben, wählen Sie **Specify the user account for the exported virtual machine** (Das Benutzerkonto für die exportierte virtuelle Maschine eingeben) aus, und geben Sie dann die folgenden Informationen ein. Dies bezieht sich auf ein bestimmtes Benutzerkonto, für das die virtuelle Maschine registriert wird, wenn mehrere Benutzerkonten auf der virtuellen Maschine verfügbar sind. Wenn dieses Benutzerkonto angemeldet wird, wird nur für diesen Benutzer diese virtuelle Maschine im VirtualBox Manager angezeigt. Wenn ein Konto nicht angegeben ist, wird die virtuelle Maschine für alle vorhandenen Benutzer auf der Windows-Maschine mit Oracle VirtualBox registriert.
   - **User Name** (Benutzername) – Geben Sie den Benutzernamen ein, für den die virtuelle Maschine registriert ist.
   - **Password** (Kennwort) – Geben Sie das Kennwort für dieses Benutzerkonto ein.
7. Klicken Sie auf **Weiter**.

   Der Name, den Sie eingeben, erscheint in der Liste der virtuellen Maschinen in der Hyper-V-Manager-Konsole.
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: \.
9. Klicken Sie auf der Seite **Summary** (Zusammenfassung) auf **Finish** (Fertigstellen), 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.

Ausführen eines dauerhaften Oracle VirtualBox-Exports (virtueller Standby)

Führen Sie die Schritte in diesem Verfahren aus, um einen virtuellen Standby zu erstellen und einen dauerhaften Oracle VirtualBox-Export auszuführen.

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

1. Führen Sie in AppAssure Core Console eine der folgenden Maßnahmen aus:
   - Klicken Sie auf der Registerkarte **Virtual Standby** (Virtueller Standby) auf **Add** (Hinzufügen), um den Export Wizard (Assistenten für den Export) zu starten. Wählen Sie auf der Seite **Protected Machines** (Geschützte Maschinen) des Export Wizard (Assistenten für den Export) die zu exportierende geschützte Maschine aus, und klicken Sie dann auf **Next** (Weiter).

- Navigieren Sie zu der Maschine, die Sie exportieren möchten, und klicken Sie auf der Registerkarte **Summary** (Zusammenfassung) im Drop-Down-Menü **Actions** (Maßnahmen) dieser Maschine auf **Export** (Exportieren) > **Virtual Standby** (Virtueller Standby).

2. Wählen Sie auf der Seite **Destination** (Ziel) im Export Wizard (Assistenten für den Export) im Dropdown-Menü **Recover to Virtual machine** (Auf virtuelle Maschine wiederherstellen) die Option **VirtualBox** aus, und klicken Sie dann auf **Next** (Weiter).
3. Wählen Sie auf der Seite **Virtual Machine Options** (Optionen für die virtuelle Maschine) die Option **Use Windows machine** (Windows-Maschine verwenden) aus.
4. Geben Sie die Parameter zum Zugriff auf die virtuelle Maschine wie in der folgenden Tabelle beschrieben ein.

Option	Beschreibung
Virtual Machine Name (Name der virtuellen Maschine)	Geben Sie einen Namen für die zu erstellende virtuelle Maschine ein. ANMERKUNG: Es wird empfohlen, einen Namen zu verwenden, der vom Agentennamen abgeleitet ist oder mit dem Namen des Agenten übereinstimmt. Sie können auch einen Namen erstellen, der von dem Hypervisor-Typ, der IP-Adresse oder dem DNS-Namen abgeleitet ist.
Target Path (Zielpfad)	Geben Sie einen lokalen oder Remote-Ziel-Pfad für die Erstellung der virtuellen Maschine an. ANMERKUNG: Der Zielpfad sollte kein Stammverzeichnis sein. Wenn Sie einen Netzwerkfreigabepfad angeben, müssen Sie gültige Anmeldeinformationen (Benutzername und Kennwort) für ein Konto eingeben, das auf der Zielmaschine registriert ist. Das Konto muss über Lese- und Schreibberechtigungen auf die Netzwerkfreigabe verfügen.
Speicher	Geben Sie die Speichernutzung für die virtuelle Maschine ein, indem Sie auf eine der folgenden Optionen klicken: • Klicken Sie auf **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. • Klicken Sie auf **Use a specific amount of RAM** (Eine bestimmte RAM-Größe verwenden), um anzugeben, wie viel RAM verwendet werden soll, zum Beispiel: 4096 MB. Die kleinste zulässige Größe ist 512 MB. Die maximale Größe wird durch das Fassungsvermögen und die Begrenzungen der Host-Maschine bestimmt. (Empfohlen)

5. Um ein Benutzerkonto für die virtuelle Maschine anzugeben, wählen Sie **Specify the user account for the exported virtual machine** (Das Benutzerkonto für die exportierte virtuelle Maschine eingeben) aus, und geben Sie dann die folgenden Informationen ein. Dies bezieht sich auf ein bestimmtes Benutzerkonto, für das die virtuelle Maschine registriert wird, wenn mehrere Benutzerkonten auf der virtuellen Maschine verfügbar sind. Wenn dieses Benutzerkonto angemeldet wird, wird nur für diesen Benutzer diese virtuelle Maschine im VirtualBox Manager angezeigt. Wenn ein Konto nicht angegeben ist, wird die virtuelle Maschine für alle vorhandenen Benutzer auf der Windows-Maschine mit VirtualBox registriert.
   - **User Name** (Benutzername) – Geben Sie den Benutzernamen ein, für den die virtuelle Maschine registriert ist.
   - **Password** (Kennwort) – Geben Sie das Kennwort für dieses Benutzerkonto ein.
6. Wählen Sie **Perform initial one-time export** (Anfänglichen einmaligen Export ausführen) aus, um den virtuellen Export sofort auszuführen, statt nach dem nächsten geplanten Snapshot.

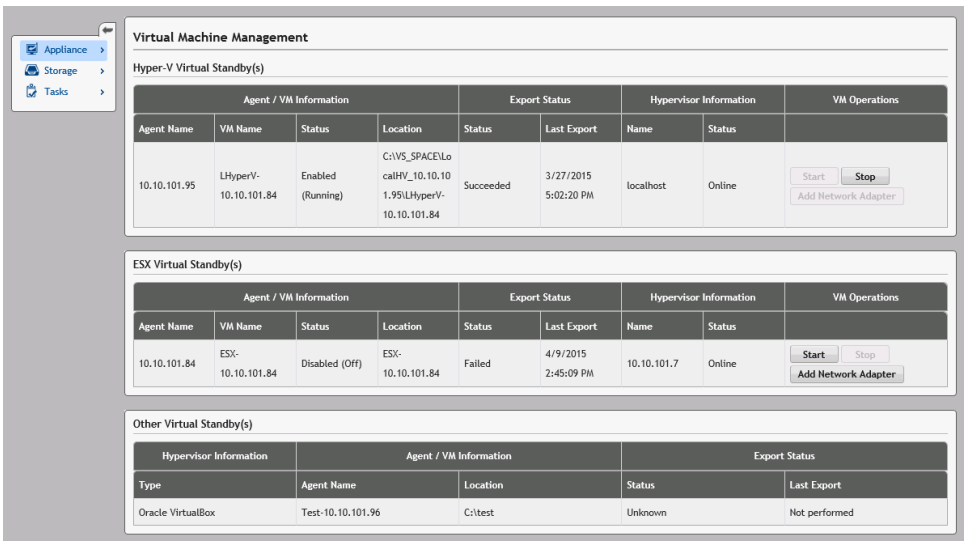
7. Wählen Sie auf der Seite „Volumes“ (Datenträger) den bzw. die Datenträger aus, die exportiert werden sollen. Schließen Sie das Boot-Laufwerk der geschützten Maschine ein, damit die virtuelle Maschine ein erfolgreiches Backup der geschützten Maschine darstellen kann. Beispiel: C: \.
8. Klicken Sie auf der Seite **Summary** (Zusammenfassung) auf **Finish** (Fertigstellen), 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.

Verwaltung der virtuellen Maschine

Die Registerkarte **VM Management** (VM-Verwaltung) zeigt den Status der geschützten Maschinen an. Sie können Netzwerkadapter starten, stoppen, und hinzufügen (nur für virtuelle Maschinen des Typs Hyper-V und ESXi anwendbar). Um zur Registerkarte „VM Management“ (VM-Verwaltung) zu navigieren, klicken Sie auf **Appliance (Gerät)** → **VM Management (VM-Verwaltung)**.

ANMERKUNG: Es kann, jedes Mal, wenn die Registerkarte **Appliance (Gerät)** → **VM Management (VM-Verwaltung)** ausgewählt wird, bis zu 30 Sekunden dauern, bis die Schaltflächen „Start“, „Stop“ (Stopp) und „Add Network Adapter“ (Netzwerkadapter hinzufügen) angezeigt werden.



VM-Verwaltung für den bzw. die virtuellen Standbys des Typs Hyper-V und ESXi

Feld	Beschreibung
Agent/VM-Informationen	**Agent Name** (Agentenname): Gibt den Namen der geschützten Maschine an, für die Sie ein virtuelles Standby erstellt haben. **VM Name** (VM-Name): Gibt den Namen des VM an. ANMERKUNG: Es wird empfohlen, einen Namen zu verwenden, der vom Agentennamen abgeleitet ist oder mit dem Namen des Agenten übereinstimmt. Sie können auch einen Namen erstellen, der von dem Hypervisor-Typ, der IP-Adresse oder dem DNS-Namen abgeleitet ist. **Status**: Zeigt den Status der virtuellen Maschine an. Mögliche Werte sind: • Wird ausgeführt

Feld	Beschreibung
	• Angehalten • Wird gestartet • Unterbrochen • Wird angehalten • Unbekannt (zeitweiliger Status) ANMERKUNG: Die oben aufgeführten Statuswerte hängen vom Hypervisor-Typ ab. Nicht alle Hypervisoren zeigen alle Statuswerte an. **Location** (Speicherort): Zeigt den Speicherort der virtuellen Maschine an, 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.
Export-Status	**Status** 1. Zeigt den Status eines Export-Prozesses mit den folgenden Optionen an: • Abgeschlossen • Fehlgeschlagen • Wird durchgeführt • Nicht durchgeführt 2. Wenn derzeit ein Export ausgeführt wird, wird der Prozentsatz des Exports angezeigt. **Last Export** (Letzter Export): Gibt die Uhrzeit des letzten Exports an.
Hypervisor-Informationen	**Name**: Gibt den Namen des Hypervisors an, auf dem die VM erstellt wird. **Status**: Gibt den Status der Verbindung mit dem Hyper-V- und ESXi-Hypervisor an. • Online • Offline • Unbekannt (zeitweiliger Status) ANMERKUNG: Der Status wird nur für Hyper-V und ESXi angezeigt.
VM-Vorgänge	Ermöglicht es, die virtuelle Maschine zu starten oder zu stoppen und einen Netzwerkadapter hinzuzufügen.

VM-Verwaltung für weitere virtuelle Standbys

Feld	Beschreibung
Hypervisor-Informationen	**Type** (Typ): Gibt den Typ des Hypervisors an.
Agent/VM-Informationen	**Agent Name** (Agentenname): Gibt den Namen der geschützten Maschine an, für die Sie ein virtuelles Standby erstellt haben. **Location** (Speicherort): Zeigt den Speicherort der virtuellen Maschine an, zum Beispiel D:\export. Der VM-Speicherort muss über ausreichend Speicherplatz

Feld	Beschreibung
	verfügen, um die VM-Metadaten und die virtuellen Laufwerke zu beherbergen, die für die virtuelle Maschine erforderlich sind.
Export-Status	**Status** 1. Zeigt den Status eines Export-Prozesses mit den folgenden Optionen an: • Abgeschlossen • Fehlgeschlagen • Wird durchgeführt • Nicht durchgeführt 2. Wenn derzeit ein Export ausgeführt wird, wird der Prozentsatz des Exports in einer Statusleiste angezeigt. **Last Export** (Letzter Export): Gibt die Uhrzeit des letzten Exports an.

Erstellen eines virtuellen Netzwerkadapters

Virtuelle Maschinen müssen über einen oder mehrere virtuelle Netzwerkadapter (VNAs) verfügen, um eine Verbindung mit dem Internet herzustellen. Eine VM muss über einen VNA für jeden echten Netzwerkadapter (RNA) auf der geschützten Maschine verfügen. Das VNA und das angepasste RNA, müssen ähnlich konfiguriert sein. Sie können beim Erstellen des virtuellen Standbys den VMs VNAs hinzufügen oder VNAs zu einem späteren Zeitpunkt hinzufügen.

Beim Erstellen eines virtuellen Standbys wird für jeden Adapter in der geschützten Maschine ein Adapter vorgeschlagen, wenn Sie die virtuelle Maschine konfigurieren. Sie können alle oder nur einige dieser vorgeschlagenen Adapter hinzufügen oder entfernen. Die Maximalzahl von VNAs pro VM hängt von dem Hypervisor-Typ ab. Für Hyper-V können Sie bis zu 8 Adapter für jede virtuelle Maschine hinzufügen.

So erstellen Sie einen virtuellen Netzwerkadapter:

1. Navigieren Sie zur Seite **VM Management** (VM-Verwaltung).
2. Klicken Sie auf die Schaltfläche **Add Network Adapter** (Netzwerkadapter hinzufügen), die der VM zugeordnet ist, um ein VNA hinzuzufügen.

   ANMERKUNG: Fügen Sie keine Adapter zu einer VM für einen virtuellen Standby hinzu, der noch Backups oder Exporte für geschützte Maschinen ausführt. Die zusätzlichen VNAs können zu Fehlern bei zukünftigen Exportvorgängen führen.

   ANMERKUNG: Es wird empfohlen, VNAs hinzuzufügen, kurz bevor Sie die VM als Ersatz für die geschützte Maschine starten. Stellen Sie sicher, dass Sie über die Registerkarte des virtuellen Standby alle ausstehenden Exporte für die VM stoppen oder anhalten.

   Das Fenster **Virtual Network Adapters and Switches** (Virtuelle Netzwerkadapter und -switches) wird angezeigt.
3. Klicken Sie auf **Create** (Erstellen), um einen virtuellen Netzwerkadapter zu erstellen.

   Das Fenster **Create Virtual Network Adapter** (Virtuellen Netzwerkadapter erstellen) wird angezeigt.
4. Wählen Sie aus dem Dropdown-Menü einen existierenden virtuellen Switch aus.

ANMERKUNG: Bei der Auswahl virtueller Switches für ESXi werden in der Dropdown-Liste nur Switches angezeigt, die „VM“ oder „Virtual Machine“ (virtuelle Maschine) in ihrem Namen enthalten. Wählen Sie nur Switches vom Typ **Virtual Machine Port Group** (Schnittstellengruppe der virtuellen Maschine) aus. Sie können den Switch-Typ über die ESXi-Hypervisor-GUI überprüfen.

5. Klicken Sie auf **Erstellen**.

ANMERKUNG: Entfernen Sie einen virtuellen Netzwerkadapter über die Benutzeroberfläche der Hypervisor-Verwaltung.

Starten eines VM-Vorgangs

So starten Sie einen VM-Vorgang:

1. Navigieren Sie zum Fenster **VM Management** (VM-Verwaltung).
2. Klicken Sie auf die Schaltfläche **Start**, die zur VM gehört, die gestartet werden soll.

ANMERKUNG: Die GUI zeigt den richtigen Status der Maschine eventuell verzögert an. Die Start-Schaltfläche kann bis zu 30 Sekunden nach Verwendung der Schaltflächen deaktiviert sein. Die Start-Schaltfläche wird nur aktiviert, wenn die virtuelle Maschine gestartet werden kann.

ANMERKUNG: Klicken Sie nicht auf die Start-Schaltfläche, wenn derzeit die Export-Task auf die virtuelle Maschine ausgeführt wird oder bald beginnen wird. Überprüfen Sie den Zeitplan der nächsten Export-Task in der Registerkarte **Protected Machines** (Geschützte Maschinen) und der Registerkarte **Virtual Standby** (Virtuelles Standby). Wenn bald eine Export-Task geplant ist, können Sie vor dem Start der virtuellen Maschine die Export-Task beenden, überspringen oder warten, bis diese abgeschlossen ist. Das Exportieren von Daten funktioniert nicht, wenn der Vorgang begonnen wird, während die virtuelle Maschine läuft. Sie können jedoch eine virtuelle Maschine starten, während eine Export-Task ausgeführt wird.

ANMERKUNG: Es wird empfohlen, die VM, die als virtuelles Standby verwaltet wird, nicht zu starten. Virtuelle Standby-VMs sind dafür vorgesehen aktiv zu sein, oder als Ersatz für eine fehlerhafte geschützte Maschine gestartet zu werden. Wenn die geschützte Maschine weiterhin aktiv ist, müssen Sie erst alle ausstehenden Exporte für die VM über die Registerkarte „Virtual Standby“ (Virtuelles Standby) stoppen oder anhalten, bevor Sie die VM starten.

Beenden eines VM-Vorgangs

So beenden Sie einen VM-Vorgang:

1. Navigieren Sie zum Fenster **VM Management** (VM-Verwaltung).
2. Klicken Sie auf die Schaltfläche **Stop** (Stopp), die zur VM gehört, die gestoppt werden soll.

ANMERKUNG: Die Stopp-Schaltfläche ist nur aktiviert, wenn die virtuelle Maschine derzeit ausgeführt wird und wenn sie nach dem Starten der VM innerhalb einer (ca.) 30 Sekunden dauernden Aktualisierung verfügbar ist.

ANMERKUNG: Die Start-Schaltfläche ist innerhalb von (ca.) 30 Sekunden nach dem Beenden der VM aktiviert.

ANMERKUNG: Entfernen Sie, sobald die geschützte VM wiederhergestellt ist, die VM aus dem Hypervisor und dem zugehörigen virtuellen Standby. Erstellen Sie das virtuelle Standby für die wiederhergestellte geschützte Maschine neu. Dadurch wird sichergestellt, dass die virtuelle Standby-VM genau die geschützte Maschine spiegelt.

Durchführen eines Rollbacks

In AppAssure ist ein Rollback der Prozess der Wiederherstellung von Volumes auf einer Maschine unter Verwendung von Wiederherstellungspunkten.

ANMERKUNG: Die Rollback-Funktionalität wird auch für Ihre geschützten Linux-Maschinen unter Verwendung des Befehlszeilen-Dienstprogramms `aamount` unterstützt. Weitere Informationen finden Sie unter Durchführen eines Rollbacks für eine Linux-Maschine unter Verwendung der Befehlszeile.

So führen Sie ein Rollback durch:

1. Führen Sie in der Core Console eine der folgenden Maßnahmen aus:
   - Klicken Sie auf die Registerkarte **Machines** (Maschinen) und führen Sie dann eine der folgenden Maßnahmen aus:

   a. Aktivieren Sie in der Liste der geschützten Maschinen das Kontrollkästchen neben der Maschine, die Sie exportieren möchten.
   b. Klicken Sie im Drop-Down-Menü **Actions(Maßnahmen)** für diese Maschine auf **Rollback.**
   c. Wählen Sie anschließend im Dialogfeld **Rollback — Select Recovery Point** (Rollback – Wiederherstellungspunkt auswählen) einen Wiederherstellungspunkt zum Exportieren aus, und klicken Sie auf **Next** (Weiter).
      - Wählen Sie im linken Navigationsbereich der AppAssure Core Console die Maschine aus, für die Sie ein Rollback durchführen möchten. Daraufhin wird die Registerkarte **Summary** (Zusammenfassung) für diese Maschine gestartet.
   d. Klicken Sie auf die Registerkarte **Recovery Points** (Wiederherstellungspunkte), und wählen Sie dann einen Wiederherstellungspunkt aus der Liste aus.
   e. Erweitern Sie die Details für diesen Wiederherstellungspunkt und klicken Sie dann auf **Rollback**.
2. Bearbeiten Sie die in der folgenden Tabelle beschriebenen Rollback-Optionen.

