Benutzerhandbuch

PlateSpin® Protect 10.2

4. Mai 2012

Novell

Rechtliche Hinweise

Novell, Inc. leistet keinerlei Gewähr bezüglich des Inhalts oder Gebrauchs dieser Dokumentation. Insbesondere werden keine ausdrücklichen oder stillschweigenden Gewährleistungen hinsichtlich der handelsüblichen Qualität oder Eignung für einen bestimmten Zweck übernommen. Novell, Inc. behält sich weiterhin das Recht vor, diese Dokumentation zu revidieren und ihren Inhalt jederzeit und ohne vorherige Ankündigung zu ändern.

Des Weiteren übernimmt Novell, Inc. für Software keinerlei Haftung und schließt insbesondere jegliche ausdrücklichen oder impliziten Gewährleistungsansprüche bezüglich der Marktfähigkeit oder der Eignung für einen bestimmten Zweck aus. Außerdem behält sich Novell, Inc. das Recht vor, Novell-Software ganz oder teilweise jederzeit inhaltlich zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen von diesen Überarbeitungen oder Änderungen in Kenntnis zu setzen.

Alle im Zusammenhang mit dieser Vereinbarung zur Verfügung gestellten Produkte oder technischen Informationen unterliegen möglicherweise den US-Gesetzen zur Exportkontrolle sowie den Handelsgesetzen anderer Länder. Sie erkennen alle Ausfuhrkontrollbestimmungen an und erklären sich damit einverstanden, alle für ausstehende Exporte, Re-Exporte oder Importe erforderlichen Lizenzen bzw. Klassifizierungen einzuholen. Sie erklären sich damit einverstanden, nicht an juristische Personen, die in der aktuellen US-Exportausschlussliste enthalten sind, oder an in den US-Exportgesetzen aufgeführte terroristische Länder oder Länder, die einem Embargo unterliegen, zu exportieren oder zu reexportieren. Sie stimmen zu, keine Lieferungen für verbotene nukleare oder chemisch-biologische Waffen oder Waffen im Zusammenhang mit Flugkörpern zu verwenden. Weitere Informationen zum Export von Novell-Software finden Sie auf der Webseite Novell International Trade Services (http://www.novell.com/info/exports/). Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online-Dokumentation: Die neueste Online-Dokumentation für dieses und andere Novell-Produkte finden Sie auf der Dokumentations-Webseite von Novell (http://www.novell.com/documentation).

Novell-Marken

Hinweise zu Novell-Marken finden Sie in der Novell Trademark and Service Mark-Liste (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materialien von Drittanbietern

Die Rechte für alle Marken von Drittanbietern liegen bei den jeweiligen Eigentümern.

Inhalt

Informationen zu diesem Handbuch

Dieses Handbuch enthält Informationen zur Verwendung von PlateSpin Protect.

Zielgruppe

Dieses Handbuch ist für IT-Mitarbeiter wie beispielsweise Rechenzentrumsadministratoren und -operatoren vorgesehen, die PlateSpin Protect in Workload-Schutzprojekten verwenden.

Rückmeldungen

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Bitte verwenden Sie die Funktion für Benutzerkommentare im unteren Bereich jeder Seite der Online-Dokumentation oder senden Sie uns Ihre Kommentare über die Novell Documentation Feedback-Website (http://www.novell.com/documentation/feedback.html).

Weitere Dokumentation

Dieses Handbuch ist Bestandteil der PlateSpin Protect-Dokumentation.

Eine vollständige Liste der Publikationen, die diese Version unterstützen, finden Sie auf der Website mit der Online-Dokumentation für PlateSpin Protect 10 (http://www.novell.com/documentation/platespin_protect_10).

Aktualisierungen der Dokumentation

Die neueste Version dieses Handbuchs finden Sie auf der Online-Dokumentations-Website zu PlateSpin Protect 10 (http://www.novell.com/documentation/platespin_protect_10):

Zusätzliche Ressourcen

Wir empfehlen Ihnen, die folgenden zusätzlichen Ressourcen im Web zu nutzen:

- Novell User Forum (http://forums.novell.com): eine webbasierte Community mit verschiedenen Diskussionsthemen.
- Novell Knowledgebase (http://www.novell.com/support): eine Sammlung ausführlicher technischer Artikel.

Technischer Support

- Telefon (Nordamerika): +1-877-528-3774 (1 87 PlateSpin)
- Telefon (international): +1-416-203-4799
- Email: support@platespin.com

Sie können Support auf der Service-Anforderungs-Webseite (http://support.novell.com/contact/getsupport.html) auch online abfragen.

1 Produktübersicht

1.1 Informationen zu PlateSpin Protect

PlateSpin Protect ist eine Software zur Geschäftskontinuität und Wiederherstellung im Katastrophenfall, die physische und virtuelle Workloads (Betriebssysteme, Middleware und Daten) anhand von Virtualisierungstechniken schützt. Im Fall eines Ausfalls oder einer Katastrophe am Produktionsserver, kann eine virtualisierte Reproduktion eines Workloads im Ziel*container* (einem VM-Host) aktiviert werden und weiterhin normal ausgeführt werden bis die Produktionsumgebung wiederhergestellt ist.

PlateSpin Protect ermöglicht Ihnen Folgendes:

- Schnelle Wiederherstellung von Workloads nach einem Fehler
- Schutz von mehreren Workloads gleichzeitig
- Testen des Failover-Workloads ohne Ihre Produktionsumgebung zu beeinträchtigen
- Failback für Failover-Workloads durchführen, entweder auf ihre ursprünglichen oder auf völlig neue Infrastrukturen, ob physische oder virtuelle
- Unterstützung externer Speicherlösungen, z. B. SANs

1.2 Unterstützte Konfigurationen

1.2.1 Unterstützte Workloads in VM-Containern

PlateSpin Protect unterstützt sowohl Windows- als auch Linux-Workloads.

Tabelle 1-1 *Unterstützte Windows-Workloads*

Betriebssystem	Anmerkungen
Windows 7	Nur Professional, Enterprise und Ultimate Editions
Windows Server 2008 R2	Einschließlich Domänencontroller- und Small Business Server-Editionen
Windows Server 2008	Einschließlich Domänencontroller- und Small Business Server-Editionen
Windows Vista	Business-, Enterprise- und Ultimate-Editionen; SP1 und höher
Windows Server 2003 R2	Einschließlich Domänencontroller- und Small Business Server-Editionen
Windows Server 2003	Einschließlich Domänencontroller- und Small Business Server-Editionen
Windows XP Professional	
Windows Server 2000	Service Pack 4 mit Update-Rollup 1 erforderlich.
Windows-Cluster	Weitere Informationen zu bestimmten unterstützten Cluster-Konfigurationen finden Sie unter „Schützen von Windows-Clustern“, auf Seite 72

Unterstützte internationale Versionen (Windows): Französisch, Deutsch, Japanisch, Chinesisch (traditionell) und Chinesisch (vereinfacht)

Tabelle 1-2 *Unterstützte Linux-Workloads*

Betriebssystem
Red Hat Enterprise Linux (RHEL) 4, 5
SUSE Linux Enterprise Server (SLES) 9, 10, 11 (bis SP1)
Open Enterprise Server 2, SP2 und SP3
Oracle Enterprise Linux (OEL) 5.3, 5.4

Unterstützte internationale Versionen (Linux): Alle internationalen Versionen dieser Linux-Systeme werden unterstützt.

1.2.2 Unterstützte VM-Containern

Tabelle 1-3 *Virtualisierungsplattformen, die als VM-Container unterstützt werden*

Plattform	Hinweise
VMware DRS-Cluster in vSphere 5.0	◆ Die DRS-Konfiguration muss entweder **Teilweise automatisiert** oder **Vollautomatisch** sein (sie darf nicht auf **Manuell** gesetzt sein) ◆ Der Cluster darf nur aus ESXi 5.0-Servern bestehen und darf nur von vCenter 5.0 verwaltet werden
VMware DRS-Cluster in vSphere 4.1	◆ Die DRS-Konfiguration muss entweder **Teilweise automatisiert** oder **Vollautomatisch** sein (sie darf nicht auf **Manuell** gesetzt sein) ◆ Der Cluster kann eine Kombination aus ESX 4.1- und ESX**i** 4.1-Servern verwenden und darf nur von vCenter 4.1 verwaltet werden
VMware ESX**i** 4.1, 5.0	ESX**i**-Versionen erfordern eine erworbene Lizenz. Der Schutz wird bei diesen Systemen nicht unterstützt, wenn sie mit einer kostenlosen Lizenz ausgeführt werden.
VMware ESX 4.1	

1.3 Sicherheit und Datenschutz

PlateSpin Protect stellt Ihnen eine Reihe von Funktionen zur Verfügung, mit denen Sie Ihre Daten schützen und die Sicherheit Ihres Systems erhöhen können.

- Abschnitt 1.3.1, „Sicherheit der Workload-Daten bei der Übertragung“, auf Seite 11
- Abschnitt 1.3.2, „Sicherheit der Client-Server-Kommunikation“, auf Seite 12
- Abschnitt 1.3.3, „Sicherheit von Berechtigungsnachweisen“, auf Seite 12
- Abschnitt 1.3.4, „Benutzerautorisierung und -authentifizierung“, auf Seite 12

1.3.1 Sicherheit der Workload-Daten bei der Übertragung

Sie können den Workload-Schutz so konfigurieren, dass die Daten verschlüsselt werden, um die Übertragung Ihrer Workload-Daten sicherer zu machen. Wenn die Verschlüsselung aktiviert ist, werden über das Netzwerk reproduzierte Daten unter Verwendung von AES (Advanced Encryption Standard) verschlüsselt.

Falls erforderlich, können Sie Ihren PlateSpin Protect-Server für die Verwendung eines Datenverschlüsselungs-Algorithmus konfigurieren, der FIPS (Federal Information Processing Standards, Publication 140-2) entspricht. Weitere Informationen hierzu finden Sie unter “Aktivieren der Unterstützung für FIPS-konforme Datenverschlüsselungs-Algorithmen (optional)” in Ihrer *Installationsanleitung*.

Sie können die Verschlüsselung für jeden Workload einzeln aktivieren oder deaktivieren. Weitere Informationen hierzu finden Sie in „Workload-Schutz-Details“, auf Seite 48.

1.3.2 Sicherheit der Client-Server-Kommunikation

Die Datenübertragung zwischen Ihrem Webbrowser und dem PlateSpin Protect-Server kann entweder für HTTP (Standard) oder HTTPS (Hypertext Transfer Protocol Secure) konfiguriert werden.

Um die Datenübertragung zwischen dem Client und dem Server abzusichern, müssen Sie SSL auf Ihrem PlateSpin Protect-Server-Host aktivieren, die Serverkonfiguration entsprechend ändern (siehe „Aktivieren der SSL-Kommunikation mit dem PlateSpin-Server“, auf Seite 25) und für die Angabe der Server-URL HTTPS verwenden.

1.3.3 Sicherheit von Berechtigungsnachweisen

Der Berechtigungsnachweis, den Sie für den Zugriff auf verschiedene Systeme (z. B. Workloads und Failback-Ziele) verwenden, wird in der PlateSpin Protect-Datenbank gespeichert und unterliegt daher denselben Sicherheitsmechanismen, die Sie für den PlateSpin Protect-Server-Host implementiert haben.

Darüber hinaus sind Berechtigungsnachweise in der Diagnose enthalten, die für berechtigte Benutzer zugänglich ist. Sie sollten sicherstellen, dass Workload-Schutz-Projekte von befugten Mitarbeitern bearbeitet werden.

1.3.4 Benutzerautorisierung und -authentifizierung

PlateSpin Protect bietet einen umfassenden und sicheren Benutzerautorisierungs- und authentifizierungsmechanismus, der auf Benutzerrollen basiert und den Anwendungszugriff sowie die Aktionen steuert, die Benutzer ausführen können. Weitere Informationen hierzu finden Sie in Abschnitt 2.2, „Einrichten der Benutzerautorisierung und -authentifizierung“, auf Seite 16.

1.4 Leistung

1.4.1 Allgemeines zu Produktleistungsmerkmalen

Die Leistungsmerkmale Ihres PlateSpin Protect-Produkts sind von einer Reihe von Faktoren abhängig, darunter:

- Hardware- und Softwareprofile Ihrer Ursprungs-Workloads
- Hardware- und Softwareprofile Ihrer Ziel-Container
- Hardware- und Softwareprofil Ihres PlateSpin Protect-Server-Hosts
- Eigenschaften Ihrer Netzwerkbandbreite, -konfiguration und -bedingungen
- Die Anzahl der geschützten Workloads
- Die Anzahl der Volumes unter Schutz

- Die Größe der Volumes unter Schutz
- Dateidichte (Anzahl der Dateien pro Kapazitätseinheit) auf den Volumes des Ursprungs-Workloads
- Ursprungs-E/A-Ebenen (die Auslastung Ihrer Workloads)
- Die Anzahl der gleichzeitigen Reproduktionen
- Ob die Datenverschlüsselung aktiviert oder deaktiviert ist
- Ob die Datenkomprimierung aktiviert oder deaktiviert ist

Bei umfangreichen Workload-Schutz-Plänen sollten Sie einen Testschutz eines typischen Workloads und einige Reproduktionen durchführen und das Ergebnis als Benchmark verwenden, wobei Sie Ihre Metriken während des gesamten Projekts regelmäßig feineinstellen sollten.

