# Dell DL1000 Appliance
# 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

# Vorstellung Ihres Dell DL1000

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

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

## Dell DL1000-Kerntechnologien

Ihr Gerät kombiniert die folgenden Technologien:

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

### Live Recovery

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

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

### Universal Recovery

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

Die Universal Recovery-Technologie beschleunigt auch plattformübergreifende Verschiebungen zwischen virtuellen Maschinen, zum Beispiel von VMware zu Hyper-V bzw. von Hyper-V zu VMware. Sie

umfasst die Wiederherstellung auf Anwendungs-, Element- und Objektebene von einzelnen Dateien, Ordnern, E-Mails, Kalenderelementen, Datenbanken und Anwendungen.

### True Global Deduplication

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

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


**Abbildung 1. Diagramm der echten globalen Deduplizierung**

### Verschlüsselung

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

# Dell DL1000-Datenschutzfunktionen

## Dell DL1000 Core

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

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

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

## Dell DL1000-Smart Agent

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

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

## Snapshot-Prozess

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

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

## Replikation – Notfallwiederherstellungsstandort oder Dienstanbieter

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

Der Quellkern kopiert die Wiederherstellungspunkte der ausgewählten geschützten Maschinen und überträgt die inkrementellen Snapshot-Daten asynchron und dauerhaft auf den Zielkern an einem Remote-Notfallwiederherstellungsstandort. Sie können eine ausgehende Replikation auf ein

unternehmenseigenes Rechenzentrum oder auf einen Remote-Notfallwiederherstellungsstandort (selbstverwalteter Zielkern) konfigurieren. Außerdem können Sie eine ausgehende Replikation auch auf einen MSP-Standort (Managed Service Provider) eines Drittanbieters oder auf einen Cloud-Anbieter, der externe Backups und einen Notfall-Wiederherstellungs-Service bereitstellt, konfigurieren. Bei der Replikation auf einen Zielkern eines Drittanbieters können Sie integrierte Arbeitsabläufe verwenden, über die Sie Verbindungen anfordern und automatische Rückmeldungen erhalten können.

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

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

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

## Wiederherstellung

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

## Recovery-as-a-Service (RaaS)

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

DL1000 kann keine mehrere Mandanten verwalten. Die MSPs können das DL1000 an mehreren Standorten verwenden und eine mandantenfähige Umgebung an deren Ende erstellen.

## Virtualisierung und Cloud

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

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

- VMware Workstation oder Server in einem Ordner
- Direkter Export auf einen VSphere- oder VMware ESXi-Host
- Export zu Oracle VirtualBox
- Microsoft Hyper-V-Server auf Windows Server 2008 (x64)
- Microsoft Hyper-V Server auf Windows Server 2008 R2
- Microsoft Hyper-V Server auf Windows Server 2012 R2

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

# Dell DL1000-Bereitstellungsarchitektur

Die DL1000-Bereitstellungsarchitektur besteht aus lokalen 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 Sicherungsserver, der Kern genannt wird, und mindestens einer geschützten Maschine, die als Agent bezeichnet wird. Die externe Komponente ist mithilfe von Replikation aktiviert, die volle Wiederherstellungsfähigkeiten im DR-Ort bietet. Der DL1000-Kern verwendet Basisabbilder und inkrementelle Snapshots, um die Wiederherstellungspunkte der geschützten Agenten zu kompilieren.

Darüber hinaus ist DL1000 mit Anwendungserkennung ausgestattet, da es die Fähigkeit besitzt, vorhandene Microsoft Exchange- und SQL-Anwendungen und ihre entsprechenden Datenbanken und Protokolldateien zu erkennen. Sicherungen werden mithilfe anwendungsspezifischer Snapshots auf Blockebene durchgeführt. DL1000 führt das Abschneiden des Protokolls der geschützten Microsoft Exchange-Server aus.

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

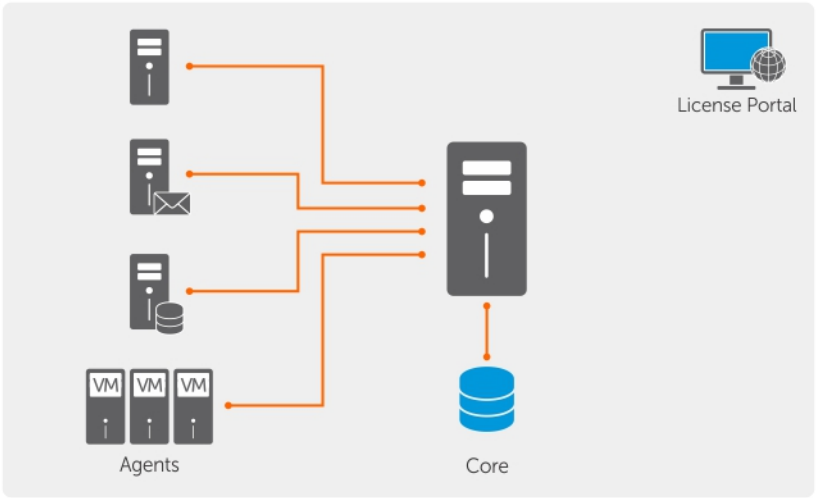


**Abbildung 2. Dell DL1000-Bereitstellungsarchitektur**

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

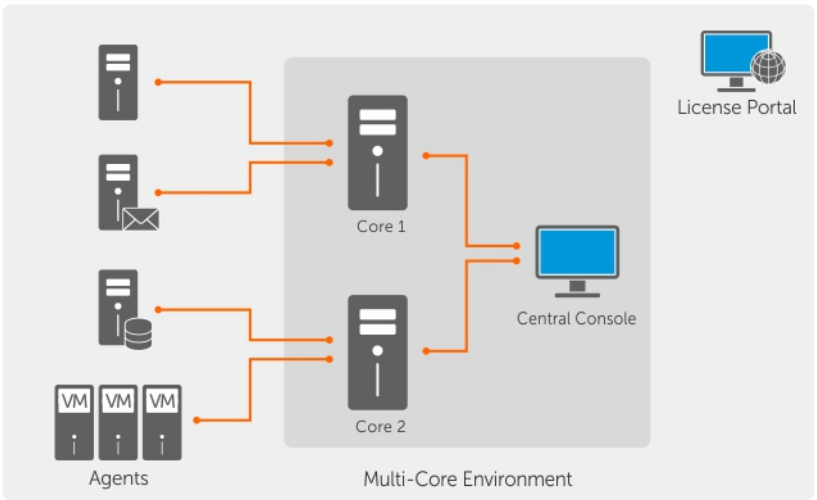


**Abbildung 3. DL1000 Multi – Core Deployment Architecture (Multi-Kern-Bereitstellungsarchitektur)**

# Weitere nützliche Informationen

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

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

**ANMERKUNG:** Lesen Sie für sämtliche Dokumentation im Zusammenhang mit Dell OpenManage Server Administrator die Seite **dell.com/openmanage/manuals**.

Die Produktdokumentation beinhaltet:

| | |
|---|---|
| **Handbuch zum Einstieg** | Stellt eine Übersicht über die Systemfunktionen, das Einrichten des Systems und die technischen Spezifikationen bereit. Dieses Dokument wird auch mit dem System mitgeliefert. |
| **System-Platzset** | Enthält Informationen zum Einrichten und Installieren der Software in Ihrer AppAssure-Lösung. |
| **Benutzerhandbuch** | Bietet Informationen zu Systemfunktionen, zur Fehlerbehebung am System und zur Installation oder zum Austausch von Systemkomponenten. |
| **Bereitstellungshandbuch** | Enthält Informationen zur Hardwarebereitstellung und zur Erstbereitstellung der Appliance. |
| **Benutzerhandbuch** | Enthält Informationen über die Konfiguration und die Verwaltung des Systems. |
| **Versionshinweise** | Bietet Produktinformationen und weitere Informationen über die Dell DL 1000 Appliance. |
| **Interoperabilitätshandbuch** | Enthält Informationen zu unterstützter Software und Hardware für die DL1000 Appliance, sowie Überlegungen, Empfehlungen und Richtlinien zur Nutzung. |
| **OpenManageServer Administrator Benutzerhandbuch** | Enthält Informationen über die Verwendung von Dell OpenManage Server Administrator zur Verwaltung des Systems. |
| **Resource-Medien** | Alle im Lieferumfang des Systems enthaltenen Medien mit Dokumentationen und Hilfsmitteln zur Konfiguration und Verwaltung des Systems. Dazu gehören diejenigen in Bezug auf das Betriebssystem, Systemverwaltungssoftware, Systemaktualisierungen und mit dem System erworbene Komponenten. |

2

# Verwendung von DL1000

## Zugriff auf die DL1000-Kern-Konsole

So greifen Sie auf die DL1000-Core Console zu:

1. Aktualisieren Sie vertrauenswürdige Sites im Browser.
2. Konfigurieren Sie Ihre Browser für den Remote-Zugriff auf die DL1000-Core Console. Weitere Informationen finden Sie unter Konfigurieren des Browsers für den Remote-Zugriff auf die Core Console.
3. Führen Sie für den Zugriff auf die DL1000-Core Console einen der folgenden Schritte aus:
   - Melden Sie sich lokal bei Ihrem DL1000-Kernserver an, und klicken Sie dann doppelt auf das Symbol **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 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**.

### 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.

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**.

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 Host-Namen oder die IP-Adresse, durch Kommas getrennt, des Gerätesystems ein, das den AppAssure 5-Kern hostet; zum Beispiel: *IP-Adresse*,*Host-Name*.
4. Starten Sie Firefox neu.

# Lizenzverwaltung

Sie können Ihre DL1000-Lizenzen direkt über die Core Console verwalten. Über die Konsole aus können Sie den Lizenzschlüssel ändern und den Lizenzserver kontaktieren. Sie können auch auf das Dell AppAssure License Portal (Lizenzportal) von der Seite **Licensing** (Lizenzierung) in der Core Console zugreifen.

Die Seite **Licensing** (Lizenzierung) enthält die folgenden Informationen:

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

## Ändern eines Lizenzschlüssels

So ändern Sie einen Lizenzschlüssel:

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

   Die Seite **Licensing** (Lizenzierung) wird angezeigt.
2. Klicken Sie auf der Seite **License Details** (Lizenzdetails) auf **Change** (Ändern).

   Das Dialogfeld **Change License Key** (Lizenzschlüssel ändern) wird angezeigt.
3. Geben Sie im Dialogfeld **Lizenzschlüssel ändern** den neuen Lizenzschlüssel ein und klicken Sie auf **OK**.

## Kontaktieren des Lizenzportalservers

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

So kontaktieren Sie den Portalserver:

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

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

## 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 bei 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 während der erstmaligen Konfiguration der Appliance einen dauerhaften Anzeigenamen auswählen. Wenn Sie ihn zu einem späteren Zeitpunkt ändern, müssen Sie mehrere Schritte manuell ausführen, um sicherzustellen, dass der neue Hostname in Kraft tritt und das System richtig funktioniert.

So ändern Sie den Anzeigenamen des Kerns

1. Navigieren Sie zur Core Console, und klicken Sie auf **Configuration (Konfiguration)** → **Settings** (Einstellungen).
2. Klicken Sie im Bereich **General** (Allgemein) auf **Change** (Ändern).
   Das Dialogfeld **Display Name** (Anzeigename) wird angezeigt.
3. Geben Sie im Textfeld **Display Name** (Anzeigename) einen neuen Anzeigenamen für den Kern ein.
4. Klicken Sie auf **OK**.

## Ändern der Zeit für eine nächtliche Aufgabe

Die Option „Nightly Job" (Nächtliche Aufgaben) plant Aufgaben wie Rollup, Anfügbarkeit und Abschneiden für Agenten, die durch den Kern geschützt werden.

So passen Sie die Zeit für eine nächtliche Aufgabe an:

1. Navigieren Sie zur Core Console, und wählen Sie **Configuration (Konfiguration)** → **Settings** (Einstellungen) aus.
2. Klicken Sie im Bereich **Nightly Jobs** (Nächtliche Aufgaben) auf **Change** (Ändern).
   Das Dialogfeld **Nächtliche Aufgaben** wird angezeigt.
3. Geben Sie im Textfeld **Nightly Jobs Time** (Startzeit für nächtliche Aufgaben) eine neue Startzeit ein.
4. 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 Wiederholungen für die Übertragung der Daten einrichtet.

So ändern Sie die Einstellungen für die Übertragungswarteschlange:

1. Navigieren Sie zur Core Console, und klicken Sie auf **Configuration (Konfiguration)** → **Settings** (Einstellungen).
2. Klicken Sie im Bereich **Transfer Queue** (Übertragungswarteschlange) auf **Change** (Ändern).

   Das Dialogfeld **Übertragungswarteschlange** wird angezeigt.
3. 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.
4. Geben Sie im Textfeld **Maximum Retries** (Maximale Anzahl erneuter Versuche) einen Wert ein, um die maximale Anzahl an Wiederholungsversuchen zu aktualisieren.
5. Klicken Sie auf **OK**.

## Anpassen der Client-Zeitüberschreitungseinstellungen

Die Einstellungen für Client-Zeitüberschreitungen geben die Anzahl von Sekunden oder Minuten an, die der Server abwartet, bevor ein Timeout auftritt, wenn er versucht, eine Verbindung zu einem Client herzustellen.

So stellen Sie die Client-Zeitüberschreitungseinstellungen ein:

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

   Das Dialogfeld **Client-Zeitüberschreitungseinstellungen** wird angezeigt.
3. Geben Sie im Textfeld **Connection Timeout** (Verbindungszeitüberschreitung) die Anzahl an Minuten und Sekunden ein, die vor einem Verbindungstimeout verstreichen müssen.
4. Geben Sie im Textfeld **Lese-/Schreibzeitüberschreitung** die Anzahl an Minuten und Sekunden ein, die vor einem Timeout während eines Lese-/Schreibereignisses verstreichen müssen.
5. Klicken Sie auf **OK**.

## Konfigurieren von Deduplizierungs-Cache-Einstellungen

Die globale Deduplizierung verringert die Menge an Speicherplatz für die gesicherten Daten. Der Deduplizierungs-Volume-Manager (Deduplication Volume Manager, DVM) vereint eine Reihe von Speicherorten in einem Repository. Der Deduplizierungs-Cache enthält Verweise auf einzigartige Blöcke. Standardmäßig hat der Deduplizierungs-Cache eine Größe von 1,5 GB. Wenn die Menge an redundanten Daten so groß ist, dass der Deduplizierungs-Cache voll ist, kann das Repository nicht mehr den vollen Nutzen aus der weiteren Deduplizierung über das Repository hinweg für neu hinzugefügte Daten bringen. Sie können dann die Größe des Deduplizierungs-Cache erhöhen, indem Sie die Deduplizierungs-Cache-Konfiguration in der Core Console anpassen.

So konfigurieren Sie Deduplizierungs-Cache-Einstellungen:

1. Navigieren Sie zur Core Console, und klicken Sie auf **Configuration (Konfiguration)** → **Settings** (Einstellungen).
2. Klicken Sie im Bereich **Deduplication Cache Configuration** (Konfiguration des Deduplizierungs-Cache) auf **Change** (Ändern).

Das Dialogfeld **Konfiguration des Deduplizierungs-Cache** wird angezeigt.

3. Geben Sie im Textfeld **Primary Cache Location** (Primärer Cache-Speicherort) den aktualisierten primären Cache-Speicherort ein.
4. Geben Sie im Textfeld **Secondary Cache Location** (Sekundärer Cache-Speicherort) den aktualisierten sekundären Cache-Speicherort ein.
5. Geben Sie im Textfeld **Metadata Cache Location** (Metadaten-Cache-Speicherort) den aktualisierten Metadaten-Cache-Speicherort ein.
6. 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, und klicken Sie auf **Configuration (Konfiguration)** → **Settings** (Einstellungen).
2. Klicken Sie im Abschnitt **Replay Engine Configuration** (Replay-Modulkonfiguration) auf **Change** (Ändern).

   Das Dialogfeld **Replay-Modulkonfiguration** wird angezeigt.
3. Geben Sie im Dialogfeld **Replay Engine Configuration** (Replay-Modulkonfiguration) die **IP-Adresse** an. Wählen Sie eine der folgenden Optionen aus:
   - 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 **Use a specific IP Address** (Spezifische Adresse verwenden).
4. Geben Sie die nachfolgend beschriebenen Konfigurationsinformationen ein:

| Textfeld | Beschreibung |
|---|---|
| **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. |
| **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. |

| Textfeld | Beschreibung |
|---|---|
| **Read Timeout (Zeitüberschreitung 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 (Zeitüberschreitung beim Schreiben)** | Geben Sie einen Wert für die Zeitüberschreitung beim Schreiben ein oder wählen Sie die Standardeinstellung aus. Die Standardeinstellung ist 00:00:30. |

5. Wählen Sie **No Delay** (Keine Verzögerung) aus.
6. Klicken Sie auf **OK**.

## Ändern von Bereitstellungseinstellungen

So ändern Sie die Bereitstellungseinstellungen:

1. Wechseln Sie zur Core Console, klicken Sie auf die Registerkarte **Configuration** (Konfiguration) und dann **Settings** (Einstellungen).
2. Klicken Sie im Bereich **Deploy Settings** (Einstellungen bereitstellen) auf **Change** (Ändern).

   Das Dialogfeld **Deploy Settings** (Einstellungen bereitstellen) wird angezeigt.
3. Geben Sie im Textfeld **Agent Installer Name** (Name des Agenteninstallationsprogramms) den Namen der ausführbaren Datei für den Agenten ein. Der Standardwert ist **Agentweb.exe**.
4. Geben Sie in das Textfeld **Core Address** (Kernadresse) die Adresse für den Kern ein.
5. Geben Sie im Textfeld **Failed Receive Timeout** (Zeitüberschreitung Empfang fehlgeschlagen) ein, nach wie vielen Minuten ohne Aktivität die Zeitüberschreitung aktiviert werden soll.
6. Geben Sie in das Feld **Max Parallel Installs** (Maximale parallele Installiert) einen Wert für die Höchstanzahl von Installationen ein, die parallel installiert werden können.
7. Wählen Sie eine oder beide der folgenden optionalen Einstellungen aus:
   - Automatic reboot after install (Automatischer Neustart nach Installation)
   - Protect After Deploy (Nach der Bereitstellung schützen)
8. Klicken Sie auf **OK**.