Textfeld	Beschreibung
Geschützte Maschine	Geben Sie die ursprüngliche Agentenmaschine als Ziel für den Rollback an. Quelle bezieht sich auf den Agenten, von dem der Wiederherstellungspunkt, der für den Rollback verwendet wird, erstellt wurde.
Recovery Console Instance (Recovery Console-Instanz)	Um den Wiederherstellungspunkt zu einem Computer, der im URC-Modus gebootet wurde wiederherzustellen, geben Sie den Besitzernamen und das Kennwort ein.

3. Klicken Sie auf **Load Volumes** (Volumes laden).

   Das Dialogfeld **Volume-Zuweisung** wird angezeigt.

   ANMERKUNG: Die Kern-Console weist Linux-Volumes nicht automatisch zu. Um ein Linux-Volume zu finden, suchen Sie das Volume, für das Sie ein Rollback durchführen möchten.
4. Wählen Sie die Volumes aus, für die Sie ein Rollback durchführen möchten.
5. Wählen Sie unter Verwendung der **Destination** (Ziel)-Optionen das Ziel-Volume aus, auf welches das ausgewählte Volume zurückgesetzt werden soll.
6. Wählen Sie aus folgenden Optionen aus:
   - **Live Recovery**. Wenn Sie Live Recovery auswählen, wird das Rollback für Windows Volumes sofort ausgeführt. Dies ist standardmäßig ausgewählt.

     ANMERKUNG: Die Option **Live Recovery** ist für Linux Volumes nicht verfügbar.

- **Force Dismount** (Erzwungene Aufhebung der Bereitstellung). Wenn Sie dies auswählen, wird die Aufhebung der Bereitstellung von einem jeglichen bereitgestellten Wiederherstellungspunkt vor der Ausführung eines Rollback erzwungen. Dies ist standardmäßig ausgewählt.

7. Klicken Sie auf **Rollback**.

   Das System beginnt den Prozess des Rollback zu einem ausgewählten Wiederherstellungspunkt.

Durchführen eines Rollbacks für eine Linux-Maschine unter Verwendung der Befehlszeile

Ein Rollback bezeichnet den Vorgang der Wiederherstellung von Volumes auf einer Maschine anhand von Wiederherstellungspunkten. In AppAssure können Sie ein Rollback für Volumes auf Ihren geschützten Linux-Maschinen unter Verwendung des Befehlszeilen-Dienstprogramms `aamount` durchführen.

VORSICHT: Versuchen Sie nicht, ein Rollback auf dem System- oder root (/)-Volume auszuführen.

ANMERKUNG: Die Rollback-Funktion wird für Ihre geschützten Windows-Maschinen in der Core Console unterstützt. Weitere Informationen finden Sie unter Durchführen eines Rollbacks.

So führen Sie ein Rollback für ein Volume auf einer Linux-Maschine durch:

1. Führen Sie das Dienstprogramm AppAssure `aamount` als root durch, wie zum Beispiel:

   ```
   sudo aamount
   ```

2. Geben Sie den folgenden Befehl bei der AppAssure-Bereitstellungsaufforderung ein, um die geschützten Maschinen aufzulisten.

   ```
   lm
   ```

3. Wenn Sie dazu aufgefordert werden, geben Sie die IP-Adresse oder den Hostnamen Ihres AppAssure-Kernservers an.
4. Geben Sie die Anmeldeinformationen für den Kernserver, das heißt, den Benutzernamen und das Kennwort, ein.

   Eine Liste, welche die von diesem AppAssure Server geschützten Maschinen anzeigt, wird angezeigt. Sie listet die gefundenen Maschinen mit deren Zeilenobjektnummer, Host/IP-Adresse und einer ID-Nummer für die Maschine auf. (Beispiel: `293cc667-44b4-48ab-91d8-44bc74252a4f`).
5. Um die derzeit bereitgestellten Wiederherstellungspunkte für die angegebene Maschine aufzuführen, geben Sie den folgenden Befehl ein:

   ```
   lr <machine_line_item_number>
   ```

   ANMERKUNG: MIt diesem Befehl können Sie auch die ID-Nummer anstatt der Zeilenobjektnummer der Maschine eingeben.

   Eine Liste, die die grundlegenden und inkrementellen Wiederherstellungspunkte für diese Maschine anzeigt, wird angezeigt. Diese Liste schließt die Zeilenobjektnummer, den Datum/Zeitstempel, den Speicherort des Volumes, die Größe des Wiederherstellungspunkts und eine ID-Nummer für das Volume ein, das am Ende eine Sequenznummer einschließt (zum Beispiel, `”293cc667-44b4-48ab-91d8-44bc74252a4f:2”`), die den Wiederherstellungspunkt identifiziert.
6. Um einen Wiederherstellungspunkt für das Zurücksetzen auszuwählen, geben Sie den folgenden Befehl ein:

   ```
   r [volume_recovery_point_ID_number] [path]
   ```

   Dieser Befehl setzt das Volume-Abbild, das von der ID-Nummer des Kerns auf einen angegebenen Pfad festgelegt wurde, zurück. Der Pfad für das Rollback ist der Pfad für den Beschreiber der Gerätedatei und nicht das Verzeichnis, in dem es bereitgestellt ist.

ANMERKUNG: Um den Wiederherstellungspunkt zu identifizieren, können Sie in dem Befehl auch eine Zeilennummer anstatt der ID-Nummer festlegen. Verwenden Sie in diesem Fall die Zeilennummer des Agenten/der Maschine (von der `lm` Ausgabe), gefolgt von der Zeilennummer des Wiederherstellungspunkts und des Buchstabens des Volumes, gefolgt vom Pfad, wie, **r [machine_line_item_number] [recovery_point_line_number] [volume_letter] [path]**. In diesem Befehl ist [path] der Beschreiber der Datei für das tatsächliche Volume.

Wenn zum Beispiel die Ausgabe `lm` drei Agentenmaschinen auflistet und Sie den Befehl `lr` für Nummer 2 eingeben und Sie möchten das Volume B mit 23 Wiederherstellungspunkten auf das Volume, das auf dem Verzeichnis `/mnt/data` bereitgestellt wurde, zurücksetzen, dann heißt der Befehl: `r2 23 b /mnt/data`.

ANMERKUNG: Es ist möglich, ein Rollback auf / durchzuführen, aber nur bei Durchführung einer Bare-Metal-Wiederherstellung, die mit einer Live-CD gestartet wird. Weitere Informationen finden Sie unter Durchführen einer Bare-Metal-Wiederherstellung für eine Linux-Maschine.

7. Wenn Sie dazu aufgefordert werden, fortzufahren, klicken Sie auf `y` for Yes (Ja).

   Nachdem der Rollback-Vorgang fortfährt, wird eine Reihe von Meldungen angezeigt, die Sie über den Status informieren.

8. Nach einem erfolgreichen Rollback stellt das Dienstprogramm `aamount` automatisch die Kernelmodule bereit und bringt sie wieder am zurückgesetzten Volume an, wenn das Ziel zuvor geschützt und bereitgestellt war. Wenn nicht, stellen Sie das zurückgesetzte Volume auf dem lokalen Laufwerk bereit und überprüfen Sie dann, dass die Dateien wiederhergestellt wurden.

   Sie können zum Beispiel den Befehl `sudo mount` und dann den Befehl `ls` verwenden.

   VORSICHT: Heben Sie die Bereitstellung für ein geschütztes Linux-Volume nicht manuell auf. Falls Sie ein geschütztes Linux-Volume manuell aufheben müssen, müssen Sie vor der Aufhebung der Bereitstellung des Volumes den folgenden Befehl ausführen: `bsctl -d [path to volume].`

   In diesem Befehl bezieht sich [path to volume] nicht auf den Bereitstellungspunkt des Volumes, sondern er bezieht sich auf den Beschreiber der Datei oder des Volumes; das in einer ähnlichen Form wie dieses Beispiel sein muss: `/dev/sda1`.

Wissenswertes über die Bare-Metal-Wiederherstellung für Windows-Maschinen

Wenn Server wie erwartet funktionieren, führen sie ihre Aufgaben gemäß ihrer Konfiguration aus. Bei einem schwerwiegenden Ereignis, durch das der Server funktionsunfähig wird, müssen sofortige Maßnahmen zur Wiederherstellung des Servers auf seinen vorherigen Funktionszustand ergriffen werden. Dabei werden üblicherweise die Maschine neu formatiert, das Betriebssystem neu installiert, Daten über Sicherungen wiederhergestellt und Softwareanwendungen neu installiert.

In AppAssure können Sie eine Bare-Metal-Wiederherstellung (BMR) für Ihre Windows-Maschinen durchführen, egal ob die Hardware gleichartig oder unterschiedlich ist. Dieser Vorgang umfasst das Erstellen des Start-CD-Abbilds, das Brennen des Abbilds auf einen Datenträger, das Starten der Zielserver vom Laufwerk aus, das Herstellen einer Verbindung mit einer Wiederherstellungskonsolen-Instanz, das Zuordnen von Volumes, die Initiierung der Wiederherstellung und anschließend die Überwachung des Vorgangs. Nachdem die Bare-Metal-Wiederherstellung abgeschlossen ist, können Sie das Betriebssystem und dann die Softwareanwendungen auf dem wiederhergestellten Server wieder laden sowie Ihre besonderen Einstellungen und Konfigurationen vornehmen.

Mögliche andere Zustände, in denen Sie eventuell eine Bare-Metal-Wiederherstellung durchführen möchten, könnten Hardware-Aktualisierungen oder der Austausch eines Servers sein.

Die BMR-Funktionalität wird auch für Ihre geschützten Linux-Maschinen unter Verwendung des Befehlszeilen-Dienstprogramms `aamount` unterstützt. Weitere Informationen finden Sie unter Durchführen einer Bare-Metal-Wiederherstellung für eine Linux-Maschine.

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 des Servers und des intakten Kerns
- Hardware zur Wiederherstellung (neu oder alt, ähnlich oder unterschiedlich)
- Leere CD und CD-Brenner-Software
- VNC Viewer (optional)
- Windows 7 PE (32-Bit)-kompatible Treiberspeicher und Netzwerk-Adapter-Treiber für die Zielmaschine
- Speicher-Controller, RAID, AHCI und Chipsatz-Treiber für das Zielbetriebssystem

ANMERKUNG: Die Speicher-Controller-Treiber sind nur erforderlich, wenn der Wiederherstellungsvorgang von einer unterschiedlichen Hardware durchgeführt wird.

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

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

1. Erstellen Sie eine Start-CD. Lesen Sie den Abschnitt unter Erstellen eines startfähigen CD/ISO-Abbilds.
2. Brennen Sie das Abbild auf einen Datenträger.
3. Starten Sie den Zielserver von der Start-CD. Lesen Sie den Abschnitt unter Laden einer Start-CD.
4. Stellen Sie eine Verbindung zum Wiederherstellungsdatenträger her.
5. Weisen Sie die Volumes zu. Lesen Sie den Abschnitt unter Zuweisen von Volumes.
6. Initiieren Sie die Wiederherstellung. Lesen Sie den Abschnitt unter Starten eines Wiederherstellungsvorgangs vom AppAssure-Kern.
7. Überwachen Sie den Fortschritt. Lesen Sie den Abschnitt unter Anzeigen des Fortschritts der Wiederherstellung.

Erstellen eines startfähigen CD/ISO-Abbildes

Um eine BMR für eine Windows-Maschine durchzuführen, müssen Sie ein startfähiges CD/ISO-Abbild in der Core Console erstellen, in dem die AppAssure Universal Recovery Console-Schnittstelle enthalten ist. Die AppAssure Universal Recovery Console ist eine Umgebung, die dazu verwendet wird, das Systemlaufwerk oder den kompletten Server direkt vom AppAssure-Kern wiederherzustellen.

Das ISO-Abbild, das Sie erstellen, ist auf die Maschine, die wiederhergestellt wird, zugeschnitten; deshalb muss es die korrekten Netzwerk- und Massenspeichertreiber enthalten. Wenn Sie davon ausgehen, dass Sie auf andere Hardware wiederherstellen werden als die der Maschine, auf der sie die Start-CD erstellen,

müssen Sie den Speicher-Controller und andere Treiber in die Start-CD einschließen. Siehe Einfügen von Treibern in eine Start-CD.

ANMERKUNG: Die Internationale Organisation für Normung (International Organization for Standardization, ISO) ist eine internationale Organisation von Vertretern aus verschiedenen nationalen Organisationen, die Normen für Dateisysteme ausarbeitet und festlegt. ISO 9660 ist eine Norm für Dateisysteme, die für optische Datenträger beim Austauschen von Daten verwendet wird. Sie unterstützt mehrere Betriebssysteme, z. B. Windows. Ein ISO-Abbild ist die Archivdatei oder das Datenträgerabbild, das die Daten für jeden Sektor des Datenträgers und seines Dateisystems enthält.

So erstellen Sie ein startfähiges CD/ISO-Abbild:

1. Wählen Sie in der Core Console, auf der sich der wiederherzustellende Server befindet, **Core** (Kern) und dann die Registerkarte **Tools** (Extras) aus.
2. Klicken Sie auf **Boot CDs** (Start-CDs).
3. Wählen Sie **Actions** (Maßnahmen) und dann **Create Boot ISO** (Start-ISO erstellen) aus.

   Das Dialogfeld **Create Boot CD** (Start-CD erstellen) wird angezeigt. Verwenden Sie die folgende Option, um das Dialogfeld zu beenden.

Benennen der Start-CD-Datei und Festlegen des Pfads

So benennen Sie die Start-CD-Datei und richten den Pfad ein:

Geben Sie im Dialogfeld **Create Boot CD** (Start-CD erstellen) den ISO-Pfad ein, unter dem das Start-Abbild auf dem Kernserver gespeichert wird.

Wenn auf der Freigabe, auf der Sie das Image speichern möchten, nicht mehr ausreichend Speicherplatz vorhanden ist, können Sie den Pfad nach Bedarf anpassen, z. B. D:\Dateiname.iso.

ANMERKUNG: Die Dateierweiterung muss .iso sein. Wenn Sie den Pfad angeben, verwenden Sie nur alphanumerische Zeichen, den Bindestrich und den Punkt (nur zur Trennung von Hostnamen und Domänen). Für die Buchstaben a bis z wird Groß-/Kleinschreibung nicht beachtet. Verwenden Sie keine Leerstellen. Keine anderen Symbole oder Satzzeichen sind erlaubt.

Erstellen von Verbindungen

So erstellen Sie Verbindungen:

1. Führen Sie in **Connection Options** (Verbindungsoptionen) einen der folgenden Schritte aus:
   - Um die IP-Adresse dynamisch unter Verwendung des Dynamic Host Configuration Protocol (DHCP) (Dynamisches Host-Konfigurationsprotokoll) zu erhalten, wählen sie **Obtain IP address automatically** (IP-Adresse automatisch beziehen) aus.
   - Sie können optional auch eine statische IP-Adresse für die Recovery Console angeben. Wählen Sie dazu **Use the following IP address** (Folgende IP-Adresse verwenden) und geben Sie die IP-Adresse, Subnetzmaske, Standard-Gateway und den DNS-Server in die entsprechenden Felder ein. Sie müssen alle diese Bereiche angeben.
2. Falls notwendig, wählen Sie in **UltraVNC Options** (UltraVNC-Optionen) **Add UltraVNC** (UltraVNC hinzufügen) aus und geben Sie dann die UltraVNC-Optionen ein. Die UltraVNC-Einstellungen ermöglichen es Ihnen, die Recovery Console remote, während sie sich im Gebrauch befindet, zu verwalten.

   ANMERKUNG: Dieser Schritt ist optional. Wenn Sie Remote-Zugriff auf die Recovery Console benötigen, verwenden und konfigurieren Sie Ultra VNC. Sie können sich nicht über die Microsoft-Terminaldienste anmelden, während Sie die CD starten.

Einfügen von Treibern in eine Start-CD

Die Treibereinfügung wird dazu verwendet, die Funktionsfähigkeit zwischen Recovery Console, Netzwerkadapter und Speicher auf dem Zielserver zu unterstützen.

Wenn Sie davon ausgehen, auf unterschiedliche Hardware wiederherzustellen, müssen Sie Speichercontroller, RAID, AHCI, Chipset und andere Treiber in die Start-CD einfügen. Diese Treiber ermöglichen es dem Betriebssystem, alle Geräte auf Ihrem Zielsystem erfolgreich zu erkennen und auszuführen.

ANMERKUNG: Beachten Sie, dass die Start-CD automatisch Windows 7 PE 32-Bit-Treiber enthält.

So fügen Sie Treiber in eine Start-CD ein:

1. Laden Sie die Treiber von der Webseite des Server-Herstellers herunter und entpacken Sie sie.
2. Komprimieren Sie den Ordner, in dem sich die Treiber befinden, mithilfe eines Dateikomprimierungsprogramms, z. B. WinZip.
3. Klicken Sie im Dialogfeld **Create Boot CD** (Start-CD erstellen), im Fenster **Drivers** (Treiber), auf **Add a Driver** (Treiber hinzufügen).
4. Um die komprimierte Treiberdatei zu finden, navigieren Sie durch das Dateisystem. Wählen Sie die Datei aus und klicken Sie auf **Open** (Öffnen).

   Die eingefügten Treiber erscheinen hervorgehoben im Fensterbereich **Drivers** (Treiber).

Erstellen der Start-CD

Um eine Start-CD von dem Bildschirm **Create Boot CD** (Start-CD erstellen) zu erstellen, nachdem Sie die Start/CD benannt haben und ihren Pfad angegeben haben, eine Verbindung erstellt haben und optional die Treiber eingefügt haben, klicken Sie auf **Create Boot CD** (Start-CD erstellen). Das ISO-Abbild wird dann erstellt.

Anzeigen des Fortschritts der ISO-Abbilderstellung

Zum Anzeigen des Erstellungsfortschritts des ISO-Abbilds, wählen Sie die Registerkarte **Events** (Ereignisse), und dann können Sie unter **Tasks** (Aufgaben) den Erstellungsfortschritts des ISO-Abbilds überwachen.

ANMERKUNG: Sie können den Erstellungsfortschritt des ISO-Abbilds auch im Dialogfeld **Monitor Active Task** (Aktive Aufgaben überwachen) ansehen.

Wenn die Erstellung des ISO-Abbilds abgeschlossen ist, wird es auf der Seite **Boot CD** (Start-CD) vom Menü **Tools** (Extras) aus zugänglich, angezeigt.

Zugreifen auf das ISO-Abbild

Um auf das ISO-Abbild zuzugreifen, navigieren Sie zu dem von Ihnen angegebenen Ausgabepfad. Sie können aber auch auf den Link klicken, um das Abbild in einen Speicherort herunterzuladen, von dem aus Sie es auf dem neuen System laden können, z. B. ein Netzlaufwerk.