1.4.2 Datenkomprimierung

Falls erforderlich, kann PlateSpin Protect die Workload-Daten vor der Übertragung über das Netzwerk komprimieren. So können Sie die Gesamtmenge der während Reproduktionen übertragenen Daten verringern.

Die Komprimierungsverhältnisse hängen von der Art der Dateien auf den Volumes eines Ursprungs-Workloads ab und können von 0,9 (100 MB Daten komprimiert auf 90 MB) bis etwa 0,5 (100 MB komprimiert auf 50 MB) variieren.

Hinweis: Die Datenkomprimierung verwendet die Prozessorleistung des Ursprungs-Workloads.

Die Datenkomprimierung kann für jeden Workload einzeln oder auf einer Schutzebene konfiguriert werden. Weitere Informationen hierzu finden Sie in „Schutzebenen“, auf Seite 63.

1.4.3 Bandbreitendrosselung

In PlateSpin Protect können Sie die Menge an Netzwerkbandbreite, die im Verlauf eines Workload-Schutzes durch die direkte Ursprung-zu-Ziel-Kommunikation verbraucht wird, steuern. Sie können für jeden Schutzplan eine Durchsatzrate festlegen. Dies verhindert, dass Reproduktionsverkehr Ihr Produktionsnetzwerk verstopft, und verringert die Gesamtlast Ihres PlateSpin Protect-Servers.

Die Bandbreitendrosselung kann für jeden Workload einzeln konfiguriert werden oder auf einer Schutzebene. Weitere Informationen hierzu finden Sie in „Schutzebenen“, auf Seite 63.

1.4.4 RPO-, RTO- und TTO-Spezifikationen

- **Angestrebter Wiederherstellungszeitpunkt (RPO):** Beschreibt die akzeptable Menge an Datenverlust, gemessen in Zeit. Der RPO ermittelt sich aus der Zeit zwischen den inkrementellen Reproduktionen eines geschützten Workloads und wird vom aktuellen

Nutzungsumfang von PlateSpin Protect, der Rate und dem Ausmaß von Änderungen im Workload sowie von der Netzwerkgeschwindigkeit und dem gewählten Reproduktionszeitplan beeinflusst.

- **Angestrebte Wiederherstellungszeit (RTO):** Beschreibt die Zeit, die für einen Failover-Vorgang (einen Failover-Workload in den Online-Modus versetzen, um einen geschützten Produktions-Workload vorübergehend zu ersetzen) benötigt wird.

  Die für einen Failover eines Workloads auf dessen virtuelle Reproduktion benötigte RTO wird von der Zeit beeinflusst, die für das Konfigurieren und Ausführen des Failover-Vorgangs benötigt wird (10 bis 45 Minuten). Weitere Informationen hierzu finden Sie in „Failover“, auf Seite 52.

- **Angestrebte Testzeit (TTO):** Beschreibt die Zeit, die zum Testen des Wiederherstellungsplans benötigt wird, damit der Dienst erfolgreich wiederhergestellt werden kann.

  Verwenden Sie die Funktion *Failover testen*, um verschiedene Szenarien zu durchlaufen und Vergleichsdaten zu generieren. Weitere Informationen hierzu finden Sie unter „Verwenden der Funktion "Failover testen"“, auf Seite 54.

Zu den Faktoren, die Auswirkungen auf den RPO sowie die RTO und TTO haben, gehört die Anzahl der erforderlichen gleichzeitigen Failover-Vorgänge. Ein einzelner Failover-Workload verfügt über mehr Arbeitsspeicher und CPU-Ressourcen als mehrere Failover-Workloads, die sich die Ressourcen der ihnen zugrunde liegenden Infrastruktur teilen.

Führen Sie zum Ermitteln der durchschnittlichen Failover-Zeiten für Workloads in Ihrer Umgebung Test-Failovers zu unterschiedlichen Zeiten durch und verwenden Sie sie als Vergleichsdaten in Ihren Gesamtwiederherstellungsplänen. Weitere Informationen hierzu finden Sie in „Generieren von Workload- und Workload-Schutz-Berichten“, auf Seite 41.

1.4.5 Skalierbarkeit

Die Skalierbarkeit hängt von den folgenden Hauptmerkmalen Ihres PlateSpin Protect-Produkts ab:

- **Workloads pro Server:** Die Anzahl der Workloads pro PlateSpin Protect-Server kann zwischen 5 und 40 variieren. Dies hängt von verschiedenen Faktoren ab, z. B. Ihren RPO-Anforderungen und den Hardware-Eigenschaften des Server-Hosts.
- **Schutz pro Container:** Der maximale Schutz pro Container basiert auf den VMware-Spezifikationen bezüglich der maximalen Anzahl an unterstützten VMs pro ESX-Host (ist aber nicht identisch). Weitere Faktoren sind die Wiederherstellungsstatistik (einschließlich der gleichzeitigen Reproduktionen und Failovers) sowie die Händlerspezifikationen für die Hardware.

Sie sollten Tests durchführen, Ihre Kapazitätszahlen stufenweise anpassen und sie zur Bestimmung der maximalen Skalierbarkeit verwenden.

2 Anwendungskonfiguration

2.1 Produktlizenzierung

Dieser Abschnitt enthält Informationen für die Aktivierung der PlateSpin Protect-Software.

2.1.1 Abrufen eines Lizenzaktivierungscodes

Für die Produktlizenzierung benötigen Sie einen Lizenzaktivierungscode. Falls Sie nicht über einen Lizenzaktivierungscode verfügen, können Sie diesen über die Novell Customer Center-Website (http://www.novell.com/customercenter/) anfordern. Sie erhalten dann eine Email mit einem Lizenzaktivierungscode.

Wenn Sie sich zum ersten Mal bei PlateSpin Protect anmelden, wird der Browser automatisch zur Seite für die Lizenzaktivierung umgeleitet. Sie haben zwei Möglichkeiten, um Ihre Produktlizenz zu aktivieren: Online-Lizenzaktivierung oder Offline-Lizenzaktivierung.

2.1.2 Online-Lizenzaktivierung

Für die Online-Aktivierung von PlateSpin Protect benötigen Sie einen Internetzugang.

Hinweis: HTTP-Proxys können während der Online-Aktivierung Fehler verursachen. Benutzern in Umgebungen mit einem HTTP-Proxy wird die Offline-Aktivierung empfohlen.

1. Klicken Sie auf der PlateSpin Protect-Weboberfläche auf *Einstellungen* > *Lizenzen* > *Lizenz hinzufügen*. Die Seite „Lizenzaktivierung“ wird angezeigt.

2 Wählen Sie *Online-Aktivierung*, geben Sie die Email-Adresse, die Sie auch bei der Auftragserteilung angegeben haben, sowie den erhaltenen Aktivierungscode an und klicken Sie anschließend auf *Aktivieren*.

   Das System ruft die erforderliche Lizenz über das Internet ab und aktiviert das Produkt.

2.1.3 Offline-Lizenzaktivierung

Für die Offline-Aktivierung erhalten Sie einen Lizenzschlüssel über das Internet, indem Sie einen Computer mit Internetzugang verwenden.

Hinweis: Sie müssen über ein Novell-Konto verfügen, um einen Lizenzschlüssel abrufen zu können. Wenn Sie bereits PlateSpin-Kunde sind und kein Novell-Konto besitzen, müssen Sie zunächst eines erstellen. Verwenden Sie Ihren bestehenden PlateSpin-Benutzernamen (eine gültige bei PlateSpin registrierte Email-Adresse) als Benutzernamen für Ihr Novell-Konto.

---

1 Klicken Sie auf *Einstellungen* > *Lizenz* und dann auf *Lizenz hinzufügen*. Die Seite „Lizenzaktivierung“ wird angezeigt.

2 Wählen Sie *Offline-Aktivierung* aus und kopieren Sie die angezeigte Hardware-ID.

3 Navigieren Sie in einem Webbrowser auf einem Computer mit Internetanschluss zur PlateSpin-Produktaktivierungs-Website (http://www.platespin.com/productactivation/ActivateOrder.aspx). Melden Sie sich mit Ihrem Novell-Benutzernamen an.

4 Füllen Sie die entsprechenden Felder aus:

   - Den erhaltenen Aktivierungscode
   - Die bei der Auftragserteilung angegebene Email-Adresse
   - Die in Schritt 2 kopierte Hardware-ID

5 Klicken Sie auf *Aktivieren*.

   Das System generiert eine Lizenzschlüsseldatei und fordert Sie auf, diese zu speichern.

6 Speichern Sie die generierte Lizenzschlüsseldatei, übertragen Sie sie zum Produkt-Host, der über keine Internet-Konnektivität verfügt, und verwenden Sie sie zur Aktivierung des Produkts.

2.2 Einrichten der Benutzerautorisierung und -authentifizierung

- Abschnitt 2.2.1, „Info über die Benutzerautorisierung und -authentifizierung von PlateSpin Protect“, auf Seite 17
- Abschnitt 2.2.2, „Verwalten von PlateSpin Protect-Zugriff und -Berechtigungen“, auf Seite 18
- Abschnitt 2.2.3, „Verwalten von PlateSpin Protect-Sicherheitsgruppen und -Workload-Berechtigungen“, auf Seite 19

2.2.1 Info über die Benutzerautorisierung und -authentifizierung von PlateSpin Protect

Der Benutzerautorisierungs- und authentifizierungsmechanismus von PlateSpin Protect basiert auf Benutzerrollen und steuert den Anwendungszugriff sowie die Aktionen, die Benutzer ausführen können. Diesem Mechanismus liegen die Integrierte Windows-Authentifizierung (IWA) und deren Interaktion mit den Internetinformationsdiensten (IIS) zugrunde.

Der rollenbasierte Zugriffsmechanismus bietet Ihnen verschiedene Möglichkeiten, die Autorisierung und Authentifizierung von Benutzern zu implementieren:

- Anwendungszugriff auf bestimmte Benutzer beschränken
- Bestimmte Aktionen nur bestimmten Benutzern erlauben
- Jedem Benutzer Zugriff auf bestimmte Workloads gewähren, um die durch die zugewiesene Rolle definierten Aktionen durchzuführen

Jede PlateSpin Protect-Instanz verfügt auf der Betriebssystemebene über folgende Benutzergruppen, die entsprechende funktionale Rollen definieren:

- **Workload-Schutz-Administratoren:** Besitzen unbegrenzten Zugriff auf alle Funktionen der Anwendung. Ein lokaler Administrator ist implizit Teil dieser Gruppe.
- **Workload-Schutz-Hauptbenutzer:** Besitzen Zugriff auf die meisten Funktionen der Anwendung, jedoch mit einigen Einschränkungen, z. B. hinsichtlich des Änderns von Systemeinstellungen für die Lizenzierung und Sicherheit.
- **Workload-Schutz-Operatoren:** Besitzen Zugriff auf einen eingeschränkten Teil der Systemfunktionen, und zwar jene, die für die alltägliche Nutzung ausreichen.

Wenn ein Benutzer versucht, eine Verbindung mit PlateSpin Protect herzustellen, wird der über den Browser angegebene Berechtigungsnachweis vom IIS geprüft. Wenn der Benutzer keiner der Workload-Schutz-Rollen angehört, wird die Verbindung verweigert.

Tabelle 2-1 *Details zu Workload-Schutz-Rollen und -Berechtigungen*

Details zu Workload-Schutz-Rollen	Administratoren	Power-Benutzer	Operatoren
Workload hinzufügen	Zulässig	Zulässig	Verweigert
Workload entfernen	Zulässig	Zulässig	Verweigert
Schutz konfigurieren	Zulässig	Zulässig	Verweigert
Reproduktion vorbereiten	Zulässig	Zulässig	Verweigert
(Voll-)Reproduktion durchführen	Zulässig	Zulässig	Zulässig
Inkrementelle Reproduktion ausführen	Zulässig	Zulässig	Zulässig
Zeitplan unterbrechen/wieder aufnehmen	Zulässig	Zulässig	Zulässig
Failover testen	Zulässig	Zulässig	Zulässig
Failover	Zulässig	Zulässig	Zulässig
Failover abbrechen	Zulässig	Zulässig	Zulässig
Abbrechen	Zulässig	Zulässig	Zulässig
Zurückweisen (Aufgabe)	Zulässig	Zulässig	Zulässig
Einstellungen (Alle)	Zulässig	Verweigert	Verweigert
Berichte/Diagnose ausführen	Zulässig	Zulässig	Zulässig
Failback	Zulässig	Verweigert	Verweigert
Erneut schützen	Zulässig	Zulässig	Verweigert

Darüber hinaus bietet die PlateSpin Protect-Software einen auf *Sicherheitsgruppen* basierenden Mechanismus, der definiert, welche Benutzer auf welche Workloads im Workload-Inventar von PlateSpin Protect zugreifen dürfen.