## Ändern der Datenbankverbindungseinstellungen

So ändern Sie die Datenbankverbindungseinstellungen:

1. Navigieren Sie zur Core Console, und klicken Sie auf **Configuration (Konfiguration)** → **Settings** (Einstellungen).
2. Führen Sie im Bereich **Database Connection Settings** (Datenbankverbindungseinstellungen) einen der folgenden Schritte aus:
   - Um die Standardkonfiguration wiederherzustellen, klicken Sie auf **Restore Default** (Standardwerte wiederherstellen).
   - Klicken Sie zum Ändern der Datenbankverbindungseinstellungen auf **Change** (Ändern).

   Nachdem Sie auf „Change" (Ändern) geklickt haben, wird das Dialogfeld **Database Connection Settings** (Datenbankverbindungseinstellungen) angezeigt.
3. 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. |

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

# Verwalten von Ereignissen

Der Kern umfasst vordefinierte Einrichtungen von Ereignissen, mit denen Administratoren über entscheidende Probleme auf dem Kern oder bei Sicherungsaufgaben benachrichtigt werden können.

Über die Registerkarte **Events** (Ereignisse) können Sie Benachrichtigungsgruppen, E-Mail-SMTP-Einstellungen, Servereinstellungen, Enabled-Server-Einstellungen, Cloud-Konfiguration, Wiederholungsreduzierung und die Ereignisaufbewahrung verwalten.

Über die Option „Notification Groups“ (Benachrichtigungsgruppen) können Sie Benachrichtigungsgruppen verwalten, die Folgendes ermöglichen:

- 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
- 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. Klicken Sie in der Core Console auf **Configuration (Konfiguration)** → **Events** (Ereignisse).
2. Klicken Sie auf **Add Group** (Gruppe hinzufügen).

   Das Dialogfeld **Add Notification Group** (Benachrichtigungsgruppe hinzufügen) wird geöffnet. Es enthält die folgenden zwei Bereiche:

   - **Warnungen aktivieren**
   - **Notification Options (Benachrichtigungsoptionen)**

### Aktivieren von Warnmeldungen

Durch das Aktivieren von Warnmeldungen können Sie die Systemereignisse festlegen, die Sie protokollieren möchten, außerdem Berichte erstellen und Warnungen festlegen.

ANMERKUNG: Wählen Sie zum Erstellen von Warnungen für alle Ereignisse **All Alerts** (Alle Warnungen) aus.

- Wählen Sie zum Erstellen von Warnmeldungen, die sich auf Fehler beziehen, von Warnungen, Informationsmeldungen oder einer Kombination eine der folgenden Optionen aus:
  - red triangle icon (Error) (rotes Dreieck-Symbol (Fehler))
  - yellow triangle icon (Warning) (gelbes Dreieck-Symbol (Warnung))
  - blue circle (Information) (blauer Kreis (Information))
  - curved arrow (Restores default) (gebogener Pfeil (stellt die Standardeinstellungen wieder her))
- Klicken Sie zum Erstellen von Warnungen für bestimmte Ereignisse auf das Symbol **>** neben der relevanten Gruppe, und aktivieren Sie das Kontrollkästchen, um die Warnung zu aktivieren.

### Konfigurieren von Benachrichtigungsoptionen

1. 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 E-Mail-Benachrichtigung an. Sie können separate E-Mail-Adressen und, wie unten gezeigt, Blindkopien und Kopien eingeben:<br>• **in:**<br>• **Cc:**<br>• **Bcc:** |
| **Notify by Windows Event Log (Über Windows-** | Wählen Sie diese Option aus, wenn Warnmeldungen durch das Windows-Ereignisprotokoll gemeldet werden sollen. |

| Textfeld | Beschreibung |
|---|---|
| **Ereignisprotokoll benachrichtigen)** | |
| **Notify by sys logd (Durch sys logd benachrichtigen).** | Wählen Sie diese Option aus, wenn Benachrichtigungen durch „sys logd" gemeldet werden sollen. Geben Sie die Details für „sys logd" in die folgenden Textfeldern ein:<br>• **Hostname**<br>• **Port 1** |
| **Notify by Toast alerts (Über Pop-up-Warnungen benachrichtigen)** | Wählen Sie diese Option aus, damit die Warnung in einem Popup-Fenster in der rechten unteren Ecke des Bildschirms angezeigt wird. |

2. Klicken Sie auf **OK**.

   Die folgende Meldung wird angezeigt: **The Group name cannot be changed after the creation of the Notification Group. are you sure you want to use this name?** (Der Gruppenname kann nach der Erstellung der Benachrichtigungsgruppe nicht geändert werden. Sind Sie sicher, dass Sie diesen Namen verwenden möchten?)

   - Um den Gruppennamen zu speichern, klicken Sie auf **Yes** (Ja).
   - Um den Gruppennamen zu ändern, klicken Sie auf **No** (Nein). Kehren Sie zum Fenster **Notification Options** (Benachrichtigungsoptionen) zurück, aktualisieren Sie den Gruppennamen und andere Benachrichtigungsgruppeneinstellungen, und speichern Sie die Arbeit.

## Konfigurieren eines E-Mail-Servers

ANMERKUNG: Sie müssen die Benachrichtigungsgruppeneinstellungen konfigurieren und außerdem die Option **Notify by email** (Per E-Mail benachrichtigen) aktivieren, bevor Sie E-Mail-Warnmeldungen versenden.

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

1. Klicken Sie in der Core Console auf **Configuration (Konfiguration)** → **Events** (Ereignisse).
2. Klicken Sie auf der Seite **Email Settings** (E-Mail-Einstellungen) auf **SMTP server** (SMTP-Server).

   Daraufhin wird das Dialogfeld **SMTP Server Settings** (SMTP-Server-Einstellungen) angezeigt.
3. Geben Sie die Details für den E-Mail-Server wie folgt ein:

| Textfeld | Beschreibung |
|---|---|
| **SMTP-Server** | Geben Sie den Namen des E-Mail-Servers, der von der E-Mail-Benachrichtigungsvorlage verwendet werden soll, ein. Die Benennungskonvention umfasst Hostname, Domain und Suffix; z.B. **smtp.gmail.com.** |
| **Von** | Geben Sie eine Absender-E-Mail-Adresse ein. Diese Option wird zur Angabe der Absender-E-Mail-Adresse für die E-Mail-Benachrichtigungsvorlage verwendet; z.B. **noreply@localhost.com**. |
| **Benutzername** | Geben Sie einen Benutzernamen für den E-Mail-Server ein. |
| **Kennwort** | Geben Sie ein Kennwort für den Zugriff auf den E-Mail-Server ein. |

| Textfeld | Beschreibung |
|---|---|
| **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.<br>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.<br>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. |

4. Klicken Sie auf **Send Test Email** (Test-E-Mail senden), um Folgendes auszuführen:
   a. Geben Sie im Dialogfeld „Send Test Email" (Test-E-Mail senden) eine Empfänger-E-Mail-Adresse für die Testnachricht ein, und klicken Sie dann auf **Send** (Senden).
   b. Wenn die Test-E-Mail nicht erfolgreich versendet wird, beenden Sie das Fehler-Dialogfeld und das Dialogfeld **Send Test Email** (Test-E-Mail senden), und überarbeiten Sie die Einstellungen Ihrer E-Mail-Server-Konfiguration. Wiederholen Sie dann Schritt 4.
   c. Klicken Sie zum Bestätigen auf **OK**.
   d. Überprüfen Sie, ob die Test-E-Mail-Nachricht gesendet wurde.
   e. Kehren Sie zurück zum Dialogfeld „SMTP Server Settings" (SMTP-Server-Einstellungen), klicken Sie dort zum Schließen des Dialogfelds auf **Save** (Speichern), und speichern Sie die Einstellungen.

## Konfigurieren einer E-Mail-Benachrichtigungsvorlage

Zum Empfangen von E-Mail-Benachrichtigungen über Ereignisse müssen Sie einen E-Mail-Server und eine E-Mail-Benachrichtigungsvorlage konfigurieren.

ANMERKUNG: Um E-Mail-Warnmeldungen zu empfangen, konfigurieren Sie Benachrichtigungsgruppeneinstellungen, und aktivieren Sie die Option **Notify by email** (Per E-Mail benachrichtigen).

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

1. Klicken Sie in der Core Console auf **Configuration (Konfiguration)** → **Events** (Ereignisse).
2. Klicken Sie im Bereich **Email Settings** (E-Mail-Einstellungen) auf **Change** (Ändern).
   Das Dialogfeld **Edit Email Notification Configuration** (Konfiguration der E-Mail-Benachrichtigung bearbeiten) wird angezeigt.
3. Wählen Sie die Option **Enable email notifications** (E-Mail-Benachrichtigungen aktivieren) aus, und geben Sie dann wie folgt die Details für den E-Mail-Server ein:

| Textfeld | Beschreibung |
|---|---|
| **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>`. |

| Textfeld | Beschreibung |
|---|---|
| **E-Mail** | Geben Sie Informationen für den Nachrichtentext der Vorlage ein, mit denen das Ereignis, der Ereigniszeitpunkt und der Schweregrad beschrieben werden. |

4. Klicken Sie auf **Send Test Email** (Test-E-Mail senden), um die folgenden Schritte auszuführen:
   a. Geben Sie im Dialogfeld „Send Test Email" (Test-E-Mail senden) eine Empfänger-E-Mail-Adresse für die Testnachricht ein, und klicken Sie dann auf **Send** (Senden).
   b. Wenn die Test-E-Mail nicht versendet werden kann, schließen Sie das Fehlerdialogfeld und das Dialogfeld „Send Test Email" (Test-E-Mail senden), klicken Sie dann auf **OK**, um die aktuellen E-Mail-Vorlageeinstellungen zu speichern, und ändern Sie Ihre E-Mail-Server-Einstellungen. Weitere Informationen finden Sie unter Configuring An Email Server And Email Notification Template (Konfigurieren eines E-Mail-Servers und einer E-Mail-Benachrichtigungs-Vorlage). Stellen Sie sicher, dass Sie das Kennwort für dieses E-Mail-Konto erneut eingeben. Speichern Sie die Einstellungen, und kehren Sie zu Schritt 4 zurück.
   c. Klicken Sie zum Bestätigen auf **OK**.
   d. Überprüfen Sie, ob die Test-E-Mail-Nachricht gesendet wurde.
   e. Kehren Sie zum Dialogfeld **Edit Email Notification Configuration** (Konfiguration der E-Mail-Benachrichtigung bearbeiten) zurück, und klicken Sie auf **OK**, um das Dialogfeld zu schließen; speichern Sie dann die Einstellungen.

### Konfigurieren der Wiederholungsreduzierung

So konfigurieren Sie die Wiederholungsreduzierung:

1. Klicken Sie in der Core Console auf **Configuration (Konfiguration)** → **Events** (Ereignisse).
2. Klicken Sie im Bereich **Repetition Reduction** (Wiederholungsreduzierung) auf **Change** (Ändern).

   Das Dialogfeld **Enable Repetition Reduction** (Wiederholungsreduzierung aktivieren) wird angezeigt.
3. Wählen Sie **Enable Repetition Reduction** (Wiederholungsreduzierung aktivieren) aus.
4. Geben Sie im Textfeld **Store events for** (Ereignisse speichern für) die Anzahl an Minuten ein, die die Ereignisse für die Wiederholungsreduzierung gespeichert werden sollen.
5. Klicken Sie auf **OK**.

### Konfigurieren der Ereignisaufbewahrung

So konfigurieren Sie die Ereignisaufbewahrung:

1. Klicken Sie in der Core Console auf **Configuration (Konfiguration)** → **Settings (Einstellungen)**.
2. Klicken Sie unter **Database Connection Settings** (Datenbankverbindungseinstellungen) auf **change** (Ändern).

   Das Dialogfeld **Datenbankverbindungseinstellungen** wird angezeigt.
3. 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.
4. Klicken Sie auf **Save** (Speichern).

## Verwalten von Repositories

Ein Repository speichert die Snapshots, die von den geschützten Arbeitsstationen und Servern erfasst werden. Das Repository für DL1000 ist vorkonfiguriert. Das Repository befindet sich auf dem internen Speicher des Systems.

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.

## Anzeigen von Details zu einem Repository

So zeigen Sie die Details eines Repositorys an:

1. Klicken Sie in der Core Console auf **Configuration (Konfiguration)** → **Repositories (Repositories)**.
2. Klicken Sie **>** neben der **Status**-Spalte des Repositorys, das Sie ändern möchten.
3. Details für das Repository 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), der Leserate (MB/s) und der Schreibrate (MB/s).
   - **Storage Engine** (Speicher Engine) – Schließt die Rate (MB/s) Leserate (MB/s) und die Schreibrate (MB/s) ein.

## Überprüfen eines Repositorys

Die Core Console kann bei Auftreten eines Fehlers eine Diagnoseprüfung eines Repository-Volumes durchführen. Fehler am Kern können auf das nicht vorschriftsmäße Heruntergefahren oder einen Hardware-Fehler zurückzuführen sein.

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

So überprüfen Sie ein Repository:

1. Klicken Sie auf **Configuration (Konfiguration)** → **Repositories** (Repositories).
2. Klicken Sie auf das Symbol „Settings" (Einstellungen) neben der Spalte „Compression Ratio" (Komprimierungsgrad) unterhalb der Schaltfläche **Actions** (Vorgänge).
3. Klicken Sie auf **Check** (Prüfen).

   Das Dialogfeld **Repository überprüfen** wird angezeigt.
4. Klicken Sie im Dialogfeld **Check Repository** (Repository überprüfen) auf **Check** (Überprüfen).

   ANMERKUNG: Wenn Sie eine Überprüfung ausführen, werden alle aktiven Aufgaben im Zusammenhang mit diesem Repository abgebrochen. Bevor die Prüfung beginnt, wird eine Meldung angezeigt, in der Sie aufgefordert werden, zu bestätigen, dass die Prüfung fortgesetzt wird. Es wird empfohlen, den Cache für Wiederherstellungspunkte neu zu erstellen. Das Fehlschlagen einer Prüfung wird dazu führen, dass Sie das Repository aus einem Archiv wiederherstellen müssen.

# Verwalten von Sicherheit

DL1000 bietet starke Verschlüsselung, bei der Sicherungen von geschützten Maschinen nicht zugänglich sind. Nur der Benutzer mit dem Verschlüsselungsschlüssel kann auf diese Daten zugreifen und sie entschlüsseln. Die Verschlüsselung wirkt sich nicht auf die Leistung aus. Wichtige Repository-Konzepte und -Überlegungen sind u. a.:

- 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 Verschlüsselungsschlüssel zum Kern hinzufügen, davon entfernen, importieren, exportieren, ändern und löschen.

## Hinzufügen eines Verschlüsselungscodes

So fügen Sie einen Verschlüsselungsschlüssel hinzu:

1. Klicken Sie in der Core Console auf **Configuration (Konfiguration)** → **Security** (Sicherheit).
2. Klicken Sie im Drop-Down-Menü **Actions** (Aktionen) auf **Add Encryption Key** (Verschlüsselungsschlüssel hinzufügen).

   Das Dialogfeld **Create Encryption Key** (Verschlüsselungsschlüssel erstellen) wird angezeigt.
3. 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. |

4. Klicken Sie auf **OK**.

   **VORSICHT: Es wird empfohlen, dass Sie die Passphrase sicher aufbewahren. Wenn Sie Ihren Passphrase verlieren oder vergessen, können Sie Ihre Daten nicht wiederherstellen.**

## Bearbeiten eines Verschlüsselungscodes

So bearbeiten Sie einen Verschlüsselungsschlüssel:

1. Klicken Sie in der Core Console auf **Configuration (Konfiguration)** → **Security** (Sicherheit).

   Der Bildschirm **Encryption Keys** (Verschlüsselungsschlüssel) wird angezeigt.
2. Klicken Sie auf das Symbol der rechten spitzen Klammer **>** neben dem Namen des Verschlüsselungsschlüssels, den Sie bearbeiten möchten. Klicken Sie dann auf **Bearbeiten**.

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

## Ändern einer Verschlüsselungscode-Passphrase

So ändern Sie eine Verschlüsselungsschlüssel-Passphrase:

1. Klicken Sie in der Core Console auf **Configuration (Konfiguration)** → **Security** (Sicherheit).
2. Klicken Sie auf das Symbol der rechten spitzen Klammer **>** neben dem Namen des Verschlüsselungsschlüssels, den Sie bearbeiten möchten. Klicken Sie dann auf **Passphrase ändern**.

   Das Dialogfeld **Passphrase ändern** wird angezeigt.
3. 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.
4. 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. Klicken Sie in der Core Console auf **Configuration (Konfiguration)** → **Security** (Sicherheit).
2. Klicken Sie im Drop-Down-Menü **Actions** (Maßnahmen) auf **Import** (Importieren).

   Das Dialogfeld **Schlüssel importieren** wird angezeigt.
3. 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).
4. Klicken Sie auf **OK**.

## Exportieren eines Verschlüsselungscodes

So exportieren Sie einen Verschlüsselungsschlüssel:

1. Klicken Sie in der Core Console auf **Configuration (Konfiguration)** → **Security** (Sicherheit).
2. Wählen Sie im Dropdown-Menü „Configuration" (Konfiguration) für den Verschlüsselungsschlüssel, den Sie exportieren möchten, die Option **Export** (Exportieren) aus.