Laden einer Start-CD

Nachdem Sie das Start-CD-Abbild erstellt haben, müssen Sie den Zielserver mit der neu erstellten Start-CD starten.

ANMERKUNG: Falls Sie die Start-CD mit DHCP erstellt haben, notieren Sie sich die IP-Adresse und das Kennwort.

So laden Sie eine Start-CD:

1. Navigieren Sie zum neuen Server, laden Sie die Start-CD und starten Sie dann die Maschine.
2. Geben Sie **Boot from CD-ROM** (Starten von CD-ROM) an, wodurch Folgendes geladen wird:
   - Windows 7 PE
   - AppAssure-Agentsoftware

   Die AppAssure Universal Recovery Console wird gestartet und zeigt die IP-Adresse und das Authentifizierungskennwort für die Maschine an.
3. Notieren Sie die IP-Adresse, die im Einstellungsbereich des Netzwerkadapters angezeigt wird, und das Authentifizierungskennwort, das im Authentifizierungsbereich angezeigt wird. Sie benötigen diese Information später während des Datenwiederherstellungsvorgangs, um sich wieder bei der Konsole anzumelden.
4. Wenn Sie die IP-Adresse ändern möchten, wählen Sie sie und klicken Sie auf **Change** (Ändern).

   ANMERKUNG: Wenn Sie eine IP-Adresse im Dialogfeld „Create Boot CD Builder" (Start-CD-Generator erstellen) eingegeben haben, wird diese Adresse durch die Universal Recovery Console verwendet und auf dem Bildschirm **Network Adapter settings** (Netzwerkadaptereinstellungen) angezeigt.

Einfügen von Treibern in Ihren Zielserver

Wenn Sie auf unterschiedliche Hardware wiederherstellen, müssen Sie Speichercontroller, RAID, AHCI, Chipset und andere Treiber in die Start-CD einfügen, wenn sie sich nicht schon auf der Start-CD befinden. Diese Treiber ermöglichen es dem Betriebssystem, alle Geräte auf Ihrem Zielsystem erfolgreich auszuführen.

Wenn Sie sich nicht sicher sind, welche Treiber Ihr Zielserver erfordert, klicken Sie auf die Systeminformationen-Registerkarte in der Universal Recovery Console. Diese Registerkarte zeigt die komplette System-Hardware und die Gerätetypen für den Zielserver an, auf den Sie wiederherstellen möchten.

ANMERKUNG: Beachten Sie, dass Ihr Zielserver Windows 7 PE 32-Bit-Treiber automatisch einschließt.

So fügen Sie Treiber auf Ihren Zielserver ein:

1. Laden Sie die Treiber von der Webseite des Server-Herstellers herunter und entpacken Sie sie.
2. Komprimieren Sie den Ordner, in dem sich die Treiber befinden, mithilfe eines Dateikomprimierungsprogramms (z. B. WinZip) und kopieren Sie ihn auf den Zielserver.
3. Klicken Sie in der Universal Recovery Console auf **Driver Injection** (Treiber einfügen).
4. Um die komprimierte Treiberdatei zu finden, navigieren Sie durch das Dateisystem und wählen Sie die Datei aus.
5. Wenn Sie in Schritt 3 auf **Driver Injection** (Treibereinfügung) geklickt haben, klicken Sie auf **Add Driver** (Treiber hinzufügen). Wenn Sie stattdessen in Schritt 3 auf **Load driver** (Treiber laden) geklickt haben, klicken Sie auf **Open** (Öffnen).

   Die ausgewählten Treiber werden eingefügt und werden nach dem Neustart des Zielservers auf das Betriebssystem geladen.

Starten eines Wiederherstellungsvorgangs vom Kern aus

So starten Sie einen Wiederherstellungsvorgang vom Kern aus:

1. Wenn die NICs auf allen Systemen, die wiederhergestellt werden, teambasiert (gebunden) sind, entfernen Sie alle, bis auf einen, der Netzwerkkabel.

ANMERKUNG: AppAssure Restore (AppAssure Wiederherstellung) erkennt teambasierte NICs nicht. Der Vorgang kann nicht erkennen, welchen NIC zu verwenden, wenn er mit mehr als einer aktiven Verbindung präsentiert wird.

2. Navigieren Sie zurück zum Core-Server, und öffnen Sie die Core Console.
3. Wählen Sie auf der Registerkarte **Machines** (Maschinen) die Maschine, aus der Sie Daten wiederherstellen möchten.
4. Klicken Sie im Menü **Actions** (Aktionen) für die Maschine, klicken Sie dann auf **Recovery Points** (Wiederherstellungspunkte), um eine Liste aller Wiederherstellungspunkte für diese Maschine anzuzeigen.
5. Erweitern Sie den Wiederherstellungspunkt, von dem aus Sie die Wiederherstellung durchführen möchten, und klicken Sie dann auf **Rollback** (Rollback).
6. Im **Rollback**-Dialogfeld wählen Sie unter Choose **Destination** (Ziel auswählen) die Option **Recovery Console Instance** (Recovery Console-Instanz) aus.
7. Geben Sie in das Textfeld **Host** bzw. **Password** (Kennwort) die IP-Adresse bzw. das Authentifizierungskennwort für den neuen Server ein, auf dem Sie Daten wiederherstellen möchten.

   ANMERKUNG: Die Host- und Kennwortwerte sind die Anmeldeinformationen, die Sie in der vorherigen Aufgabe aufgezeichnet haben. Weitere Informationen finden Sie unter Laden einer Start-CD.
8. Klicken Sie auf **Load Volumes** (Volumes laden), um die Zielvolumes auf die neue Maschine zu laden.

Zuweisen von Volumes

Sie haben die Auswahl, Volumes den Datenträgern auf dem Zielserver automatisch oder manuell zuzuordnen. Bei einer automatischen Datenträgerzuordnung wird der Datenträger bereinigt und neu partitioniert, und alle Daten werden gelöscht. Die Anordnung erfolgt in der Reihenfolge, in der die Volumes aufgelistet sind, und die Volumes werden den Datenträgern ordnungsgemäß entsprechend der Größe usw. zugewiesen. Ein Datenträger kann von mehreren Volumes genutzt werden. Wenn Sie die Laufwerke manuell zuordnen, bedenken Sie, dass Sie den gleichen Datenträger nicht zweimal verwenden können.

Für die manuelle Zuweisung muss die neue Maschine bereits richtig formatiert sein, bevor sie wiederhergestellt wird. Weitere Informationen finden Sie unter Starten eines Wiederherstellungsvorgangs vom AppAssure-Kern.

So ordnen Sie Volumes zu:

1. Um Volumes automatisch zuzuordnen, gehen Sie wie folgt vor:
   a. Wählen Sie im Dialogfeld **RollbackURC** die Registerkarte **Automatically Map Volumes** (Volumes automatisch zuordnen) aus.
   b. Überprüfen Sie im Bereich **Disk Mapping** (Laufwerk zuordnen) unter **Source Volume** (Quellvolume), dass das Quellvolume ausgewählt wurde und das die entsprechenden Volumes darunter aufgelistet und ausgewählt sind.
   c. Wenn das Ziellaufwerk, das automatisch zugeordnet wurde, das korrekte Zielvolume ist, wählen Sie **Destination Disk** (Ziellaufwerk) aus.
   d. Klicken Sie auf **Rollback** (Zurücksetzen) und fahren Sie dann mit Schritt 3 fort.
2. Um Volumes manuell zuzuordnen, gehen Sie wie folgt vor:
   a. Wählen Sie im Dialogfeld **RollbackURC** die Registerkarte **Manually Map Volumes** (Volumes manuell zuordnen) aus.
   b. Überprüfen Sie im Bereich **Volume Mapping** (Laufwerk zuordnen) unter **Source Volume** (Quellvolume), dass das Quellvolume ausgewählt wurde und das die entsprechenden Volumes darunter aufgelistet und ausgewählt sind.

c. Wählen Sie aus dem Drop-Down-Menü unter **Destination** (Ziel) das entsprechende Ziel aus, das aus dem Ziel-Volume besteht, das die Bare-Metal-Wiederherstellung des ausgewählten Wiederherstellungspunktes ausführt, und klicken Sie dann auf **Rollback** (Zurücksetzen).

3. Überprüfen Sie im Bestätigungsdialogfeld **RollbackURC** die Zuordnung der Quelle des Wiederherstellungspunktes und das Ziel-Volume für den Rollback. Um den Rollback auszuführen, klicken Sie auf **Begin Rollback** (Rollback starten).

   WARNUNG: Wenn Sie Begin Rollback (Rollback starten) auswählen, werden alle bestehenden Partitionen und Daten auf dem Zielvolume dauerhaft entfernt, und sie werden mit dem Inhalt des ausgewählten Wiederherstellungspunkts, einschließlich des Betriebssystems und aller Daten ersetzt.

Anzeigen des Fortschritts der Wiederherstellung

So zeigen Sie den Fortschritt der Wiederherstellung an:

1. Nachdem Sie den Rollback-Vorgang initiiert haben, wird das Dialogfeld **Active Task** (Aktiver Task) angezeigt, welches anzeigt das der Rollback-Vorgang eingeleitet wurde.

   ANMERKUNG: Wenn das Dialogfeld **Active Task** (Aktiver Task) erscheint, bedeutet das nicht, dass der Task erfolgreich beendet wurde.

2. Um den Fortschritt des Rollback optional vom Dialogfeld „Active Task" (Aktiver Task) zu überwachen, klicken Sie auf **Open Monitor Window** (Überwachungsfenster öffnen). Sie können den Status, als auch die Anfangs- und Endzeiten der Wiederherstellung vom Fenster **Monitor Open Task** (Überwachung offener Tasks) anzeigen.

   ANMERKUNG: Um die Wiederherstellungspunkte durch das Dialogfeld **Active Task** (Aktive Tasks) wieder auf die Quellmaschine zurückzustellen, klicken Sie auf **Close** (Schließen).

Starten des wiederhergestellten Zielservers

So starten Sie den wiederhergestellten Zielserver:

1. Navigieren Sie zurück zum Zielserver und klicken Sie in der Benutzeroberfläche **AppAssure Universal Recovery Console** auf die Option **Neu starten** (Neu starten), um die Maschine zu starten.
2. Legen Sie fest, dass Windows normal gestartet werden soll.
3. Melden Sie sich bei der Maschine an.

   Das System wird auf seinen Zustand vor der Bare-Metal-Wiederherstellung wiederhergestellt.

Beheben von Problemen beim Systemstart

Beachten Sie, dass Sie, wenn Sie auf unterschiedliche Hardware wiederhergestellt haben, Speichercontroller, RAID, AHCI, Chipset und andere Treiber wieder einfügen müssen, falls sie nicht schon auf der Start-CD vorhanden sind. Diese Treiber ermöglichen es dem Betriebssystem, alle Geräte auf Ihrem Zielsystem erfolgreich auszuführen.

So beheben Sie Probleme beim Start:

1. Wenn beim Starten eines wiederhergestellten Zielservers Probleme auftreten sollten, öffnen Sie die Universal Recovery Console durch neu laden der Start-CD.
2. Klicken Sie in der Universal Recovery Console auf **Driver Injection** (Treiber einfügen).
3. Klicken Sie im Dialogfeld Driver Injection (Treiber einfügen) auf **Repair Boot Problems** (Startprobleme reparieren).

   Die Startparameter im Boot Record des Zielservers werden automatisch repariert.
4. Klicken Sie in der Universal Recovery Console, auf **Reboot** (Erneut starten).

Durchführen einer Bare-Metal-Wiederherstellung für eine Linux-Maschine

Die haben die Möglichkeit, eine Bare-Metal-Wiederherstellung (BMR) für eine Linux-Maschine, einschließlich Rollback des System-Volumes, durchzuführen. Unter Verwendung des AppAssure-Befehlszeilendienstprogramms `aamount` können Sie einen Rollback-Vorgang zum Boot-Volume-Basisabbild durchführen. Damit Sie eine BMR für eine Linux-Maschine durchführen können, müssen Sie folgende Schritte ausführen:

- Legen Sie eine BMR Live CD-Datei von AppAssure-Unterstützung, die eine Startversion von Linux enthält, bereit.

  ANMERKUNG: Sie können auch die Linux Live CD-Datei vom Lizenzportal von **https://licenseportal.com** herunterladen.
- Stellen Sie sicher, dass auf dem Laufwerk genug Speicherplatz zur Erstellung von Zielpartitionen auf der Zielmaschine vorhanden ist, um die Quellvolumen zu enthalten. Die Zielpartitionen sollten mindestens so groß sein, wie die ursprüngliche Zielpartition.
- Identifizieren Sie den Pfad für das Rollback, der der Pfad für den Beschreiber der Gerätedatei ist. Um den Pfad für den Beschreiber der Gerätedatei zu identifizieren, verwenden Sie den Befehl `fdisk` von einem Terminalfenster.

  ANMERKUNG: Bevor Sie mit der Nutzung der AppAssure-Befehle beginnen, können Sie das Bildschirm-Dienstprogramm installieren. Das Bildschirm-Dienstprogramm ermöglicht Ihnen, den Bildschirm zu durchblättern, um größere Datenmengen anzuzeigen, zum Beispiel eine Liste der Wiederherstellungspunkte. Weitere Informationen über das Installieren des Bildschirm-Dienstprogramms finden Sie unter Installieren des Bildschirm-Dienstprogramms

So führen Sie eine Bare-Metal-Wiederherstellung für eine Linux-Maschine aus:

1. Verwenden Sie die Live CD-Datei, die Sie von AppAssure erhalten haben, starten Sie die Linux Maschine und öffnen Sie ein Terminalfenster.
2. Erstellen Sie bei Bedarf eine neue Datenträgerpartition. Zum Beispiel können Sie den Befehl `fdisk` als root ausführen. Machen Sie dann diese Partition durch `a` (einen) Befehl startfähig.
3. Führen Sie das Dienstprogramm AppAssure `aamount` als root durch, wie zum Beispiel:

   ```
   sudo aamount
   ```
4. Geben Sie den folgenden Befehl bei der AppAssure-Bereitstellungsaufforderung ein, um die geschützten Maschinen aufzulisten.

   ```
   lm
   ```
5. Wenn Sie dazu aufgefordert werden, geben Sie die IP-Adresse oder den Hostnamen Ihres AppAssure-Kernservers an.
6. Geben Sie die Anmeldeinformationen für den Kernserver, das heißt, den Benutzernamen und das Kennwort, ein.

   Eine Liste wird angezeigt, welche die von diesem AppAssure-Server geschützten Maschinen anzeigt. Sie listet die gefundenen Maschinen mit deren Zeilenobjektnummer, Host/IP-Adresse und einer ID-Nummer für die Maschine auf. (Beispiel: `293cc667-44b4-48ab-91d8-44bc74252a4f`).
7. Um die derzeit bereitgestellten Wiederherstellungspunkte für die Maschine, die Sie wiederherstellen möchten aufzulisten, geben Sie den folgenden Befehl ein:

   ```
   lr <machine_line_item_number>
   ```

   ANMERKUNG: MIt diesem Befehl können Sie auch die ID-Nummer anstatt der Zeilenobjektnummer der Maschine eingeben.

   Eine Liste, die die grundlegenden und inkrementellen Wiederherstellungspunkte für diese Maschine anzeigt, wird angezeigt. Diese Liste schließt die Zeilenobjektnummer, den Datum/Zeitstempel, den

Speicherort des Volumes, die Größe des Wiederherstellungspunkts und eine ID-Nummer für das Volume ein, das am Ende eine Sequenznummer einschließt (zum Beispiel: "293cc667-44b4-48ab-91d8-44bc74252a4f:2"), welche den Wiederherstellungspunkt identifiziert.

8. Um den Basisabbild-Wiederherstellungspunkt für den Rollback-Vorgang auszuwählen, geben Sie den folgenden Befehl ein:

   `r <volume_base_image_recovery_point_ID_number> <path>`

   VORSICHT: Sie müssen sicherstellen, dass das Systemvolume nicht bereitgestellt ist.

   Dieser Befehl setzt das Volume-Abbild, das von der ID-Nummer des Kerns auf einen angegebenen Pfad festgelegt wurde, zurück. Der Pfad für das Rollback ist der Pfad für den Beschreiber der Gerätedatei und nicht das Verzeichnis, in dem es bereitgestellt ist.

   ANMERKUNG: Um den Wiederherstellungspunkt zu identifizieren, können Sie in dem Befehl auch eine Zeilennummer anstatt der ID-Nummer festlegen. Verwenden Sie die Zeilennummer des Agenten/der Maschine (von der Im-Ausgabe), gefolgt von der Zeilennummer des Wiederherstellungspunkts und des Buchstabens des Volumes, gefolgt vom Pfad, z. B. **r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>**. In diesem Befehl ist **<path>** der Beschreiber der Datei für das tatsächliche Volume.

9. Wenn Sie dazu aufgefordert werden, fortzufahren, klicken Sie auf `y` for Yes (Ja).

   Nachdem der Rollback-Vorgang fortfährt, wird eine Reihe von Meldungen angezeigt, die Sie über den Status informieren.

10. Nach einem erfolgreichen Rollback können Sie bei Bedarf den Haupt-Boot Record mit dem wiederhergestellten Bootloader aktualisieren.

    ANMERKUNG: Das Reparieren oder Erstellen des Bootloaders ist nur notwendig, wenn das Laufwerk neu ist. Wenn Sie ein einfaches Rollback auf demselben Laufwerk ausgeführt haben, ist das Erstellen des Bootloaders nicht notwendig.

    VORSICHT: Sie dürfen die Bereitstellung für ein geschütztes Linux-Volume nicht manuell aufheben. Falls Sie dies tun müssen, müssen Sie vor der Aufhebung der Bereitstellung des Volumes den folgenden Befehl ausführen: bsctl -d <path to volume>

    In diesem Befehl bezieht sich `<path to volume>` (Pfad zu Volume) nicht auf den Bereitstellungspunkt des Volumes, sondern auf den Datei-Beschreiber des Volume; der Pfad muss in einer ähnlichen Form wie im folgenden Beispiel vorliegen: **/dev/sda1**.

Installieren des Bildschirm-Dienstprogramms

Bevor Sie anfangen, die AppAssure-Befehle zu nutzen, können Sie das Bildschirm-Dienstprogramm installieren. Das Bildschirm-Dienstprogramm ermöglicht es Ihnen, durch den Bildschirm zu scrollen, um größere Datenmengen, wie zum Beispiel eine Liste der Wiederherstellungspunkte anzuzeigen.

So installieren Sie das Bildschirm-Dienstprogramm:

1. Starten Sie die the Linux Maschine mithilfe der Live CD-Datei.

   Ein Terminalfenster wird geöffnet.

2. Geben Sie den folgenden Befehl ein: `sudo apt-get install screen`.
3. Um das das Bildschirm-Dienstprogramm zu starten, geben Sie in der Eingabeaufforderung `screen` (Bildschirm) an.