Das Einrichten eines ordnungsgemäßen rollenbasierten Zugriffs auf PlateSpin Protect umfasst zwei Aufgaben:

1. Hinzufügen von Benutzern zu den erforderlichen Benutzergruppen, zu denen Sie unter Tabelle 2-1 (in Ihrer Windows-Dokumentation) detaillierte Informationen finden können.
2. Erstellen von Sicherheitsgruppen auf Anwendungsebene, die diese Benutzer bestimmten Workloads zuordnen (weitere Informationen finden Sie unter „Verwalten von PlateSpin Protect-Sicherheitsgruppen und -Workload-Berechtigungen“, auf Seite 19).

2.2.2 Verwalten von PlateSpin Protect-Zugriff und -Berechtigungen

- „Hinzufügen von PlateSpin Protect-Benutzern“, auf Seite 19
- „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Protect-Benutzer“, auf Seite 19

Hinzufügen von PlateSpin Protect-Benutzern

Gehen Sie wie in diesem Abschnitt beschrieben vor, um einen neuen PlateSpin Protect-Benutzer hinzuzufügen.

Falls Sie einem auf dem PlateSpin Protect Server-Host vorhandenen Benutzer bestimmte Rollenberechtigungen gewähren möchten, lesen Sie bitte unter „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Protect-Benutzer“, auf Seite 19 weiter.

1. Öffnen Sie auf Ihrem PlateSpin Protect-Server-Host die Systemkonsole „Lokale Benutzer und Gruppen“ (*Start* > *Ausführen* > `lusrmgr.msc` > *Eingabetaste*).
2. Klicken Sie mit der rechten Maustaste auf den Knoten *Benutzer*, wählen Sie *Neuer Benutzer* aus, geben Sie die erforderlichen Details an und klicken Sie auf *Erstellen*.

Jetzt können Sie dem gerade erstellten Benutzer eine Workload-Schutz-Rolle zuweisen. Weitere Informationen hierzu finden Sie unter „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Protect-Benutzer“, auf Seite 19.

Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Protect-Benutzer

Bevor Sie einem Benutzer eine Rolle zuweisen, ermitteln Sie, welche Berechtigungen für diesen Benutzer am Besten geeignet sind. Weitere Informationen hierzu finden Sie unter Tabelle 2-1, „Details zu Workload-Schutz-Rollen und -Berechtigungen“, auf Seite 18.

1. Öffnen Sie auf Ihrem PlateSpin Protect-Server-Host die Systemkonsole „Lokale Benutzer und Gruppen“ (*Start* > *Ausführen* > `lusrmgr.msc` > *Eingabetaste*).
2. Klicken Sie auf den Knoten *Benutzer* und doppelklicken Sie im rechten Fenster auf den erforderlichen Benutzer.
3. Klicken Sie in der Registerkarte *Mitglied von* auf *Hinzufügen*, suchen Sie nach der erforderlichen Workload-Schutz-Gruppe und weisen Sie sie dem Benutzer zu.

   Es kann einige Minuten dauern, bis die Änderung wirksam wird. Wenn Sie versuchen möchten, die Änderungen manuell anzuwenden, starten Sie Ihren Server neu. Weitere Informationen hierzu finden Sie unter „Neustart des PlateSpin Protect-Servers, um Systemänderungen anzuwenden“, auf Seite 31.

Jetzt können Sie diesen Benutzer einer PlateSpin Protect-Sicherheitsgruppe hinzufügen und ihm eine angegebene Sammlung von Workloads zuweisen. Weitere Informationen hierzu finden Sie unter „Verwalten von PlateSpin Protect-Sicherheitsgruppen und -Workload-Berechtigungen“, auf Seite 19.

2.2.3 Verwalten von PlateSpin Protect-Sicherheitsgruppen und -Workload-Berechtigungen

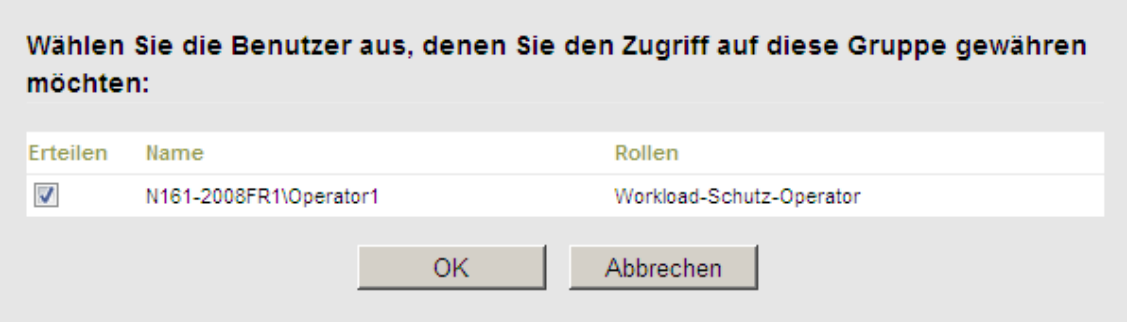
PlateSpin Protect bietet auf der Anwendungsebene einen genauer definierten Zugriffsmechanismus, der es bestimmten Benutzern erlaubt, bestimmte Workload-Schutz-Aufgaben für angegebene Workloads durchzuführen. Dies wird durch die Einrichtung von *Sicherheitsgruppen* erreicht.

1. Weisen Sie einem PlateSpin Protect-Benutzer die Workload-Schutz-Rolle zu, deren Berechtigungen am besten für die Rolle dieses Benutzers in Ihrer Organisation geeignet sind. Weitere Informationen hierzu finden Sie unter „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Protect-Benutzer“, auf Seite 19.
2. Greifen Sie als Administrator auf der PlateSpin Protect-Weboberfläche auf PlateSpin Protect zu und klicken Sie anschließend auf *Einstellungen* > *Berechtigungen*.

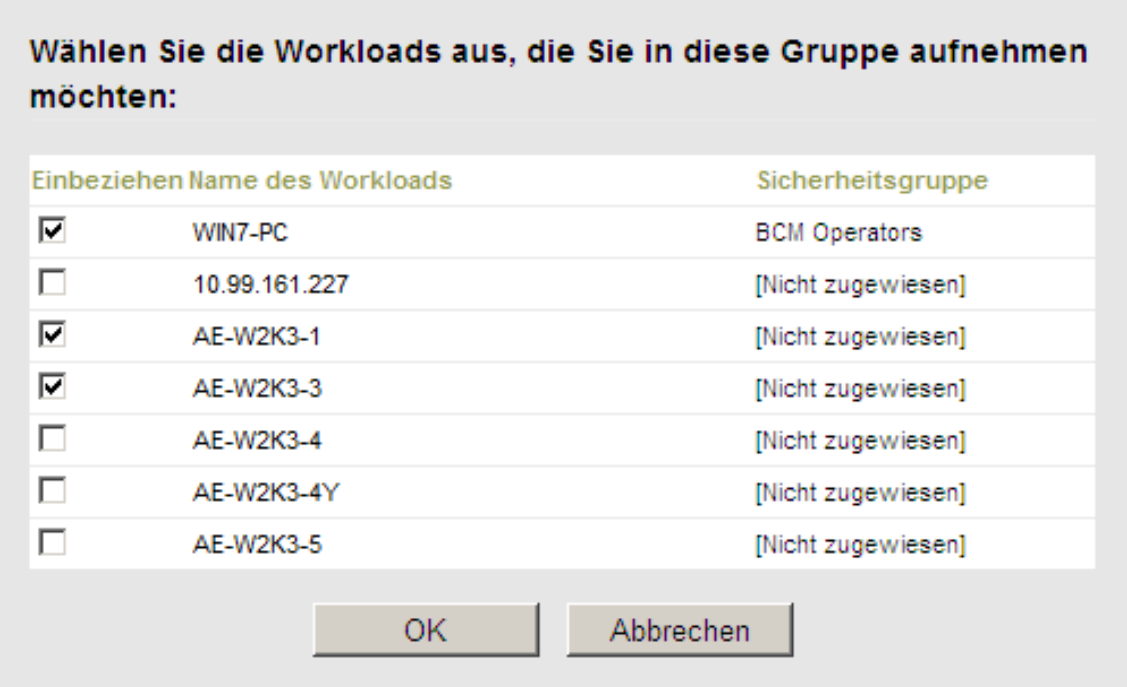
Die Seite „Sicherheitsgruppen“ wird angezeigt:

3. Klicken Sie auf *Sicherheitsgruppe erstellen*.
4. Geben Sie im Feld *Name der Sicherheitsgruppe* einen Namen für Ihre Sicherheitsgruppe ein.
5. Klicken Sie auf *Benutzer hinzufügen* und wählen Sie die erforderlichen Benutzer für diese Sicherheitsgruppe aus.

   Wenn Sie einen PlateSpin Protect-Benutzer hinzufügen möchten, der kürzlich zum PlateSpin Protect-Server-Host hinzugefügt wurde, wird er möglicherweise nicht sofort auf der Benutzeroberfläche angezeigt. Klicken Sie in diesem Fall auf *Benutzerkonten aktualisieren*.



6. Klicken Sie auf *Workload hinzufügen* und wählen Sie die erforderlichen Workloads aus:



   Nur die Benutzer in dieser Sicherheitsgruppe haben Zugriff auf die ausgewählten Workloads.

7. Klicken Sie auf *Erstellen*.

   Die Seite wird neu geladen und zeigt Ihre neue Gruppe in der Liste der Sicherheitsgruppen an.

Wenn Sie eine Sicherheitsgruppe bearbeiten möchten, klicken Sie in der Liste der Sicherheitsgruppen auf ihren Namen.

2.3 Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk

2.3.1 Zugriffs- und Kommunikationsanforderungen für Workloads

Im folgenden Abschnitt werden die Software-, Netzwerk- und Firewall-Anforderungen für Workloads beschrieben, die mithilfe von PlateSpin Protect geschützt werden sollen.

Tabelle 2-2 *Zugriffs- und Kommunikationsanforderungen für Workloads*

Workload-Typ	Voraussetzungen	Erforderliche Ports
Alle Workloads	Ping-Funktion (ICMP-Echoanfrage und -antwort).	
Alle Windows-Workloads	Microsoft .NET Framework Version 2.0 oder 3.5 SP1	

Workload-Typ	Voraussetzungen	Erforderliche Ports
Windows 7; Windows Server 2008; Windows Vista	◆ Integrierter `Administrator`- oder Domänen-Administrator-Kontoberechtigungsnachweis (die Mitgliedschaft in der lokalen Administratorgruppe reicht nicht aus). Unter Vista muss das Konto aktiviert sein (es ist standardmäßig deaktiviert). ◆ Die Windows-Firewall, die so konfiguriert ist, dass sie die *Datei- und Druckerfreigabe* zulässt. Verwenden Sie eine der folgenden Optionen: ◆ **Option 1 mit der Windows-Firewall:** Verwenden Sie das grundlegende Systemsteuerungselement *Windows-Firewall* (`firewell.cpl`) und wählen Sie in der Liste der Ausnahmen die Option *Datei- und Druckerfreigabe* aus. - ODER - ◆ **Option 2 mit der Firewall mit erweiterter Sicherheit:** Verwenden Sie das Dienstprogramm *Windows-Firewall mit erweiterter Sicherheit* (`wf.msc`), bei dem die folgenden *Eingangsregeln* aktiviert und auf `Zulassen` festgelegt sind: ◆ *Datei- und Druckerfreigabe (Echoanforderung - ICMPv4In)* ◆ *Datei- und Druckerfreigabe (Echoanforderung - ICMPv6In)* ◆ *Datei- und Druckerfreigabe (NB-Datagramm eingehend)* ◆ *Datei- und Druckerfreigabe (NB-Name eingehend)* ◆ *Datei- und Druckerfreigabe (NB-Sitzung eingehend)* ◆ *Datei- und Druckerfreigabe (SMB eingehend)* ◆ *Datei- und Druckerfreigabe (Spoolerdienst - RPC)* ◆ *Datei- und Druckerfreigabe (Spoolerdienst - RPC-EPMAP)*	TCP 3725 NetBIOS 137 - 139 SMB (TCP 139, 445 und UDP 137, 138) TCP 135/ 445
Windows Server 2000; Windows XP	◆ Installierte Windows Management Instrumentation (WMI) WMI (RPC/DCOM) kann die TCP-Ports 135 und 445 sowie zufällig oder dynamisch zugewiesene Ports oberhalb von 1024 verwenden. Wenn beim Hinzufügen des Workloads Probleme auftreten, erwägen Sie, den Workload vorübergehend in ein DMZ zu stellen oder die durch die Firewall geschützten Ports vorübergehend zu öffnen, während Sie den Workload zu PlateSpin Protect hinzufügen. Weitere Informationen, z. B. eine Anleitung für das Beschränken des Portbereichs für DCOM und RPC, finden Sie in den folgenden technischen Artikeln von Microsoft. ◆ Verwenden von DCOM mit Firewalls (http://msdn.microsoft.com/en-us/library/ms809327.aspx) ◆ Konfigurieren der dynamischen RPC-Port-Zuordnung für die Verwendung mit Firewalls (http://support.microsoft.com/default.aspx?scid=kb;en-us;154596) ◆ Konfigurieren von DCOM für die Verwendung mit einer NAT-basierten Firewall (http://support.microsoft.com/kb/248809)	TCP 3725 NetBIOS 137 - 139 SMB (TCP 139, 445 und UDP 137, 138) TCP 135/ 445
Alle Linux-Workloads	Secure Shell (SSH)-Server	TCP 22, 3725

2.3.2 Zugriffs- und Kommunikationsanforderungen für Container

Die folgenden Software-, Netzwerk- und Firewall-Anforderungen gelten für die unterstützten Workload-Container.