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

## Entfernen eines Verschlüsselungsschlüssels

So entfernen Sie einen Verschlüsselungsschlüssel:

1. Klicken Sie in der Core Console auf **Configuration (Konfiguration)** → **Security** (Sicherheit).
2. Wählen Sie aus dem Drop-Down-Menü „Configuration" (Konfiguration) für den Verschlüsselungsschlüssel, den Sie entfernen möchten, die Option **Remove** (Entfernern) aus.

   Das Dialogfeld **Remove Key** (Schlüssel entfernen) wird angezeigt.
3. 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 |

| Cloud Type (Cloud-Typ) | Textfeld | Beschreibung |
|---|---|---|
| | | 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. |
| | 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.

# Überwachen der DL1000

Sie können den Status der DL1000 Appliance-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 Zustand des Subsystems anzeigt.

Die Seite „Overall Status" (Allgemeiner Status) enthält außerdem Links zu Tools, die bis zu den Details der jeweiligen Subsysteme vordringen; dies kann zum Beheben von Warnungen oder Fehlern nützlich sein. Der **Systemadministrator**-Link, der für die Geräte-Hardware- und Speicher-Hardware-Subsysteme zur Verfügung steht, fordert Sie zur Anmeldung an der Systemadministrator-Anwendung für die Verwaltung der Hardware auf. Weitere Informationen zur Systemadministrator-Anwendung finden Sie im *OpenManage Server Administrator User's Guide* (OpenManage Server-Administrator-Benutzerhandbuch) auf **dell.com/support/manuals**.

# Aktualisieren des DL1000

ANMERKUNG: Dell empfiehlt, dass Sie aktuelle Version von AppAssure über das Dell License Activation-Portal unter Verwendung des Installationsprogramms herunterladen.

ANMERKUNG: Für Software-Aktualisierungen erhalten Sie eine Benachrichtigung für ein Upgrade auf die neueste Version.

# Reparieren des DL1000

ANMERKUNG: Vergewissern Sie sich vor Beginn der Reparaturen, dass die Kerndienste gestoppt sind.

## Appliance-Schnellselbstwiederherstellung

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

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

1. Setzen Sie den erstellten RASR-USB-Schlüssel ein.
2. Starten Sie die Appliance über den RASR-USB-Schlüssel neu.
3. Klicken Sie auf **Rapid Appliance Self Recovery** (Appliance-Schnellselbstwiederherstellung).
   Ein Willkommensbildschirm wird eingeblendet.
4. Klicken Sie auf **Weiter**.
   Der Bildschirm zum Überprüfen der **Prerequisites** (Voraussetzungen) wird angezeigt.

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

5. Klicken Sie auf **Weiter**.

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

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

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

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

7. Klicken Sie auf **Weiter**.

   Daraufhin wird der Bildschirm **Storage Configuration** (Speicherkonfiguration) angezeigt.

8. Auf dem Bildschirm **OS Recovery** (Betriebssystemwiederherstellung) wird die folgende Warnmeldung angezeigt: `This operation will recover the operating system. All OS disk data will be overwritten.` (Mit diesem Vorgang wird das Betriebssystem wiederhergestellt. Alle Betriebssystemlaufwerksdaten werden überschrieben.)

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

   Der Betriebssystemdatenträger beginnt mit der Wiederherstellung der Werkseinstellungen.

10. Klicken Sie auf **Fertigstellen**.

### Erstellen des RASR-USB-Sticks

ANMERKUNG: Nach der Erstinstallation der Software wird der **AppAssure Appliance Configuration Wizard** (AppAssure-Gerätekonfigurationsassistent) automatisch gestartet. Das Statussymbol auf der Registerkarte **Appliance** (Gerät) wird gelb angezeigt.

So erstellen Sie einen RASR-USB-Speicherstick:

1. Navigieren Sie zur Registerkarte **Appliance** (Gerät).
2. Wählen Sie im Navigationsbereich auf der linken Seite die Optionen **Appliance (Gerät)** → **Backup** aus.

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

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

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

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

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

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

   Es wird ein Warndialogfeld angezeigt.

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

   Der RASR-USB-Laufwerks-Stick wurde erstellt.

6. ANMERKUNG: Stellen Sie sicher, dass Sie die Funktionen „Safely Remove USB Drive“ (USB-Laufwerk sicher entfernen) oder „Windows Eject Drive“ (Windows Laufwerk auswerfen) verwenden, um den USB-Stick auf das Entfernen vorzubereiten. Andernfalls wird der Inhalt auf dem USB-Stick gegebenenfalls beschädigt und der USB-Stick funktioniert nicht wie erwartet.

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

3

# Schutz von Arbeitsstationen und Servern

## Wissenswertes über den Schutz von Workstations und Servern

Um Ihre Daten mit DL1000 zu schützen, müssen Sie die Arbeitsstationen und Server, die Sie schützen möchten, zur Core Console hinzufügen; zum Beispiel Ihren Exchange Server, SQL Server, oder Ihren Linux Server.

ANMERKUNG: In diesem Kapitel bezieht sich das Wort *Maschine* auch auf die AppAssure-Agentensoftware, 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).

## Bereitstellen eines Agenten (Push-Installation)

Mit DL1000 können Sie das AppAssure-Agenten-Installationsprogramm auf einzelne zu schützende Windows-Maschinen bereitstellen. Führen Sie die folgenden Schritte aus, um das Installationsprogramm einem Agenten hinzuzufügen. Weitere Informationen zum Bereitstellen von Agenten auf mehreren Maschinen zur selben Zeit finden Sie unter 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. Klicken Sie über den linken Navigationsbereich der Core Console auf **Protected Machines** (Geschützte Maschinen).
2. Klicken Sie auf **Actions (Aktionen)** → **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. |

| Textfeld | Beschreibung |
|---|---|
| **Kennwort** | Geben Sie das Kennwort ein, um eine Verbindung mit dieser Maschine herzustellen. |
| **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**.

# Schützen einer Maschine

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

ANMERKUNG: Um geschützt zu sein, muss in der Maschine die AppAssure-Agentensoftware installiert sein. Sie haben die Wahl, die AppAssure-Agentensoftware vor diesem Vorgang zu installieren, oder die Software auf dem Agenten bereitzustellen, wenn Sie im Dialogfeld **Connection** (Verbindung) den Schutz definieren. Wenn Sie die AppAssure-Agentensoftware während des Schützens einer Maschine installieren möchten, finden Sie weitere Informationen unter Bereitstellen der Agentensoftware während des Schützens 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. Starten Sie die Maschine neu, auf dem die AppAssure-Agentensoftware installiert ist, wenn Sie dies nicht bereits getan haben.
2. Klicken Sie in der Core Console auf der Kern-Maschine auf der Symbolleiste auf die Optionen **Protect (Schützen)** → **Protect Machine (Maschine schützen)**.

   Daraufhin wird der **Protect Machine Wizard** (Assistent zum Schützen der Maschine) angezeigt.
3. Wählen Sie auf der Seite **Welcome** (Willkommen) die entsprechenden Installationsoptionen aus:

- Wenn Sie kein Repository definieren oder eine Verschlüsselung aufbauen müssen, wählen Sie **Typical** (Typisch).
- Wenn die Seite **Welcome** (Willkommen) für den **Assistenten zum Schützen der Maschine** künftig nicht angezeigt werden soll, wählen Sie die Option **Skip this Welcome page the next time the wizard opens** (Seite „Willkommen" beim nächsten Öffnen des Assistenten ignorieren) aus.

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

| Textfeld | Beschreibung |
|---|---|
| **Host** | Der Hostname oder die IP-Adresse der Maschine, die Sie schützen möchten. |
| **Schnittstelle** | Die Portnummer, über die der AppAssure-Kern mit der Maschine kommuniziert. Der standardmäßige Port ist 8006. |
| **Benutzername** | Der Benutzername, der für die Verbindung mit dieser Maschine verwendet wird, z. B. Administrator. |
| **Kennwort** | Das Kennwort, das für die Verbindung mit dieser Maschine verwendet wird. |

6. Klicken Sie auf **Next** (Weiter). Wenn die Seite **Protection** (Schutz) als Nächstes im **Assistenten zum Schützen der Maschine** angezeigt wird, gehen Sie zu Schritt 7.

   ANMERKUNG: Wenn die Seite **Install Agent** (Agent installieren) als Nächstes im **Assistenten zum Schützen des Rechners** angezeigt wird, bedeutet dies, dass die Agentensoftware noch nicht auf der designierten Maschine installiert ist. Klicken Sie auf **Next** (Weiter), um die Agentensoftware zu installieren. Die Agentensoftware muss auf der Maschine installiert sein, die Sie schützen möchten; diese muss neu gestartet werden, bevor sie auf dem Kern gesichert werden kann. Damit das Installationsprogramm der Agentenmaschine neu starten kann, wählen Sie die Option **After installation, restart the machine automatically (recommended)** (Maschine nach Abschluss der Installation automatisch neu starten (empfohlen)) aus, und klicken Sie dann auf **Next** (Weiter).

7. Der Hostname oder die IP-Adresse, die Sie im Dialogfeld **Connect** (Verbinden) angegeben haben, erscheint in diesem Dialogfeld. Geben Sie optional einen neuen Namen für die Maschine ein, die in der Core Console angezeigt werden soll.
8. Wählen Sie den entsprechenden Zeitplan für den Schutz aus:
   - Um den Standard-Schutzzeitplan zu verwenden, wählen Sie unter **Schedule Settings** (Zeitplaneinstellungen) die Option **Default protection (hourly snapshots of all volumes)** (Standard-Schutz (stündlich Snapshots von allen Volumes)) aus. Bei einem Standard-Schutzzeitplan erstellt der Core alle drei Stunden Snapshots der Agentenmaschine. Snapshots der Agentenmaschine können mindestens einmal pro Stunde erstellt werden. Zum Ändern der Sicherheitseinstellungen zu einem beliebigen Zeitpunkt, nachdem Sie den Assistenten geschlossen haben, einschließlich der Entscheidung, welche Volumes geschützt werden sollen, gehen Sie zu der Registerkarte „Summary" (Zusammenfassung) für die jeweilige Agentenmaschine.
   - Um einen anderen Schutzzeitplan zu definieren, wählen Sie unter **Schedule Settings** (Zeitplaneinstellungen) die Option **Custom Protection** (Benutzerdefinierter Schutz) aus.
9. Wählen Sie eine der folgenden Optionen:
   - Wenn Sie eine typische Konfiguration im **Protect Machine Wizard** (Assistenten zum Schützen der Maschine) ausgewählt und den Standardschutz angegeben haben, klicken Sie auf **Finish** (Fertig stellen), um die Auswahl zu bestätigen, schließen Sie dann den Assistenten, und schützen Sie die angegebene Maschine.
   - Wenn einer Maschine zum ersten Mal Schutz hinzugefügt wird, beginnt ein Basisabbild (welches ein Snapshot aller Daten im geschützten Volume ist) sofort mit der Übertragung zum Repository auf dem AppAssure-Kern, außer, wenn Sie angegeben haben, anfänglich den Schutz anzuhalten.

- Wenn Sie eine typische Konfiguration für den **Protect Machine Wizard** (Assistenten zum Schützen der Maschine) ausgewählt und einen benutzerdefinierten Schutz angegeben haben, klicken Sie auf **Next** (Weiter), um einen benutzerdefinierten Schutzzeitplan einzurichten. Weitere Informationen über das Definieren eines benutzerdefinierten Schutzzeitplans finden Sie unter „Erstellen von benutzerdefinierten Schutzzeitplänen".
- Wenn Sie „Advanced Configuration" (Erweiterte Konfiguration) für den **Protect Machine Wizard** (Assistenten zum Schützen der Maschine) und den Standardschutz ausgewählt haben, klicken Sie auf **Next** (Weiter), und fahren Sie mit Schritt 12 fort, um die Repository- und Verschlüsselungsoptionen anzuzeigen.
- Wenn Sie „Advanced Configuration" (Erweiterte Konfiguration) für den **Protect Machine Wizard** (Assistenten zum Schützen der Maschine) und den benutzerdefinierten Schutz ausgewählt haben, klicken Sie auf **Next** (Weiter), und fahren Sie mit Schritt 10 fort, um auszuwählen, welche Volumes geschützt werden sollen.

10. Wählen Sie auf der Seite **Protection Volumes** (Zu schützende Volumes) die auf der Agentenmaschine zu schützenden Volumes aus. Wenn Volumes aufgelistet sind, die Sie nicht in den Schutz aufnehmen möchten, klicken Sie in die Spalte „Check" (Prüfen), um die Auswahl zu löschen. Klicken Sie anschließend auf **Next** (Weiter).

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

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

    Die Seite **Encryption** (Verschlüsselung) wird angezeigt.

14. Wählen Sie optional zum Aktivieren der Verschlüsselung auf der Seite **Encryption** (Verschlüsselung) die Option **Enable Encryption** (Verschlüsselung aktivieren) aus.

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

    ANMERKUNG: Wenn Sie Verschlüsselung aktivieren, wird sie auf alle Daten für alle geschützten Volumes für diese Agentenmaschine angewendet. Sie können die Einstellungen später in der Core Console von der Registerkarte **Configuration** (Konfiguration) ändern.

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

15. Geben Sie die in der folgenden Tabelle beschriebenen Informationen ein, um einen Verschlüsselungsschlüssel für den Kern hinzuzufügen.

| Textfeld | Beschreibung |
|---|---|
| **Name** | Geben Sie einen Namen für den Verschlüsselungsschlüssel ein. |
| **Beschreibung** | Geben Sie eine Beschreibung ein, um zusätzliche Details für den Verschlüsselungsschlüssel bereitzustellen. |
| **Passphrase** | Geben Sie die Passphrase zur Steuerung des Zugriffs ein. |

| Textfeld | Beschreibung |
|---|---|
| **Passphrase bestätigen** | Geben Sie zuvor eingegebene Passphrase erneut ein. |

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

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

## 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:

1. Klicken Sie in der Core Console auf das Drop-Down-Menü **Protected Machines** (Geschützte Maschinen) im linken Navigationsbereich.
2. Wählen Sie **Pause Protection** (Schutz anhalten) für die Maschine aus, für die Sie den Schutz anhalten möchten.

   Das Dialogfeld **Pause Protection** (Schutz anhalten) wird angezeigt.
3. Wählen Sie eine der folgenden Optionen aus, und klicken Sie auf **OK**.
   - Wenn Sie den Schutz anhalten möchten, bis Sie ihn explizit wieder aufnehmen, wählen Sie **Pause until resumed** (Unterbrechen bis zur Fortsetzung).
   - Wenn Sie den Schutz für einen bestimmten Zeitraum anhalten möchten, wählen Sie **Pause for** (Anhalten für) aus, und wählen Sie dann über die Felder „Days" (Tage), „Hours" (Stunden) und „Minutes" (Minuten) den gewünschten Unterbrechungszeitraum aus, oder geben Sie ihn ein.

   ANMERKUNG: Wählen Sie zum Aufnehmen des Schutzes die Option **Resume Protection** (Schutz wieder aufnehmen) aus dem Drop-Down-Menü **Protected Machines** (Geschützte Maschinen) aus.

## 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 auf **Protected Machines** (Geschützte Maschinen) im Navigationsbereich auf der linken Seite.
2. Klicken Sie auf **Actions (Aktionen) → Deploy Agent (Agenten bereitstellen)**.

   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.
   - **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.
- **Protect machine after install** (Maschine nach dem Installieren schützen) – Wenn Sie diese Option auswählen, kann AppAssure einen Basis-Snapshot der Daten erstellen, nachdem Sie die Maschine zum Schutz hinzugefügt haben. Diese Option ist standardmäßig ausgewählt. Wenn Sie diese Option deaktivieren, müssen Sie manuell einen Snapshot erzwingen, wenn Sie bereit sind, den Datenschutz zu starten.
- **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.
- **Port** (Port) – Legt die Portnummer fest, auf der der Kern mit dem Agenten auf der Maschine kommuniziert. Der Standardwert ist 8006.
- **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.

# Verstehen von Schutzzeitplänen

Ein Schutzzeitplan definiert, wann Backups von geschützten Agentenmaschinen auf den AppAssure-Kern übertragen werden.

Schutzzeitpläne werden anfänglich über den **Protect Machine Wizard** (Assistenten zum Schützen von Maschinen) oder den **Protect Multiple Machines Wizard** (Assistenten zum Schützen mehrerer Maschinen) definiert. Sie können die bestehenden Pläne jederzeit über die Registerkarte „Summary" (Zusammenfassung) für eine bestimmte Agentenmaschine ändern.

AppAssure stellt einen Standard-Schutzzeitplan mit zwei definierten Schutzperioden zur Verfügung. Die erste Periode gilt für die Werktage (Montag bis Freitag) mit einem einzelnen definierten Zeitraum (von 0.00 Uhr bis 23:59). Das Standardintervall (die Zeitperiode zwischen Snapshots) beträgt drei Stunden. Die zweite Periode gilt für Wochenenden (Samstag und Sonntag). Das Standardintervall für die zweite Periode beträgt drei Stunden.

Nachdem der Schutz erstmalig aktiviert wurde, wird der Zeitplan aktiviert. Auf diese Weise ist sichergestellt, dass auf Basis der Standardeinstellungen, und zwar unabhängig von der aktuellen Uhrzeit, das Backup alle drei Stunden erfolgt.

Die erste auf den Kern gespeicherte Backup-Übertragung wird als Basis-Image-Snapshot bezeichnet. Alle Daten auf allen angegebenen Volumes (einschließlich Betriebssystem, Anwendungen und Einstellungen) werden auf den Kern gespeichert. Danach werden inkrementelle Snapshots (also kleinere Backups, die ausschließlich aus Daten bestehen, die seit dem letzten Backup geändert wurden) regelmäßig auf den Kern gespeichert, und zwar auf Basis des definierten Intervalls.