Erstellen von startbaren Partitionen auf einer Linux-Maschine

So erstellen Sie startbare Partitionen auf einer Linux-Maschine unter Verwendung der Befehlszeile:

1. Verbinden Sie alle Geräte under Verwendung des Dienstprogramms **bsctl** mit dem folgenden Befehl als root: `sudo bsctl --attach-to-device /dev/<restored volume>`

   ANMERKUNG: Wiederholen Sie diesen Schritt für jedes wiederhergestelltes Volume.
2. Stellen Sie jedes wiederhergestelltes Volume unter Verwendung der folgenden Befehle bereit:

   ```
   mount /dev/<restored volume> /mnt

   mount /dev/<restored volume> /mnt
   ```

   ANMERKUNG: Einige Systemkonfigurationen könnten das Startverzeichnis als Teils des root-Volume einschließen.
3. Stellen Sie Snapshot-Metadaten für jedes wiederhergestellte Volume unter Verwendung der folgenden Befehle bereit:

   ```
   sudo bsctl --reset-bitmap-store /dev/<restored volume>

   sudo bsctl --map-bitmap-store /dev/<restored volume>
   ```
4. Stellen Sie durch Verwendung des `blkid`-Befehls oder des `ll /dev/disk/by-uuid`-Befehls sicher, dass der Universally Unique Identifier (UUID) die neuen Volumes enthält.
5. Stellen Sie sicher, dass `/etc/fstab` die korrekten UUIDs für die neuen Root- und Boot-Volumes enthält.
6. Installieren Sie Grand Unified Bootloader (GRUB) unter Verwendung der folgenden Befehle:

   ```
   mount --bind /dev/ /mnt/dev

   mount --bind /proc/ /mnt/proc

   chroot/mnt/bin/bash

   grub-install/dev/sda
   ```
7. Stellen Sie sicher, dass die Datei **/boot/grub/grub.conf** den korrekten UUID für das Root-Volume enthält, oder aktualisieren Sie ihn unter Verwendung eines Texteditors.
8. Entfernen sie die Live CD aus dem CD-ROM-Laufwerk und starten Sie die Linux-machine neu.

Anzeigen von Ereignissen und Benachrichtigungen

So zeigen Sie Ereignisse und Benachrichtigungen an:

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Core Console auf der Registerkarte „Maschinen" auf den Hyperlink für die Maschine, deren Ereignisse Sie anzeigen möchten.
   - Wählen Sie im linken **Navigationsbereich** der Core Console die Maschine aus, deren Ereignisse Sie anzeigen möchten.
2. Klicken Sie auf die Registerkarte **Events** (Ereignisse).

   Es wird ein Protokoll aller Ereignisse für aktuelle Aufgaben und Benachrichtigungen angezeigt.

5

Schützen von Server-Clustern

Wissenswertes über den Schutz von Server-Clustern

In AppAssure ist der Schutz von Server-Clustern mit den AppAssure-Agenten verbunden, die auf individuellen Cluster-Knoten installiert sind (d. h. auf individuellen Maschinen im Cluster), und dem Kern, der diese Agenten so schützt, als würde es sich um eine einzige Maschine handeln.

Sie können einen Kern ohne Weiteres für den Schutz und die Verwaltung eines Clusters konfigurieren. In der Core Console ist ein Cluster als separate Einheit organisiert, die einen „Container" bildet, in dem die entsprechenden Knoten enthalten sind. Im linken Navigationsbereich etwa ist der Kern oben in der Navigationsstruktur aufgeführt. Die Cluster befinden sich unter dem Kern und enthalten die zugeordneten individuellen Knoten (auf denen AppAssure-Agenten installiert sind).

Auf den Kern- und Cluster-Ebenen können Sie Informationen über die Cluster anzeigen, z. B. die Liste der damit in Beziehung stehenden Knoten und die freigegebenen Volumes. Ein Cluster wird in der Core Console auf der Registerkarte „Machines" (Maschinen) angezeigt. Sie können die Ansicht (mithilfe von „Show/Hide" (Ein-/Ausblenden)) umschalten, um die Knoten in einem Cluster anzuzeigen. Auf der Cluster-Ebene können Sie auch die entsprechenden Exchange- und SQL-Cluster-Metadaten für die Knoten im Cluster anzeigen. Sie können Einstellungen für den gesamten Cluster und für die in diesem Cluster freigegebenen Volumes festlegen oder Sie können zu einem individuellen Knoten (Maschine) im Cluster navigieren, um die Einstellungen nur für diesen Knoten und die zugewiesenen Volumes festlegen.

Unterstützte Anwendungen und Cluster-Typen

Um Ihren Cluster richtig zu schützen, muss die AppAssure-Agentsoftware auf allen Maschinen oder Knoten im Cluster installiert sein. AppAssure unterstützt die Anwendungsversionen und Cluster-Konfigurationen, die in der folgenden Tabelle aufgeführt sind.

Tabelle 4. Unterstützte Anwendungen und Cluster-Typen

Anwendung	Anwendungsversion und dazugehörige Cluster-Konfiguration	Windows Failover Cluster
Microsoft Exchange	2007 Single Copy Cluster (SCC)	2003, 2008, 2008 R2
	2007 Cluster Continuous Replication (CCR)	
	2010 Database Availability Group (DAG)	2008, 2008 R2
Microsoft SQL	2005, 2008, 2008 R2 Single Copy Cluster (SCC)	2003, 2008, 2008 R2
	2007 Single Copy Cluster (SCC)	2008, 2008 R2, 2012

Zu den unterstützten Laufwerkstypen gehören:

- GUID-Partitionstabellen (GPT)-Laufwerke mit einer Kapazität von mehr als 2 TB
- Dynamische Laufwerke
- Grundlegende Laufwerke

Zu den unterstützten Bereitstellungstypen gehören:

- Freigegebene Laufwerke, die als Laufwerksbuchstaben verbunden werden (zum Beispiel: D:)
- Einfache dynamische Volumes auf einem einzelnen physischen Laufwerk (keine gestriped, gespiegelte, oder übergreifende Volumes)
- Freigegebene Laufwerke, die als Bereitstellungspunkte verbunden werden

Schützen eines Clusters

In diesem Thema wird beschrieben, wie Sie einen Cluster hinzufügen und in AppAssure schützen können. Wenn Sie einen Cluster für den Schutz hinzufügen, müssen Sie den Host-Namen oder die IP-Adresse des Clusters, die Cluster-Anwendung oder einen der Cluster-Knoten/-Maschinen angeben, der bzw. die einen AppAssure Agenten enthalten.

ANMERKUNG: Es wird ein Repository wird verwendet, um Daten-Snapshots zu speichern, die von Ihren geschützten Knoten erstellt wurden. Bevor Sie damit beginnen, die Daten in Ihrem Cluster zu schützen, erstellen Sie mindestens ein Repository das Ihrem AppAssure-Kern zugewiesen ist.

Informationen zum Einrichten von Repositories finden Sie unter Wissenswertes über Repositories.

So schützen Sie einen Cluster:

1. Führen Sie einen der folgenden Vorgänge aus:
   - Navigieren Sie in der Core Console zur Registerkarte **Home** (Startseite) und klicken Sie auf die Schaltfläche **Protect Cluster** (Cluster schützen).
   - Klicken Sie in der Core-Konsole auf der Registerkarte **Machines** (Maschinen) auf **Actions** (Maßnahmen) und dann auf **Protect Cluster** (Cluster schützen).
2. Geben Sie im Dialogfeld **Connect to Cluster** (Mit Cluster verbinden) die folgenden Informationen ein:

Textfeld	Beschreibung
Host	Der Hostname oder die IP-Adresse des Clusters, die Cluster-Anwendung oder einer der Cluster-Knoten, den Sie schützen wollen. ANMERKUNG: Wenn Sie die IP-Adresse von einem der Knoten verwenden, muss für diesen Knoten ein AppAssure-Agent installiert und gestartet werden.
Schnittstelle	Die Portnummer der Maschine, auf der der AppAssure-Kern mit dem Agenten kommuniziert.
Benutzername	Der Benutzername, den der Domainadministrator verwendet, um sich mit dieser Maschine zu verbinden: z. B. **domain_name\administrator** oder **administrator@domain_name.com** ANMERKUNG: Der Domainname ist ein Pflichtfeld. Mit dem lokalen Benutzernamen des Administrators können Sie keine Verbindung zum Cluster herstellen.
Kennwort	Das Kennwort, das für die Verbindung mit dieser Maschine verwendet wird.

3. Wählen Sie im Dialogfeld **Protect Cluste**r (Cluster schützen) ein Repository für diesen Cluster aus.

4. Um den Cluster mithilfe der Standardeinstellungen zu schützen, wählen Sie die Knoten für den Standardschutz aus und klicken Sie auf **Protect** (Schützen).

   ANMERKUNG: Die Standardeinstellungen stellen sicher, dass alle Volumes durch einen Zeitplan alle 60 Minuten geschützt werden.

5. Um benutzerdefinierte Einstellungen für den Cluster einzugeben (z. B. um den zeitlichen Verlauf des Schutzes für die freigegebenen Volumes anzupassen), gehen Sie wie folgt vor:
   a. Klicken Sie auf **Settings** (Einstellungen).
   b. Wählen Sie im Dialogfeld **Volumes** das/die zu schützende(n) Volume(s) aus und klicken Sie auf **Edit** (Bearbeiten).
   c. Wählen Sie im Dialogfeld **Protection Schedule** (Schutzzeitplan) eine der folgenden in der Tabelle beschriebenen Zeitplanoptionen für den Schutz Ihrer Daten aus.

Textfeld	Beschreibung
Intervall	Folgende Optionen stehen zur Auswahl: • **Wochentag** – Um Daten in einem bestimmten Intervall zu schützen, wählen Sie **Interval** (Intervall) und dann Folgendes aus: – Wenn Sie anpassen möchten, wann Daten während Spitzenauslastungszeiten geschützt werden sollen, können Sie eine Startzeit, eine Endzeit sowie ein Intervall angeben. – Um Daten während Nebenzeiten zu schützen, aktivieren Sie das Kontrollkästchen **Protect during off-peak times** (Während Nebenzeiten schützen), und wählen Sie dann ein Intervall für den Schutz aus. • **Wochenenden** – Wenn Daten auch an den Wochenenden geschützt werden sollen, aktivieren Sie das Kontrollkästchen **Protect during weekends** (An Wochenenden schützen), und wählen Sie dann ein Intervall aus.
Täglich	Wenn die Daten täglich geschützt werden sollen, wählen Sie die Option **Daily** (Täglich) und dann in **Protection Time** (Schutzzeit) eine Zeit aus, zu der der Schutz der Daten gestartet werden soll.
No Protection (Kein Schutz)	Um den Schutz für dieses Volume zu entfernen, wählen Sie die Option **No Protection** (Kein Schutz) aus.

6. Nachdem Sie alle notwendigen Änderungen vorgenommen haben, klicken Sie auf **Save** (Speichern).
7. Um benutzerdefinierte Einstellungen für einen Knoten in den Cluster einzugeben, wählen Sie einen Knoten aus und klicken Sie anschließend auf den Link **Settings** (Einstellungen) neben dem Knoten.
   • Wiederholen Sie Schritt 5, um den Schutzzeitplan zu bearbeiten.

   Weitere Informationen zum Anpassen von Knoten finden Sie unter Schützen von Knoten in einem Cluster.
8. Klicken Sie im Dialogfeld **Protect Cluster** (Cluster schützen) auf **Protect** (Schützen).

Schützen von Knoten in einem Cluster

In diesem Thema wird beschrieben, wie Sie die Daten auf einem Clusterknoten oder einer Maschine schützen, auf der ein AppAssure-Agent installiert ist. Wenn Sie Schutz hinzufügen, müssen Sie einen Knoten aus der Liste mit verfügbaren Knoten auswählen und den Hostnamen, den Benutzernamen und das Kennwort des Domainadministrators angeben.

So schützen Sie Knoten in einem Cluster:

1. Nachdem Sie einen Cluster hinzugefügt haben, navigieren Sie zu diesem Cluster und klicken Sie auf die Registerkarte **Machines** (Maschinen).
2. Klicken Sie auf das Menü **Actions** (Maßnahmen) und dann auf **Protect Cluster Node** (Cluster-Knoten schützen).
3. Wählen Sie im Dialogfeld **Protect Cluster Node** (Cluster-Knoten schützen) die folgenden Informationen aus oder geben Sie diese ein und klicken Sie anschließend auf **Connect** (Verbinden), um die Maschine oder den Knoten hinzuzufügen.

Textfeld	Beschreibung
Host	Eine Drop-Down-Liste mit den Knoten, die im Cluster zum Schutz zur Verfügung stehen.
Schnittstelle	Die Portnummer, über die der Kern mit dem Agenten auf dem Knoten kommuniziert.
Benutzername	Der Benutzername, den der Domainadministrator verwendet, um sich mit diesem Knoten zu verbinden, z. B. **example_domain\administrator** oder **administrator@example_domain.com**.
Kennwort	Das Kennwort, das für die Verbindung mit dieser Maschine verwendet wird.

4. Klicken Sie auf **Protect** (Schützen), um den Schutz dieser Maschine mit den standardmäßigen Schutzeinstellungen zu beginnen.

   ANMERKUNG: Die Standardeinstellungen stellen sicher, dass alle Volumes auf der Maschine durch einen Zeitplan alle 60 Minuten geschützt werden.

5. Um benutzerdefinierte Einstellungen für diese Maschine einzugeben (z. B. um den Anzeigenamen zu ändern, eine Verschlüsselung hinzuzufügen oder den Schutzzeitplan anzupassen), klicken Sie auf **Show Advanced Options** (Erweiterte Optionen anzeigen).
6. Bearbeiten Sie bei Bedarf die nachfolgend beschriebenen Einstellungen.

Textfeld	Beschreibung
Anzeigename	Geben Sie einen neuen Namen für die Maschine ein, der in der Core Console angezeigt werden soll.
Repository	Wählen Sie das Repository auf dem Kern aus, in dem die Daten für diese Maschine gespeichert werden sollen.
Verschlüsselung	Geben Sie an, ob Verschlüsselung auf die Daten jedes Volume auf dieser Maschine angewendet werden soll, die in dem Repository gespeichert wird. **ANMERKUNG:** Die Verschlüsselungseinstellungen für ein Repository werden auf der Registerkarte **Configuration** (Konfiguration) in der Core Console definiert.
Zeitplan	Wählen Sie eine der folgenden Optionen: • Protect all volumes with default schedule (Alle Volumes gemäß Standardzeitplan schützen) • Schützen Sie spezifische Volumes mit einem benutzerdefiniertem Zeitplan. Wählen Sie anschließend unter **Volumes** ein Volume aus, und klicken Sie

Textfeld	Beschreibung
	auf **Bearbeiten**. Informationen zum Einstellen benutzerdefinierter Intervalle finden Sie unter Schützen eines Clusters.

Vorgang des Änderns der Einstellungen für Cluster-Knoten

Nachdem Sie Schutz für Cluster-Knoten hinzugefügt haben, können Sie einfach grundlegende Konfigurationseinstellungen für diese Maschinen oder Knoten (z. B. Anzeigename, Hostname usw.), Schutzeinstellungen (z. B. Schutzzeitplan für lokale Volumes auf der Maschine ändern, Volumes hinzufügen oder entfernen und/oder den Schutz anhalten) und vieles mehr ändern.

Um Cluster-Knoteneinstellungen zu ändern, müssen folgende Tasks ausgeführt werden:

1. Führen Sie einen der folgenden Vorgänge aus:
   - Navigieren Sie zu dem Cluster, der den Knoten enthält, den Sie bearbeiten möchten, klicken Sie auf die Registerkarte **Machines** (Maschinen) und wählen Sie dann die/den zu bearbeitende/n Maschine oder Knoten aus.
   - Oder wählen Sie im Bereich **Navigation** unter der Überschrift **Cluster** die Maschine oder den Knoten, die/den Sie bearbeiten wollen aus.
2. Informationen zum Ändern und Anzeigen von Konfigurationseinstellungen finden Sie unter Anzeigen und Ändern von Konfigurationseinstellungen.
3. Informationen zum Konfigurieren von Benachrichtigungsgruppen für Systemereignisse finden Sie unter Konfigurieren von Benachrichtigungsgruppen für Systemereignisse.
4. Informationen zum Anpassen der Einstellungen von Aufbewahrungsrichtlinien finden Sie unter Anpassen der Einstellungen von Aufbewahrungsrichtlinien.
5. Informationen zum Ändern des Schutzzeitplans finden Sie unter Ändern von Schutzzeitplänen.
6. Informationen zum Ändern von Übertragungseinstellungen finden Sie unter Ändern von Übertragungseinstellungen.

Ablaufplan für das Konfigurieren von Cluster-Einstellungen

Der Ablaufplan für die Konfiguration von Cluster-Einstellungen umfasst die folgenden Tasks:

- Ändern der Cluster-Einstellungen
- Konfigurieren von Benachrichtigungen für Cluster-Ereignisse
- Bearbeiten der Cluster-Aufbewahrungsrichtlinie
- Bearbeiten der Cluster-Schutzzeitpläne
- Bearbeiten von Cluster-Übertragungseinstellungen

Ändern von Cluster-Einstellungen

Nachdem Sie einen Cluster hinzugefügt haben, können Sie grundlegende Einstellungen (z. B. den Anzeigenamen), Schutzeinstellungen (z. B. Schutzzeitpläne, das Hinzufügen oder Entfernen von Volumes bzw. das vorübergehende Anhalten von Schutzvorgängen) usw. leicht ändern.

So ändern Sie Cluster-Einstellungen

1. Führen Sie einen der folgenden Vorgänge aus:

- Klicken Sie in der Core-Konsole auf die Registerkarte **Machinen**. Wählen Sie anschließend den Cluster aus, den Sie bearbeiten möchten.
- Wählen Sie im linken Navigationsbereich den Cluster aus, den Sie bearbeiten möchten.

2. Klicken Sie auf das Register **Configuration** (Konfiguration).

   Die Seite **Einstellungen** wird angezeigt.

3. Klicken Sie auf **Bearbeiten**, um die auf dieser Seite beschriebenen Cluster-Einstellungen wie folgt zu bearbeiten:

Textfeld	Beschreibung
Anzeigename	Geben Sie einen Anzeigenamen für den Cluster ein. Ein Name für diesen Cluster wird in der Core Console angezeigt. Standardmäßig ist das der Hostname für den Cluster. Auf Wunsch können Sie ihn jedoch auch in einen benutzerfreundlicheren Namen ändern.
Host-Name	Diese Einstellung stellt den Hostnamen für den Cluster dar. Sie ist hier nur zu Informationszwecken aufgeführt und kann nicht bearbeitet werden.
Repository	Geben Sie das Kern-Repository an, das mit dem Cluster verknüpft ist. ANMERKUNG: Wenn für diesen Cluster bereits Snapshots erstellt wurden, ist diese Einstellung nur zu Informationszwecken aufgeführt und kann nicht bearbeitet werden.
Verschlüsselungsschlüssel	Bearbeiten und wählen Sie einen Verschlüsselungsschlüssel bei Bedarf. Gibt an, ob Verschlüsselung auf die Daten jedes Volume auf diesem Cluster angewendet werden soll, die in dem Repository gespeichert wird.

Konfigurieren von Benachrichtigungen für Cluster-Ereignisse

Indem Sie Benachrichtigungsgruppen erstellen, können Sie konfigurieren, wie Systemereignisse für Ihren Cluster gemeldet werden. Diese Ereignisse können Systembenachrichtigungen oder Fehler sein.

So konfigurieren Sie Benachrichtigungen für Cluster-Ereignisse:

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Core-Konsole auf die Registerkarte **Machinen**. Wählen Sie anschließend den Cluster aus, den Sie bearbeiten möchten.
   - Wählen Sie im linken Navigationsbereich den Cluster aus, den Sie bearbeiten möchten.
2. Klicken Sie auf die Registerkarte **Configuration** (Konfiguration), und klicken Sie dann auf **Events** (Ereignisse).
3. Wählen Sie eine der in der folgenden Tabelle beschriebenen Optionen aus.