Tabelle 2-3 *Zugriffs- und Kommunikationsanforderungen für Container*

System	Voraussetzungen	Erforderliche Ports
Alle Container	Ping-Funktion (ICMP-Echoanfrage und -antwort).	
VMware ESX/ESXi 4.1 VMware ESXi 5.0 vCenter Server	◆ VMware-Konto mit Administratorrolle ◆ VMware Web-Services-API und Dateiverwaltungs-API	HTTPS TCP 443

2.3.3 Anforderungen für geöffnete Ports für PlateSpin Protect-Server-Hosts

Die folgenden Anforderungen gelten für geöffnete Ports für PlateSpin Protect-Server-Hosts.

Tabelle 2-4 *Anforderungen für geöffnete Ports für PlateSpin Protect-Server-Hosts*

Anschluss	Anmerkungen
TCP 80	Für HTTP-Kommunikation
TCP 443	Für die HTTPS-Kommunikation (wenn SSL aktiviert ist)

2.3.4 Schutz über öffentliche und private Netzwerke durch NAT

In einigen Fällen kann sich ein Ursprung, ein Ziel oder PlateSpin Protect selbst in einem internen (privaten) Netzwerk hinter einem NAT-Gerät (Network Address Translator) befinden, wodurch eine Kommunikation mit dem Gegenstück während des Schutzes nicht möglich ist.

PlateSpin Protect ermöglicht Ihnen, dieses Problem zu umgehen, je nachdem, welcher der folgenden Hosts sich hinter dem NAT-Gerät befindet:

- **PlateSpin Protect-Server:** Fügen Sie die diesem Host zugewiesenen zusätzlichen IP-Adressen zur Konfigurationsdatei `web.config` Ihres Servers hinzu. Weitere Informationen hierzu finden Sie in „Konfigurieren der Anwendung zum Funktionieren im gesamten NAT“, auf Seite 26.
- **Ziel-Container:** Wenn Sie versuchen, einen Container zu ermitteln, z. B. VMware ESX, geben Sie die öffentlichen (oder externen) IP-Adressen dieses Hosts in den Parametern für die Ermittlung an.
- **Workload:** Geben Sie bei dem Versuch, einen Workload hinzuzufügen, die öffentliche (interne) IP-Adresse dieses Workloads in den Ermittlungsparametern an.
- **Failover-VM:** Bei einem Failback können Sie eine alternative IP-Adresse für den Failover-Workload in Failback-Details (Workload an VM) (Seite 57) angeben.

- **Failback-Ziel:** Wenn Sie bei dem Versuch, ein Failback-Ziel zu registrieren, dazu aufgefordert werden, die IP-Adresse des PlateSpin-Servers anzugeben, müssen Sie entweder die lokale Adresse des Protect-Server-Hosts angeben oder eine seiner öffentlichen (externen) Adressen, die in der Konfigurationsdatei `web.config` des Servers aufgezeichnet wurde (weitere Informationen hierzu finden Sie oben unter "PlateSpin Protect-Server").

2.3.5 Optimieren des Datentransfers über WAN-Verbindungen

Sie können die Datentransferleistung optimieren und sie für WAN-Verbindungen fein abstimmen. Dazu können Sie die Konfigurationsparameter ändern, die das System von den `*.config`-Dateien auf Ihrem PlateSpin Protect-Server-Host liest. Weitere Informationen zu dem generischen Vorgang finden Sie unter „Konfigurieren des Produktverhaltens mithilfe von XML-Konfigurationsparametern“, auf Seite 30.

Verwenden Sie diese Einstellungen zur Optimierung der Datentransfers über ein WAN. Diese globalen Einstellungen gelten für alle dateibasierten und VSS-Reproduktionen.

- **Konfigurationsdatei:** `productinternal.config`
- **Standort:** `\Programme\PlateSpin Protect Server\Web`

Hinweis: Wenn diese Werte geändert werden, können die Reproduktionszeiten in Hochgeschwindigkeits-Netzwerken wie Gigabit Ethernet möglicherweise negativ beeinflusst werden. Wenden Sie sich lieber zuerst an den PlateSpin-Support bevor Sie diese Parameter ändern.

In Tabelle 2-5 sind die Konfigurationsparameter in zwei Gruppen aufgeführt: die Standardwerte und die Werte, die für den optimalen Betrieb in einer WAN-Umgebung mit hoher Latenz empfohlen werden.

Tabelle 2-5 *Standard- und optimale Konfigurationsparameter in* `productinternal.config`

Parameter	Standardwert	Optimaler Wert
`fileTransferThreadcount` Steuert die Anzahl der TCP-Verbindungen, die für den dateibasierten Datentransfer geöffnet werden.	2	4 bis 6
`fileTransferMinCompressionLimit` Gibt den Schwellwert für die Komprimierung auf Paketebene in Byte an.	0 (deaktiviert)	Max. 65536 (64 KB)
`fileTransferCompressionThreadsCount` Steuert die Anzahl der Threads, die für die Datenkomprimierung auf Paketebene verwendet werden. Wird ignoriert, wenn die Komprimierung deaktiviert ist. Da die Komprimierung CPU-abhängig ist, kann sich diese Einstellung auf die Arbeitsgeschwindigkeit auswirken.	2	nicht zutreffend

Parameter	Standardwert	Optimaler Wert

`fileTransferSendReceiveBufferSize`
 	
Einstellung der TCP/IP-Fenstergröße für Dateiübertragungsverbindungen. Sie steuert die Anzahl der Byte, die ohne TCP-Acknowledgement gesendet werden. Angabe in Byte.
 	
Wenn der Wert auf 0 gesetzt wird, wird die Standard-TCP-Fenstergröße (8 KB) verwendet. Geben Sie bei benutzerdefinierten Größen die Größe in Byte an. Verwenden Sie folgende Formel, um den geeigneten Wert zu ermitteln:
 	
((Verbindungsgeschwindigkeit(MB/s)/ 8)*Verzögerung(Sek.))*1000*1000
 	
Beispielsweise wäre die geeignete Puffergröße bei einer 100-Mb/s-Verbindung mit 10 ms Latenz wie folgt:
 	
`(100/8)*0,01 * 1000 * 1000 = 125000 Byte`
	0 (8192 Byte)	Max. 5242880 (5 MB)

2.3.6 Aktivieren der SSL-Kommunikation mit dem PlateSpin-Server

Verwenden Sie diese Einstellungen, um die Kommunikation zwischen Ihrem Webbrowser und dem PlateSpin-Server, auf dem Sie SSL aktiviert haben, *nach* der Installation des Produkts zu aktivieren. Wenn SSL zum Zeitpunkt der Produktinstallation auf dem Server-Host aktiviert war, ist dies nicht erforderlich.

Weitere Informationen zum Aktualisierungsvorgang finden Sie unter „Konfigurieren des Produktverhaltens mithilfe von XML-Konfigurationsparametern“, auf Seite 30.

- **Konfigurationsdatei:** `Platespin.Config`
- **Standort:** `\Programme\PlateSpin Protect Server\Configs`
- **Wert:** Änderung

  ```
  <add key="PowerConvertURL" value="http://localhost:80/PlateSpinMigrate" />
  ```

  in

  ```
  <add key="PowerConvertURL" value="https://localhost:443/PlateSpinMigrate" />
  ```

2.3.7 Anforderungen für VMware DRS-Cluster als Container

Um ein gültiges Schutzziel sein zu können, muss Ihr VMware DRS-Cluster dem Satz der (inventarisierten) Container als VMware-Cluster hinzugefügt werden. Sie sollten nicht versuchen, einen DRS-Cluster als einen Satz von individuellen ESX-Servern hinzuzufügen. Weitere Informationen hierzu finden Sie unter „Hinzufügen von Containern“, auf Seite 44.

Außerdem muss Ihr VMware-Cluster die folgenden Konfigurationsanforderungen erfüllen:

- DRS ist aktiviert und auf `Teilweise automatisiert` oder auf `Vollautomatisch` gesetzt sein.
- Mindestens eine Datenablage muss für alle ESX-Server im VMware-Cluster freigegeben sein.

- Mindestens ein vSwitch und eine virtuelle Portgruppe bzw. ein dezentraler vNetwork-Schalter ist für alle ESX-Server im VMware-Cluster gleich.
- Die Failover-Workloads (VMs) für jeden Schutzvertrag werden ausschließlich in Datenablagen, vSwitches und virtuellen Portgruppen platziert, die über alle ESX-Server im VMware-Cluster gemeinsam genutzt werden.

2.3.8 Konfigurieren der Anwendung zum Funktionieren im gesamten NAT

Damit der PlateSpin Protect-Server in allen NAT-aktivierten Umgebungen funktioniert, müssen Sie zusätzliche IP-Adressen Ihres PlateSpin Protect-Servers in einer Konfigurationsdatei aufzeichnen, die der Server beim Starten liest.

Weitere Informationen zum Aktualisierungsvorgang finden Sie unter „Konfigurieren des Produktverhaltens mithilfe von XML-Konfigurationsparametern“, auf Seite 30.

- **Konfigurationsdatei:** `Web.config`
- **Standort:** `\Programme\PlateSpin Protect Server\Web`
- **Values:** `<add key="AlternateServerAddresses" value="" />`

  Fügen Sie die zusätzlichen IP-Adressen getrennt durch Semicolons (;) hinzu, z. B.:

  ```
  <add key="AlternateServerAddresses" value="10.99.106.108;10.99.106.109" />
  ```

2.4 Konfigurieren von PlateSpin Protect-Standardoptionen

2.4.1 Einrichten automatischer Email-Benachrichtigungen zu Ereignissen und Berichten

Sie können PlateSpin Protect so konfigurieren, dass es automatisch Benachrichtigungen zu Ereignissen und Reproduktionsberichte an angegebene Email-Adressen sendet. Für diese Funktion ist es erforderlich, dass Sie zuerst einen gültigen SMTP-Server für PlateSpin Protect angeben.

SMTP-Konfiguration

Konfigurieren Sie auf der PlateSpin Protect-Weboberfläche die SMTP-Einstellungen für den Server, der zum Zustellen von Email-Benachrichtigungen zu Ereignissen und Reproduktionsberichten verwendet wird.