Sie können einen benutzerdefinierten Zeitplan erstellen, um die Häufigkeit von Backups zu ändern. Sie können z. B. das Intervall für die Periode am Wochentag auf 60 Minuten ändern, damit wird alle 60 Minuten ein Snapshot erstellt. Alternativ können Sie das Intervall an Wochenenden von 60 Minuten auf 180 Minuten erhöhen, damit wird bei geringerem Datenverkehr alle drei Stunden ein Snapshot erstellt.

Andere Optionen auf der Seite für den **Protection Schedule Wizard** (Assistenten für den Schutzzeitplan) sind die Einstellung der Uhrzeit für den täglichen Schutz. Damit erfolgt täglich während der festgelegten Periode ein Backup (die Standardeinstellung ist 24:00).

Die Option zum Anhalten des anfänglichen Schutzes verhindert, dass ein Basis-Image erstellt wird (bzw. werden alle Backups verhindert), bis Sie explizit den Schutz fortsetzen. Wenn Sie bereit sind, Ihre Maschinen auf Basis des bewährten Schutzzeitplans zu schützen, müssen Sie den Schutz ausdrücklich fortsetzen.

## Erstellen von benutzerdefinierten Zeitplänen

1. Führen Sie zum Ändern des Intervallzeitplans für eine beliebige Periode auf der Seite **Protection Schedule** (Schutzzeitplan) unter **Protect Machine** (Maschine schützen) oder **Protect Multiple Machines Wizard** (Assistent zum Schützen mehrerer Maschinen) die folgenden Schritte aus:
   a. Wählen Sie **Periods** (Perioden) aus.

      Die vorhandenen Perioden werden angezeigt und können geändert werden. Zu den bearbeitbaren Feldern zählen eine Startzeit, eine Endzeit und das Intervall (in Minuten) für jede Periode.
   b. Klicken Sie in das Feld „Interval" (Intervall), und geben Sie ein entsprechendes Intervall in Minuten ein.

      Markieren Sie beispielsweise das vorhandene Intervall aus, und ersetzen Sie es durch den Wert **60**, um alle 60 Minuten in diesem Zeitraum Snapshots zu erstellen.
2. Um Spitzenzeiten und Nebenzeiten für Werktage zu erstellen, ändern Sie den Zeitraum der Periode für die Werktage, so dass diese keinen 24-Stunden-Zeitraum enthält, legen Sie ein optimales Intervall für die Spitzenzeiten fest, wählen Sie die Option **Take snapshots for the remaining time** (Snapshots die verbleibenden Zeit erstellen) aus, und legen Sie ein Intervall für Nebenzeiten fest, indem Sie die folgenden Schritte ausführen:
   a. Wählen Sie **Periods** (Perioden) aus.

      Die vorhandenen Perioden werden angezeigt und können geändert werden.
   b. Klicken Sie in das Feld **From** (Von), um die Startzeit für diese Periode zu ändern.

      Das Dialogfeld **Choose Time** (Uhrzeit auswählen) wird angezeigt.
   c. Ziehen Sie den Schieberegler für Stunden und Minuten auf die gewünschte Startzeit, und klicken Sie anschließend auf **Done** (Fertig). Klicken Sie zum Festlegen der aktuellen Zeit auf **Now** (Jetzt).
   d. Klicken Sie zum Ändern der Endzeit für diese Periode in das Feld **To** (Bis).

      Das Dialogfeld **Choose Time** (Uhrzeit auswählen) wird angezeigt.
   e. Ziehen Sie den Schieberegler für Stunden und Minuten auf die gewünschte Startzeit, und klicken Sie anschließend auf **Done** (Fertig). Klicken Sie zum Festlegen der aktuellen Zeit auf **Now** (Jetzt).
3. Um eine einzelne Uhrzeit für eine einzelne, täglich auszuführende Sicherung festzulegen, wählen Sie die Option **Daily protection time** (Tägliche Schutzzeit) aus, und geben Sie eine Uhrzeit im Format HH:MM (bis 12 Uhr mittags) ein.
4. Um den Zeitplan ohne das Starten von Sicherungen zu definieren, wählen Sie die Option **Initially pause protection** (Schutz anfänglich anhalten) aus.

   Wenn Sie den Schutz über den Assistenten anhalten, bleibt er angehalten, bis Sie ihn explizit fortzusetzen. Sobald Sie den Schutz fortzusetzen, werden wieder Sicherungen auf Basis des von Ihnen erstellten Zeitplans erstellt.

5. Klicken Sie auf **Finish** (Fertig stellen) oder **Next** (Weiter).

## Ändern von Schutzzeitplänen

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

So ändern Sie Schutzzeitpläne:

1. Wählen Sie in der Core Console die Maschine mit einem definierten Schutzzeitplan aus, den Sie ändern möchten.

   Die Registerkarte Summary (Zusammenfassung) wird für die Maschine angezeigt.
2. Wählen Sie die Volumes für die geschützte Maschine aus, die Sie ändern möchten, und klicken Sie auf **Set a schedule** (Zeitplan festlegen). Um alle Volumes auf einmal zu ändern, aktivieren Sie in das Kontrollkästchen in der Überschriftenzeile.

   Anfänglich verwenden alle Volumes den gleichen Schutzzeitplan. In der Regel ist es sinnvoll, mindestens das systemreservierte Volume und das Volume mit dem Betriebssystem (in der Regel Laufwerk C) zu schützen.

   Das Dialogfeld **Schutzzeitplan** wird angezeigt.
3. Wählen Sie im Dialogfeld **Protection Schedule** (Schutzzeitplan), wenn Sie zuvor eine Schutzzeitplanvorlage erstellt haben und diese auf den Agenten anwenden möchten, die Vorlage aus der Dropdown-Liste aus, und wechseln Sie dann zu Schritt 9.
4. Wenn Sie planen, diesen neuen Schutzzeitplan als Vorlage zu speichern, geben Sie einen Namen für die Vorlage in das Textfeld ein.
5. Wenn Sie einen vorhandenen Zeitraum aus dem Zeitplan entfernen möchten, deaktivieren Sie die Kontrollkästchen neben den einzelnen Optionen für den Zeitraum. Die folgenden Optionen sind verfügbar:
   - **Mon – Fr.** (Mo.-Fr.): Dieser Zeitraum steht für eine typische 5-Tage-Woche.
   - **Sat - Sun.** (Sa.-So.): Dieser Zeitraum steht für ein typisches Wochenende.
6. Wenn der Wochentag für den Anfang und das Ende von 00:00 bis 23:59 Uhr definiert ist, ist eine einzelne Periode vorhanden. Gehen Sie zum Ändern der Start- oder Endzeit eines definierten Zeitraums folgendermaßen vor:
   a. Wählen Sie den entsprechenden Zeitraum aus.
   b. Klicken Sie in das Feld **Start Time** (Startzeit), um die Startzeit für diese Periode zu ändern.
   c. Ziehen Sie den Schieberegler für Stunden und Minuten auf die gewünschte Startzeit, und klicken Sie anschließend auf **Done** (Fertig). Klicken Sie zum Festlegen der aktuellen Zeit auf **Now** (Jetzt).
   d. Klicken Sie in das Feld **End Time** (Endzeit), um die Endzeit für diese Periode zu ändern.

      Das Dialogfeld **Choose Time** (Uhrzeit auswählen) wird angezeigt.
   e. Ziehen Sie den Schieberegler für Stunden und Minuten auf die gewünschte Startzeit, und klicken Sie anschließend auf **Done** (Fertig). Klicken Sie zum Festlegen der aktuellen Zeit auf **Now** (Jetzt).
   f. Ändern Sie das Intervall entsprechend Ihren Anforderungen. Beispiel: Wenn Sie eine Hochauslastungsperiode definieren, ändern Sie das Intervall von 60 Minuten auf 20 Minuten, um drei Mal pro Stunden einen Snapshot zu erstellen.
7. Wenn Sie einen anderen Zeitraum als 00:00 bis 23:59 PM in Schritt 6 definiert haben und Datensicherungen in den verbleibenden Zeiträumen ausgeführt werden sollen, müssen Sie anhand der folgenden Schritte zusätzliche Zeiträume hinzufügen, um den Schutz zu definieren:
   a. Klicken Sie auf **+Add Periode** (+Zeitraum hinzufügen).

      Unter der entsprechenden Kategorie (Werktage oder Wochenende) wird ein neuer Zeitraum angezeigt. Wenn der erste Zeitraum später als 12:00 Uhr startet, startet AppAssure diese Periode automatisch um 12:00 Uhr. Entsprechend dem Beispiel oben beginnt dieser zweite Zeitraum um 12:00. Sie müssen ggf. die Stunden oder Minuten für die Start- und Endzeiten anpassen.

b. Ziehen Sie den Schieberegler für Stunden und Minuten entsprechend den gewünschten Start- und Endzeiten.
c. Ändern Sie das Intervall entsprechend Ihren Anforderungen. Beispiel: Wenn Sie eine Periode mit geringer Auslastung definieren, ändern Sie das Intervall von 60 Minuten auf 120 Minuten, um alle zwei Stunden einen Snapshot zu erstellen.

8. Erstellen Sie bei Bedarf weiterhin zusätzliche Perioden, indem Sie Start- und Endzeiten nach Bedarf festlegen.

   ANMERKUNG: Wenn Sie eine von Ihnen hinzugefügte Periode entfernen möchten, klicken Sie auf das **X** rechts in dieser Periode. Wenn Sie dabei sind, unbeabsichtigt eine Periode zu entfernen, klicken Sie auf **Cancel** (Abbrechen).

9. Wenn Ihr Schutzzeitplan Ihren Anforderungen entspricht, klicken Sie auf **Anwenden**.

   Das Dialogfeld **Protection Schedule** (Schutzzeitplan) wird geschlossen.

# Konfigurieren von geschützten 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. Navigieren Sie in der Core Console zu der Maschine, die Sie ändern möchten.
2. Klicken Sie auf **Configuration (Konfiguration)** → **Settings (Einstellungen)**.
3. Klicken Sie auf **Change** (Ändern), um die in der folgenden Tabelle beschriebenen Maschineneinstellungen zu bearbeiten.

| Textfeld | Beschreibung |
|---|---|
| **Anzeigename** | Geben Sie einen Anzeigenamen für die Maschine ein.<br>Ein Name für die Maschine, der in der Core Console angezeigt werden soll. Standardmäßig ist das der Hostname der Maschine. Nach Wunsch können Sie 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.<br>Der Kern verwendet den Standardport 8006, um mit dieser Maschine zu kommunizieren. |
| **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. |
| **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. |

| Textfeld | Beschreibung |
| --- | --- |
| | **ANMERKUNG:** Die Einstellung kann nur dann geändert werden, falls keine Wiederherstellungspunkte vorhanden sind oder ein vorheriges Repository fehlt. |

## Anzeigen von Systeminformationen für eine Maschine

Die Core Console zeigt alle Maschinen an, die geschützt werden.

So zeigen Sie die Systeminformationen für eine Maschine an:

1. Wählen Sie im linken Navigationsbereich der Core Console unter **Protected Machines** (Geschützte Maschinen) die Maschine aus, um detaillierte Informationen anzuzeigen.
2. Klicken Sie auf die Registerkarte **Tools** (Extras).

   Auf der Registerkarte „System Information" (Systeminformationen) werden die folgenden Informationen 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)

   Außerdem werden die folgenden Maschineninformationen angezeigt:

   - Prozessoren
   - Netzwerkadapter
   - Mit dieser Maschine verknüpfte IP-Adressen

## Anzeigen von Lizenzinformationen

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

So zeigen Sie Lizenzinformationen an:

1. Oder wählen Sie im Navigationsbereich die Maschine aus, die Sie anzeigen möchten.
2. Klicken Sie auf **Configuration (Konfiguration)** → **Licensing** (Lizensierung).

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

## 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 AppAssure-Umgebung haben. Bevor Sie die Einstellungswerte der Übertragungen ändern, lesen Sie das „Transfer Performance Tuning Guide" (Handbuch für Leistungssteigerung von Übertragungen) in der Dell AppAssure Wissensdatenbank.**

Es stehen drei Übertragungsarten in DL 1000 zur Auswahl:

| | |
|---|---|
| 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. |
| Wiederherstellung | Ein Vorgang, der Sicherungsinformationen auf einer geschützten Maschine wiederherstellt. |

Die Datenübertragung im DL 1000 beinhaltet die Übertragung einer Datenmenge entlang einem Netzwerk von AppAssure 5-Agentenmaschinen zum Kern. Bei Replikation kann die Übertragung auch vom Ursprungs- oder 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. Navigieren Sie in der Core Console zu der Maschine, die Sie ändern möchten.
2. Klicken Sie auf die Registerkarte **Configuration** (Konfiguration) und dann auf **Transfer Settings** (Übertragungseinstellungen).

   Daraufhin wird die aktuelle Seite **Transfer Settings** (Übertragungseinstellungen) angezeigt.
3. Klicken sie auf der Seite **Transfer Settings** (Übertragungseinstellungen) auf **Change** (Ändern).

   Das Dialogfeld **Übertragungseinstellungen** wird angezeigt.
4. 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.<br>**ANMERKUNG:** Priorität wird auf Übertragungen angewendet, die sich in der Warteschlange befinden. |
| **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.<br>**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.<br>**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.<br>**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.<br>**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 |

| Textfeld | Beschreibung |
|---|---|
| | sind, können Sie eventuell nicht alle aufgeführten Writer sehen. Einige Writer, die Sie sehen, könnten diese einschließen:<br>• ASR Writer (ASR-Generator)<br>• BITS Writer (BITS-Generator)<br>• COM+ REGDB Writer (COM+REGDB-Generator)<br>• Performance Counters Writer (Leistungsindikatoren-Generator)<br>• Registry Writer (Registrierungsgenerator)<br>• Shadow Copy Optimization Writer (Generator zur Optimierung der Schattenkopie)<br>• SQLServerWriter<br>• System Writer (Systemgenerator)<br>• Task Scheduler Writer (Aufgabenplanungsgenerator)<br>• VSS Metadata Store Writer (VSS-Metadaten-Speichergenerator)<br>• 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. |

5. Klicken Sie auf **OK**.

# Archivieren von Daten

Aufbewahrungsrichtlinien erzwingen die Zeitdauer, für die Sicherungen auf (schnellen und teuren) Kurzzeitmedien gespeichert werden. Mitunter machen geschäftliche und technische Anforderungen eine längere Aufbewahrung dieser Sicherungen erforderlich, schnelle Speicherung ist jedoch unerschwinglich teuer. Deshalb wird durch diese Anforderung (langsame und kostengünstige) Langzeitspeicherung

notwendig. Unternehmen verwenden Langzeitspeicherung oftmals zur Archivierung von konformen sowie nicht-konformen Daten. Die Archivierungsfunktion in AppAssure wird zur Unterstützung der verlängerten Aufbewahrung für konforme und nicht-konforme Daten verwendet. Außerdem können Sie mit dieser Funktion Replikationsdaten auf einem Remote-Replikatkern platzieren.

## Erstellen eines Archivs

So erstellen Sie ein Archiv:

1. Klicken Sie in der Core Console auf **Tools (Extras)** → **Archive (Archiv)** → **Create (Erstellen)**.
   Daraufhin wird das Dialogfeld **Add Archive Wizard** (Archivassistent hinzufügen) angezeigt.
2. Wählen Sie auf der Seite **Create** (Erstellen) des **Add Archive Wizard** (Assistenten zum Hinzufügen von Archiven) eine der folgenden Optionen aus der Drop-Down-Liste **Location Type** (Speicherorttyp) aus:
   - Lokal
   - Netzwerk
   - Cloud
3. Geben Sie die in der folgenden Tabelle beschriebenen Details für das Archiv auf Basis der Position, die Sie in Schritt 3 ausgewählt haben, ein.