Textfeld	Beschreibung
Use Core alert settings (Kern-Benachrichtigungseinstellungen verwenden)	Mit dieser Option werden die Einstellungen angewendet, die durch den verknüpften Kern verwendet werden: a. Klicken Sie auf **Anwenden**. b. Führen Sie Schritt 5 aus.

Textfeld	Beschreibung
Use Custom alert settings (Benutzerdefinierte Benachrichtigungseinstellungen verwenden)	Mit dieser Option können Sie benutzerdefinierte Einstellungen konfigurieren. Fahren Sie mit Schritt 4 fort.

4. Wenn Sie **Custom alert settings**, (Benutzerdefinierte Benachrichtigungseinstellungen) ausgewählt haben, klicken Sie auf **Add Group** (Gruppe hinzufügen), um eine neue Benachrichtigungsgruppe für den Versand einer Liste der Systemereignisse hinzuzufügen.

   Das Dialogfeld **Add Notification Group** (Benachrichtigungsgruppe hinzufügen) wird geöffnet.

5. Fügen Sie die in der folgenden Tabelle beschriebenen Benachrichtigungsoptionen hinzu.

Textfeld	Beschreibung
Name	Geben Sie einen Namen für die Benachrichtigungsgruppe ein.
Beschreibung	Geben Sie eine Beschreibung für die Benachrichtigungsgruppe ein.
Enable Events (Ereignisse aktivieren)	Wählen Sie die Ereignisse für die Benachrichtigung aus, z. B. Cluster. Sie können Ihre Auswahl auch nach Typ vornehmen: • **Fehler** • **Warnung** • **Info** ANMERKUNG: Wenn Sie sich für die Auswahl nach Typ entscheiden, werden standardmäßig die entsprechenden Ereignisse automatisch aktiviert. Bei Auswahl von Warning (WARNUNG) werden beispielsweise die folgenden Ereignisse aktiviert: „Attachability“ (Anfügbarkeit), „Jobs“ (Aufgaben), „Licensing“ (Lizenzierung), „Archive“ (Archivierung), „CoreService“ (Kern-Service), „Export“, „Protection“ (Schutz), „Replication“ (Replikation) und „Rollback“.
Notification Options (Benachrichtigungsoptionen)	Wählen Sie das Verfahren aus, wie Benachrichtigungen behandelt werden, die Sie aus den folgenden Optionen auswählen können: • **Notify by Email** (Per E-Mail benachrichtigen) – Geben Sie in den Textfeldern „To“ (An), „CC“ (Cc) und „BCC“ (Bcc) die E-Mail-Adressen an, an die die Ereignisse gesendet werden sollen. • **Notify by Windows Event log** (Über Windows-Ereignisprotokoll benachrichtigen) – Das Windows-Ereignisprotokoll steuert die Benachrichtigung. • **Notify by syslogd** (Durch syslogd benachrichtigen) – Geben Sie den Hostnamen und Anschluss ein, an den die Ereignisse gesendet werden sollen.

6. Klicken Sie auf **OK,** um Ihre Änderungen zu speichern und anschließend auf **Apply** (Übernehmen).
7. Um eine vorhandene Benachrichtigungsgruppe zu bearbeiten, klicken Sie neben einer Benachrichtigungsgruppe in der Liste auf **Edit** (Bearbeiten).

   Das Dialogfeld **Benachrichtigungsgruppe bearbeiten**, in dem Sie die Einstellungen bearbeiten können, wird angezeigt.

Bearbeiten der Cluster-Aufbewahrungsrichtlinie

Die Aufbewahrungsrichtlinie für einen Cluster gibt an, wie lange die Wiederherstellungspunkte für die freigegebenen Volumes im Cluster im Repository gespeichert werden. 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 Rollup-Prozess umgesetzt, der Sie bei der Bestimmung der Fälligkeit und beim Löschen alter Sicherungen unterstützt.

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der **Core-Konsole** auf die Registerkarte **Machinen**. Wählen Sie anschließend den Cluster aus, den Sie bearbeiten möchten.
   - Wählen Sie im linken Navigationsbereich den Cluster aus, den Sie bearbeiten möchten.
2. Klicken Sie auf die Registerkarte **Configuration** (Konfiguration), und klicken Sie dann auf **Retention Policy** (Aufbewahrungsrichtlinie).
3. Wählen Sie eine Option aus der folgenden Tabelle aus:

Textfeld	Beschreibung
Use Core default retention policy (Standard-Aufbewahrungsrichtlinie für Kern verwenden)	Mit dieser Option werden die Einstellungen angewendet, die durch den verknüpften Kern verwendet werden. Klicken Sie auf **Apply** (Anwenden).
Use Custom retention policy (Benutzerdefinierte Aufbewahrungsrichtlinie verwenden)	Mit dieser Option können Sie benutzerdefinierte Einstellungen konfigurieren.

ANMERKUNG: Wenn Sie **Benutzerdefinierte Benachrichtigungseinstellungen** ausgewählt haben, befolgen Sie die Anweisungen zum Einrichten einer benutzerdefinierten Aufbewahrungsrichtlinie, wie unter Anpassen der Einstellungen von Aufbewahrungsrichtlinien beschrieben, und beginnen Sie mit Schritt 4.

Bearbeiten von Cluster-Schutzzeitplänen

Sie können die Schutzzeitpläne nur dann bearbeiten, wenn Ihr Cluster über freigegebene Volumes verfügt.

So ändern Sie Cluster-Schutzzeitpläne:

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Core-Konsole auf die Registerkarte **Machinen**. Wählen Sie anschließend den Cluster aus, den Sie bearbeiten möchten.
   - Wählen Sie im linken Navigationsbereich den Cluster aus, den Sie bearbeiten möchten.
2. Klicken Sie auf die Registerkarte **Configuration** (Konfiguration) und dann auf **Protection Settings** (Schutzeinstellungen).
3. Befolgen Sie die Anweisungen zur Bearbeitung der Schutzeinstellungen unter Ändern von Schutzzeitplänen, und beginnen Sie mit Schritt 2.

Ändern von Cluster-Übertragungseinstellungen

In AppAssure können Sie die Einstellungen zum Verwalten des Datenübertragungsprozesses für einen geschützten Cluster ändern.

ANMERKUNG: Sie können Cluster-Übertragungseinstellungen nur bearbeiten, wenn Ihr Cluster über freigegebene Volumes verfügt.

Es stehen drei Übertragungsarten in AppAssure zur Auswahl:

Textfeld	Beschreibung
Snapshots	Sichert die Daten auf Ihrem geschützten Cluster.
VM-Export	Erstellt eine virtuelle Maschine mit allen Sicherungsinformationen und Parametern, wie durch den für den Schutz des Clusters definierten Zeitplan angegeben.
Rollback	Stellt die Sicherungsinformationen für einen geschützten Cluster wieder her.

So ändern Sie Cluster-Übertragungseinstellungen

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Core-Konsole auf die Registerkarte **Machinen**. Wählen Sie anschließend den Cluster aus, den Sie bearbeiten möchten.
   - Wählen Sie im linken Navigationsbereich den Cluster aus, den Sie bearbeiten möchten.
2. Klicken Sie auf die Registerkarte **Configuration** (Konfiguration) und dann auf **Transfer Settings** (Übertragungseinstellungen).
3. Ändern Sie die Schutzeinstellungen wie unter Ändern von Schutzzeitplänen beschrieben, und beginnen Sie mit Schritt 2.

Konvertieren eines geschützten Cluster-Knotens in einen Agenten

In AppAssure können Sie einen geschützten Cluster-Knoten in einen AppAssure-Agenten konvertieren, sodass dieser weiterhin vom Kern verwaltet wird, jedoch nicht mehr Teil des Clusters ist. Dies ist z. B. nützlich, wenn Sie einen Cluster-Knoten aus dem Cluster entfernen möchten, jedoch den Schutz für den Knoten beibehalten wollen.

So konvertieren Sie einen geschützten Cluster-Knoten in einen Agenten:

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Core-Konsole auf die Registerkarte **Machinen**. Wählen Sie anschließend den Cluster aus, der die Maschinen enthält, die Sie konvertieren möchten, und klicken Sie auf die Registerkarte **Machinen** im Cluster.
   - Wählen Sie im linken Navigationsbereich den Cluster aus, der die Maschine enthält, die Sie konvertieren möchten und klicken Sie auf die Registerkarte **Machinen**.
2. Wählen Sie die Maschine aus, die Sie konvertieren möchten und klicken Sie anschließend im Drop-Down-Menü **Actions** (Maßnahmen), im oberen Bereich der Registerkarte „Machines“ (Maschinen) auf **Convert to Agent** (In Agenten konvertieren).
3. Um die Maschine dem Cluster wieder hinzuzufügen, wählen Sie die Maschine aus und klicken Sie anschließend auf der Registerkarte **Summary** (Zusammenfassung) im Menü **Actions** (Maßnahmen) auf **Convert to Node** (In Knoten konvertieren).

Anzeigen von Informationen über Server-Cluster

Anzeigen von Cluster-Systeminformationen

So zeigen Sie Cluster-Systeminformationen an:

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Core-Konsole auf die Registerkarte **Machinen**. Wählen Sie anschließend den Cluster aus, den Sie anzeigen möchten.
   - Wählen Sie im linken **Navigationsbereich** den Cluster aus, den Sie anzeigen möchten.
2. Klicken Sie auf die Registerkarte **Tools** (Extras).

   Die Seite mit **Systeminformationen** wird aufgerufen. Auf dieser Seite werden Systemdetails über den Cluster angezeigt, z. B. den Namen, beinhaltete Knoten mit jeweiligem Zustand und Windows-Versionen, Informationen über Netzwerkschnittstellen sowie Informationen über die Volume-Kapazität.

Anzeigen von Cluster-Ereignissen und Benachrichtigungen

Weitere Informationen zum Anzeigen von Ereignissen und Benachrichtigungen für einzelne Maschinen oder Knoten in einem Cluster finden Sie unter Anzeigen von Ereignissen und Benachrichtigungen.

So zeigen Sie Cluster-Ereignisse und Benachrichtigungen an:

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Core-Konsole auf die Registerkarte **Machinen**. Wählen Sie anschließend den Cluster aus, den Sie anzeigen möchten.
   - Wählen Sie im linken **Navigationsbereich** unter **Clusters** den Cluster aus, den Sie anzeigen möchten.
2. Klicken Sie auf die Registerkarte **Events** (Ereignisse).

   Ein Protokoll zeigt alle Ereignisse für aktuelle Aufgaben sowie sämtlichen Benachrichtigungen für den Cluster an.
3. Um die Liste der Ereignisse zu filtern, können Sie die Kontrollkästchen **Active** (Aktiv), **Complete** (Vollständig), oder **Failed** (Fehlgeschlagen) aktivieren oder deaktivieren.
4. Klicken Sie in der Tabelle **Alerts** (Benachrichtigungen) auf **Dismiss All** (Alle schließen), um alle Benachrichtigungen in der Liste zu schließen.

Anzeigen von zusammenfassenden Informationen

So zeigen Sie zusammenfassende Informationen an:

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Core-Konsole auf die Registerkarte **Machinen**. Wählen Sie anschließend den Cluster aus, den Sie anzeigen möchten.
   - Wählen Sie im linken **Navigationsbereich** unter **Clusters** den Cluster aus, den Sie anzeigen möchten.
2. Auf der Registerkarte **Summary** (Zusammenfassung) können Sie Informationen wie z. B. Cluster-Name, Cluster-Typ, Quorumtyp (sofern zutreffend) und Quorumpfad (sofern zutreffend) anzeigen.

   Auf dieser Registerkarte werden auch Überblicksinformationen zu den Volumes in diesem Cluster, einschließlich Größe und Schutzzeitplan angezeigt.
3. Um die Informationen zu aktualisieren, klicken Sie im Drop-Down-Menü **Actions** (Maßnahmen) auf **Refresh Metadata** (Metadaten aktualisieren).

Weitere Informationen zum Anzeigen von zusammenfassenden und Statusinformationen für eine individuelle Maschine oder einen Knoten im Cluster finden Sie unter Anzeigen des Maschinenstatus und anderer Details.

Arbeiten mit Cluster-Wiederherstellungspunkten

Ein Wiederherstellungspunkt – auch als Snapshot bezeichnet – ist eine zeitgenaue Kopie der Ordner und Dateien für die freigegebenen Datenträger in einem Cluster, die im Repository gespeichert sind. Wiederherstellungspunkte werden zum Wiederherstellen geschützter Maschinen oder zum Bereitstellen auf einem lokalen Dateisystem verwendet. In AppAssure können Sie eine Liste der Wiederherstellungspunkte im Repository anzeigen. Führen Sie die hier beschriebenen Schritte aus, um Wiederherstellungspunkte zu überprüfen.

ANMERKUNG: Wenn Sie Daten von einem DAG- oder CCR-Server-Cluster schützen, erscheinen die zugeordneten Wiederherstellungspunkte nicht auf Cluster-Ebene. Sie sind nur auf Knoten- oder Maschinenebene sichtbar.

Informationen zum Anzeigen von Wiederherstellungspunkten für einzelne Maschinen in einem Cluster finden Sie unter Anzeigen von Wiederherstellungspunkten.

So arbeiten Sie mit Cluster-Wiederherstellungspunkten:

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Core-Konsole auf die Registerkarte **Machinen**, und wählen Sie anschließend den Cluster aus, für den Sie Wiederherstellungspunkten anzeigen möchten.
   - Wählen Sie im linken Navigationsbereich, unter **Cluster** den Cluster aus, für den Sie Wiederherstellungspunkte anzeigen möchten.
2. Klicken Sie auf die Registerkarte **Recovery Points** (Wiederherstellungspunkte).
3. Um ausführliche Informationen zu einem bestimmten Wiederherstellungspunkt anzuzeigen, klicken Sie auf das Symbol der rechten spitzen Klammer **>** neben einem Wiederherstellungspunkt in der Liste, um die Ansicht zu erweitern.

   Weitere Informationen zu den Vorgängen, die Sie an Wiederherstellungspunkten durchführen können, finden Sie unter Anzeigen eines bestimmten Wiederherstellungspunkts.
4. Wählen Sie einen Wiederherstellungspunkt zum Bereitstellen aus.

   Informationen zum Bereitstellen eines Wiederherstellungspunkts finden Sie unter Bereitstellen eines Wiederherstellungspunkts für eine Windows-Maschine, ab Schritt 2.
5. Informationen zum Löschen von Wiederherstellungspunkten finden Sie unter Entfernen von Wiederherstellungspunkten.

Verwalten von Snapshots für einen Cluster

Sie können Snapshots durch Erzwingen eines Snapshots oder durch Anhalten momentaner Snapshots verwalten. Durch das Erzwingen eines Snapshots können Sie eine Datenübertragung für den zurzeit geschützten Cluster erzwingen. Wenn Sie einen Snapshot erzwingen, wird die Übertragung entweder sofort gestartet oder zur Warteschlange hinzugefügt. Dabei werden nur die Daten übertragen, die seit einem vorherigen Wiederherstellungspunkt geändert wurden. Falls kein vorheriger Wiederherstellungspunkt vorhanden ist, werden alle Daten (das Basisabbild) auf den geschützten Volumes übertragen. Wenn Sie einen Snapshot anhalten, unterbrechen Sie vorübergehend alle Übertragungen der Daten von der aktuellen Maschine.

Informationen zum Erzwingen von Snapshots für die einzelnen Maschinen eines Clusters finden Sie unter Erzwingen eines Snapshots. Informationen zum Anhalten und Wiederaufnehmen von Snapshots für die einzelnen Maschinen eines Clusters finden Sie unter Anhalten und Wiederaufnehmen des Schutzes.

Erzwingen eines Snapshots für einen Cluster

So erzwingen Sie einen Snapshot für einen Cluster:

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Core-Konsole auf die Registerkarte **Machinen**, und wählen Sie anschließend den Cluster aus, für den Sie Wiederherstellungspunkten anzeigen möchten.
   - Wählen Sie im linken Navigationsbereich, unter **Cluster** den Cluster aus, für den Sie Wiederherstellungspunkte anzeigen möchten.
2. Klicken Sie in der Registerkarte **Summary** (Zusammenfassung) auf das Drop-Down-Menü **Actions** (Maßnahmen), und dann auf **Force Snapshot** (Snapshot erzwingen).

Anhalten und Wiederaufnehmen von Snapshots

So halten Sie Cluster-Snapshots an und nehmen sie wieder auf:

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Core-Konsole auf die Registerkarte **Machinen**, und wählen Sie anschließend den Cluster aus, für den Sie Wiederherstellungspunkten anzeigen möchten.
   - Wählen Sie im linken Navigationsbereich, unter **Cluster** den Cluster aus, für den Sie Wiederherstellungspunkte anzeigen möchten.
2. Klicken Sie in der Registerkarte **Summary** (Zusammenfassung) auf das Drop-Down-Menü Actions (Maßnahmen), und dann auf **Pause Snapshot** (Snapshot anhalten).
3. Wählen Sie im Dialogfeld **Schutz anhalten** eine der nachstehend beschriebenen Optionen aus:

Textfeld	Beschreibung
Pause until resumed (Anhalten bis Wiederaufnahme).	Hält den Snapshot an, bis Sie den Schutz manuell wieder aufnehmen. Klicken Sie zum Aufnehmen des Schutzes auf das Menü **Actions** (Maßnahmen) und dann auf **Resume** (Wiederaufnehmen).
Pause for (Anhalten für)	Hier können Sie einen Zeitraum in Tagen, Stunden und Minuten angeben, in dem Snapshots angehalten werden sollen.

Entfernen der Bereitstellung lokaler Wiederherstellungspunkte

So entfernen Sie die Bereitstellung lokaler Wiederherstellungspunkte:

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Core-Konsole auf die Registerkarte **Machinen** Wählen Sie anschließend den Cluster aus, für den Sie die Bereitstellung von Wiederherstellungspunkten entfernen möchten.
   - Wählen Sie im linken Navigationsbereich den Cluster aus, für den Sie die Bereitstellung von Wiederherstellungspunkten entfernen möchten.
2. Klicken Sie in der Registerkarte **Tools** (Extras) im Menü **Tools** (Extras) auf **Mounts** (Bereitstellungen) aus.
3. Führen Sie in der Liste der lokalen Bereitstellungen eine der folgenden Maßnahmen aus:

- Um die lokale Einzel-Bereitstellung zu entfernen, suchen Sie die Bereitstellungen für den Wiederherstellungspunkt aus, die Sie entfernen möchten, markieren Sie sie und klicken Sie dann auf **Dismount** (Bereitstellung entfernen).
- Um alle lokalen Bereitstellungen zu entfernen, klicken Sie auf die Schaltfläche **Dismount All** (Alle Bereitstellungen entfernen).

Durchführen eines Rollbacks für Cluster und Cluster-Knoten

Ein Rollback ist der Vorgang zur Wiederherstellung der Volumes auf einer Maschine von Wiederherstellungspunkten aus. Bei einem Server-Cluster führen Sie ein Rollback auf Knoten- oder Maschinenebene durch. In diesem Abschnitt werden Richtlinien zum Durchführen eines Rollbacks für Cluster-Volumes gegeben.