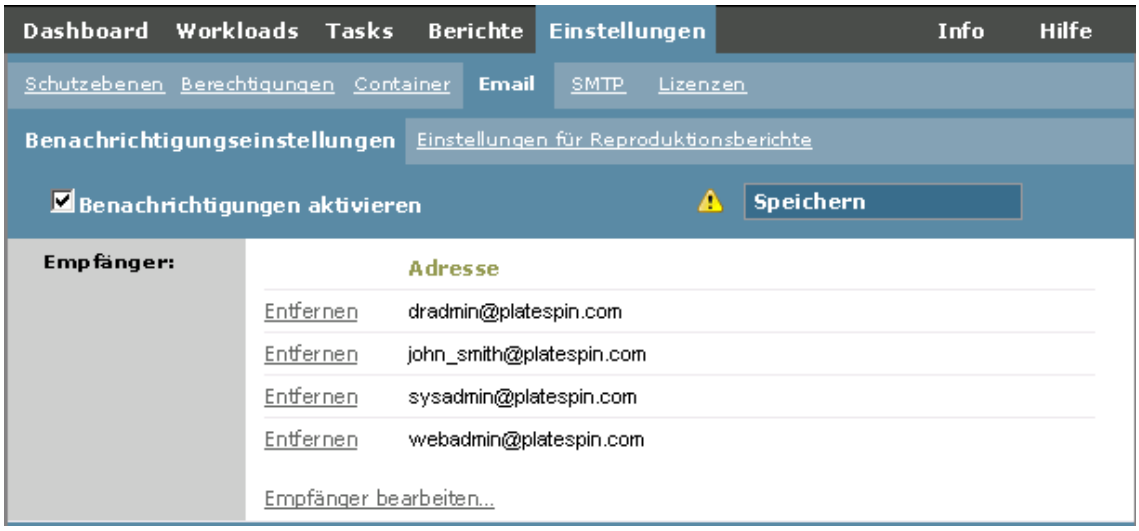
Abbildung 2-1 *SMTP-Einstellungen (Simple Mail Transfer Protocol)*

So konfigurieren Sie die SMTP-Einstellungen:

1. Klicken Sie auf Ihrer PlateSpin Protect-Weboberfläche auf *Einstellungen* > *SMTP*.
2. Geben Sie die *Adresse* und den *Port* (Standardport ist 25) Ihres SMTP-Servers sowie eine *Antwortadresse* für den Empfang von Email-Benachrichtigungen zu Ereignissen und zum Fortschritt an.
3. Geben Sie den *Benutzernamen* und das *Passwort* ein. Bestätigen Sie anschließend das Passwort.
4. Klicken Sie auf *Speichern*.

Einrichten automatischer Ereignisbenachrichtigungen per Email

1. Richten Sie einen SMTP-Server für PlateSpin Protect ein. Weitere Informationen hierzu finden Sie in „SMTP-Konfiguration“, auf Seite 26.
2. Klicken Sie auf Ihrer PlateSpin Protect-Weboberfläche auf *Einstellungen* > *Email* > *Benachrichtigungseinstellungen*.
3. Wählen Sie die Option *Benachrichtigungen aktivieren*.
4. Klicken Sie auf *Empfänger bearbeiten*, geben Sie die erforderlichen Email-Adressen getrennt durch Kommas ein und klicken Sie anschließend auf *OK*.



5. Klicken Sie auf *Speichern*.

   Klicken Sie zum Löschen aufgelisteter Email-Adressen auf *Löschen* neben den zu entfernenden Adressen.

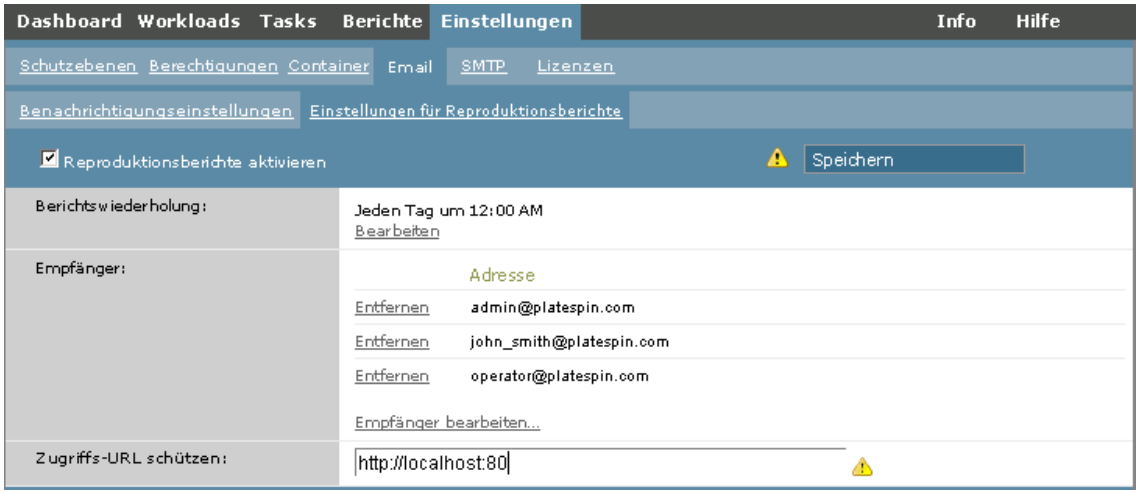
Folgende Ereignisse lösen E-Mail-Benachrichtigungen aus:

Ereignis	Anmerkungen
`Workload online erkannt`	Wird generiert, wenn das System erkennt, dass ein Workload, der zuvor offline war, nun online ist. Betrifft Workloads, deren Schutzzeitplan-Status nicht *Unterbrochen* lautet.
`Workload offline erkannt`	Wird generiert, wenn das System erkennt, dass ein Workload, der zuvor online war, nun offline ist. Betrifft Workloads, deren Schutzzeitplan-Status nicht *Unterbrochen* lautet.
`Fehler bei der inkrementellen Reproduktion`	
`Fehler bei der Vollreproduktion`	
`Failover-Test abgeschlossen`	Wird generiert, wenn ein Failover-Test-Vorgang manuell als ordnungsgemäß durchgeführt oder als Fehler gekennzeichnet wird.
`Failover abgeschlossen`	
`Failover-Vorbereitung abgeschlossen`	
`Failover-Vorbereitung fehlgeschlagen`	
`Failover-Fehler`	
`Inkrementelle Reproduktion verpasst`	Wird generiert, wenn Folgendes zutrifft: ◆ Eine Reproduktion wird manuell angehalten, wenn eine geplante inkrementelle Reproduktion fällig ist. ◆ Das System versucht, eine geplante inkrementelle Reproduktion auszuführen, während gerade eine manuell ausgelöste Reproduktion stattfindet. ◆ Das System stellt fest, dass das Ziel nicht über genügend freien Speicherplatz verfügt.
`Vollreproduktion verpasst`	Ähnlich dem Ereignis `Inkrementelle Reproduktion verpasst` weiter oben.

Einrichten automatischer Reproduktionsberichte per Email

Führen Sie folgende Schritte aus, um PlateSpin Protect so einzurichten, dass es automatisch Reproduktionsberichte per Email sendet:

1. Richten Sie einen SMTP-Server für PlateSpin Protect ein. Weitere Informationen hierzu finden Sie in SMTP-Konfiguration (Seite 26).
2. Klicken Sie auf Ihrer PlateSpin Protect-Weboberfläche auf *Einstellungen* > *Email* > *Einstellungen für Reproduktionsberichte*.
3. Wählen Sie die Option *Reproduktionsberichte aktivieren*.
4. Klicken Sie im Abschnitt *Berichtswiederholung* auf *Konfigurieren* und geben Sie das erforderliche Wiederholungsmuster für die Berichte an.
5. Klicken Sie im Abschnitt *Empfänger* auf *Empfänger bearbeiten*, geben Sie die erforderlichen Email-Adressen getrennt durch Kommas ein und klicken Sie anschließend auf *OK*.



6. (Optional) Geben Sie im Abschnitt *Protect-Zugriff-URL* eine nicht standardmäßige URL für Ihren PlateSpin Protect-Server ein (z. B. wenn Ihr PlateSpin Protect-Server-Host mehrere Netzwerkkarten hat oder sich hinter einem NAT-Server befindet). Diese URL hat Einfluss auf den Titel des Berichts und auf die Funktionalität für den Zugriff auf relevante Inhalte auf dem Server über Hyperlinks in Email-Berichten.
7. Klicken Sie auf *Speichern*.

Informationen zu anderen Arten von Berichten, die Sie jederzeit generieren können, finden Sie unter „Generieren von Workload- und Workload-Schutz-Berichten“, auf Seite 41.

2.4.2 Einrichtung der Sprache bei internationalen Versionen von PlateSpin Protect

PlateSpin Protect bietet Unterstützung von Landessprachen (NLS, National Language Support) für Chinesisch (vereinfacht), Chinesisch (traditionell), Französisch, Deutsch und Japanisch.

Zur Verwendung der PlateSpin Protect-Weboberfläche und der integrierten Hilfe in einer dieser Sprachen muss die entsprechende Sprache in Ihrem Webbrowser hinzugefügt und an die erste Position der Rangfolge gesetzt werden:

1. Rufen Sie in Ihrem Webbrowser die Spracheinstellung auf:
   - **Internet Explorer:** Klicken Sie auf *Extras* > *Internetoptionen* > *Registerkarte „Allgemein“* > *Sprachen*.
   - **Firefox:** Klicken Sie auf *Extras* > *Einstellungen* > *Registerkarte „Inhalt“* > *Sprachen*.
2. Fügen Sie die gewünschte Sprache hinzu und setzen Sie sie an die oberste Position in der Liste.
3. Speichern Sie die Einstellungen und starten Sie anschließend die Client-Anwendung, indem Sie eine Verbindung zu Ihrem PlateSpin Protect-Server herstellen. Weitere Informationen hierzu finden Sie in „Starten der PlateSpin Protect-Weboberfläche“, auf Seite 33.

Hinweis: (Für Benutzer der Chinesisch-Versionen) Der Versuch, über einen Browser ohne spezifische Chinesisch-Version eine Verbindung zum PlateSpin Protect Server herzustellen, kann zu Webserver-Fehlern führen. Verwenden Sie für den ordnungsgemäßen Betrieb die Konfigurationseinstellungen des Browsers, um eine spezifische chinesische Spracheinstellung hinzuzufügen (`Chinesisch [zh-cn]` oder `Chinesisch [zh-tw]`). Verwenden Sie die kulturneutrale Spracheinstellung `Chinesisch [zh]` nicht.

Die Sprache eines geringen Anteils der vom PlateSpin Protect-Server generierten Systemmeldungen hängt von der Oberflächensprache des Betriebssystems ab, die auf Ihrem PlateSpin Protect Server-Host ausgewählt ist:

1. Rufen Sie Ihren PlateSpin Protect Server-Host auf.
2. Starten Sie das Applet für die Regions- und Sprachoptionen (klicken Sie auf *Start* > *Ausführen*, geben Sie `intl.cpl` ein und drücken Sie die Eingabetaste) und klicken Sie anschließend auf die Registerkarte *Sprachen* (Windows Server 2003) bzw. *Tastaturen und Sprachen* (Windows Server 2008).
3. Installieren Sie das erforderliche Sprachpaket, sofern es noch nicht installiert ist. Möglicherweise benötigen Sie Zugriff auf die Installationsmedien Ihres Betriebssystems.
4. Wählen Sie die erforderliche Sprache als Oberflächensprache des Betriebssystems aus. Wenn eine entsprechende Aufforderung angezeigt wird, melden Sie sich ab oder starten Sie das System neu.

2.4.3 Konfigurieren des Produktverhaltens mithilfe von XML-Konfigurationsparametern

Einige Aspekte des Verhaltens des PlateSpin Protect-Servers werden von Konfigurationsparametern gesteuert, die aus `.config`-Dateien auf Ihrem PlateSpin Protect-Server-Host gelesen werden.

Normalerweise brauchen Sie diese Einstellungen nicht zu ändern, es sei denn, der PlateSpin-Support rät Ihnen dazu. In diesem Abschnitt werden einige häufig vorkommende Fälle zusammen mit Informationen zur erforderlichen Prozedur aufgeführt.

Gehen Sie wie folgt vor, um `*.config`-Parameter zu ändern oder anzuwenden:

1. Wechseln Sie auf Ihrem PlateSpin Protect Server-Host in das Basisverzeichnis.
2. Öffnen Sie die `*.config`-Datei in einem Texteditor.
3. Wählen Sie den entsprechenden Parameter in der `.config`-Datei aus und ändern Sie dessen Wert. Der Wert ist in Anführungszeichen (" ") gesetzt. Löschen Sie nicht die Anführungszeichen. Verwenden Sie vertretbare Werte, wie in diesem Abschnitt angegeben, bzw. die Werte, die vom PlateSpin-Support angegeben werden.
4. Speichern und schließen Sie die `*.config`-Datei.
5. Starten Sie den PlateSpin Protect-Server neu. Weitere Informationen hierzu finden Sie in „Neustart des PlateSpin Protect-Servers, um Systemänderungen anzuwenden“, auf Seite 31.

Neustart des PlateSpin Protect-Servers, um Systemänderungen anzuwenden

1. Navigieren Sie zum PlateSpin Protect-Server-Unterverzeichnis `bin\RestartPlateSpinServer`.
2. Doppelklicken Sie auf die Programmdatei `RestartPlateSpinServer.exe`.

   Es wird ein Befehlszeilenfenster geöffnet, in dem Sie aufgefordert werden, den Vorgang zu bestätigen.
3. Geben Sie `Y` ein und drücken Sie die `Eingabetaste`.

3 Aufgestellt und in Betrieb

In diesem Kapitel werden die wichtigsten Funktionen von PlateSpin Protect und seiner Schnittstelle beschrieben.

3.1 Starten der PlateSpin Protect-Weboberfläche

Die meisten Aktionen mit PlateSpin Protect führen Sie auf der browserbasierten PlateSpin Protect-Weboberfläche aus.