**Tabelle 2. Erstellen eines Archivs**

| Option | Textfeld | Beschreibung |
|---|---|---|
| Lokal | Output location (Ausgabespeicherort) | Geben Sie den Speicherort für die Ausgabe ein. Er wird für die Definition des Pfades verwendet, auf dem sich das Archiv befinden soll, zum Beispiel „d:\work\archive“. |
| Netzwerk | Output location (Ausgabespeicherort) | Geben Sie den Speicherort für die Ausgabe ein. Er wird für die Definition des Pfades verwendet, auf dem sich das Archiv befinden soll, zum Beispiel „\\servername \sharename“. |
| | Benutzername | Geben Sie einen Benutzernamen ein. Es wird zur Festlegung von Anmeldeinformationen für die Netzwerkfreigabe verwendet. |
| | Kennwort | Geben Sie ein Kennwort für den Netzwerkpfad ein. Es wird zur Festlegung von Anmeldeinformationen für die Netzwerkfreigabe verwendet. |
| Cloud | Account (Konto) | Wählen Sie ein Konto aus der Drop-Down-Liste aus. |

| Option | Textfeld | Beschreibung |
|---|---|---|
| | | **ANMERKUNG:** Zum Auswählen eines Cloud-Konto müssen Sie es zuerst zur Core Console hinzufügen. Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos. |
| | 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-Archivierung – [ERSTELLT AM] – [ERSTELLTE UM]“. |

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

| Textfeld | Beschreibung |
|---|---|
| Maximale Größe | Große Datenarchive können in mehrere Segmente unterteilt werden. Wählen Sie die maximale Menge an Speicherplatz aus, die Sie für die Erstellung des Archivs reservieren möchten. Führen Sie dazu einen der folgenden Schritte aus:<br>• Wählen Sie „Entire Target“ (Gesamtes Ziel) aus, um den gesamten verfügbaren Speicherplatz im Pfad zu reservieren, der in Schritt 4 auf dem Ziel bereitgestellt wurde (wenn z. B. der Speicherort „D:\work\archive“ lautet, wird der gesamte verfügbare Speicherplatz auf Laufwerk D: reserviert).<br>• Wählen Sie das leere Textfeld aus, verwenden Sie die Pfeile nach oben und unten, um eine Menge einzugeben, und wählen Sie dann eine Maßeinheit aus der Dropdown-Liste aus, um den maximalen Speicherplatz anzupassen, der reserviert werden soll.<br>**ANMERKUNG:** Amazon-Cloud-Archive werden automatisch in 50-GB-Segmente unterteilt. Windows Azure Cloud-Archive werden automatisch in 200 GB-Segmente unterteilt. |

| Textfeld | Beschreibung |
|---|---|
| Recycle action (Maßnahme wiederverwenden) | Wählen Sie eine der folgenden Recycling-Optionen aus:<br>• **Do not reuse** (Nicht wiederverwenden) – Vorhandene Daten am Speicherort werden nicht überschrieben oder gelöscht. Wenn der Speicherort nicht leer ist, schlägt der Schreibvorgang in das Archiv fehl.<br>• **Replace this core** (Diesen Kern ersetzen) – Alle bereits vorhandenen archivierten Daten auf diesem Kern werden überschrieben, die Daten für andere Kerne bleiben aber intakt.<br>• **Erase Completely** (Vollständig löschen): Löscht alle archivierten Daten aus dem Verzeichnis, bevor das neue Archiv geschrieben wird.<br>• **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. |
| Kommentar | Geben Sie alle zusätzlichen Informationen ein, die zur Erfassung für das Archiv notwendig sind. Der Kommentar wird angezeigt, wenn Sie das Archiv später importieren. |
| Use compatible format (Kompatibles Format verwenden) | Wählen Sie diese Option aus, um Ihre Daten in einem Format zu archivieren, das mit früheren Kernversionen kompatibel ist.<br>**ANMERKUNG:** Das neue Format bietet eine bessere Leistung, es ist jedoch nicht kompatibel mit älteren Kerne. |

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

## Importieren eines Archivs

So importieren Sie ein Archiv:

1. Klicken Sie in der Core Console auf **Tools (Extras)** → **Archive (Archivieren)** → **Import (Importieren)**.
2. Wählen Sie für **Location Type** (Speicherorttyp) eine der folgenden Optionen aus der Drop-Down-Liste aus:
   - Lokal
   - Netzwerk
   - Cloud
3. Geben Sie die in der folgenden Tabelle beschriebenen Details für das Archiv auf Basis der Position, die Sie in Schritt 3 ausgewählt haben, ein.

**Tabelle 3. Importieren eines Archivs**

| Option | Textfeld | Beschreibung |
|---|---|---|
| Lokal | Output location (Ausgabespeicherort) | Geben Sie den Speicherort für die Ausgabe ein. Er wird für die Definition des Pfads verwendet, auf dem sich das Archiv befinden soll, zum Beispiel `d:\work\archive`ea. |
| Netzwerk | Output location (Ausgabespeicherort) | Geben Sie den Speicherort für die Ausgabe ein. Er wird für die Definition des Pfades verwendet, auf dem sich das Archiv befinden soll, zum Beispiel „\\servername \sharename“. |
| | Benutzername | Geben Sie einen Benutzernamen ein. Es wird zur Festlegung von Anmeldeinformationen für die Netzwerkfreigabe verwendet. |
| | Kennwort | Geben Sie ein Kennwort für den Netzwerkpfad ein. Es wird zur Festlegung von Anmeldeinformationen für die Netzwerkfreigabe verwendet. |
| Cloud | Account (Konto) | Wählen Sie ein Konto aus der Drop-Down-Liste aus.<br>**ANMERKUNG:** Zum Auswählen eines Cloud-Konto müssen Sie es zuerst zur Core Console hinzufügen. Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos. |
| | 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 |

| Option | Textfeld | Beschreibung |
|---|---|---|
| | | „AppAssure-5-Archivierung – [ERSTELLT AM] – [ERSTELLTE UM]“. |

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.

## 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.

# Anzeigen von Systemdiagnosedaten

In AppAssure stehen Diagnosedaten zur Verfügung, um Maschinenprotokolldaten für eine beliebige Maschine anzuzeigen. Darüber hinaus können Sie Diagnosedaten für den Kern anzeigen und hochladen.

## Anzeigen von Maschinenprotokollen

Falls Fehler oder Probleme mit der Maschine auftreten, kann die Anzeige der Protokolle zur Fehlersuche hilfreich sein.

So zeigen Sie Maschinenprotokolle an:

1. Klicken Sie in der Core Console auf **Tools (Extras)** → **Diagnostics (Diagnoseprogramm)** → **View Log (Protokoll anzeigen)**.

   Daraufhin wird die Seite **Download Core Log** (Kernprotokoll herunterladen) angezeigt.
2. Wählen Sie die Option **Click here to begin the download** (Zum Herunterladen hier klicken) aus.

   Es wird eine Meldung angezeigt, in der Sie gefragt werden, ob Sie die Datei öffnen oder speichern möchten.
3. Wählen Sie Ihre bevorzugte Methode für die Behandlung der Protokolldatei aus.

## Hochladen der Maschinenprotokolle

1. Navigieren Sie zur Core Console, klicken Sie auf **Tools (Extras)** → **Diagnostics (Diagnoseprogramm)** → **Upload Log** (Protokoll hochladen).

Die Seite **Upload Log** (Protokoll hochladen) wird angezeigt.

2. Wählen Sie die Option **Click here to begin the upload** (Zum Herunterladen hier klicken) aus.

   Die Registerkarte „Events" (Ereignisse) wird angezeigt, hier können Sie Fortschritt des Uploads von Protokollinformationen für den Kern und aller geschützten Maschinen anzeigen.

## Abbrechen von Vorgängen auf einer Maschine

Sie können Vorgänge, die aktuell für eine Maschine ausgeführt werden, abbrechen. Sie können einen aktuellen Snapshot oder alle Vorgänge abbrechen, dazu gehören Exporte und Replikationen.

So brechen Sie Vorgänge auf einer Maschine ab:

1. Wählen Sie in der Core Console die Maschine aus, für die Sie Vorgänge abbrechen möchten.
2. Erweitern Sie im Feld **Events** (Ereignisse) die Ereignisdetails für das Ereignis oder den Vorgang, den Sie abbrechen möchten.
3. Klicken Sie auf **Cancel** (Abbrechen).

## Anzeigen des Maschinenstatus und anderer Details

So zeigen Sie den Maschinenstatus und andere Details an:

1. Navigieren Sie in der Core Console zur geschützten Maschine, die Sie anzeigen möchten.

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:

- Name
- File System type (Dateisystemtyp)
- Space Usage (Speicherplatznutzung)
- Current Schedule (Aktueller Zeitplan)
- Next Snapshot (Nächster Snapshot)
- 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:

- Online-Status

- Name
- Install Path (Installierungspfad)
- Version

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

- Version
- 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 AppAssure-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.
   Siehe 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
   Siehe 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-Agenteninstallationsprogramms zur Bereitstellung der Installationskomponenten nutzt. Wenn kein Zugriff auf das Internet verfügbar ist, laden Sie das AppAssure-Agenteninstallationsprogramm von der Kernmaschine. Sie können Kern- und Agentenaktualisierungen vom Lizenzportal herunterladen.

## 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 **Events (Ereignisse)** → **Alerts (Warnungen)**.
2. Navigieren Sie zur Registerkarte „AppAssure Core Home" (AppAssure-Core-Startseite), und klicken Sie dort auf die Registerkarte **Events** (Ereignisse).

   Es werden Warnungsereignisse in der Liste mit der Uhrzeit des initiierten Ereignisses und einer Meldung angezeigt. Für jede erfolgreiche Bereitstellung der Agentensoftware wird eine Warnmeldung angezeigt, die darauf hinweist, dass die geschützte Maschine hinzugefügt wurde.
3. Klicken Sie optional auf einen beliebigen Link für eine geschützte Maschine.

   Die Registerkarte „Summary" (Zusammenfassung) für die ausgewählte Maschine wird mit den damit verknüpften Informationen angezeigt. Darunter:

   - Der Host-Name der geschützten Maschine
   - Der letzte Snapshot, falls zutreffend
   - Der geplante Zeitpunkt für den nächsten Snapshot, basierend auf den von Ihnen ausgewählten Zeitplan für den Schutz
   - Time Remaining (Verbleibende Zeit)
   - Der Verschlüsselungsschlüssel, der, falls vorhanden, für diesen geschützten Agenten verwendet wird
   - Die Version der Agentensoftware

## Schützen mehrerer Maschinen

Nach der Massenbereitstellung der AppAssure-Agentensoftware auf den Windows-Maschinen müssen Sie diese nun so schützen, dass sie die Daten schützen können. Wenn Sie **Protect Machine After Install** (Maschine nach dem Installieren schützen) auswählen, wenn Sie den Agenten bereitstellen, 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. Klicken Sie in der Core Console auf **Protect (Schützen)** → **Bulk Protect** (Massenschutz).

   Daraufhin wird das Fenster **Protect Multiple Machines Wizard** (Assistent zum Schützen mehrerer Maschinen) angezeigt.
2. Wählen Sie die geeignete Installationsoption aus.
   - Wenn Sie kein Repository definieren oder eine Verschlüsselung aufbauen müssen, wählen Sie **Typical** (Typisch).

- Wenn die Seite „Welcome" (Willkommen) für den Assistenten zum Schützen der Maschine künftig nicht angezeigt werden soll, wählen Sie die Option **Skip this Welcome page the next time the wizard opens** (Seite „Willkommen" beim nächsten Öffnen des Assistenten ignorieren) aus.

3. Klicken Sie auf **Weiter**.

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

4. Fügen Sie die Maschinen, die Sie schützen möchten durch Anklicken einer der folgenden Optionen hinzu.
   - Klicken Sie auf **Active Directory** (Aktives Verzeichnis), um Maschinen auf einer Active Directory-Domäne anzugeben. Geben Sie die Anmeldeinformationen gemäß der Tabelle unten ein, und klicken Sie auf **Next** (Weiter).
   - Klicken Sie auf **vCenter/ESXi**, um virtuelle Maschinen auf einem virtuellen vCenter/ESXi-Host anzugeben. Geben Sie die Anmeldeinformationen gemäß der Tabelle unten ein, und klicken Sie dann auf **Next** (Weiter).

     | Textfeld | Beschreibung |
     |---|---|
     | **Host** | Der Hostname oder die IP-Adresse der Active Directory-Domäne oder des virtuellen Hosts für VMware vCenter Server/ESX (i). |
     | **Benutzername** | Geben Sie den Benutzernamen ein, der für die Verbindung mit dieser Maschine verwendet wird, z. B. Administrator. |
     | **Kennwort** | Geben Sie das sichere Kennwort ein, um eine Verbindung mit dieser Maschine herzustellen. |

   - Um die Maschinen manuell hinzuzufügen, wählen Sie **Add the machines manually** (Maschine manuell auswählen) aus, und klicken Sie dann auf **Next** (Weiter).

5. Geben Sie auf der Seite **Machines** (Maschine) zum manuellen Angeben der Rechner die folgenden Verbindungsdetails für jede Maschine in einer eigenen Zeile an, und klicken Sie dann auf **Next** (Weiter). `hostname::username::password::port`

6. Wählen Sie auf der Seite **Machines** (Maschine) zum Angeben von Maschinen, die in einer Active Directory-Domäne oder einem virtuellen VMware vCenter/ESX(i)-Host identifiziert wurden, jede geeignete Maschine, die Sie schützen möchten, aus der Liste aus, und klicken Sie dann auf **Next** (Weiter).

   Das System prüft jede Maschine, die Sie automatisch hinzugefügt haben; daraufhin wird die Seite **Protection** (Schutz) angezeigt.

7. Wählen Sie auf der Seite **Protection** (Schutz) den entsprechenden Schutzzeitplan aus:
   - Um den Standardschutzzeitplan zu verwenden, wählen Sie anschließend über die Option **Schedule Settings** (Zeitplaneinstellungen) die Option **Default protection (hourly snapshots of all volumes)** (Standardschutz (stündlich Snapshots von allen Volumes)) aus.
   - Wenn Sie einen anderen Schutzzeitplan verwenden möchten, wählen Sie unter der Option „Schedule Settings" (Zeitplaneinstellungen) die Option **Custom protection** (Benutzerdefinierter Schutz) aus, und klicken Sie dann auf **Next** (Weiter).

8. Fahren Sie mit der Konfiguration wie folgt fort:
   - Wenn Sie eine typische Konfiguration für den **Protect Multiple Machines Wizard** (Assistenten zum Schützen von mehreren Maschinen) und den Standardschutz ausgewählt haben, klicken Sie anschließend auf **Finish** (Fertig stellen), um die Auswahl zu bestätigen, den Assistenten zu schließen und die von Ihnen angegebenen Maschinen zu schützen.
   - Wenn Sie eine typische Konfiguration für den **Protect Multiple Machines Wizard** (Assistenten zum Schützen von mehreren Maschinen) und den angegebenen benutzerdefinierten Schutz ausgewählt haben, klicken Sie auf **Next** (Weiter), und richten Sie dann einen benutzerdefinierten Zeitplan ein.
   - Wenn Sie die Option „Advanced Configuration" (Erweiterte Konfiguration) für den Assistenten zum Schützen von Maschinen ausgewählt haben, klicken Sie auf **Next** (Weiter), und fahren Sie mit Schritt 9 fort, um die Optionen für das Repository und die Verschlüsselung anzuzeigen.

9. Wählen Sie auf der Seite **Repository** (Repository) die Option **Use an existing repository** (Vorhandenes Repository verwenden) aus.
10. Klicken Sie auf **Weiter**.

    Die Seite **Encryption** (Verschlüsselung) wird angezeigt.
11. Um die Verschlüsselung zu aktivieren, wählen Sie auf der Seite **Encryption** (Verschlüsselung) die Option **Enable Encryption** (Verschlüsselung aktivieren) aus.

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

    ANMERKUNG: Wenn Sie die Verschlüsselung aktivieren, wird sie auf alle geschützten Volumes für die zu schützenden Rechner angewendet. Sie können die Einstellungen später in der Core Console auf der Registerkarte **Configuration** (Konfiguration) ändern. Weitere Informationen zur Verschlüsselung finden Sie unter Verwalten der Sicherheit.
12. Geben Sie die in der folgenden Tabelle beschriebenen Informationen ein, um einen Verschlüsselungsschlüssel für den Kern hinzuzufügen.

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

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

## Überwachen des Schutzes von mehreren Maschinen

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

Um den Schutz mehrerer Maschinen zu überwachen, navigieren Sie zur Registerkarte „Core Console Home“ (Core-Console-Startseite), und klicken Sie auf **Events** (Ereignisse).

Auf der Registerkarte „Events“ (Ereignisse) werden Aufgaben, Warnungen und Ereignisse angezeigt. Wenn Volumes übertragen werden, werden der Status, die Startzeiten und die Endzeiten im Fenster „Tasks“ (Aufgaben) angezeigt. Sie können Aufgaben außerdem nach Status (Active (Aktiv), Waiting (Wartet), Completed (Abgeschlossen) und Failed (Fehlgeschlagen)) filtern.

Beim Hinzufügen jeder geschützten Maschine wird eine Warnung protokolliert, die anzeigt, ob der Vorgang erfolgreich war oder ob Fehler berichtet wurden.

4

# Wiederherstellen von Daten

## Verwalten der Wiederherstellung

Der AppAssure-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, um Folgendes einzuschließen:

- 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

## 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 klicken Sie dann auf die Registerkarte **Recovery Points** (Wiederherstellungspunkte).
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:<br>**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.<br>**Export** (Exportieren) – Über die Option „Export" (Exportieren) können Sie den ausgewählten Wiederherstellungspunkt auf ESXi, VMWare Workstation oder HyperV exportieren.<br>**Restore** (Wiederherstellen) – Wählen Sie diese Option, um eine Wiederherstellung von dem ausgewählten Wiederherstellungspunkt auf ein Volume auszuführen, das Sie angeben. |

| | |
|---|---|
| Inhalt | Der Bereich „Contents“ (Inhalt) enthält eine Zeile für jedes Volume auf dem erweiterten Wiederherstellungspunkt und listet für jedes Volume die folgenden Informationen auf:<br><br>**Status** (Status) zeigt den aktuellen Status des Wiederherstellungspunktes an.<br>**Title** (Titel) enthält das jeweilige Volume auf dem Wiederherstellungspunkt.<br><br>**Size** (Größe) zeigt die Speicherplatzmenge an, die der Wiederherstellungspunkt in dem Repository belegt. |

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. 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.
2. Wählen Sie die Registerkarte **Recovery Points** (Wiederherstellungspunkte) aus.
3. Klicken Sie in der Liste der Wiederherstellungspunkte auf **>** , um den bereitzustellenden Wiederherstellungspunkt zu erweitern.
4. Klicken Sie in den erweiterten Details für diesen Wiederherstellungspunkt auf **Mount** (Bereitstellen).

   Das Dialogfeld **Wiederherstellungspunkte bereitstellen** wird angezeigt.
5. 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:<br>• Mount Read-only (Schreibgeschützt bereitstellen).<br>• Mount Read-only with previous writes (Schreibgeschützt mit vorherigen Schreibvorgängen bereitstellen).<br>• 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. |

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

## Entfernen der Bereitstellung ausgewählter Wiederherstellungspunkte

So entfernen Sie die Bereitstellung ausgewählter Wiederherstellungspunkte

1. Navigieren Sie zu Core Console, und klicken Sie auf **Tools (Extras)** → **Mounts (Bereitstellungen)**.
2. Klicken Sie auf der Seite **Local Mounts** (Lokale Bereitstellungen) neben dem Bereitstellungspunkt für den Wiederherstellungspunkt, für den Sie die Bereitstellung aufheben möchten, auf **Dismount** (Bereitstellung aufheben).
3. Klicken Sie im Fenster „Dismounting the Recovery Point" (Aufheben der Bereitstellung für den Wiederherstellungspunkt) auf **Yes** (Ja).