Durchführen eines Rollbacks für CCR- (Exchange-) und DAG-Cluster

So führen ein Rollbacks für SCC (Exchange, SQL)-Cluster aus:

1. Schalten Sie alle Knoten außer einem aus.
2. Führen Sie ein Rollback mithilfe des Standardverfahrens von AppAssure für die Maschine durch, wie in den Abschnitten Durchführen eines Rollbacks und Durchführen eines Rollbacks für eine Linux-Maschine unter Verwendung der Befehlszeile beschrieben.
3. Wenn das Rollback abgeschlossen ist, stellen Sie alle Datenbanken aus den Cluster-Volumes bereit.
4. Fahren Sie alle anderen Knoten hoch.
5. Bei Exchange navigieren Sie zur Exchange Management Console und führen für jede Datenbank den Vorgang **Update Database Copy** (Datenbankkopie aktualisieren) aus.

Durchführen eines Rollbacks für SCC- (Exchange-, SQL-) Cluster

So führen ein Rollbacks für SCC (Exchange, SQL)-Cluster aus:

1. Schalten Sie alle Knoten außer einem aus.
2. Führen Sie ein Rollback mithilfe des Standardverfahrens von AppAssure für die Maschine durch, wie in den Abschnitten Durchführen eines Rollbacks und Durchführen eines Rollbacks für eine Linux-Maschine unter Verwendung der Befehlszeile beschrieben.
3. Wenn das Rollback abgeschlossen ist, stellen Sie alle Datenbanken aus den Cluster-Volumes bereit.
4. Schalten Sie alle anderen Knoten einzeln ein.

ANMERKUNG: Sie müssen kein Rollback für den Quorumdatenträger durchführen. Er kann automatisch oder mithilfe der Funktion Cluster-Dienst neu erstellt werden.

Replizieren von Cluster-Daten

Wenn Sie Daten für ein Cluster replizieren, dann konfigurieren Sie die Replikation auf Maschinenebene für die einzelnen Maschinen in diesem Cluster. Sie können die Replikation auch so konfigurieren, dass die Wiederherstellungspunkte für freigegebene Volumes repliziert werden, z. B. wenn Sie fünf Agenten haben, die Sie von der Quelle auf das Ziel replizieren möchten.

Weitere Informationen und Anweisungen zum Replizieren von Daten finden Sie unter Replizieren von Agentendaten auf einer Maschine.

Entfernen eines Clusters aus dem Schutz

So entfernen Sie einen Cluster aus dem Schutz:

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Core-Konsole auf die Registerkarte **Machinen**. Wählen Sie anschließend den Cluster aus, den Sie entfernen möchten.
   - Wählen Sie im linken Navigationsbereich den Cluster aus, den Sie entfernen möchten, um die Registerkarte **Zusammenfassung** anzuzeigen.
2. Klicken Sie im Drop-Down-Menü auf **Actions** (Maßnahmen), und wählen Sie dann **Remove Machine** (Maschine entfernen).
3. Wählen Sie eine der folgenden Optionen:

Option	Beschreibung
Keep Recovery Points (Wiederherstellungspunkte beibehalten).	Um alle derzeit gespeicherten Wiederherstellungspunkte für diesen Cluster beizubehalten.
Remove Recovery Points (Wiederherstellungspunkte entfernen).	Um alle derzeit gespeicherten Wiederherstellungspunkte für diesen Cluster aus dem Repository zu entfernen.

Entfernen von Cluster-Knoten aus dem Schutz

Führen Sie die Schritte in den folgenden Verfahren aus, um Cluster-Knoten aus dem Schutz zu entfernen. Wenn Sie nur einen Knoten aus dem Cluster entfernen möchten, lesen Sie den Abschnitt Konvertieren eines geschützten Cluster-Knotens in einen Agenten. So entfernen Sie einen Cluster-Knoten aus dem Schutz.

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Core-Konsole auf die Registerkarte **Machinen**. Wählen Sie anschließend den Cluster aus, der den Knoten enthält, den Sie entfernen möchten. Wählen Sie in der Registerkarte **Machinen**für den Cluster den Knoten aus, den Sie entfernen möchten.
   - Wählen Sie im linken Navigationsbereich unter dem entsprechenden Cluster den Knoten aus, den Sie entfernen möchten.
2. Klicken Sie im Drop-Down-Menü auf **Actions** (Maßnahmen), und wählen Sie dann **Remove Machine** (Maschine entfernen).
3. Wählen Sie eine der in der folgenden Tabelle beschriebenen Optionen aus.

Option	Beschreibung
Relationship Only (Nur Beziehung)	Der Quellkern wird aus der Replikation entfernt, die replizierten Wiederherstellungspunkte werden aber beibehalten.
With Recovery Points (Mit	Der Quellkern wird aus der Replikation entfernt und alle von dieser Maschine empfangenen replizierten Wiederherstellungspunkte werden gelöscht.

Option	Beschreibung
Wiederherstellungspunkten)	

Entfernen aller Knoten eines Clusters aus dem Schutz

So entfernen Sie alle Knoten in einem Cluster aus dem Schutz

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Core-Konsole auf die Registerkarte **Machinen**, und wählen Sie anschließend den Cluster aus, der die Knoten enthält, die Sie entfernen möchten. Klicken Sie anschließend auf die Registerkarte **Machinen** im Cluster.
   - Wählen Sie im linken Navigationsbereich den Cluster aus, der die Knoten enthält, die Sie entfernen möchten, und klicken Sie auf die Registerkarte **Machinen**.
2. Klicken Sie auf das Drop-Down-Menü **Actions** (Maßnahmen) oben auf der Registerkarte **Machines** (Maschinen) und dann auf **Remove Machines** (Maschinen entfernen).
3. Wählen Sie eine der in der folgenden Tabelle beschriebenen Optionen aus.

Option	Beschreibung
Relationship Only (Nur Beziehung)	Der Quellkern wird aus der Replikation entfernt, die replizierten Wiederherstellungspunkte werden aber beibehalten.
With Recovery Points (Mit Wiederherstellungspunkten)	Der Quellkern wird aus der Replikation entfernt und alle von dieser Maschine empfangenen replizierten Wiederherstellungspunkte werden gelöscht.

Anzeigen eines Cluster- oder Knotenberichts

Sie können Konformitäts- und Fehlerberichte über AppAssure-Vorgänge für den Cluster und für individuelle Knoten erstellen und anzeigen. Die Berichte enthalten AppAssure-Aktivitätsinformationen zum Cluster, Knoten und den freigegebenen Datenträgern. Weitere Informationen über AppAssure-Berichte siehe About Reports (Wissenswertes über Berichte).

Weitere Informationen zu den Export- und Druckoptionen, die sich auf der Berichte-Symbolleiste befinden, finden Sie unter Wissenswertes über die Symbolleiste „Berichte“.

So zeigen Sie einen Cluster- oder Knotenbericht an:

1. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie in der Core-Konsole auf die Registerkarte **Machinen**. Wählen Sie anschließend den Cluster oder den Knoten aus, für den Sie einen Bericht erstellen möchten.
   - Wählen Sie im linken **Navigationsbereich** den Cluster oder den Knoten aus, für den Sie einen Bericht erstellen möchten.
2. Klicken Sie auf die Registerkarte **Tools** (Extras) und wählen Sie dann unter dem Menü **Reports** (Berichte) eine der folgenden Optionen:
   - **Übereinstimmungsreport**
   - **Fehlerbericht**
3. Wählen Sie aus dem Drop-Down-Kalender **Start Time** (Startzeit) ein Startdatum aus, und geben Sie dann eine Startzeit für den Bericht ein.

ANMERKUNG: Vor der Zeit, bevor der AppAssure-Kern oder die AppAssure-Agentsoftware bereitgestellt wurde, sind keine Daten verfügbar.

4. Wählen Sie im Drop-Down-Kalender **End Time** (Endzeit) ein Enddatum aus, und geben Sie dann eine Endzeit für den Bericht ein.
5. Klicken Sie auf **Generate Report** (Bericht erstellen).

   Wenn der Bericht mehrere Seiten abdeckt, können Sie auf die Seitenzahlen oder auf die Pfeilschaltflächen über den Ergebnissen des Berichts klicken, um durch diese zu navigieren.

   Die Ergebnisse des Berichts werden auf der Seite angezeigt.
6. Wählen Sie zum Exportieren der Berichtsergebnisse in eines der verfügbaren Formate – PDF, XLS, XLSX, RTF, MHT, HTML, TXT, CSV oder Bilddatei – das Format für den Export aus der Drop-Down-Liste aus, und wählen Sie anschließend eine der folgenden Vorgehensweisen:
   - Klicken Sie auf das erste Symbol **Save** (Speichern), um einen Bericht zu exportieren und ihn auf dem Laufwerk zu speichern.
   - Klicken Sie auf das zweite Symbol **Save** (Speichern), um einen Bericht zu exportieren und ihn in einem neuen Webbrowser anzuzeigen.
7. Führen Sie zum Drucken der Berichtsergebnisse einen der folgenden Schritte aus:
   - Klicken Sie auf das erste Symbol **Printer** (Drucken), um den gesamten Bericht zu drucken.
   - Klicken Sie auf das zweite Symbol **Printer** (Drucken), um die aktuelle Seite des Berichts zu drucken.

6

Berichterstellung

Informationen über Berichte

Mit DL können Sie Informationen über Übereinstimmung, Fehler und zusammenfassende Informationen für mehrere Kerne und Agentenmaschinen erstellen und ansehen.

Sie können den Bericht online ansehen, Berichte drucken oder exportieren und sie in einem von mehreren unterstützen Formaten speichern. Sie können aus den folgenden Formaten wählen:

- PDF
- XLS
- XLSX
- RTF
- MHT
- HTML
- TXT
- CSV
- Image

Informationen über die Symbolleiste „Reports" (Berichte)

Die Symbolleiste, die für all Berichte verfügbar ist, erlaubt es Ihnen, auf zwei verschiedene Arten zu drucken und zu speichern. Die folgende Tabelle beschreibt die Druck- und Speicheroptionen.

Symbol	Beschreibung
	Den Bericht drucken
	Druckt die aktuelle Seite
	Exportiert einen Bericht und speichert ihn auf dem Laufwerk
	Exportiert einen Bericht und zeigt ihn in einem neuen Fenster an Verwenden Sie diese Option, um die URL für Andere, die den Bericht mit einem Webbrowser anzeigen möchten, zu kopieren, einzufügen und mit E-Mail zu senden.

Informationen über Übereinstimmungsberichte

Übereinstimmungsberichte sind für den Kern und AppAssure-Agenten verfügbar. Sie bieten Ihnen die Möglichkeit zum Anzeigen von Jobs, die von ausgewählten Kernen oder Agenten durchgeführt werden. Fehlgeschlagene Jobs erscheinen in rotem Text. Informationen im Kern-Übereinstimmungsbericht, die nicht mit einem Agenten assoziiert sind, verbleiben leer.

Einzelheiten zu den Kernen werden in Spaltenansicht angezeigt, die die folgenden Kategorien beinhaltet:

- Kern
- Geschützter Agent
- Typ
- Zusammenfassung
- Status
- Fehler
- Startzeit
- Endzeit
- Uhrzeit
- Arbeit, gesamt

Informationen über Fehlerberichte

Fehlerberichte sind Teilmengen der Übereinstimmungsberichte und sind für Kerne und AppAssure-Agenten verfügbar. Fehlerberichte schließen nur die fehlgeschlagenen Jobs ein, die in den Übereinstimmungsberichten aufgelistet sind, und sie kompilieren diese Berichte in einen einzelnen Bericht, der gedruckt und exportiert werden kann.

Einzelheiten zu den Fehlern werden in Spaltenansicht angezeigt, die die folgenden Kategorien beinhaltet:

- Kern
- Agent
- Typ
- Zusammenfassung
- Fehler
- Startzeit
- Endzeit
- Verstrichene Zeit
- Arbeit, gesamt

.

Informationen über den Kern-Zusammenfassungsbericht

Der **Core Summary Report** (Kern-Zusammenfassungsbericht) schließt Informationen über die Repositorys auf dem ausgewählten Kern und über die Agenten, die von diesem Kern geschützt sind ein. Diese Informationen werden als zwei Zusammenfassungen in einem Bericht angezeigt.

Repository-Zusammenfassung

Der Teil **Repositories** (Repositorys) des **Core Summary Report** (Kern-Zusammenfassungsberichts) enthält Datenwerte für die Repositorys, die sich auf dem ausgewählten Kern befinden. Einzelheiten zu den Repositorys werden in Spaltenansicht mit den folgenden Kategorien angezeigt.

- Name
- Datenpfad
- Metadatenpfad

- Allocated Space (Zugewiesener Speicherplatz)
- Used Space (Belegte Speicherkapazität)
- Free Space (Freier Speicherplatz)
- Compression/Dedupe Bezugsverhältnis

Agentenzusammenfassung

Der Anteil **Agents** (Agenten) des **Core Summary Report** (Kern-Zusammenfassungsbericht) enthält Datenwerte für alle Agenten, die vom ausgewählten Kern geschützt werden.

Einzelheiten zu den Kernen werden in Spaltenansicht angezeigt, die die folgenden Kategorien beinhaltet:

- Name
- Geschützte Volumes
- Insgesamt geschützter Speicherplatz
- Aktueller geschützter Speicherplatz
- Tägliche Änderungsrate (**Average** (Durchschnittlich), **Median** (Mittel))
- Aufgaben-Statistik (**Passed** (Erfolgreich) **Failed** (Fehlerhaft) **Canceled** (Abgebrochen))

Erstellen eines Berichts für einen Kern oder Agenten

So erstellen Sie einen Bericht für einen Kern oder Agenten:

1. Navigieren Sie zur Core Console, und wählen Sie den Kern oder Agenten aus, für den Sie den Bericht ausführen möchten.
2. Klicken Sie auf die Registerkarte **Tools** (Extras).
3. Erweitern Sie in der Registerkarte **Tools** (Extras) die Option **Reports** (Berichte) im linken Navigationsbereich.
4. Wählen Sie im linken Navigationsbereich den Bericht, den Sie ausführen möchten. Die verfügbaren Berichte hängen von der Wahl ab, die Sie in Schritt 1 gemacht haben, und werden nachfolgend beschrieben.

Maschine	Verfügbare Reports
Kern	Übereinstimmungsreport
	Zusammenfassungsbericht
	Fehlerbericht
Agent	Übereinstimmungsreport
	Fehlerbericht

5. Wählen Sie aus dem Drop-Down-Kalender **Start Time** (Startzeit) ein Startdatum aus, und geben Sie dann eine Startzeit für den Bericht ein.

   ANMERKUNG: Es sind keine Daten von der Zeit verfügbar, bevor der Kern oder der Agent bereitgestellt wurde.
6. Wählen Sie im Drop-Down-Kalender **End Time** (Endzeit) ein Enddatum aus, und geben Sie dann eine Endzeit für den Bericht ein.
7. Wählen Sie das Kontrollkästchen **All Time** (Alle Zeiten) für einen **Core Summary Report** (Kern-Zusammenfassungsbericht), wenn Sie möchten, dass die **Start-** und die **Endzeit** die Lebensdauer des Kerns umfasst.

8. Verwenden Sie die Drop-Down-Liste **Target Cores** (Zielkerne), um den Kern auszuwählen, für den sie Daten wie den **Core Compliance Report** (Übereinstimmungsbericht) oder den **Core Errors Report**, (Kernfehlerbericht) anzeigen möchten.
9. Klicken Sie auf **Generate Report** (Bericht erstellen).

   Nach dem Erzeugen des Berichts können Sie ihn durch Verwendung der Symbolleiste drucken oder exportieren.

Informationen über Berichte zu Kernen von zentralen Verwaltungskonsolen

Mit DL können Sie Informationen zur Übereinstimmung, zu Fehlern und zusammenfassende Informationen für mehrere Kerne generieren und anzeigen. Einzelheiten zu den Kernen werden in Spaltenansichten mit denseleben Kategorien dargestellt, wie sie in diesem Abschnitt beschrieben werden.

Erstellen eines Berichts von der Central Management Console

So erstellen Sie einen Bericht von der The Central Management Console

1. Klicken Sie auf dem Bildschirm **Central Management Console Welcome** (Central Management Console Willkommen) auf das Drop-Down-Menü in der oberen rechten Ecke.
2. Klicken Sie im Drop-Down-Menü auf **Reports** (Berichte) und wählen Sie dann eine der folgenden Optionen aus:
   - **Übereinstimmungsreport**
   - **Zusammenfassungsbericht**
   - **Failure Report (Fehlerbericht)**
3. Wählen Sie im linken Navigationsbereich den Kern oder die Kerne aus, für den/die Sie den Bericht erstellen möchten.
4. Wählen Sie aus dem Drop-Down-Kalender **Start Time** (Startzeit) ein Startdatum aus, und geben Sie dann eine Startzeit für den Bericht ein.

   ANMERKUNG: Es sind keine Daten von der Zeit verfügbar, bevor der Kern oder der Agent bereitgestellt wurde.
5. Wählen Sie im Drop-Down-Kalender **End Time** (Endzeit) ein Enddatum aus, und geben Sie dann eine Endzeit für den Bericht ein.
6. Klicken Sie auf **Generate Report** (Bericht erstellen).

   Nach dem Erzeugen des Berichts können Sie ihn durch Verwendung der Symbolleiste drucken oder exportieren.

7

Durchführen einer vollständigen Wiederherstellung des DL4000-Geräts

Erstellen einer RAID 1-Partition für das Betriebssystem

VORSICHT: Es ist notwendig, dass Sie diese Vorgänge nur auf dem virtuellen RAID 1-Laufwerk, welches das Betriebssystem enthält, durchführen. Führen Sie diese Vorgänge nicht auf den virtuellen RAID 6-Laufwerken durch, die Daten enthalten.

So erstellen Sie eine RAID 1-Partition:

1. Stellen Sie sicher, dass die Festplatten in den Steckplätzen 0 und 1 bekannte funktionierende Festplatten sind.
2. Starten Sie das DL4000 Backup to Disk-Gerät.
3. Wenn Sie während des Starts dazu aufgeforderd werden, drücken Sie auf <Strg><R>.

   Der Bildschirm **PERC BIOS Configuration Utility** (PERC BIOS-Konfigurationsdienstprogramm) wird angezeigt.
4. Markieren Sie oben auf der Registerkarte **VD Management** (Verwaltung der virtuellen Laufwerke) die Option „Controller," drücken Sie auf <F2> und wählen Sie dann **Create New VD** (Neues virtuelles Laufwerk erstellen).

   ANMERKUNG: Wenn das RAID-1 OS VD bereits vorhanden ist, schnell-initialisieren Sie das RAID-1 OS VD.
5. Wählen Sie auf der Seite **Virtual Disk Management** (Verwaltung der virtuellen Laufwerke) RAID 1 als RAID-Stufe aus.
6. Wählen Sie im Textfeld **Physical Disks** (Physische Laufwerke) beide Laufwerke aus.

   ANMERKUNG: Die Größe des virtuellen Laufwerks darf höchstens 278,87 GB betragen.
7. Geben Sie einen Namen für das virtuelle Laufwerk ein, z. B. "OS", der das virtuelle Laufwerk als dasjenige identifiziert, welches das Betriebssystem enthält.
8. Drücken Sie die <Tabulatortaste>, um den Cursor auf die Option Initialisieren zu setzen und drücken Sie dann die <Eingabetaste>.