Die folgenden Browser werden unterstützt:

- Microsoft Internet Explorer 7 und höher
- Mozilla Firefox (unter Windows) 3.6 und höher

JavaScript (Active Scripting) muss in Ihrem Browser aktiviert sein:

- **Internet Explorer:** Klicken Sie auf *Extras* > *Internetoptionen* > *Sicherheit* > *Zone „Internet“* > *Stufe anpassen* und wählen Sie anschließend die Option *Aktivieren* für die Active Scripting-Funktion aus.
- **Firefox:** Klicken Sie auf *Extras* > *Einstellungen* > *Inhalt* und wählen Sie anschließend die Option *JavaScript aktivieren* aus.

Informationen zur Verwendung der PlateSpin Protect-Weboberfläche und der integrierten Hilfe in einer der unterstützten Sprachen finden Sie unter Abschnitt 2.4.2, „Einrichtung der Sprache bei internationalen Versionen von PlateSpin Protect“, auf Seite 30.

So starten Sie die PlateSpin Protect-Weboberfläche:

1. Öffnen Sie einen Webbrowser und wechseln Sie zu folgender Adresse:

   `http://`<*Hostname* | *IP-Adresse*>`/Protect`

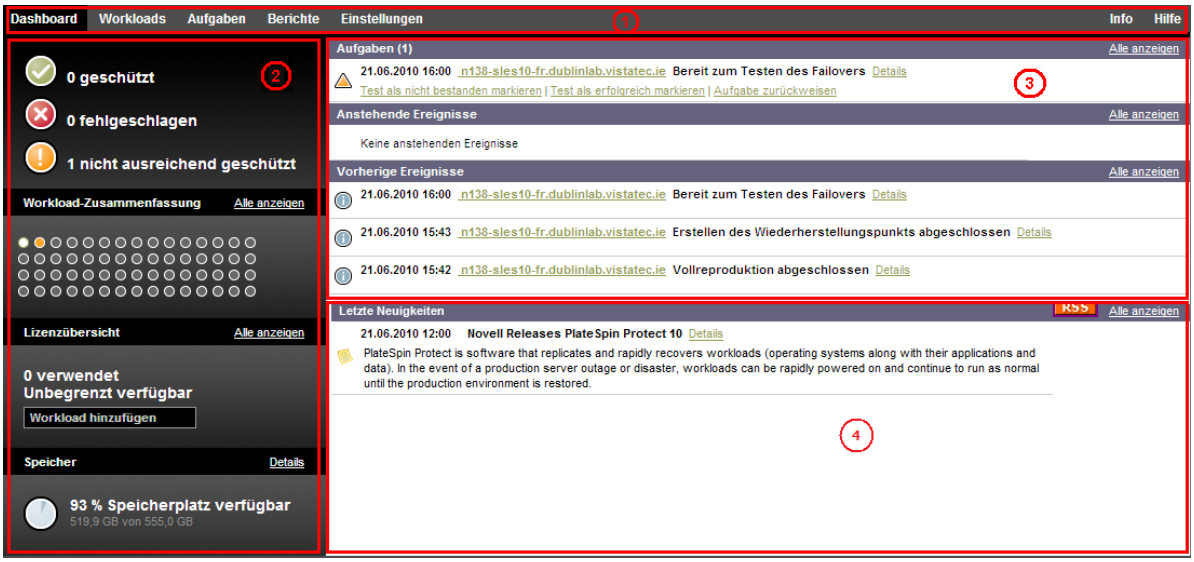
   Ersetzen Sie <*Hostname* | *IP-Adresse*> durch den Hostnamen oder die IP-Adresse Ihres PlateSpin Protect Server-Hosts.

   Wenn SSL aktiviert ist, verwenden Sie `https` in der URL.

3.2 Elemente der PlateSpin Protect-Weboberfläche

Die Standardoberfläche der PlateSpin Protect-Weboberfläche ist die Seite „Dashboard“, die Elemente zum Navigieren zu verschiedenen Funktionsbereichen der Oberfläche und zum Durchführen von Workload-Schutz- und Wiederherstellungsaufgaben bereitstellt.

Abbildung 3-1 *Die Standard-Dashboard-Seite der PlateSpin Protect-Weboberfläche*



Die Dashboard-Seite besteht aus den folgenden Elementen:

1. **Navigationsleiste:** Auf den meisten Seiten der PlateSpin Protect-Weboberfläche enthalten.
2. **Teilfenster mit visueller Zusammenfassung:** Bietet einen umfassenden Überblick über den Gesamtstatus des Workload-Inventars von PlateSpin Protect.
3. **Teilfenster mit Aufgaben und Ereignissen:** Bietet Informationen über Ereignisse und Aufgaben, die einen Eingriff des Benutzers erfordern.
4. **Teilfenster „Letzte Neuigkeiten“:** Bietet mittels RSS Informationen zum Produkt und zu zugehörigen Aktualisierungen. Wenn Sie den RSS-Feed zu PlateSpin Protect abonnieren möchten, klicken Sie auf *RSS*.

Die folgenden Abschnitte enthalten weitere Informationen.

- Abschnitt 3.2.1, „Navigationsleiste“, auf Seite 35
- Abschnitt 3.2.2, „Teilfenster mit visueller Zusammenfassung“, auf Seite 35
- Abschnitt 3.2.3, „Teilfenster mit Aufgaben und Ereignissen“, auf Seite 36

3.2.1 Navigationsleiste

Die Navigationsleiste enthält folgende Links:

- **Dashboard:** Zeigt die Standardseite „Dashboard“ an.
- **Workloads:** Zeigt die Seite „Workloads“ an. Weitere Informationen hierzu finden Sie unter „Workloads und Workload-Befehle“, auf Seite 36.
- **Aufgaben:** Zeigt die Seite „Aufgaben“ mit den Elementen an, die einen Benutzereingriff erfordern.
- **Berichte:** Zeigt die Seite „Berichte“ an. Weitere Informationen hierzu finden Sie unter „Generieren von Workload- und Workload-Schutz-Berichten“, auf Seite 41.
- **Einstellungen:** Zeigt die Seite „Einstellungen“ an, die Zugriff auf die folgenden Konfigurationsoptionen bietet:
  - **Schutzebenen:** Weitere Informationen hierzu finden Sie unter „Schutzebenen“, auf Seite 63.
  - **Berechtigungen:** Weitere Informationen hierzu finden Sie in „Einrichten der Benutzerautorisierung und -authentifizierung“, auf Seite 16.
  - **Container:** Weitere Informationen hierzu finden Sie unter „Hinzufügen von Containern“, auf Seite 44.
  - **Email/SMTP:** Weitere Informationen hierzu finden Sie in „Einrichten automatischer Email-Benachrichtigungen zu Ereignissen und Berichten“, auf Seite 26.
  - **Lizenzen/Lizenzbezeichnungen:** Weitere Informationen hierzu finden Sie in „Produktlizenzierung“, auf Seite 15.

3.2.2 Teilfenster mit visueller Zusammenfassung

Im Fenster „Visuelle Zusammenfassung“ werden effizient alle lizenzierten Workloads sowie die Menge an verfügbarem Speicher angezeigt.

Inventarisierte Workloads werden in drei Kategorien dargestellt:

- **Geschützt:** Gibt die Anzahl der aktiv geschützten Workloads an.
- **Fehlgeschlagen:** Gibt die Anzahl der geschützten Workloads an, die das System gemäß der Schutzebene dieses Workloads als fehlgeschlagen ausgegeben hat.
- **Nicht ausreichend geschützt:** Gibt die Anzahl der geschützten Workloads an, die einen Eingriff des Benutzers erfordern.

Der Bereich in der Mitte des linken Teilfensters stellt eine grafische Zusammenfassung der Seite „Workloads“ dar. Er verwendet Punktsymbole, um die verschiedenen Statusformen der Workloads anzuzeigen:

Tabelle 3-1 *Punktsymbol-Darstellung des Workload-Status*

● Ungeschützt	● *Nicht ausreichend geschützt*
○ *Ungeschützt – Fehler*	● *Fehlgeschlagen*
● *Geschützt*	● *Abgelaufen*
● *Nicht verwendet*	

Die Symbole werden in alphabetischer Reihenfolge gemäß dem Workload-Namen angezeigt. Richten Sie den Mauszeiger auf ein Punktsymbol, um den Namen des Workloads anzuzeigen, oder klicken Sie darauf, um die zugehörige Seite mit den Workload-Details zu öffnen.

Speicher bietet Informationen über den für PlateSpin Protect verfügbaren Container-Speicherplatz.

3.2.3 Teilfenster mit Aufgaben und Ereignissen

Das Teilfenster mit den Aufgaben und Ereignissen zeigt die letzten Aufgaben und vorherigen Ereignisse sowie die nächsten anstehenden Ereignisse an.

Ereignisse werden protokolliert, wenn sie für das System oder den Workload relevant sind. Ereignisse sind beispielsweise das Hinzufügen eines neuen geschützten Workloads, das Starten oder Fehlschlagen der Reproduktion eines Workloads oder die Erkennung eines Fehlers eines geschützten Workloads. Einige Ereignisse generieren automatische Email-Benachrichtigungen, wenn SMTP konfiguriert ist. Weitere Informationen hierzu finden Sie in „Einrichten automatischer Email-Benachrichtigungen zu Ereignissen und Berichten“, auf Seite 26.

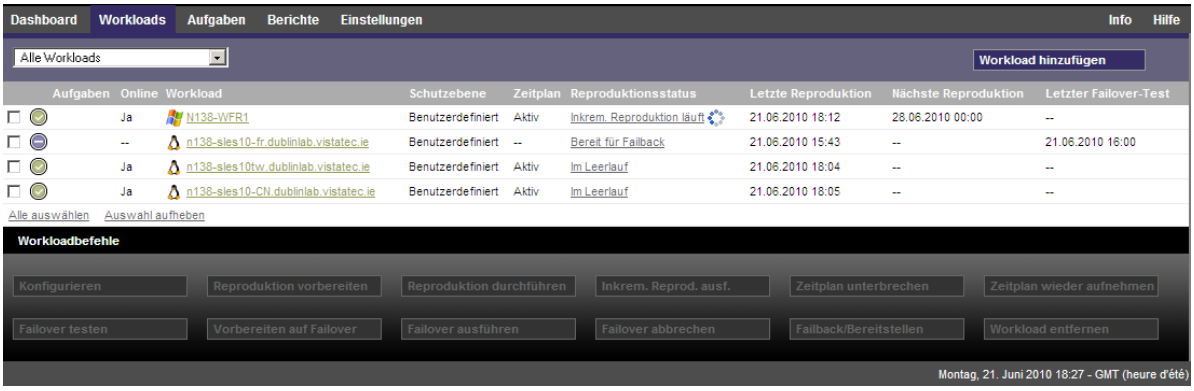
Aufgaben sind spezielle Befehle, die mit Ereignissen verbunden sind, die den Eingriff des Benutzers erfordern. Beispiel: Nach Abschluss des Befehls „Failover testen“ generiert das System ein Ereignis, das mit zwei Aufgaben verbunden ist: `Test als erfolgreich markieren` und `Test als nicht bestanden markieren`. Wenn Sie auf eine der Aufgaben klicken, wird der Failover-Test abgebrochen und es wird ein entsprechendes Ereignis in das Protokoll geschrieben. Ein weiteres Beispiel ist das Ereignis `FullReplicationFailed`, das zusammen mit einer `StartFull`-Aufgabe gezeigt wird. Sie finden eine vollständige Liste der aktuellen Aufgaben auf der Registerkarte *Aufgaben*.

Im Teilfenster „Aufgaben und Ereignisse“ auf dem Dashboard werden für jede Kategorie maximal drei Einträge angezeigt. Wenn alle Aufgaben oder vergangene und anstehende Ereignisse angezeigt werden sollen, klicken Sie im entsprechenden Abschnitt auf *Alle anzeigen*.

3.3 Workloads und Workload-Befehle

Die Seite „Workloads“ enthält eine Tabelle mit einer Zeile pro inventarisiertem Workload. Klicken Sie auf einen Workload-Namen, um die zugehörige Seite „Workload-Details“ anzuzeigen, in der Sie für den Workload und seinen Status relevante Konfigurationen ansehen und bearbeiten können.