## Entfernen der Bereitstellung aller Wiederherstellungspunkte

So entfernen Sie die Bereitstellung aller Wiederherstellungspunkte:

1. Navigieren Sie zur Core Console, und klicken Sie dort auf **Tools (Extras)** → **Mounts (Bereitstellungen)** .
2. Klicken Sie auf der Seite **Local Mounts** (Lokale Bereitstellungen) auf **Dismount All** (Bereitstellung für alle aufheben).
3. Klicken Sie im Fenster **Dismounting the Recovery Point** (Bereitstellung für Wiederherstellungspunkt aufheben) auf **Yes** (Ja).

## Bereitstellen eines Wiederherstellungspunktes für eine Linux-Maschine

Mit dem Dienstprogramm **aamount** in AppAssure können Sie ein Volume remote über einen Wiederherstellungspunkt als lokales Volume auf einer Linux-Maschine bereitstellen.

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 **aamount** als Root oder als Superuser aus, z. B. **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 Core-Servers an.
6. Geben Sie die Anmeldeinformationen für den Core-Server ein, das heißt, den Benutzernamen und das Kennwort.

   Es wird eine Liste der Maschinen angezeigt, die durch den AppAssure-Server geschützt werden. Jede Maschine wird durch Folgendes identifiziert: Zeilenobjektnummer, Host/IP-Adresse und ID-Nummer für die Maschine. Beispiel: 293cc667-44b4-48ab-91d8-44bc74252a4f
7. Geben Sie den folgenden Befehl ein, um die Wiederherstellungspunkte für eine bestimmte Maschine aufzulisten: **lr <line_number_of_machine>**
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>**
9. Um sicherzustellen, dass die Bereitstellung erfolgreich durchgeführt wurde, geben Sie den folgenden Befehl ein; damit wird eine Liste des angefügten Remote-Volumes erstellt: **l**

## 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 Schnappschüsse werden weiterhin auf diesem Wiederherstellungspunkt erstellt. Ohne das Basisabbild sind die resultierenden Wiederherstellungspunkte unvollständig und es ist unwahrscheinlich, dass sie die erforderlichen Daten für den Abschluss einer Wiederherstellung enthalten. Diese Wiederherstellungspunkte werden als Teil der verwaisten Wiederherstellungspunkt-Kette angesehen. Wenn diese Situation eintritt, besteht die beste Lösung aus der Löschung der Kette und der Erstellung eines neuen Basisabbilds. Weitere Informationen über das Erzwingen eines Basisabbilds finden Sie unter Erzwingen eines Snapshots.

**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.**

## 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 Basis-Image bezeichnet.

So erzwingen Sie einen Snapshot

1. Wählen Sie in der Core Console die Maschine oder den Cluster mit dem Wiederherstellungspunkt aus, für die Sie einen Snapshot erzwingen möchten.
2. Klicken Sie auf der Registerkarte **Summary** (Zusammenfassung) im Abschnitt **Volumes** (Volumes), und wählen Sie dann eine der oben 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.

# Wiederherstellen von Daten

Mit AppAssure können Sie Daten umgehend auf Ihre physikalischen Maschinen (für Windows oder Linux Maschinen) oder auf virtuelle Maschinen von gespeicherten Wiederherstellungspunkten für Windows-Maschinen aus 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) Replikation erstellt haben, können Sie Daten nur vom Zielkern exportieren, nachdem die erste Replikation abgeschlossen ist.

## 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.

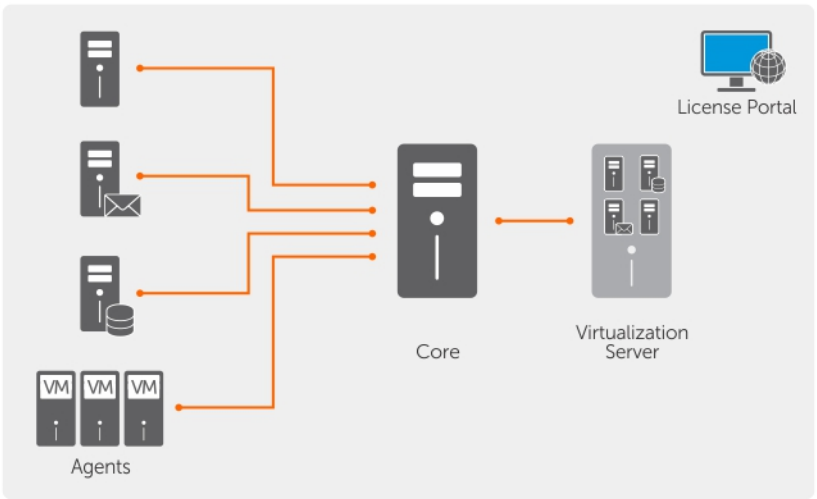


**Abbildung 4. Exportieren von Daten auf eine virtuelle Maschine**

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

Dell AppAssure unterstützt das Erstellen von Snapshots auf allen dynamischen und Basisvolumes. AppAssure unterstützt auch den Export von einfachen dynamischen Volumes, die auf einem einzigen physischen Laufwerk bestehen. Einfache dynamische Volumes sind nicht gestriped, gespiegelt oder verkettet.

Dynamische Datenträger (mit Ausnahme der oben beschriebenen einfachen dynamischen Festplatten), die für die Auswahl im Export-Assistenten nicht verfügbar sind. Nicht-einfache dynamische Volumes haben willkürliche Festplattengeometrien, die nicht vollständig interpretiert werden können. AppAssure unterstützt daher nicht das Exportieren von komplexen oder nicht-einfachen dynamischen Volumes.

## Verwalten von Exporten

In der Core Console auf die Registerkarte **Virtual Standby** (Virtueller Standby) können Sie den Status von Exporten, die Sie eingerichtet haben, einschließlich der einmaligen Exporte und der fortlaufenden Exporte für einen virtuellen Standby anzeigen. Auf dieser Registerkarte können Sie Exporte durch Unterbrechen, Stoppen und Entfernern von Exporten oder durch das Anzeigen einer Warteschlange mit anstehenden Exporten verwalten.

**ANMERKUNG:** Nur Dell DL1000 mit einer Konfiguration mit 3 TB und zwei VMs unterstützt die Funktionen für den einmaligen und dauerhaften Export (virtueller Standby).

1. Navigieren Sie in der Core Console auf die Registerkarte **Virtual Standby** (Virtueller Standby) .
   Auf der Registerkarte **Virtual Standby** (Virtueller Standby) können Sie eine Tabelle mit gespeicherten Exporteinstellungen anzeigen, die die in der folgenden Tabelle beschriebenen Informationen enthält.

| Menü | Beschreibung |
|---|---|
| Status | **ANMERKUNG:** Der Status der Konfiguration des virtuellen Standby wird durch die Farbe des Symbols definiert.<br>Grün – Der virtuelle Standby wurde erfolgreich konfiguriert, ist aktiv und nicht angehalten. Der nächste Export für den virtuellen Standby wird nach dem nächsten Snapshot ausgeführt.<br>Gelb – Der virtuelle Standby wurde angehalten und wird weiterhin durch den Kern gespeichert. Bei einer neuen Übertragung wird der Exportvorgang jedoch nicht automatisch gestartet, und es sind keine neuen Exporte für den virtuellen Standby für diesen Agenten verfügbar. |
| Maschinenname | Die Namen der Quellmaschine. |
| Ziel | Die virtuelle Maschine und der Pfad, in den die Daten exportiert werden. |

| Menü | Beschreibung |
|---|---|
| Exporttyp | Der Typ der Plattform für virtuelle Maschinen für den Export, wie z. B. ESXi, VMware, Hyper-V oder VirtualBox. |
| Last Export (Letzter Export) | Datum und Uhrzeit des letzten Exports. Wenn ein Export soeben hinzugefügt, aber noch nicht abgeschlossen wurde, wird eine Meldung angezeigt, die besagt, dass der Export noch nicht durchgeführt wurde. Wenn der Export fehlgeschlagen ist oder abgebrochen wurde, wird ebenfalls eine entsprechende Meldung angezeigt. |

2. Um die gespeicherte Exporteinstellungen zu verwalten, wählen Sie einen Export aus, und klicken Sie dann auf eine der folgenden Optionen:
   - **Pause** (Anhalten): Unterbrechen des Exports.
   - **Resume** (Fortsetzen): Neu Starten eines unterbrochenen Exports.
   - **Force** (Erzwingen): Erzwingen eines neuen Exports. Diese Option kann hilfreich sein, wenn der virtuelle Standby angehalten wird; dies bedeutet, dass der Exportvorgang erst nach einer neuen Übertragung fortgesetzt wird. Wenn Sie die neue Übertragung nicht abwarten möchten, können Sie einen Export erzwingen.
3. Um einen Export aus dem System zu entfernen, klicken Sie auf **Remove** (Entfernen). Wenn Sie einen Export entfernen, wird er dauerhaft aus dem System entfernt, und Sie können ihn nicht erneut starten.
4. Um die Details der aktiven Exporte anzuzeigen, die sich derzeit in der Warteschlange befinden und auf Abschluss warten, klicken Sie auf **Show Export Queue** (Exportwarteschlange anzeigen).

   Die folgende Tabelle wird angezeigt:

| Menü | Beschreibung |
|---|---|
| Maschinenname | Die Namen der Quellmaschine. |
| Ziel | Der virtuelle Standby wurde erfolgreich konfiguriert, ist aktiv und nicht angehalten. Der nächste Export für den virtuellen Standby wird nach dem nächsten Snapshot ausgeführt. |
| Exporttyp | Der virtuelle Standby wurde angehalten und wird weiterhin durch den Kern gespeichert. Bei einer neuen Übertragung wird der Exportvorgang jedoch nicht automatisch gestartet, und es sind keine neuen Exporte für den virtuellen Standby für diesen Agenten verfügbar. |
| Schedule Type (Planungstyp) | Der Typ des Exports; entweder „One-time“ (Einmalig) oder „Continous“ (Fortlaufend). |
| Status | Der Fortschritt des Exports, angezeigt als Prozentsatz in einer Fortschrittsleiste. |

## Exportieren von Sicherungsinformationen von Ihrer Windows-Maschine auf eine virtuelle Maschine

Sie können Daten von Ihren Windows-Maschinen in eine virtuelle Maschine (VMware, ESXi und Hyper-V) exportieren, indem Sie alle Sicherungsinformationen aus einem Wiederherstellungspunkt sowie die für den Schutzzeitplan für Ihre Maschine definierten Parameter exportieren.

**ANMERKUNG:** Nur Dell DL1000 mit einer Konfiguration mit 3 TB und zwei VMs unterstützt die Funktionen für den einmaligen und dauerhaften Export (virtueller Standby).

So exportieren Sie Windows-Sicherungsinformationen in eine virtuelle Maschine:

1. Klicken Sie in der Core Console auf die Registerkarte **Protected Machines** (Geschützte 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:
   - One-time (Einmalig)
   - Virtual Standby (Virtueller Standby)

   Das Dialogfeld **Export Wizard** (Assistent zum Exportieren) wird 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. 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 für den Export 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 Informationen für virtuelle Maschinen zum Durchführen eines ESXi-Exports*

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

1. Wählen Sie auf der Seite **Destination** (Ziel) im **Assistent für den Export** im Drop-Down-Menü **Recover to Virtual machine** ( Auf virtuelle Maschine wiederherstellen) auf **ESX (i)**.
2. 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. |

3. Geben Sie auf der Seite **Virtual Machine Options** (Optionen für virtuelle Maschinen) die in der folgenden Tabelle beschriebenen Informationen ein.

| Textfeld | Beschreibung |
|---|---|
| **Resource Pool (Ressourcenpool)** | Wählen Sie ein Ressourcenpool aus der Dropdown-Liste aus. |
| **Data Store (Datenspeicher)** | Wählen Sie einen Datenspeicher aus der Dropdown-Liste aus. |
| **Virtual Machine Name (Name der virtuellen Maschine)** | Geben Sie einen Namen für die virtuelle Maschine ein. |
| **Speicher** | Geben Sie die Speichernutzung an. |
| **Laufwerksbereitstellung** | Wählen Sie den Typ der Laufwerksbereitstellung aus den Optionen „Thin" (Schlank) oder „Thick" (Dick) aus. |
| **Disk Mapping (Laufwerkszuweisung)** | Geben Sie den Typ der Laufwerkszuweisung aus den Optionen „Automatic" (Automatisch) oder „Manual" (Manuell) an. |
| **Version** | Wählen Sie die Version der virtuellen Maschine aus. |

4. Klicken Sie auf **Weiter**.
5. Wählen Sie auf der Seite **Volumes** die Volumes aus, die Sie exportieren möchten, und klicken Sie dann auf **Next** (Weiter).
6. 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.

### Ausführen eines dauerhaften ESXi-Exports (virtueller Standby)

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

1. Führen Sie in der Core Console eine der folgenden Aktionen aus:
   - Klicken Sie auf der Registerkarte „Virtual Standby" (Virtueller Standby) auf **Add** (Hinzufügen), um den **Assistenten für den Export** zu starten. Wählen Sie auf der Seite **Protected Machines** (Geschützte Maschinen) des **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 **Actions (Aktionen) → Export (Exportieren) → Virtual Standby (Virtueller Standby)**.
2. Wählen Sie auf der Seite **Destination** (Ziel) im **Assistenten für den Export** im Drop-Down-Menü **Recover to a Virtual Machine** (Auf eine virtuelle Maschine wiederherstellen) die Option **ESXi** aus.
3. Geben Sie die Informationen ein, die für den Zugriff auf die virtuelle Maschine gemäß der folgenden Tabelle benötigt werden, und klicken Sie dann auf **Next** (Weiter).

| Textfeld | Beschreibung |
|---|---|
| **Host-Name** | Geben Sie einen Hostnamen für die Maschine ein. |
| **Schnittstelle** | Geben Sie den Anschluss für die Host-Maschine ein. Der Standard ist 443. |
| **Benutzername** | Geben Sie die Anmeldeinformationen für die Host-Maschine ein. |

| Textfeld | Beschreibung |
|---|---|
| **Kennwort** | Geben Sie die Anmeldeinformationen für die Host-Maschine ein. |

4. Geben Sie auf der Seite **Virtual Machine Options** (Optionen für virtuelle Maschinen) die in der folgenden Tabelle beschriebenen Informationen ein.

| Textfeld | Beschreibung |
|---|---|
| **Resource Pool (Ressourcenpool)** | Wählen Sie ein Ressourcenpool aus der Dropdown-Liste aus. |
| **Data Store (Datenspeicher)** | Wählen Sie einen Datenspeicher aus der Dropdown-Liste aus. |
| **Virtual Machine Name (Name der virtuellen Maschine)** | Geben Sie einen Namen für die virtuelle Maschine ein. |
| **Speicher** | 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) |
| **Laufwerksbereitstellung** | Wählen Sie den Typ der Laufwerksbereitstellung aus den Optionen „Thin" (Schlank) oder „Thick" (Dick) aus. |
| **Disk Mapping (Laufwerkszuweisung)** | Geben Sie den Typ der Laufwerkszuweisung aus den Optionen „Automatic" (Automatisch) oder „Manual" (Manuell) an. |
| **Version** | Wählen Sie die Version der virtuellen Maschine aus. |

5. Klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite **Volumes** die Volumes aus, die Sie exportieren möchten, und klicken Sie dann auf **Next** (Weiter).
7. 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 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. 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 VMware Workstation-Exports*

So definieren Sie die einmaligen Einstellungen für das Ausführen eines VMware Workstation-Exports:

1. Wählen Sie auf der Seite **Destination** (Ziel) im **Exportassistenten** im Drop-Down-Menü **Recover to Virtual machine** (Auf virtuelle Maschine wiederherstellen) die Option **VMware Workstation** aus, und klicken Sie dann auf **Next** (Weiter).
2. Geben Sie auf der Seite **Virtual Machine Options** (Optionen für virtuelle Maschine) die Parameter für den Zugriff auf die virtuelle Maschine gemäß Beschreibung in der folgenden Tabelle ein.

| Textfeld | Beschreibung |
|---|---|
| **Standort** | Geben Sie den Pfad des lokalen Ordners oder der Netzwerkfreigabe an, auf dem/der die virtuelle Maschine erstellt werden soll.<br>ANMERKUNG: Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie gültige Anmeldeinformationen für ein Konto eingeben, das auf der Zielmaschine registriert ist. Das Konto muss über Lese- und Schreibberechtigungen auf die Netzwerkfreigabe verfügen. |
| **Benutzername** | Geben Sie die Anmeldeinformationen für die virtuelle Maschine ein.<br>• Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie einen gültigen Benutzernamen für ein Konto eingeben, der auf der Zielmaschine registriert ist.<br>• Wenn Sie einen lokalen Pfad angegeben haben, ist kein Benutzername erforderlich. |
| **Kennwort** | Geben Sie die Anmeldeinformationen für die virtuelle Maschine ein.<br>• Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie ein gültiges Kennwort für ein Konto eingeben, der auf der Zielmaschine registriert ist.<br>• Wenn Sie einen lokalen Pfad angegeben haben, ist kein Kennwort erforderlich. |
| **Virtual Machine Name (Name der virtuellen Maschine)** | Geben Sie den Namen für die zu erstellende virtuelle Maschine ein, z. B. VM-0A1B2C3D4. |

| Textfeld | Beschreibung |
|---|---|
| | ANMERKUNG: Der Standardname entspricht dem Namen der Quellmaschine. |
| **Version** | Geben Sie die Version von VMware Workstation für die virtuelle Maschine ein. Sie können aus den folgenden Optionen auswählen:<br>• VMware Workstation 7.0<br>• VMware Workstation 8.0<br>• VMware Workstation 9.0 |
| **Speicher** | Geben Sie die Speichernutzung für die virtuelle Maschine ein, indem Sie auf eine der folgenden Optionen klicken:<br>• 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.<br>• Use a specific amount of RAM (Eine bestimmte RAM-Größe verwenden) um anzugeben, wie viel RAM verwendet werden soll. Beispiel: 4096 Megabytes (MB). Die kleinste zulässige Größe ist 512 MB. Die maximale Größe wird durch das Fassungsvermögen und die Begrenzungen der Host-Maschine bestimmt. (empfohlen) |