   ANMERKUNG: Die Initialisierung, die an diesem Punkt ausgeführt wird, ist eine Schnellinitialisierung.
9. Wählen Sie **OK**, um die ausgewählten Einstellungen abzuschließen oder drücken Sie zweimal auf <Strg><N>.

   Die Seite **Ctrl Mgt** wird angezeigt.
10. Wechseln Sie zum Feld **Select boot device** (Startgerät auswählen) und wählen Sie das virtuelle Laufwerk aus, welches das Betriebssystem enthält.

    Die Kapazität der Festplatte ist ungefähr 278 GB.
11. Wählen Sie **Apply** (Übernehmen) und drücken Sie die <Eingabetaste>.

12. Beenden Sie das **PERC BIOS Configuration** (BIOS-Konfigurationsdienstprogramm) und drücken Sie zum Neustart des Systems auf <Strg><Alt><Entf>.

Installieren des Betriebssystems

Verwenden Sie das Dienstprogramm Unified Server Configurator – Lifecycle Controller Enabled (USC-LCE) auf dem Gerät, um das Betriebssystem wiederherzustellen:

1. Nehmen Sie das Installationsmedium für das Betriebssystem zur Hand.
2. Stellen Sie sicher, dass Sie ein Laufwerk haben, auf dem das Medium durchgeführt werden kann.

   Sie können ein optisches USB-Laufwerk oder einen virtuellen Datenträger verwenden. Der virtuelle Datenträger wird durch iDRAC unterstützt. Weitere Informationen zum Einrichten des virtuellen Datenträgers durch iDRAC finden Sie im Benutzerhandbuch des iDRAC-Geräts Ihres Systems.

   Wenn das Installationsmedium beschädigt oder unlesbar ist, kann USC unter Umständen das vorhandene unterstützte optische Laufwerk nicht erkennen. In diesem Fall erhalten Sie unter Umständen eine Fehlermeldung, die darauf hinweist, dass kein optisches Laufwerk verfügbar ist. Wenn das Medium ungültig ist (wenn es zum Beispiel eine ungültige CD oder DVD ist), wird eine Meldung angezeigt, die Sie dazu auffordert, ein gültiges Installationsmedium einzulegen.
3. Starten Sie den USC beim Systemstart, indem Sie die Taste <F10> innerhalb von 10 Sekunden nach der Anzeige des Dell-Logos drücken.
4. Klicken Sie im linken Fensterbereich auf **OS Deployment** (Betriebssystembereitstellung).
5. Klicken Sie im rechten Bereich auf **Deploy OS** (Betriebssystem bereitstellen).
6. Wählen Sie das entsprechende Betriebssystem aus und klicken Sie auf **Next** (Weiter).

   USC extrahiert die Laufwerke, die von dem Betriebssystem, das Sie ausgewählt haben, benötigt werden. Die Treiber werden auf ein internes USB-Laufwerk, das OEMDRV gennannt wird, extrahiert.

   ANMERKUNG: Der Vorgang zum Extrahieren der Treiber kann mehrere Minuten in Anspruch nehmen.

   ANMERKUNG: Alle Treiber, die von dem OS-Bereitstellungs-Assistent kopiert werden, werden nach 18 Stunden entfernt. Sie müssen die Installierung des Betriebssystems innerhalb von 18 Stunden abschließen, damit die kopierten Treiber verfügbar sind. Um die Treiber vor dem Ende der 18 Stunden zu entfernen, starten Sie das System neu und drücken Sie auf die Taste <F10>, um USC neu einzugeben. Die Verwendung der Taste <F10> zum Abbrechen der Installation des Betriebssystems oder zur Neueingabe des USC beim Neustart während der 18 Stunden entfernt die Treiber.
7. Nachdem die Treiber extrahiert wurden, werden Sie vom USC dazu aufgefordert, den Datenträger zur Installation des Betriebssystems einzulegen.

   ANMERKUNG: Bei der Installation des Microsoft Windows-Betriebssystems werden die extrahierten Treiber während der Betriebssysteminstallation automatisch installiert.

Ausführung des Dienstprogramms zur Wiederherstellung und Aktualisierung

So führen Sie das Dienstprogramm zur Wiederherstellung und Aktualisierung aus:

1. Laden Sie **Recovery and Update Utility** (Dienstprogramm zur Wiederherstellung und Aktualisierung) von **dell.com/support** herunter.
2. Kopieren Sie das Dienstprogramm auf den Desktop des DL4000 Backup to Disk-Geräts und entpacken Sie die Dateien.
3. Doppelklicken Sie auf **launchRUU** (RUU starten).
4. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Yes** (Ja), um zu bestätigen, dass Sie keinen der aufgelisteten Vorgänge ausführen.
5. Klicken Sie auf **Start**, wenn der Bildschirm **Recovery Update Utility** (Dienstprogramm zur Wiederherstellung und Aktualisierung) angezeigt wird.
6. Wenn Sie dazu aufgefordert werden, fortzufahren, klicken Sie auf **OK**.

   Die Windows Server Rollen und Funktionen, ASP .NET MVC3, LSI-Provider, DL-Anwendungen, OpenManage Server Administrator und AppAssure-Kern-Software sind als Teil des Dienstprogramms zur Wiederherstellung und Aktualisierung installiert.
7. Starten Sie das System neu, wenn Sie dazu aufgefordert werden.
8. Nachdem alle Dienste und Anwendungen installiert wurden, klicken Sie auf **Proceed** (Fortfahren).

   Der Assistent **AppAssure Appliance Recovery** (AppAssure Gerätewiederherstellung) wird gestartet.
9. Führen Sie die beschriebenen Schritte in der Phase **Collecting Information and Configuring** (Sammlung von Informationen und Konfiguration) des AppAssure Appliance Recovery Wizard (Assisten zur AppAssure Gerätewiederherstellung) aus und klicken Sie dann auf **Next** (Weiter).

   Die Phase **Disk Recovery** (Laufwerkswiederherstellung) beginnt.
10. Nach der Anzeige der Warnung, dass AppAssure-Dienste ausgeschaltet werden, klicken Sie auf **Next** (Weiter).

    Die virtuellen Laufwerke für Repositorys und andere virtuelle Standby-Maschinen wurden wiederhergestellt und AppAssure-Dienste wurde neu gestartet. Die Wiederherstellung ist abgeschlossen.

8

Manuelles Ändern des Host-Namens

Es wird empfohlen, dass Sie bei der anfänglichen Konfiguration von DL4000 Backup to Disk Appliance einen Host-Namen auswählen. Wenn Sie den Host-Namen zu einem späteren Zeitpunkt unter Verwendung von **Windows System Properties** (Windows-Systemeigenschaften) ändern, müssen Sie die folgenden Schritte manuell ausführen, um sicherzugehen, dass der neue Hostname in Kraft tritt und das Gerät richtig funktioniert:

1. AppAssure Kerndienst stoppen
2. AppAssure Server-Zertifikate löschen
3. Kernserver und Registrierungsschlüssel löschen
4. Anzeigenamen in AppAssure ändern
5. Vertrauenswürdige Seiten in Internet Explorer aktualisieren

Stoppen des Kerndienstes

So stoppen Sie AppAssure Kerndienst:

1. Öffnen Sie **Windows Server Manager**.
2. Wählen Sie in der Struktur auf der linken Seite **Configuration** → **Services** , aus.
3. Klicken Sie mit der rechten Maustaste auf **AppAssure Core Service** (AppAssure Kerndienst) und wählen Sie **Stop** (Stoppen).

Löschen von Serverzertifikaten

So löschen Sie AppAssure Serverzertifikate:

1. Öffnen Sie eine Befehlszeilenschnittstelle.
2. Geben Sie **Certmgr** ein und drücken Sie die <Eingabetaste>.
3. Wählen Sie im Fenster **Certificate Manager** (Zertifikatsverwalter) **Trusted Root Certification Authorities** → **Certificates** aus.
4. Löschen Sie jedes Zertifikat, für welches die Spalte **Issue To** (Ausgeben für) den alten Hostnamen anzeigt, und für welches die Spalte **Intended Purpose** (Beabsichtigte Zwecke) **Server Authentication** (Server-Authentifizierung) anzeigt.

Löschen von Kernserver und Registrierungsschlüsseln

So löschen Sie Kernserver und Registrierungsschlüssel:

1. Öffnen Sie eine Befehlszeilenschnittstelle.
2. Geben Sie **regedit** ein und drücken Sie die <Eingabetaste>, um den Registry editor (Registrierungseditor) zu öffnen.

3. Navigieren Sie in der Struktur zu **HKEY_LOCAL_MACHINE → SOFTWARE → AppRecovery** und öffnen Sie das Kernverzeichnis.
4. Löschen Sie die Verzeichnisse **webServer** und **serviceHost**.

Starten des Kerns mit dem neuen Host-Namen

So starten Sie den Kern mithilfe des neuen Host-Namens, den Sie manuell erstellt haben:

1. Starten von AppAssure-Kerndiensten.
2. Klicken Sie mit der rechten Maustaste auf das Symbol **AppAssure 5 Core** auf dem Desktop, und klicken Sie dann auf **Properties** (Eigenschaften).
3. Ersetzen Sie im Browser den alten Servernamen mit dem Neuen `<server name:8006>`.

   Zum Beispiel, **https://<servername>:8006/apprecovery/admin/Core**.
4. Klicken Sie auf **OK** und starten Sie dann die AppAssure Core Console mithilfe des Symbols **AppAssure 5 Core**.

Ändern des Anzeigenamens

So ändern Sie den Anzeigenamen:

1. Melden Sie sich bei der **AppAssure Console** (AppAssure Konsole) as Administrator an.
2. Wählen Sie die Registerkarte **Configuration** (Konfiguration) aus und klicken Sie dann auf die Schaltfläche „Change“ (Ändern) in der Tabelle **General** (Allgemein).
3. Geben Sie den neuen **Display Name** (Anzeigenamen) ein und klicken Sie auf **OK**.

Aktualisieren von vertrauenswürdigen Seiten im Internet Explorer

So aktualisieren Sie vertrauenswürdige Seiten im 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 **Add** (Hinzufügen).
8. Geben Sie in **Add this website to the zone**, (Diese Website zur Zone hinzufügen) Folgendes ein: **about:blank**.
9. Klicken Sie auf **Add** (Hinzufügen).
10. Klicken Sie auf **Close** (Schließen) und dann auf **OK**.

9

Anhang A – Scripting

Wissenswertes über PowerShell Scripting

Windows PowerShell ist eine mit Microsoft .NET Framework verbundene Umgebung zur Verwaltungsautomatisierung. AppAssure enthält umfassende Client-SDKs (Software Development Kits) für PowerShell Scripting, mit denen Administratoren Verwaltung und Management von AppAssure Ressourcen automatisieren können, indem Befehle über Skripte ausgeführt werden.

So können Administratorbenutzer in bestimmten Situationen von Benutzern bereitgestellte PowerShell-Skripte verwenden, zum Beispiel vor oder nach einem Snapshot, bei Anfügbarkeit, Überprüfung der Bereitstellungsfähigkeit usw. Administratoren können Skripte sowohl vom AppAssure Kern als auch vom Agenten aus ausführen. Skripte können Parameter annehmen, und die Ausgabe eines Skripts wird in die Kern- und Agent-Protokolldateien geschrieben.

ANMERKUNG: Bei nächtlichen Aufgaben sollten Sie eine Skriptdatei und den Eingabeparameter JobType aufbewahren, um zwischen den nächtlichen Aufgaben unterscheiden zu können.

Skriptdateien befinden sich im Ordner **%ALLUSERSPROFILE%\AppRecovery\Scripts**.

- In Windows 7 ist der Pfad zum Order **%ALLUSERSPROFILE%** der folgende: **C:\ProgramData**.
- In Windows 2003 ist der Pfad zum Ordner der folgende: **Documents and Settings\All Users \Application Data**.

ANMERKUNG: Windows PowerShell ist erforderlich und muss vor Verwendung und Ausführung von AppAssure-Skripts installiert und konfiguriert werden.

PowerShell Scripting-Voraussetzungen

Bevor Sie die PowerShell-Skripts für AppAssure verwenden und ausführen, müssen Sie Windows PowerShell 2.0 installieren.

ANMERKUNG: Stellen Sie sicher, dass Sie die Datei **powershell.exe.config** im PowerShell-Stammverzeichnis ablegen. Zum Beispiel: **C:\WindowsPowerShell\powershell.exe**.