Abbildung 3-2 *Die Seite „Workloads“*

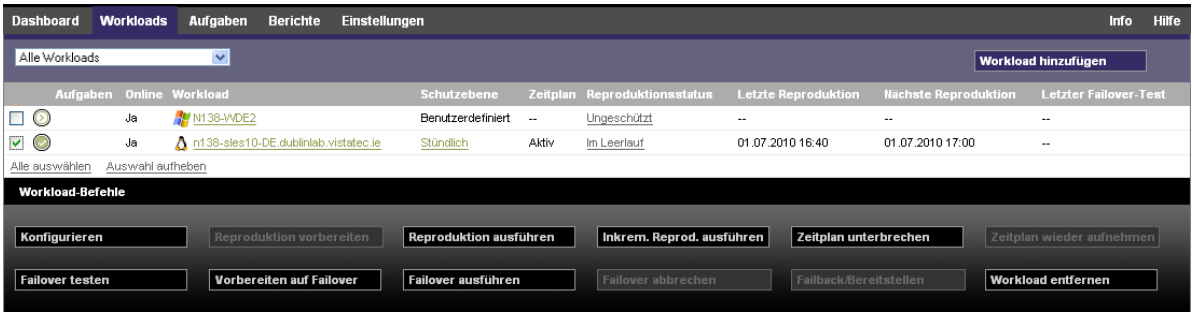


Hinweis: Alle Zeitstempel entsprechen der Zeitzone des PlateSpin Protect Server-Hosts. Diese kann sich von der Zeitzone des geschützten Workloads oder der Zeitzone des Hosts, auf dem Sie die PlateSpin Protect-Weboberfläche ausführen, unterscheiden. Unten rechts im Client-Fenster werden das Serverdatum und die Serveruhrzeit angezeigt.

3.3.1 Workload-Schutz- und Wiederherstellungsbefehle

Befehle spiegeln den Workflow des Workload-Schutzes und der Wiederherstellung wider. Wählen Sie zur Ausführung eines Befehls für einen Workload das entsprechende Kontrollkästchen auf der linken Seite aus. Anwendbare Befehle hängen vom aktuellen Status eines Workloads ab.

Abbildung 3-3 *Workload-Befehle*



In der folgenden Tabelle finden Sie eine Übersicht über die Workload-Befehle sowie deren Beschreibung.

Tabelle 3-2 *Workload-Schutz- und Wiederherstellungsbefehle*

Workload-Befehl	Beschreibung
Konfigurieren	Startet die Konfiguration des Workload-Schutzes mit Parametern, die auf einen inventarisierten Workload anwendbar sind.
Reproduktion vorbereiten	Installiert die erforderliche Datentransfersoftware im Quell-Container und erstellt einen Failover-Workload (einen virtuellen Computer) im Ziel-Container zur Vorbereitung der Workload-Reproduktion.
Reproduktion durchführen	Startet die Reproduktion des Workloads entsprechend der angegebenen Parameter (vollständige Reproduktion).
Inkremental ausführen	Führt eine inkrementelle Übertragung von geänderten Daten vom Ursprung zum Ziel außerhalb der im Zeitplan für den Workload-Schutz festgelegten Zeiten durch.
Zeitplan unterbrechen	Setzt den Schutz aus; alle geplanten Reproduktionen werden übersprungen bis der Zeitplan wieder aufgenommen wird.
Zeitplan wieder aufnehmen	Nimmt den Schutz gemäß den gespeicherten Schutzeinstellungen wieder auf.
Failover testen	Bootet und konfiguriert den Failover-Workload für Testzwecke in einer isolierten Umgebung innerhalb des Containers.
Vorbereiten auf Failover	Bootet den Failover-Workload in Vorbereitung eines Failover-Vorgangs.

Workload-Befehl	Beschreibung
Failover ausführen	Bootet und konfiguriert den Failover-Workload, der die Geschäftsdienste eines fehlgeschlagenen Workloads übernimmt.
Failover abbrechen	Bricht den Failover-Vorgang ab.
Failback	Überführt den Failover-Workload nach einem Failover-Vorgang per Failback wieder in die ursprüngliche oder in eine neue Infrastruktur (virtuell oder physisch).
Workload entfernen	Entfernt einen Workload aus dem Inventar.

3.4 Verwalten mehrerer Instanzen von PlateSpin Protect und PlateSpin Forge

PlateSpin Protect enthält eine webbasierte Client-Anwendung, die PlateSpin Protect-Verwaltungskonsole, die zentralen Zugriff auf mehrere Instanzen von PlateSpin Protect und PlateSpin Forge bietet.

In einem Rechenzentrum mit mehreren Instanzen von PlateSpin Protect können Sie eine der Instanzen als Manager festlegen und die Verwaltungskonsole von dort aus ausführen. Weitere Instanzen werden unter dem Manager hinzugefügt, sodass ein zentraler Punkt für die Steuerung und Interaktion zur Verfügung steht.

- Abschnitt 3.4.1, „Verwenden der PlateSpin Protect-Verwaltungskonsole“, auf Seite 38
- Abschnitt 3.4.2, „Informationen zu PlateSpin Protect-Verwaltungskonsolenkarten“, auf Seite 39
- Abschnitt 3.4.3, „Hinzufügen von Instanzen von PlateSpin Protect und PlateSpin Forge zur Verwaltungskonsole“, auf Seite 40
- Abschnitt 3.4.4, „Verwalten von Karten auf der Verwaltungskonsole“, auf Seite 40

3.4.1 Verwenden der PlateSpin Protect-Verwaltungskonsole

1. Öffnen Sie einen Webbrowser auf einem Computer, der Zugriff auf die PlateSpin Protect-Instanzen hat, und navigieren Sie zu folgender URL:

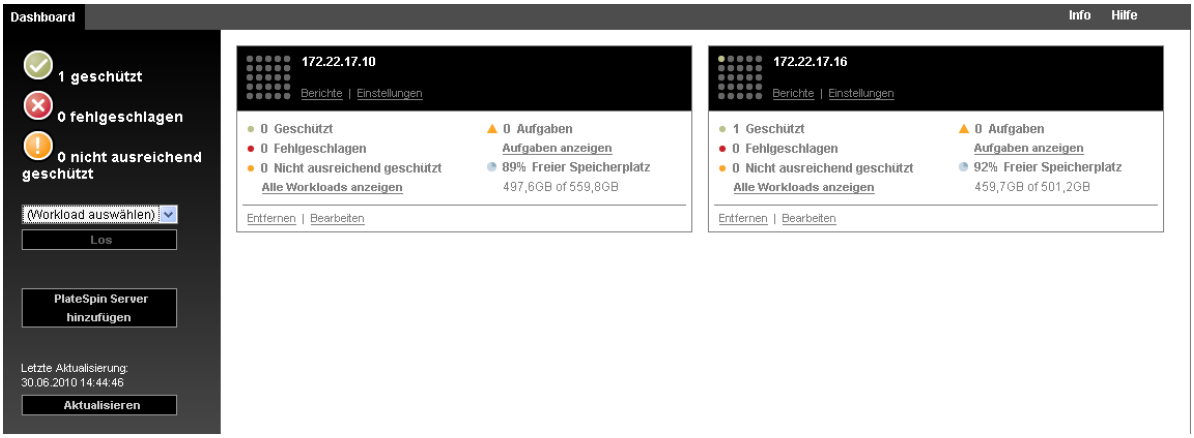
   `http://<IP-Adresse | Hostname>/console`

   Ersetzen Sie *<IP-Adresse | Hostname>* durch die IP-Adresse oder den Hostnamen des PlateSpin Protect Server-Hosts, der als Manager festgelegt wurde.

2. Melden Sie sich mit Ihrem Benutzernamen und Passwort an.

   Die Standardseite „Dashboard“ der Konsole wird angezeigt.

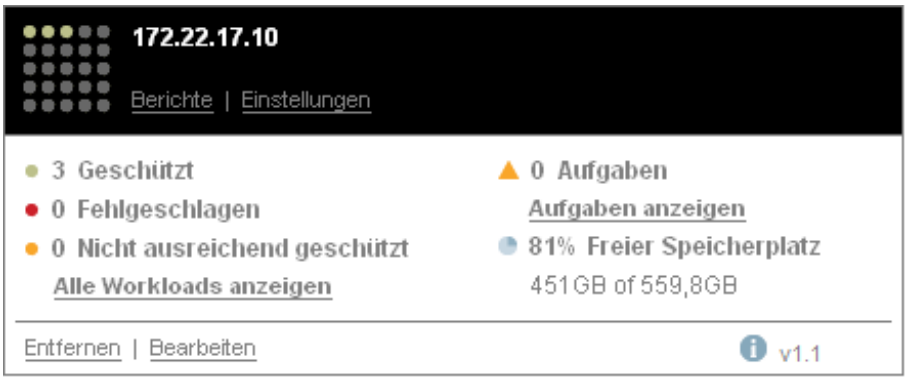
Abbildung 3-4 *Die Standardseite „Dashboard“ der Verwaltungskonsole*



3.4.2 Informationen zu PlateSpin Protect-Verwaltungskonsolenkarten

Einzelne Instanzen von PlateSpin Protect und PlateSpin Forge werden nach dem Hinzufügen zur Verwaltungskonsole als Karten dargestellt.

Abbildung 3-5 *PlateSpin Protect-Instanzkarte*



Eine Karte zeigt grundlegende Informationen über die spezifische Instanz von PlateSpin Protect oder PlateSpin Forge an, z. B.:

- IP-Adresse/Hostname
- Standort
- Versionsnummer
- Workload-Anzahl
- Workload-Status
- Speicherkapazität
- Verbleibender freier Speicherplatz

Hyperlinks auf jeder Karte ermöglichen Ihnen die Navigation zu den für diese Instanz spezifischen Seiten „Workloads“, „Berichte“, „Einstellungen“ und „Aufgaben“. Es gibt darüber hinaus Hyperlinks, über die Sie die Konfiguration einer Karte bearbeiten oder eine Karte aus der Anzeige entfernen können.

3.4.3 Hinzufügen von Instanzen von PlateSpin Protect und PlateSpin Forge zur Verwaltungskonsole

Beim Hinzufügen einer PlateSpin Protect oder Forge-Instanz zur Verwaltungskonsole wird eine neue Karte zum Dashboard der Verwaltungskonsole hinzugefügt.

Hinweis: Wenn Sie sich bei einer Verwaltungskonsole anmelden, die auf einer Instanz von PlateSpin Protect oder PlateSpin Forge ausgeführt wird, wird diese Instanz der Konsole nicht automatisch hinzugefügt. Sie muss manuell hinzugefügt werden.

So fügen Sie eine PlateSpin Protect oder Forge-Instanz zur Konsole hinzu:

1. Klicken Sie im Haupt-Dashboard der Konsole auf *PlateSpin-Server hinzufügen*.

   Die Seite *Hinzufügen/Bearbeiten* wird angezeigt.
2. Geben Sie die URL des PlateSpin Protect-Server-Hosts oder des virtuellen Computers mit PlateSpin Forge an. Verwenden Sie HTTPS, wenn SSL aktiviert ist.
3. (Optional) Aktivieren Sie das Kontrollkästchen *Berechtigungsnachweis der Verwaltungskonsole verwenden*, um denselben Berechtigungsnachweis zu verwenden, der von der Konsole verwendet wird. Wenn diese Option ausgewählt ist, füllt die Konsole automatisch das Feld *Domäne\Benutzername* aus.
4. Geben Sie im Feld *Domäne\Benutzername* einen Domänennamen und einen Benutzernamen ein, die für die von Ihnen hinzugefügte PlateSpin Protect- oder Plate Spin Forge-Instanz gültig sind. Geben Sie im Feld *Passwort* das entsprechende Passwort ein.
5. (Optional) Geben Sie einen beschreibenden oder identifizierenden *Anzeigenamen* (max. 15 Zeichen), einen *Speicherort* (max. 20 Zeichen) und ggf. erforderliche *Hinweise* ein (max. 400 Zeichen).
6. Klicken Sie auf *Hinzufügen/Speichern*.

   Es wird eine neue Karte zum Dashboard hinzugefügt.

3.4.4 Verwalten von Karten auf der Verwaltungskonsole

Sie können die Details einer --Karte auf der Verwaltungskonsole ändern.

1. Klicken Sie auf den Hyperlink *Bearbeiten* auf der Karte, die Sie bearbeiten möchten.

   Die Seite *Hinzufügen/Bearbeiten* der Konsole wird angezeigt.
2. Nehmen Sie alle gewünschten Änderungen vor und klicken Sie anschließend auf *Hinzufügen/Speichern*.

   Das aktualisierte Konsolen-Dashboard wird angezeigt.

So entfernen Sie eine --Karte von der Verwaltungskonsole:

1. Klicken Sie auf den Hyperlink *Entfernen* auf der Karte, die Sie entfernen möchten.

   Es wird eine Bestätigungsaufforderung angezeigt.
2. Klicken Sie auf *OK*.

   Die individuelle Karte wird vom Dashboard entfernt.

3.5 Generieren von Workload- und Workload-Schutz-Berichten

PlateSpin Protect ermöglicht Ihnen das Generieren von Berichten, die einen analytischen Einblick in Ihre Workload-Schutz-Zeitpläne über einen bestimmten Zeitraum hinweg gewähren.