3. Klicken Sie auf **Weiter**.
4. 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.

### Ausführen eines dauerhaften VMware Workstation-Exports (virtueller Standby)

So führen Sie einen dauerhaften VMware Workstation-Export aus (virtueller Standby):

1. Führen Sie in der Core Console eine der folgenden Aktionen 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** (Aktionen) für diese Maschine auf **Export (Exportieren)** → **Virtual Standby** (Virtueller Standby).
2. Klicken Sie auf der Seite **Destination** (Ziel) des **Assistenten zum Exportieren** auf **Recover to a Virtual Machine (Auf eine virtuelle Maschine wiederherstellen)** → **VMware Workstation** .
3. Klicken Sie auf **Weiter**.
4. Geben Sie auf der Seite **Virtual Machine Options** (Optionen für virtuelle Maschinen) die Parameter für den Zugriff auf die virtuelle Maschine gemäß Beschreibung in der folgenden Tabelle ein.

| 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. |

| Textfeld | Beschreibung |
| --- | --- |
| | **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.<br>• Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie einen gültigen Benutzernamen für ein Konto eingeben, der auf der Zielmaschine registriert ist.<br>• Wenn Sie einen lokalen Pfad angegeben haben, ist kein Benutzername erforderlich. |
| **Kennwort** | Geben Sie die Anmeldeinformationen für die virtuelle Maschine ein.<br>• Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie ein gültiges Kennwort für ein Konto eingeben, der auf der Zielmaschine registriert ist.<br>• Wenn Sie einen lokalen Pfad angegeben haben, ist kein Kennwort erforderlich. |
| **Virtual Machine (Virtuelle Maschine)** | Geben Sie den Namen für die zu erstellende virtuelle Maschine ein, z. B. VM-0A1B2C3D4.<br>**ANMERKUNG:** Der Standardname entspricht dem Namen der Quellmaschine. |
| **Version** | Geben Sie die Version von VMware Workstation für die virtuelle Maschine ein. Sie können aus den folgenden Optionen auswählen:<br>• VMware Workstation 7.0<br>• VMware Workstation 8.0<br>• VMware Workstation 9.0 |
| **Speicher** | Geben Sie die Speichernutzung für die virtuelle Maschine ein, indem Sie auf eine der folgenden Optionen klicken:<br>• 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.<br>• Use a specific amount of RAM (Eine bestimmte RAM-Größe verwenden) um anzugeben, wie viel RAM verwendet werden soll. Beispiel: 4096 Megabytes (MB). Die kleinste zulässige Größe ist 512 MB. Die maximale Größe wird durch das Fassungsvermögen und die Begrenzungen der Host-Maschine bestimmt. |

5. Wählen Sie **Perform initial ad-hoc export** (Erstmaligen Ad-hoc-Export ausführen) aus, um den virtuellen Export sofort auszuführen, statt nach dem nächsten geplanten Snapshot.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie auf der Seite **Volumes** die zu exportierenden Volumes aus, z. B. C:\ und D:\, und klicken Sie dann auf **Next** (Weiter).

8. 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 Windows-Daten mit Hyper-V-Export

In AppAssure können Sie wählen, Daten über die Option „Hyper-V Export" (Hyper-V-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 „Hyper-V Export" (Hyper-V-Export) für den entsprechenden Exporttyp durchzuführen.

### 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. |
| **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 Windows-Daten mit Oracle VirtualBox-Export

In AppAssure können Sie Daten mit VirtualBox Export exportieren, indem Sie einen einmaligen oder dauerhaften Export ausführen, oder einen dauerhaften Export (für virtuelles Standby) einrichten.

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

So führen Sie einen einmaligen Oracle VirtualBox-Export aus

1. Navigieren Sie in der Core Console zu der Linux-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).
5. Wählen Sie auf der Seite **Destination** (Ziel) im **Assistenten für den Export** im Drop-Down-Menü **Recover to Virtual machine** (Auf virtuelle Maschine wiederherstellen) die Option **VirtualBox** aus, und klicken Sie dann auf **Next** (Weiter).
6. Wählen Sie auf der Seite **Virtual Machine Options** (Optionen für virtuelle Maschine) die Option **Remote Linux Machine** (Remote-Linux-Maschine) aus.
7. Geben Sie die Parameter für den Zugriff auf die virtuelle Maschine entsprechend der folgenden Beschreibung ein.

| Textfeld | Beschreibung |
|---|---|
| **VirtualBox Host Name (VirtualBox-Host-Name)** | Geben Sie eine IP-Adresse oder einen Hostnamen für den VirtualBox-Server ein. Dieses Feld steht für eine IP-Adresse oder einen Hostnamen des Remote-VirtualBox-Servers. |
| **Schnittstelle** | Geben Sie eine Portnummer für die Maschine ein. Sie steht für den Port, über den der Kern mit dieser Maschine kommuniziert. |
| **Virtual Machine Name (Name der virtuellen Maschine)** | Geben Sie einen Zielpfad für die Erstellung der virtuellen Maschine an. |
| **Benutzername** | Der Benutzername des Kontos auf der Zielmaschine, z. B. root. |
| **Kennwort** | Geben Sie die Anmeldeinformationen für die Host-Maschine ein. |
| **Speicher** | Geben Sie den Speicher der virtuellen Maschine an. |

8. Wählen Sie auf der Seite **Volumes** die zu exportierenden Daten-Volumes aus, und klicken Sie dann auf **Next** (Weiter).
9. 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.

### Ausführen eines dauerhaften Oracle VirtualBox-Exports (virtueller Standby)

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

1. Führen Sie in der 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** (Aktionen) für diese Maschine auf **Export (Exportieren)** → **Virtual Standby** (Virtueller Standby).
2. Wählen Sie auf der Seite **Destination** (Ziel) im **Export Wizard** (Assistenten für den Export) im Drop-Down-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) auf die Option **Use Windows machine** (Windows-Maschine verwenden).
4. Geben Sie die Parameter zum Zugriff auf die virtuelle Maschine wie in der folgenden Tabelle beschrieben ein.

| Textfeld | Beschreibung |
|---|---|
| **Virtual Machine Name (Name der virtuellen Maschine)** | Geben Sie einen Namen für die zu erstellende virtuelle Maschine ein.<br>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.<br>ANMERKUNG: Der Zielpfad sollte kein Stammverzeichnis sein.<br>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 den Speicher der virtuellen Maschine an.<br>• 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.<br>• Klicken Sie **Use a specific amount of RAM** (Eine bestimmte RAM-Größe verwenden) um anzugeben, wie viel RAM verwendet werden soll. Zum Beispiel: 4096 Megabytes (MB). Die kleinste zulässige Größe ist 512 MB. Die |

| Textfeld | Beschreibung |
|---|---|
| | maximale Größe wird durch das Fassungsvermögen und die Begrenzungen der Host-Maschine bestimmt. |

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 ad-hoc export** (Erstmaligen Ad-hoc-Export ausführen) aus, um den virtuellen Export sofort auszuführen, statt nach dem nächsten geplanten Snapshot.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite **Volumes** (Volumes) die zu exportierenden Volumes aus, z. B. C:\ und D:\, und klicken Sie dann auf **Next** (Weiter).
9. 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.

## Wiederherstellen von Volumes aus einem Wiederherstellungspunkt

Sie können die Volumes auf einer geschützten Maschine von Wiederherstellungspunkten im AppAssure-Kern wiederherstellen. So stellen Sie Volumes aus einem Wiederherstellungspunkt her:

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

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

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

   Daraufhin wird die Seite **Recovery Points** (Wiederherstellungspunkte) angezeigt.
3. Suchen Sie in der Liste der Wiederherstellungspunkte den Snapshot, den Sie auf der Agentenmaschine wiederherstellen möchten.

   ANMERKUNG: Falls erforderlich, verwenden Sie die Navigationsschaltflächen am unteren Rand der Seite, um zusätzliche Wiederherstellungspunkte anzuzeigen. Wenn Sie die Anzahl der Wiederherstellungspunkte auf der Seite „Recovery Points“ (Wiederherstellungspunkte) des Assistenten begrenzen möchten, können Sie nach Volumes (falls definiert) oder nach Datum der Erstellung des Wiederherstellungspunkts filtern.
4. Klicken Sie auf einen beliebigen Wiederherstellungspunkt, um ihn auszuwählen, und klicken Sie dann auf **Next** (Weiter).

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

5. Wählen Sie auf der Seite **Destination** (Ziel) die Maschine aus, die Sie wiederherstellen möchten. Gehen Sie dabei wie folgt vor:
   - Wenn Sie die Daten aus dem ausgewählten Wiederherstellungspunkt auf die gleiche Agentenmaschine (z. B. Machine1) wiederherstellen möchten, und wenn die Volumes, die Sie wiederherstellen möchten, nicht das System-Volume enthalten, wählen Sie **Recover to a protected machine (only non-system volumes)** (Wiederherstellung auf eine geschützte Maschine (nur Nicht-System-Volumes)) aus, überprüfen Sie, ob die Zielmaschine (Machine1) ausgewählt ist, und klicken Sie dann auf **Next** (Weiter). Die Seite **Volume Mapping** (Volume-Zuweisung) wird angezeigt. Fahren Sie mit Schritt 7 fort.
   - Wenn Sie die Daten aus dem ausgewählten Wiederherstellungspunkt auf einer anderen geschützten Maschine wiederherstellen möchten, um z. B. die Inhalte von Machine2 durch die Daten aus Machine1 zu ersetzen, wählen Sie dann die Option **Recover to a protected machine (only non-system volumes)** (Wiederherstellung auf einer geschützten Maschine (nur Nicht-System-Volumes)) aus, wählen Sie dann die Zielmaschine (z. B. Machine2) aus der Liste aus, und klicken Sie dann auf **Next** (Weiter). Die Seite **Volume Mapping** (Volume-Zuweisung) wird angezeigt. Fahren Sie mit Schritt 7 fort.
   - Wenn Sie die Wiederherstellung von dem ausgewählten Wiederherstellungspunkt auf der gleichen Maschine oder einer anderen Maschine über eine Start-CD durchführen möchten und wenn die Volumes, die Sie wiederherstellen möchten, das System-Volume nicht enthalten, wählen Sie die Option **Recover to any target machine using a boot CD** (Wiederherstellung auf eine beliebige Zielmaschine über eine Start-CD) aus.
   - Um fortzufahren, erstellen Sie die Start-CD mit den Informationen des ausgewählten Wiederherstellungspunkts, klicken Sie auf **Next** (Weiter), und fahren Sie mit Schritt 10 fort.
   - Wenn Sie bereits die Start-CD bereits erstellt und die Zielmaschine bereits über die Start-CD gestartet wurde, gehen Sie zu Schritt 17.
   - Wenn Sie ein System von einem Wiederherstellungspunkt wiederherstellen möchten (z. B. Laufwerk C: der Clientmaschine mit dem Namen „Machine1“), müssen Sie eine Bare-Metal-Wiederherstellung (BMR) ausführen. Weitere Informationen zum Ausführen einer Bare Metal-Wiederherstellung für Windows finden Sie unter Starten von Bare-Metal-Wiederherstellung für Windows-Maschinen.
   - Informationen zur Durchführung einer Bare Metal-Wiederherstellung für Linux finden Sie unter „Plan für die Durchführung einer Bare-Metal-Wiederherstellung für Linux-Maschinen“ unter Starten einer Bare-Metal-Wiederherstellung für eine Linux-Maschine.
6. Um eine Verbindung zur Universal Recovery Console (URC-Verbindung) auf der Zielmaschine herzustellen, führen Sie die folgenden Schritte aus:
   a. Wählen Sie **I already have a boot CD running on the target machine** (Ich verfüge bereits über eine Start-CD, die auf der Zielmaschine ausgeführt wird) aus.
   b. Geben Sie in das Feld „IP Address“ (IP-Adresse) die IP-Adresse der Zielmaschine mit der startfähigen CD ein.
   c. Geben Sie in das Feld „Authentication Key“ (Schlüssel für die Authentifizierung) den Authentifizierungsschlüssel vom URC auf der Zielmaschine ein, und klicken Sie dann auf **Next** (Weiter).

   Die Seite **Disk Mapping** (Netzwerkzuweisung) wird angezeigt. Fahren Sie mit Schritt 20 fort.
7. Wählen Sie auf der Seite **Volume Mapping** (Volume-Zuweisung) für jedes Volume im Wiederherstellungspunkt, das Sie wiederherstellen möchten, die entsprechenden Ziel-Volumes aus. Falls Sie ein Volume nicht wiederherstellen möchten, wählen Sie in der Spalte „Destination Volumes“ (Ziel-Volumes) die Option **Do not restore** (Nicht wiederherstellen) aus.
8. Wählen Sie **Show advanced options** (Erweiterte Optionen anzeigen) aus, und führen Sie dann die folgenden Schritte aus:
   - Für Informationen zum Wiederherstellen auf Windows-Maschinen mit Live Recovery wählen Sie **Live Recovery** (Live Recovery) aus.

     Mit der Live Recovery-Technologie zur Sofortwiederherstellung in AppAssure können Sie Daten sofort wiederherstellen oder auf Ihre physikalischen Maschinen oder auf virtuelle Maschinen von

gespeicherten Wiederherstellungspunkten für Windows-Maschinen, die Microsoft Windows Storage Spaces enthalten, wiederherstellen. Live Recovery ist für Linux-Maschinen nicht verfügbar.

- Wenn Sie die Aufhebung der Bereitstellung erzwingen möchten, wählen Sie **Force Dismount** (Erzwungene Aufhebung der Bereitstellung) aus.

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

9. Fahren Sie mit Schritt 20 fort.
10. Führen Sie auf der Seite „Boot CD" (Start-CD) die folgenden Schritte aus:
    a. Geben Sie in das Textfeld **Output path** (Ausgabepfad) den Pfad ein, unter dem das Start-CD-ISO-Image gespeichert werden soll.
    b. Wählen Sie unter **Environment** (Umgebung) die Architektur aus, die sich für die wiederherzustellende Hardware am besten eignet:
       - Um eine Windows-Maschine mit einer 64-Bit-Architektur wiederherzustellen, wählen Sie **Windows 8 64-Bit** aus.
       - Um eine Windows-Maschine mit einer 32-Bit-Architektur (x86) wiederherzustellen, wählen Sie **Windows 7 32-Bit** aus.
11. Wahlweise können Sie zum Einrichten der Netzwerkparameter für den wiederhergestellten Agenten oder für die Verwendung von UltraVNC die Option **Show advanced options** (Erweiterte Optionen anzeigen) auswählen und einen der folgenden Schritte ausführen:
    - Wählen Sie zum Einrichten einer Netzwerkverbindung für die wiederhergestellte Maschine die Option **Use the following IP address** (Folgende IP-Adresse verwenden) aus – wie in der folgenden Tabelle beschrieben.

| Option | Beschreibung |
|---|---|
| **IP-Adresse** | Geben Sie eine IP-Adresse oder einen Hostnamen für die wiederhergestellte Maschine ein. |
| **Subnet Mask (Subnetzmaske)** | Geben Sie die Subnetzmaske für die wiederhergestellte Maschine ein. |
| **Default Gateway (Standard-Gateway)** | Geben Sie das Standard-Gateway für die wiederhergestellte Maschine ein. |
| **DNS Server (DNS-Server)** | Geben Sie den Domänennamenserver für die wiederhergestellte Maschine ein. |

    - Um UltraVNC-Daten zu definieren, wählen Sie die Option **Add UltraVNC** (UltraVNC hinzufügen) – wie in der folgenden Tabelle beschrieben – aus. Verwenden Sie diese Option, wenn Sie den Remote-Zugriff auf die Recovery Console benötigen. Sie können sich nicht über die Microsoft-Terminaldienste anmelden, während Sie die Start-CD verwenden.

| Option | Beschreibung |
|---|---|
| **Password (Kennwort)** | Geben Sie ein Kennwort für diese UltraVNC-Verbindung ein. |
| **Port (Schnittstelle)** | Geben Sie einen Port für diese UltraVNC-Verbindung ein. Der Standardport ist 5900. |

12. Klicken Sie auf **Weiter**.
13. Um einen Treiber zu injizieren, führen Sie die folgenden Schritte aus:

a. Wählen Sie **Add an archive of drivers** (Treiberarchiv hinzufügen) aus.
b. Navigieren Sie zu einer ZIP-Datei, die das Archiv enthält, wählen Sie die ZIP-Datei aus, und klicken Sie auf **Open** (Öffnen). Das Archiv wird hochgeladen und wird auf der Seite „Driver Injection" (Treiberinjizierung) angezeigt.
c. Klicken Sie anschließend auf **Next** (Weiter).

**14.** Auf der Seite „ISO Image" (ISO-Image) können Sie den Status des Start-CD-ISO-Images abrufen. Wenn die Start-CD erfolgreich erstellt wurde, klicken Sie auf **Next** (Weiter).

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

**15.** Starten Sie die Agentenmaschine, für die Sie Daten über die Start-CD wiederherstellen möchten.

- Starten Sie die Agentenmaschine von einem ISO-Image, sofern möglich.
- Ist dies nicht der Fall, kopieren Sie das ISO-Image auf physische Datenträger (CD oder DVD), laden Sie den Datenträger in die Agentenmaschine, konfigurieren Sie die Maschine zum Laden von der Start-CD, und führen Sie einen Neustart von der Start-CD aus.