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
        <startup useLegacyV2RuntimeActivationPolicy="true">
        <supportedRuntime version="v4.0.30319"/>
<supportedRuntime version="v2.0.50727"/>
</startup>
</configuration>
```

Testen von Skripten

Wenn Sie die Skripts, die Sie ausführen möchten, testen wollen, dann können Sie dies mithilfe des grafischen Editors von PowerShell tun: **powershell_ise**. Sie müssen auch die Konfigurationsdatei

powershell_ise.exe.config zum selben Ordner wie die Konfigurationsdatei **powershell.exe.config** hinzufügen.

ANMERKUNG: Die Konfigurationsdatei **powershell_ise.exe.config** muss den gleichen Inhalt wie die Datei **powershell.exe.config** haben.

VORSICHT: Wenn das Pre- oder Post-PowerShell-Skript fehlschlägt, schlägt auch die Aufgabe fehl.

Eingabeparameter

In den Beispielskripten werden alle verfügbaren Eingabe-Parameter verwendet. Die Parameter werden in den unten stehenden Tabellen beschrieben.

ANMERKUNG: Skriptdateien müssen den gleichen Namen wie die Beispielskriptdateien tragen.

Tabelle 5. AgentTransferConfiguration (namespace Replay.Common.Contracts.Transfer)

Methode	Beschreibung
`public uint MaxConcurrentStreams { get; set; }`	Abrufen oder Einstellen der maximalen Anzahl an gleichzeitigen TCP-Verbindungen, die der Kern zum Agenten zwecks Datenübertragung aufbaut.
`public uint MaxTransferQueueDepth { get; set; }`	Wenn ein Blockbereich von einem Übertragungsstrom aus gelesen wird, so wird dieser Bereich in einer Producer-/Consumer-Warteschlange platziert, wo ihn ein Consumer-Thread liest und auf das Epoch-Objekt schreibt. Wenn das Repository langsamer schreibt als das Netzwerk liest, so füllt sich die Warteschlange auf. Der Punkt, an dem die Warteschlange voll ist und der Lesevorgang stoppt, wird als maximale Übertragungsschlangentiefe bezeichnet.
`public uint MaxConcurrentWrites { get; set; }`	Abrufen oder Einstellen der maximalen Anzahl an Blockschreibvorgängen, die zu einem bestimmten Zeitpunkt auf einer Epoche ausstehen. Wenn zusätzliche Blöcke empfangen werden, während eine so große Anzahl an Blockschreibvorgängen noch aussteht, so werden diese zusätzlichen Blöcke ignoriert, bis einer der ausstehenden Schreibvorgänge abgeschlossen ist.
`public ulong MaxSegmentSize { get; set; }`	Abrufen oder Einstellen der maximalen Anzahl an zusammenhängenden Blöcken, um eine einzelne Anfrage zu übertragen. Abhängig vom Test sind entweder höhere oder niedrigere Werte optimal.
`public Priority Priority { get; set; }`	Abrufen oder Einstellen der Priorität von Übertragungsanfragen.
`public int MaxRetries { get; set; }`	Abrufen oder Einstellen der maximalen Anzahl der erneuten Versuche einer fehlgeschlagenen

Methode	Beschreibung
	Übertragung, bevor sie als fehlgeschlagen angezeigt wird.
`public Guid ProviderId{ get; set; }`	Abrufen oder Einstellen des GUID vom VSS-Anbieter zur Verwendung von Snapshots auf diesem Host. Administratoren akzeptieren normalerweise die Standardeinstellung.
`public Collection<ExcludedWriter>ExcludedWriterIds { get; set; }`	Abrufen oder Einstellen der Sammlung von VSS-Writer-IDs, die aus diesem Snapshot ausgeschlossen werden. Die Writer-ID wird durch den Namen des Writers bestimmt. Dieser Name dient nur zu Dokumentationszwecken und muss dem Namen des Writers nicht genau entsprechen.
`public ushort TransferDataServerPort { get; set; }`	Abrufen oder Einstellen eines Wertes, in dem der TCP-Port enthalten ist, über den Verbindungen vom Kern zur tatsächlichen Datenübertragung vom Agenten zum Kern angenommen werden. Der Agent versucht, über den Port zu kommunizieren, wenn der Port jedoch verwendet wird, kann der Agent auch einen anderen Port nutzen. Der Kern verwendet die Portnummer, die in den Eigenschaften `BlockHashesUri` und `BlockDataUri` des Objekts `VolumeSnapshotInfo` für jedes Volume angegeben ist, von dem ein Snapshot erstellt wurde.
`public TimeSpan SnapshotTimeout { get; set; }`	Abrufen oder Einstellen der Zeit, die gewartet wird, bis ein VSS-Snapshot-Vorgang abgeschlossen ist, bevor der Vorgang abgebrochen wird und eine Zeitüberschreitung auftritt.
`public TimeSpan TransferTimeout { get; set; }`	Abrufen oder Einstellen der Zeit, während auf weiteren Kontakt mit dem Kern gewartet wird, bevor der Snapshot verworfen wird.
`public TimeSpan NetworkReadTimeout { get; set; }`	Abrufen oder Einstellen der Zeitüberschreitung für Netzwerklesevorgänge, die mit dieser Übertragung in Verbindung stehen.
`public TimeSpan NetworkWriteTimeout { get; set; }`	Abrufen oder Einstellen der Zeitüberschreitung für Netzwerkschreibvorgänge, die mit dieser Übertragung in Verbindung stehen.

Tabelle 6. BackgroundJobRequest (namespace Replay.Core.Contracts.BackgroundJobs)

Methode	Beschreibung
`public Guid AgentId { get; set; }`	Abrufen oder Einstellen der Agent-ID.
`public bool IsNightlyJob { get; set; }`	Abrufen oder Einstellen des Wertes, der angibt, ob die Hintergrundaufgabe eine nächtliche Aufgabe ist.
`public virtual bool InvolvesAgentId(Guid agentId)`	Bestimmt den Wert, der angibt, ob der konkrete Agent an der Aufgabe beteiligt ist.

ChecksumCheckJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks)

Übernimmt die Werte aus dem Parameter `DatabaseCheckJobRequestBase`.

DatabaseCheckJobRequestBase (namespace Replay.Core.Contracts.Exchange)

Übernimmt die Werte aus dem Parameter `BackgroundJobRequest`.

ExportJobRequest (namespace Replay.Core.Contracts.Export)

Übernimmt die Werte aus dem Parameter `BackgroundJobRequest`.

Methode	Beschreibung
`public uint RamInMegabytes { get; set; }`	Abrufen oder Einstellen der Speichergröße für die exportierte VM. Auf null (0) einstellen, um die Speichergröße der Quellmaschine zu verwenden.
`public VirtualMachineLocation Location { get; set; }`	Abrufen oder Einstellen des Zielspeicherorts für diesen Export. Dies ist eine abstrakte Basisklasse.
`public VolumeImageIdsCollection VolumeImageIds { get; private set; }`	Abrufen oder Einstellen der Volume-Abbilder, sodass sie den VM-Export einschließen.
`public ExportJobPriority Priority { get; set; }`	Abrufen oder Einstellen der Priorität von Exportanfragen.

NightlyAttachabilityJobRequest (namespace Replay.Core.Contracts.Sql)

Übernimmt die Werte aus dem Parameter `BackgroundJobRequest`.

RollupJobRequest (namespace Replay.Core.Contracts.Rollup)

Übernimmt die Werte aus dem Parameter `BackgroundJobRequest`.

TakeSnapshotResponse (namespace Replay.Agent.Contracts.Transfer)

Methode	Beschreibung
`public Guid SnapshotSetId { get; set; }`	Abrufen oder Einstellen des GUID, den VSS diesem Snapshot zugewiesen hat.
`public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }`	Abrufen oder Einstellen der Snapshot-Informationssammlung für jedes Volume, das im Snapshot enthalten ist.

TransferJobRequest (namespace Replay.Core.Contracts.Transfer)

Übernimmt die Werte aus dem Parameter `BackgroundJobRequest`.

Methode	Beschreibung
`public VolumeNameCollection VolumeNames { get; set; }`	Abrufen oder Einstellen der Volume-Namenssammlung für die Übertragung.
`public ShadowCopyType ShadowCopyType { get; set; }`	Abrufen oder Einstellen des Kopiertyps für die Übertragung. Verfügbare Werte: `Unknown` (Unbekannt), `Copy` (Kopie) und `Full` (Belegt).
`Public AgentTransferConfiguration TransferConfiguration { get; set; }`	Abrufen oder Einstellen der Übertragungskonfiguration.
`public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }`	Abrufen oder Einstellen der Speicherkonfiguration.
`public string Key { get; set; }`	Erzeugt einen pseudozufälligen (aber kryptografisch nicht sicheren) Schlüssel, der als einmaliges Kennwort zur Authentifizierung von Übertragungsanfragen verwendet werden kann.
`public bool ForceBaseImage { get; set; }`	Abrufen oder Einstellen des Wertes, der angibt, ob das Basisabbild erzwungen wurde oder nicht.
`public bool IsLogTruncation { get; set; }`	Abrufen oder Einstellen des Wertes, der angibt, ob die Aufgabe ein Abschneiden des Protokolls ist oder nicht.

Tabelle 7. TransferPostscriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

Methode	Beschreibung
`public VolumeNameCollection VolumeNames { get; set; }`	Abrufen oder Einstellen der Volume-Namenssammlung für die Übertragung.
`public ShadowCopyType ShadowCopyType { get; set; }`	Abrufen oder Einstellen des Kopiertyps für die Übertragung. Verfügbare Werte: `Unknown` (Unbekannt), `Copy` (Kopie) und `Full` (Belegt).
`public AgentTransferConfiguration TransferConfiguration { get; set; }`	Abrufen oder Einstellen der Übertragungskonfiguration.
`public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }`	Abrufen oder Einstellen der Speicherkonfiguration.
`public string Key { get; set; }`	Erzeugt einen pseudozufälligen (aber kryptografisch nicht sicheren) Schlüssel, der als einmaliges Kennwort zur Authentifizierung von Übertragungsanfragen verwendet werden kann.
`public bool ForceBaseImage { get; set; }`	Abrufen oder Einstellen des Wertes, der angibt, ob das Basisabbild erzwungen wurde.

Methode	Beschreibung
`public bool IsLogTruncation { get; set; }`	Abrufen oder Einstellen des Wertes, der angibt, ob die Aufgabe ein Abschneiden des Protokolls ist.
`public uint LatestEpochSeenByCore { get; set; }`	Abrufen oder Einstellen des letzten Epoch-Wertes.
`public Guid SnapshotSetId { get; set; }`	Abrufen oder Einstellen des GUID, den VSS diesem Snapshot zugewiesen hat.
`public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }`	Abrufen oder Einstellen der Snapshot-Informationssammlung für jedes Volume, das im Snapshot enthalten ist.

Tabelle 8. TransferPrescriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

Methode	Beschreibung
`public VolumeNameCollection VolumeNames { get; set; }`	Abrufen oder Einstellen der Volume-Namenssammlung für die Übertragung.
`public ShadowCopyType ShadowCopyType { get; set; }`	Abrufen oder Einstellen des Kopiertyps für die Übertragung. Verfügbare Werte: `Unknown` (Unbekannt), `Copy` (Kopie) und `Full` (Belegt).
`public AgentTransferConfiguration TransferConfiguration { get; set; }`	Abrufen oder Einstellen der Übertragungskonfiguration.
`public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }`	Abrufen oder Einstellen der Speicherkonfiguration.
`public string Key { get; set;}`	Erzeugt einen pseudozufälligen (aber kryptografisch nicht sicheren) Schlüssel, der als einmaliges Kennwort zur Authentifizierung von Übertragungsanfragen verwendet werden kann.
`public bool ForceBaseImage { get; set; }`	Abrufen oder Einstellen des Wertes, der angibt, ob das Basisabbild erzwungen wurde.
`public bool IsLogTruncation { get; set; }`	Abrufen oder Einstellen des Wertes, der angibt, ob die Aufgabe ein Abschneiden des Protokolls ist.
`public uint LatestEpochSeenByCore { get; set; }`	Abrufen oder Einstellen des letzten Epoch-Wertes.

Tabelle 9. VirtualMachineLocation (namespace Replay.Common.Contracts.Virtualization)

Methode	Beschreibung
`public string Description { get; set;}`	Abrufen oder Einstellen einer lesbaren Beschreibung dieses Speicherortes.
`public string Method { get; set;}`	Abrufen oder Einstellen des VM-Namens.

VolumeImageIdsCollection (namespace Replay.Core.Contracts.RecoveryPoints)

Übernimmt die Werte aus dem Parameter `System.Collections.ObjectModel.Collection<string>`.

Tabelle 10. VolumeName (namespace Replay.Common.Contracts.Metadata.Storage)

Methode	Beschreibung
`public string GuidName { get; set;}`	Abrufen oder Einstellen der Volume-ID.
`public string DisplayName { get; set;}`	Abrufen oder Einstellen des Volume-Namens.
`public string UrlEncode()`	Abrufen einer URL-verschlüsselten Version des Namens, die sauber auf eine URL übertragen werden kann. **ANMERKUNG:** In .NET 4,0 WCF besteht ein bekanntes Problem (**https://connect.microsoft.com/VisualStudio/feedback/ViewFeedback.aspx?FeedbackID=413312**), das Pfad-Escapezeichen daran hindert, in einer URI-Vorlage korrekt zu funktionieren. Da ein Volume-Name sowohl „\" als auch „?" enthält, müssen Sie die Sonderzeichen „\" und „?" durch andere Sonderzeichen ersetzen.
`public string GetMountName()`	Gibt einen Namen für jenes Volume aus, das für das Bereitstellen des Volume-Abbildes auf einem Ordner gültig ist.

VolumeNameCollection (namespace Replay.Common.Contracts.Metadata.Storage)

Übernimmt die Werte aus dem Parameter `System.Collections.ObjectModel.Collection<VolumeName>`.

Methode	Beschreibung
`public override bool Equals(object obj)`	Legt fest, ob diese Instanz und ein bestimmtes Objekt, das auch vom Typ `VolumeNameCollection` sein muss, den gleichen Wert haben (überschreibt `Object.Equals(Object)`).
`public override int GetHashCode()`	Gibt den Hashcode für diese `VolumeNameCollection` aus (überschreibt `Object.GetHashCode()`).

Tabelle 11. VolumeSnapshotInfo (namesapce Replay.Common.Contracts.Transfer)

Methode	Beschreibung
`public Uri BlockHashesUri { get; set;}`	Abrufen oder Einstellen des URI, auf dem die MD5-Hashes von Volume-Blöcken gelesen werden können.
`public Uri BlockDataUri { get; set;}`	Abrufen oder Einstellen des URI, auf dem die Volume-Datenblöcke gelesen werden können.

VolumeSnapshotInfoDictionary (namespace Replay.Common.Contracts.Transfer)

Übernimmt die Werte aus dem Parameter `System.Collections.Generic.Dictionary<VolumeName, VolumeSnapshotInfo>`.

Pretransferscript.ps1

Das **PreTransferScript** wird auf der Agentenseite vor Übertragung eines Snapshots ausgeführt.

```
# receiving parameter from transfer job
param([object]$TransferPrescriptParameter)

# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null

# Converting input parameter into specific object
$TransferPrescriptParameterObject = $TransferPrescriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPrescriptParameter];
# Working with input object. All echo's are logged
if($TransferPrescriptParameterObject -eq $null) {
        echo 'TransferPrescriptParameterObject parameter is null'
}
else {
        echo
'TransferConfiguration:'$TransferPrescriptParameterObject.TransferConfiguration

        echo 'StorageConfiguration:'
$TransferPrescriptParameterObject.StorageConfiguration
}
```

Posttransferscript.ps1

Das **PostTransferScript** wird auf der Agentenseite nach Übertragung eines Snapshots ausgeführt.

```
 # receiving parameter from transfer job
param([object] $TransferPostscriptParameter)


# building path to Agent's Common.Contracts.dll and loading this assembly

$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
```

```
# Converting input parameter into specific object

$TransferPostscriptParameterObject = $TransferPostscriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPostscriptParameter];


# Working with input object. All echo's are logged
if($TransferPostscriptParameterObject -eq $null) {
        echo 'TransferPostscriptParameterObject parameter is null'
}
else {
echo 'VolumeNames:' $TransferPostscriptParameterObject.VolumeNames
                echo 'ShadowCopyType:'
$TransferPostscriptParameterObject.ShadowCopyType
        echo 'ForceBaseImage:'
$TransferPostscriptParameterObject.ForceBaseImage                    echo
'IsLogTruncation:' $TransferPostscriptParameterObject.IsLogTruncation
}
```

Preexportscript.ps1

Das **PreExportScript** wird auf der Kernseite vor einer Exportaufgabe ausgeführt.

```
# receiving parameter from export job

param([object]$ExportJobRequest)

# building path to Core's Common.Contracts.dll and loading this assembly

$regLM = [Microsoft.Win32.Registry]::LocalMachine$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null

# Converting input parameter into specific object

$ExportJobRequestObject = $ExportJobRequest -as
[Replay.Core.Contracts.Export.ExportJobRequest]

# Working with input object. All echo's are logged

if($ExportJobRequestObject -eq $null) {
                echo 'ExportJobRequestObject parameter is null'
}
else {
                echo 'Location:' $ExportJobRequestObject.Location
                echo 'Priority:' $ExportJobRequestObject.StorageConfiguration
}
```

Postexportscript.ps1

Das **PostExportScript** wird auf der Kernseite nach einer Exportaufgabe ausgeführt.

ANMERKUNG: Es gibt keine Eingabe-Parameter für das **PostExportScript**, wenn es einmal zur Ausführung auf dem exportierten Agenten nach dem ersten Starten verwendet wurde. Reguläre Agenten enthält dieses Skript im PowerShell-Skriptordner unter **PostExportScript.ps1**.

```
# receiving parameter from export job
```

```
param([object]$ExportJobRequest)

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2 = $regVal2 + 'CoreService\Common.Contracts.dll'

# Converting input parameter into specific object

$ExportJobRequestObject = $ExportJobRequest -as
[Replay.Core.Contracts.Export.ExportJobRequest]

# Working with input object. All echo's are logged

if($ExportJobRequestObject -eq $null) {
            echo 'ExportJobRequestObject parameter is null'
}
else {
            echo 'VolumeImageIds:' $ExportJobRequestObject.VolumeImageIds
            echo 'RamInMegabytes:' $ExportJobRequestObject.RamInMegabytes
}
```

Prenightlyjobscript.ps1

Das **PreNightlyJobScript** wird auf der Kernseite vor jeder allnächtlichen Aufgabe ausgeführt. Es trägt den Parameter **$JobClassName**, der bei der separaten Behandlung von solch untergeordneten Aufgaben hilft.

```
 # receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]
$NightlyAttachabilityJobRequest,
[object]$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest,
[object]$TransferJobRequest, [int]$LatestEpochSeenByCore)

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null

# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job,
Checksum Check Job and Log  Truncation Job. All of them are triggering the
script, and $JobClassMethod (contain job name that calls the  script) helps to
handle those child jobs separately

switch ($JobClassMethod) {

# working with NightlyAttachability Job
        NightlyAttachabilityJob {
                $NightlyAttachabilityJobRequestObject =
$NightlyAttachabilityJobRequest -as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];

                echo 'Nightly Attachability job results:';
                if($NightlyAttachabilityJobRequestObject -eq $null) {
                        echo 'NightlyAttachabilityJobRequestObject parameter is
null';
```

```
                }

                else {
                                echo 'AgentId:'
$NightlyAttachabilityJobRequestObject.AgentId;
                                echo 'IsNightlyJob:'
$NightlyAttachabilityJobRequestObject.IsNightlyJob;
                }
                break;
}


# working with Rollup Job
RollupJob {
        $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
        echo 'Rollup job results:';
        if($RollupJobRequestObject -eq $null) {
                echo 'RollupJobRequestObject parameter is null';
        }
        else {
                    echo 'SimultaneousJobsCount:'
$RollupJobRequestObject.SimultaneousJobsCount;
                    echo 'AgentId:' $RollupJobRequestObject.AgentId;
                    echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
        }
        $AgentsCollection = $Agents -as
"System.Collections.Generic.List``1[System.Guid]"
        if($AgentsCollection -eq $null) {
            echo 'AgentsCollection parameter is null';
        }
        else {
                    echo 'Agents GUIDs:'
                    foreach ($a in $AgentsCollection) {
                        echo $a
                }
        }
        break;
}

# working with Checksum Check Job
        ChecksumCheckJob {
                $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as

[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
                echo 'Exchange checksumcheck job results:';
                if($ChecksumCheckJobRequestObject -eq $null) {
                        echo 'ChecksumCheckJobRequestObject parameter is null';
                }
                else {
                                echo 'RecoveryPointId:'
$ChecksumCheckJobRequestObject.RecoveryPointId;
                                echo 'AgentId:'
$ChecksumCheckJobRequestObject.AgentId;
                                echo 'IsNightlyJob:'
$ChecksumCheckJobRequestObject.IsNightlyJob;
                }
                break;
}


# working with Log Truncation Job
        TransferJob {
                $TransferJobRequestObject = $TransferJobRequest -as
```

```
                [Replay.Core.Contracts.Transfer.TransferJobRequest];
        echo 'Transfer job results:';
        if($TransferJobRequestObject -eq $null) {
                echo 'TransferJobRequestObject parameter is null';
        }
        else {
                echo 'TransferConfiguration:'
$TransferJobRequestObject.TransferConfiguration;
                echo 'StorageConfiguration:'
$TransferJobRequestObject.StorageConfiguration;
        }
        echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
        break;
    }
}
```

Postnightlyjobscript.ps1

Das **PostNightlyJobScript** wird auf der Kernseite nach jeder nächtlichen Aufgabe ausgeführt. Es trägt den Parameter **$JobClassName**, der bei der separaten Behandlung von solch untergeordneten Aufgaben hilft.

```
 # receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]
$NightlyAttachabilityJobRequest,  [object]$RollupJobRequest, [object]$Agents,
[object]$ChecksumCheckJobRequest,  [object]$TransferJobRequest, [int]
$LatestEpochSeenByCore, [object]$TakeSnapshotResponse)

# building path to Core's Common.Contracts.dll and loading this assembly

$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2= $regVal2 + 'CoreService\Core.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal2) | out-null


# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job,
Checksum Check Job and Log Truncation Job. All of them are triggering the
script, and $JobClassMethod (contain job name that calls the script) helps to
handle those child jobs separately

switch ($JobClassMethod) {


# working with NightlyAttachability Job

NightlyAttachabilityJob {
        $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest
-as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];
        echo 'Nightly Attachability job results:';
        if($NightlyAttachabilityJobRequestObject -eq $null) {
                echo 'NightlyAttachabilityJobRequestObject parameter is null';
        }
        else {
                echo 'AgentId:' $NightlyAttachabilityJobRequestObject.AgentId;
                echo 'IsNightlyJob:'
$NightlyAttachabilityJobRequestObject.IsNightlyJob;
        }
```

```
        break;
}


# working with Rollup Job

RollupJob {
        $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
        echo 'Rollup job results:';
        if($RollupJobRequestObject -eq $null) {
                echo 'RollupJobRequestObject parameter is null';
        }
        else {
                echo 'SimultaneousJobsCount:'
$RollupJobRequestObject.SimultaneousJobsCount;
                echo 'AgentId:' $RollupJobRequestObject.AgentId;
                echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
        }
        $AgentsCollection = $Agents -as
"System.Collections.Generic.List``1[System.Guid]"
        if($AgentsCollection -eq $null) {
                echo 'AgentsCollection parameter is null';
        }
        else {
                echo 'Agents GUIDs:'
                foreach ($a in $AgentsCollection) {
                echo $a
            }
        }
        break;
}


# working with Checksum Check Job
        ChecksumCheckJob {
                $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
                echo 'Exchange checksumcheck job results:';
                if($ChecksumCheckJobRequestObject -eq $null) {
                        echo 'ChecksumCheckJobRequestObject parameter is null';
                }
                else {
                        echo 'RecoveryPointId:'
$ChecksumCheckJobRequestObject.RecoveryPointId;
                        echo 'AgentId:' $ChecksumCheckJobRequestObject.AgentId;
                        echo 'IsNightlyJob:'
$ChecksumCheckJobRequestObject.IsNightlyJob;
                }
        break;
    }


# working with Log Truncation Job
        TransferJob {
                $TransferJobRequestObject = $TransferJobRequest -as
[Replay.Core.Contracts.Transfer.TransferJobRequest];
                echo 'Transfer job results:';
                if($TransferJobRequestObject -eq $null) {
                        echo 'TransferJobRequestObject parameter is null';
                }
                else {
                        echo 'TransferConfiguration:'
$TransferJobRequestObject.TransferConfiguration;
```

```
                        echo 'StorageConfiguration:'
$TransferJobRequestObject.StorageConfiguration;
                }
                echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
                $TakeSnapshotResponseObject = $TakeSnapshotResponse -as
[Replay.Agent.Contracts.Transfer.TakeSnapshotResponse];
                if($TakeSnapshotResponseObject -eq $null) {
                        echo 'TakeSnapshotResponseObject parameter is null';
                }
                else {
                        echo 'ID of this transfer session:'
$TakeSnapshotResponseObject.Id;
                        echo 'Volumes:' $TakeSnapshotResponseObject.Volumes;
                }
                break;
        }
}
```

Beispielskripte

Die folgenden Beispielskripte werden zur Verfügung gestellt, um die Administratorbenutzer beim Ausführen von PowerShell-Skripten zu unterstützen.

Die Beispielskripte umfassen:

- PreTransferScript.ps1
- PostTransferScript.ps1
- PreExportScript.ps1
- PostExportScript.ps1
- PreNightlyJobScript.ps1
- PostNightlyJobScript.ps1

10

Wie Sie Hilfe bekommen

Ausfindig machen der Dokumentation und Software-Aktualisierungen

In der AppAssure Core Console stehen direkte Links zu AppAssure, Gerätedokumentation und Softwareaktualisierungen zur Verfügung. Um auf die Links zuzugreifen, klicken Sie auf die Registerkarte **Appliance** (Gerät), und klicken Sie dann auf **Overall Status** (Allgemeinzustand). Sie finden die Links für die Softwareaktualisierungen und Dokumentation im Abschnitt **Documentation** (Dokumentation).

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**, füllen Sie das Formular aus und klicken Sie auf **Senden**, um uns Ihre Rückmeldung zukommen zu lassen.