ANMERKUNG: Sie müssen möglicherweise die BIOS-Einstellungen der Agentenmaschine ändern, um sicherzustellen, dass das Volume, das zuerst geladen wird, die Start-CD ist.

Die Agentenmaschine zeigt, wenn sie von der Start-CD aus gestartet wird, die Universal Recovery Console (URC-)Schnittstelle an. Diese Umgebung wird zur Wiederherstellung des Systemlaufwerks oder ausgewählter Volumes direkt von der AppAssure Core verwendet. Beachten Sie die IP-Adresse und die Anmeldeinformationen für die Authentifizierung in der URC, die jedes Mal aktualisiert werden, wenn Sie von der Start-CD aus starten.

**16.** Klicken Sie in der Core-Konsole auf die Seite **Connection** (Verbindung), und geben Sie die Authentifizierungsinformationen von der URC-Instanz der Maschine, die Sie wiederherstellen möchten, wie folgt ein:

a. Geben Sie im Textfeld „IP Address" (IP-Adresse) die IP-Adresse der Maschine ein, auf die Sie die Wiederherstellung von einem Wiederherstellungspunkt aus durchführen.
b. Geben Sie in das Textfeld „Authentification Key" (Schlüssel für Authentifizierung) die Informationen der URC ein..
c. Klicken Sie auf **Weiter**.

Daraufhin wird die Seite **Disk Mapping** (Laufwerkszuweisung) angezeigt.

**17.** Um Volumes manuell zuzuordnen, gehen Sie zu Schritt 18. Um Volumes automatisch zuzuordnen, gehen Sie wie folgt vor:

a. Wählen Sie **Automatic volume mapping** (Automatische Zuordnung von Volumes) aus.
b. Wählen Sie im Bereich für **Automatic volume mapping** (Automatische Zuordnung von Volumes) die Volumes aus, die Sie wiederherstellen möchten. Wenn Sie keines der aufgeführten Volumes wiederherstellen möchten, deaktivieren Sie die Option.

ANMERKUNG: Mindestens ein Volume muss ausgewählt sein, um die Wiederherstellung durchzuführen.

c. Wählen Sie die Zielfestplatte für die Wiederherstellung aus.
d. Klicken Sie auf **Next** (Weiter), und gehen Sie dann zu Schritt 19.

**18.** Wenn Sie Volumes manuell zuordnen möchten, führen Sie die folgenden Schritte aus:

a. Wählen Sie **Manual volume mapping** (Manuelle Zuordnung von Volumes) aus.
b. Wählen Sie im Bereich **Manual volume mapping** (Manuelle Zuordnung von Volumes) in der Drop-Down-Liste **Destination Volumes** (Ziel-Volumes) für jedes Volume das Volume aus, das Sie wiederherstellen möchten. Wenn Sie keines der aufgeführten Volumes wiederherstellen möchten, deaktivieren Sie die Option.

ANMERKUNG: Mindestens ein Volume muss ausgewählt sein, um die Wiederherstellung durchzuführen.

c. Klicken Sie auf **Fertigstellen**.

**VORSICHT: Wenn Sie „Finish“ (Fertig stellen) auswählen, werden alle bestehenden Partitionen und Daten auf dem Ziellaufwerk dauerhaft entfernt, und sie werden mit den Inhalten des ausgewählten Wiederherstellungspunkts ersetzt, und zwar einschließlich des Betriebssystems und aller Daten.**

Der **Restore Machine Wizard** (Assistent für die Wiederherstellung der Maschine) wird geschlossen, und die Daten werden von den ausgewählten Volumes des Wiederherstellungspunkts auf die Zielmaschine übertragen. Fahren Sie mit Schritt 22 fort.

19. Prüfen Sie auf der Seite **Disk Mapping Preview** (Vorschau für die Laufwerkszuweisung) die Parameter der Wiederherstellungsaktionen, die Sie ausgewählt haben. Um die Wiederherstellung durchzuführen, klicken Sie auf **Finish** (Fertig stellen).

    **VORSICHT: Wenn Sie „Finish“ (Fertig stellen) auswählen, werden alle bestehenden Partitionen und Daten auf dem Ziellaufwerk dauerhaft entfernt, und sie werden mit den Inhalten des ausgewählten Wiederherstellungspunkts ersetzt, und zwar einschließlich des Betriebssystems und aller Daten.**

    Der **Restore Machine Wizard** (Assistent für die Wiederherstellung der Maschine) wird geschlossen, und die Daten werden von den ausgewählten Volumes des Wiederherstellungspunkts auf die Zielmaschine übertragen. Fahren Sie mit Schritt 22 fort.

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

## Wiederherstellen von Volumes für eine Linux-Maschine unter Verwendung der Befehlszeile

In AppAssure können Sie Volumes auf Ihren geschützten Linux-Maschinen mithilfe des Befehlszeilen-Dienstprogramms `aamount` wiederherstellen. So stellen Sie Volumes für eine Linux-Maschine unter Verwendung der Befehlszeile wieder her:

**VORSICHT: Sie sollten nicht versuchen, das System- oder Root (/)-Volume wiederherzustellen.**

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

   ```
   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`.

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.

# Starten der Bare-Metal-Wiederherstellung für Windows-Maschinen

In AppAssure können Sie eine Bare-Metal-Wiederherstellung (BMR) für Ihre Windows Maschinen durchführen, egal ob die Hardware gleichartig oder unterschiedlich ist. Dieser Vorgang enthält das Erstellen des Start-CD-Abbilds, das Brennen des Abbilds auf einen Datenträger, das Starten der Zielserver von 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 Ihre Konfiguration durchführen.

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 Starten einer Bare-Metal-Wiederherstellung für eine Linux-Maschine.

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

### 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 Zuordnung muss die neue Maschine bereits richtig formatiert sein, bevor sie wiederhergestellt wird.

So ordnen Sie Volumes zu:

1. Um Volumes automatisch zuzuordnen, gehen Sie wie folgt vor:
   a. Klicken Sie auf der Seite **Disk Mapping** (Laufwerkszuordnung) des **Restore Machine Wizard** (Assistenten zum Wiederherstellen von Maschinen) auf die Registerkarte **Automatically Map Volumes** (Volumes automatisch zuordnen).
   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 **Restore** (Wiederherstellen), und fahren Sie dann mit Schritt 3 fort.
2. Um Volumes manuell zuzuordnen, gehen Sie wie folgt vor:
   a. Klicken Sie auf der Seite **Disk Mapping** (Laufwerkszuweisung) des **Restore Machine Wizard** (Assistenten zum Wiederherstellen von Maschinen) auf die Registerkarte **Manually Map Volumes** (Volumes manuell zuordnen).
   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 das Rollback auszuführen, klicken Sie auf **Restore** (Wiederherstellen).

   **VORSICHT: 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).

## Starten einer Bare-Metal-Wiederherstellung für eine Linux-Maschine

DL1000 kann eine Bare-Metal-Wiederherstellung (BMR) für eine Linux-Maschine, einschließlich Rollback des System-Volumes, durchführen. Unter Verwendung des AppAssure Befehlszeilendienstprogramms `aamount` können Sie einen Rollback-Vorgang zum Boot-Volume-Basisabbild durchführen. Bevor Sie eine BMR für eine Linux-Maschine durchführen können, müssen Sie Folgendes tun:

- 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 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 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.

5

# Replizieren von Wiederherstellungspunkten

## Replikation

Replikation ist der Prozess des Kopierens von Wiederherstellungspunkten und des Übertragens dieser Punkte auf einen sekundären Speicherort, um diese im Falle einer Notfallwiederherstellung verwenden zu können. Für diesen Prozess benötigen Sie eine gekoppelte Quell-Ziel-Beziehung zwischen zwei Kernen. Die Replikation wird auf jeder geschützten Maschine einzeln verwaltet, d. h. dass Sicherungs-Snapshots einer geschützten Maschine auf dem Zielreplikatkern repliziert werden. Wenn eine Replikation eingerichtet wurde, überträgt der Quellkern die inkrementellen Snapshot-Daten asynchron und fortlaufend auf den Zielkern. Sie können diese bandexterne Replikation für das unternehmenseigene Rechenzentrum oder den Remote-Notfallwiederherstellungsstandort (also einen selbstverwalteten Zielkern) oder für einen Managed Service Provider (MSP) konfigurieren, der Remote-Backup- und Notfallwiederherstellungsdienste anbietet. Um eine Replikation auf einem MSP auszuführen, können Sie integrierte Arbeitsabläufe verwenden, über die Sie Verbindungen anfordern und automatische Rückmeldungen erhalten können.

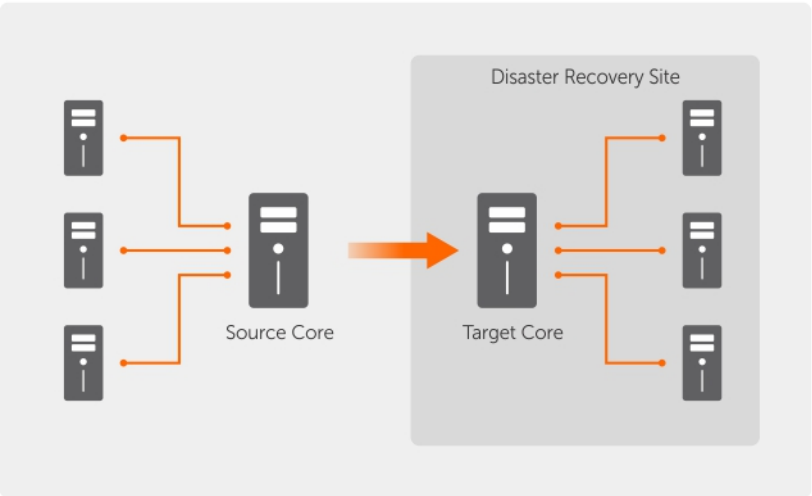


**Abbildung 5. Grundlegende Replikationsarchitektur**

Die Replikation beginnt mit dem Seeding: Die anfängliche Übertragung von deduplizierten Basisabbildern und inkrementellen Snapshots der geschützten Agenten, die sich auf Hunderte oder Tausende Gigabytes von Daten summieren können. Die erste Replikation kann mithilfe externer Medien auf dem Zielkern platziert werden. Üblicherweise ist das bei großen Datensätzen oder Standorten mit langsamer Verbindung nützlich. Die Daten im Seeding-Archiv sind komprimiert, verschlüsselt und dedupliziert. Wenn die Gesamtgröße des Archivs den auf dem Wechseldatenträger verfügbaren Speicherplatz überschreitet,

kann sich das Archiv, je nach verfügbarem Speicherplatz auf dem Datenträger, über mehrere Geräte erstrecken. Während des Seeding-Vorgangs werden die inkrementellen Wiederherstellungspunkte am Zielstandort repliziert. Nachdem der Zielkern das Seeding-Archiv konsumiert, werden die neu replizierten inkrementellen Wiederherstellungspunkte automatisch synchronisiert.

# 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:<br>• 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).<br>• 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:<br>• **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.<br>• **Replace this core** (Diesen Kern ersetzen) – Alle bereits vorhandenen Daten auf diesem Kern werden überschrieben, die Daten für andere Kerne bleiben aber intakt.<br>• **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. |
| **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.<br>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- |

| Textfeld | Beschreibung |
|---|---|
| | 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. |

| Textfeld | Beschreibung |
|---|---|
| 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.

## 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.<br>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:<br>• Protect all volumes with default schedule (Alle Volumes gemäß Standardzeitplan schützen) |

| Textfeld | Beschreibung |
|---|---|
| | • Protect specific volumes with custom schedule (Alle Volumes gemäß benutzerdefiniertem Zeitplan schützen)<br><br>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).

## 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**.

## 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 4. 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 | Auf einem Quellkern im Drop-Down-Menü können Sie die folgenden Optionen auswählen:<br>• **Details** (Einzelheiten) – ID, URI, Anzeigename, Zustand, Kunden-ID, E-Mail-Adresse und Anmerkungen zum replizierten Kern anzeigen.<br>• **Change Settings** (Einstellungen ändern) – |

| Abschnitt | Beschreibung | Verfügbare Maßnahmen |
|---|---|---|
| | Replikationsübertragung werden angezeigt. | Anzeigename anzeigen und Host und Port für den Zielkern bearbeiten.<br>• **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. |
| 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:<br>• **Details** (Einzelheiten) – ID, Hostname, Kunden-ID, E-Mail-Adresse und Anmerkungen zum replizierten Kern anzeigen.<br>• **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. |

| Option | Beschreibung |
| --- | --- |
| **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).

# Grundlegendes zu Failover und Failback

AppAssure unterstützt Failover und Failback im Falle eines schwerwiegenden Systemausfalls, bei der der Quellkern und Agenten ausfallen, in replizierten Umgebungen. Failover bedeutet das Wechseln auf ein redundantes oder Standby-Ziel (AppAssure-Kern) bei einem Systemfehler oder einer unnormalen Beendigung eines Quellkerns und der zugewiesenen Agenten. Das Hauptziel des Failovers ist das Starten eines neuen Agenten, der mit dem ausgefallen Agenten identisch ist. Das zweite Ziel besteht darin, den Zielkern in einen neuen Modus zu schalten, so dass 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 Failed-over-Maschinen starten.

Failback bezeichnet das Wiederherstellen eines Agenten und eines Kerns zurück in ihren ursprünglichen Zustand (vor dem Ausfall). Das Hauptziel des Failbacks besteht darin, den Agenten (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.

## Durchführen eines Failovers

Wenn Sie mit einer Notfallsituation konfrontiert sind, in der Ihr Quellkern und verknüpfte Agenten ausgefallen sind, können Sie in AppAssure Failover aktivieren, um den Schutz auf Ihren identischen Failover-(Ziel-)Kern zu schalten. Der Zielkern wird zum einzigen Kern, der die Daten in Ihrer Umgebung schützt. Starten Sie nun 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.**

   Das Dialogfeld **Fail Over** (Failover) wird angezeigt und zeigt die nächsten Schritte für den Abschluss eines Failover an.
4. Klicken Sie auf **Continue** (Weiter).
5. Wählen Sie im linken Navigationsbereich unter **Protected Machines** (Geschützte Maschinen) die Maschine aus, die über den verknüpften AppAssure-Agenten mit Wiederherstellungspunkten verfügt.
6. Exportieren Sie die Sicherungsinformationen über den Wiederherstellungspunkt auf dem Agenten zu einer virtuellen Maschine.
7. Exportieren Sie die Sicherungsinformationen über den Wiederherstellungspunkt auf dem Agenten zu einer virtuellen Maschine.
8. Starten Sie die virtuelle Maschine, auf der sich nun die exportierten Sicherheitsinformationen befinden.

   Sie müssen warten, bis die Gerätetreibersoftware installiert ist.

9. Starten Sie die virtuelle Maschine neu und warten Sie darauf, dass der Agent-Service gestartet wird.
10. Gehen Sie zurück zur Core Console für den Zielkern, und überprüfen Sie, ob der neue Agent unter **Protected Machines** (Geschützte Maschinen) auf der Registerkarte **Replication** (Replikation) unter **Incoming Replication** (Eingehende Replikation) angezeigt wird.
11. Erzwingen Sie mehrere Snapshots und überprüfen Sie, ob diese korrekt abgeschlossen werden.

    Weitere Informationen finden Sie unter Erzwingen eines Snapshots.
12. 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 Agenten repariert oder ausgetauscht 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 **Continue** (Weiter) klicken können, um das Failback abzuschließen.
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. Erzwingen Sie einen Snapshot der Maschine. Weitere Informationen finden Sie unter Erzwingen eines Snapshots.
7. Fahren Sie die Maschine mit dem Failover herunter.
8. Erstellen Sie ein Archiv auf dem Failed-over-Agenten und geben Sie es auf ein Laufwerk oder einen Speicherort in der Netzwerkfreigabe aus.

   Weitere Informationen zum Erstellen von Archiven finden Sie unter Erstellen eines Archivs.
9. Nachdem Sie das Archiv erstellt haben, navigieren Sie zur Core Console im neu reparierten Quell-Kern und klicken Sie auf die Registerkarte **Tools** (Extras).
10. Importieren Sie das Archiv, das Sie gerade in Schritt 8 erstellt haben.

    Weitere Informationen finden Sie unter Importieren eines Archivs.
11. Gehen Sie zur Core Console auf dem Zielkern zurück und klicken Sie auf die Registerkarte **Replication** (Replikation).
12. Wählen Sie unter **Incoming Replication** (Eingehende Replikation) den Failover-Agenten aus und vergrößern Sie die Detail-Ansicht.
13. Klicken Sie im Dialogfeld **Failback** auf **Continue** (Weiter).
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, so müssen Sie die vom Zielkern importierten Wiederherstellungspunkte auf dem Agenten auf der virtuellen Maschine verwenden.

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.

    Weitere Informationen finden Sie unter Konfigurieren der Maschineneinstellungen.
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.

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<br>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

# Wie Sie Hilfe bekommen

## Ausfindig machen der Dokumentation und Software-Aktualisierungen

Direkte Links zur AppAssure- und DL1000 Appliance-Dokumentation und zu Software-Aktualisierungen finden Sie in der Core Console.

### Dokumentation

So greifen Sie auf den Link für die Dokumentation zu:

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

### Software updates (Softwareaktualisierungen)

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

1. Klicken Sie in der Core Console auf der Registerkarte **Appliance** (Gerät).
2. Navigieren Sie im linken Fensterbereich zum Link **Appliance (Gerät)** → **Software Updates (Software-Aktualisierungen)**.

## Kontaktaufnahme mit Dell

Dell bietet verschiedene Optionen für Online- und Telefonsupport 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 an Dell für den Verkauf, den technischen Support und den Kundendienst zu wenden, 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.