Die folgenden Berichtstypen werden unterstützt:

- **Workload-Schutz:** Bericht über Reproduktionsereignisse für alle Workloads in einem auswählbaren Zeitraum.
- **Reproduktionsverlauf:** Bericht über Reproduktionstyp, Größe, Zeit und Übertragungsgeschwindigkeit pro auswählbarem Workload in einem auswählbaren Zeitraum.
- **Reproduktionsfenster:** Bericht über die Dynamik vollständiger und inkrementeller Reproduktionen, die nach *Durchschnitt*, *Zuletzt*, *Summe* und *Spitze* zusammengefasst werden können.
- **Aktueller Schutzstatus:** Statistikbericht über die Parameter *Ziel-RPO*, *RPO (tatsächlich)*, *TTO (tatsächlich)*, *RTO (tatsächlich)*, *Letzter Failover-Test*, *Letzte Reproduktion* und *Testalter*.
- **Ereignisse:** Bericht über Systemereignisse für alle Workloads in einem auswählbaren Zeitraum.
- **Routineereignisse:** Bericht über anstehende Workload-Schutz-Ereignisse.

Abbildung 3-6 *Optionen für einen Reproduktionsverlaufsbericht*

So erzeugen Sie einen Bericht:

1. Klicken Sie auf der PlateSpin Protect-Weboberfläche auf *Berichte*.

   Es wird eine Liste mit Berichtstypen angezeigt.
2. Klicken Sie auf den Namen des erforderlichen Berichtstyps.

4 Workload-Schutz

PlateSpin Protect erstellt eine Reproduktion Ihres Produktions-Workloads und aktualisiert diese Reproduktion auf Basis eines von Ihnen festgelegten Zeitplans.

Die Reproduktion bzw. der *Failover-Workload* ist eine virtuelle Maschine im VM-Container von PlateSpin Protect und übernimmt die Geschäftsfunktion des Produktions-Workloads, falls es zu einer Störung am Produktionsstandort kommt.

4.1 Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung

PlateSpin Protect definiert folgenden Workflow für den Workload-Schutz und die Wiederherstellung:

1. Vorbereitungsschritt:
   - **1a** Stellen Sie sicher, dass PlateSpin Protect Ihren Workload unterstützt.

     Weitere Informationen hierzu finden Sie in „Unterstützte Konfigurationen“, auf Seite 9.
   - **1b** Stellen Sie sicher, dass Ihre Workloads und Container die Zugriffs- und Netzwerkvoraussetzungen erfüllen.

     Weitere Informationen hierzu finden Sie in „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“, auf Seite 21.
   - **1c** (nur Linux)
     - (Bedingt) Wenn Sie planen, einen unterstützten Linux-Workload zu schützen, der einen nicht-standardmäßigen, benutzerdefinierten oder neueren Kernel hat, bauen Sie das PlateSpin `blkwatch`-Modul neu auf, das für eine Datenreproduktion auf Blockebene erforderlich ist.

Weitere Informationen hierzu finden Sie im KB-Artikel 7005873 (http://www.novell.com/support/viewContent.do?externalId=7005873).

- (Empfohlen) Bereiten Sie LVM-Snapshots für den Datentransfer auf Blockebene vor. Stellen Sie sicher, dass jede Volume-Gruppe über genügend freien Speicherplatz für LVM-Snapshots verfügt (mindestens 10 % der Summe aller Partitionen).

  Weitere Informationen hierzu finden Sie im KB-Artikel 7005872 (http://www.novell.com/support/viewContent.do?externalId=7005872).

- (Optional) Legen Sie die benutzerdefinierten Skripts fest, die auf Ihrem Ursprungs-Workload bei jeder Reproduktion ausgeführt werden sollen, und bereiten Sie sie vor.

  Weitere Informationen hierzu finden Sie in „Verwenden von Freeze- und Thaw-Skripts für alle Reproduktionen (Linux)“, auf Seite 67.

2. Fügen Sie einen Container hinzu.

   Weitere Informationen hierzu finden Sie in „Hinzufügen von Containern“, auf Seite 44.

3. Fügen Sie einen Workload hinzu.

   Weitere Informationen hierzu finden Sie in „Hinzufügen eines Workloads für den Schutz“, auf Seite 46.

4. Konfigurieren Sie Schutzdetails und bereiten Sie die Reproduktion vor.

   Weitere Informationen hierzu finden Sie in „Konfigurieren der Schutzdetails und Vorbereiten der Reproduktion“, auf Seite 47.

5. Starten Sie den Zeitplan für den Workload-Schutz.

   Weitere Informationen hierzu finden Sie unter „Starten des Workload-Schutzes“, auf Seite 50.

6. (Optional) Führen Sie manuell eine inkrementelle Reproduktion aus.

7. (Optional) Testen Sie die Failover-Funktionalität.

   Weitere Informationen hierzu finden Sie in Verwenden der Funktion "Failover testen".

8. Führen Sie einen Failover durch.

   Weitere Informationen hierzu finden Sie in „Failover“, auf Seite 52.

9. Führen Sie ein Failback durch.

   Weitere Informationen hierzu finden Sie unter „Failback“, auf Seite 54.

10. (Optional) Schützen Sie einen Workload nach einem Failback erneut.

Außer den Schritten 1, 8 und 9 können alle Schritte über Workload-Befehle auf der Seite „Workloads“ durchgeführt werden. Weitere Informationen hierzu finden Sie unter „Workloads und Workload-Befehle“, auf Seite 36.

Der Befehl *Erneut schützen* steht nach einem erfolgreichen Failback-Vorgang zur Verfügung.

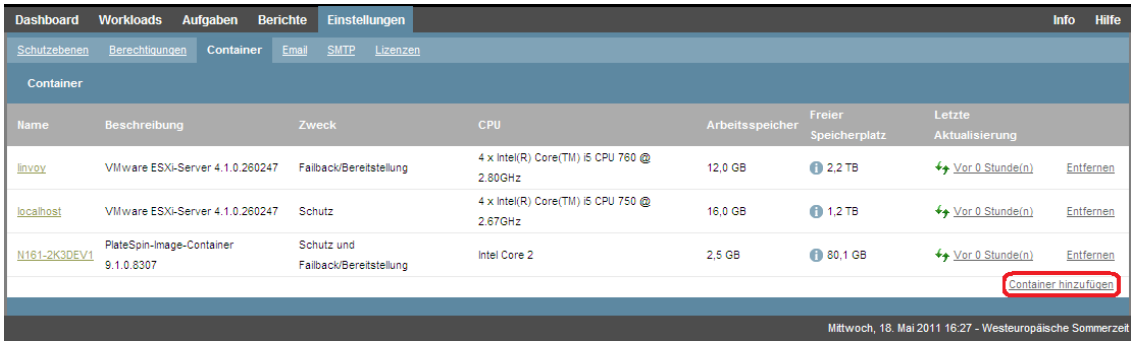
4.2 Hinzufügen von Containern

Ein Container ist eine Schutz-Infrastruktur, die als Host für die regelmäßig aktualisierte Reproduktion eines geschützten Workloads agiert. Diese Infrastruktur kann entweder ein VMware ESX-Server oder ein VMware DRS-Cluster sein.

Damit Sie einen Workload schützen können, müssen Sie entweder vor oder während des Hinzufügens des zu schützenden Workloads einen Container hinzufügen.

So fügen Sie einen Container hinzu:

1 Klicken Sie auf der PlateSpin Protect-Weboberfläche auf *Einstellungen* > *Container* > *Container hinzufügen*.



2 Geben Sie die folgenden Parameter an:

- **Typ:** Wählen Sie den Containertyp aus (*VMware ESX-Server* oder *VMware DRS-Cluster*). Stellen Sie sicher, dass der Container unterstützt wird.

  Weitere Informationen finden Sie unter „Unterstützte VM-Containern“, auf Seite 11.

- **Hostname oder IP-Adresse:** Geben Sie den Hostnamen oder die IP-Adresse des Containers ein.

- **vCenter-Hostname oder -IP-Adresse:** (Nur DRS-Cluster) Geben Sie den Hostnamen oder die IP-Adresse des vCenter-Servers ein.

- **Clustername:** (Nur DRS-Cluster) Geben Sie den Namen des erforderlichen DRS-Clusters ein.

  Wenn Sie versuchen, einen DRS-Cluster hinzuzufügen oder zu aktualisieren, kann der zugrunde liegende Ermittlungsvorgang in folgenden Fällen fehlschlagen:

  - Ein Cluster enthält keine ESX-Hosts.
  - Ein Clustername im vCenter-Server ist nicht eindeutig (auch wenn er einen eindeutigen Inventarpfad hat).
  - Keines der Cluster-Mitglieder ist zugänglich (z. B. weil der vCenter-Server im Wartungsmodus ist).

- **Benutzername/Passwort:** Geben Sie den Administrator-Berechtigungsnachweis für den Zugriff auf den erforderlichen Host ein. Weitere Informationen hierzu finden Sie unter „Richtlinien für Workload- und Container-Berechtigungsnachweise“, auf Seite 62.

- **Beschreibung:** (Betrifft nur VM-Container) Wählen Sie das erforderliche Element aus (*Schutz*, *Failback/Bereitstellung* oder beide). Wenn Sie beide Elemente auswählen (*Schutz* und *Failback/Bereitstellung*), steht dieser Container für die Auswahl als Ziel sowohl für Schutz- als auch für Failback-/Bereitstellungsvorgänge zur Verfügung.

3 Klicken Sie auf *Hinzufügen*.

PlateSpin Protect lädt die Seite „Container“ neu und blendet eine Fortschrittsanzeige für den Container ein, der hinzugefügt wird . Nach Abschluss des Vorgangs ändert sich das Symbol für die Fortschrittsanzeige in ein Symbol *Aktualisieren* .

Klicken Sie zum Aktualisieren eines Containers auf das Symbol *Aktualisieren* neben dem zu aktualisierenden Container. Dadurch wird der Container neu inventarisiert.

Klicken Sie zum Entfernen eines Containers auf *Entfernen* neben dem zu entfernenden Container.

4.3 Hinzufügen eines Workloads für den Schutz

1 Führen Sie die erforderlichen Vorbereitungsschritte durch.

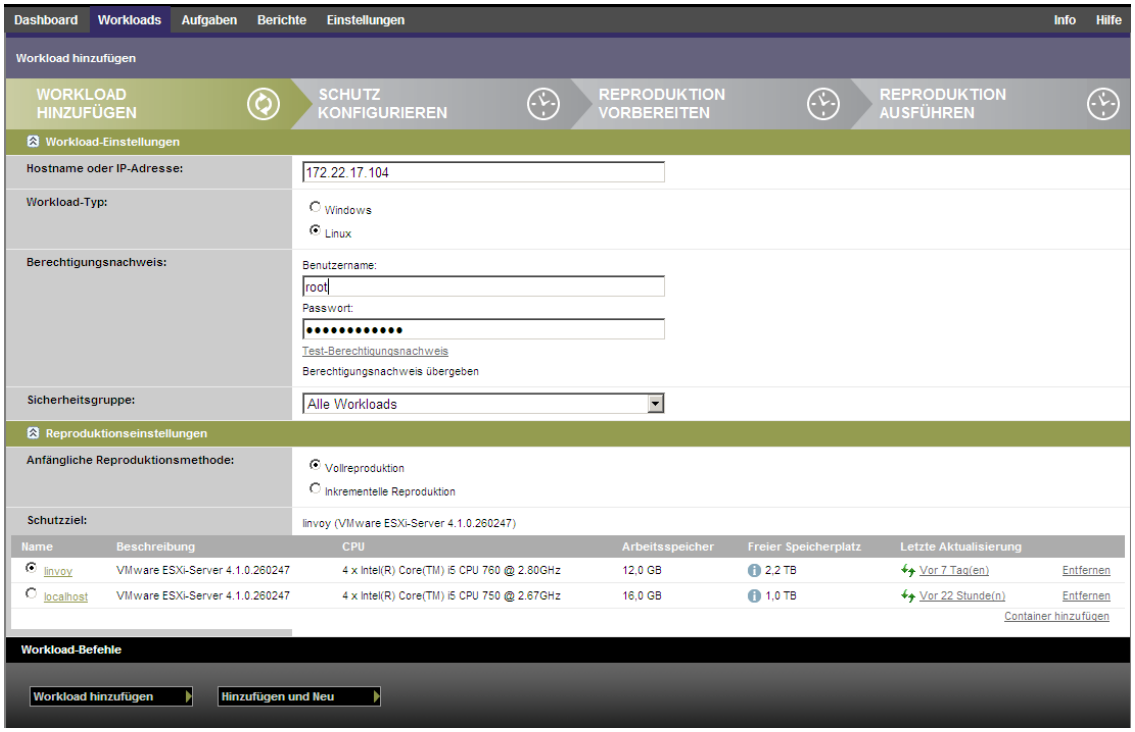
Siehe Schritt 1 unter „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“, auf Seite 43.

2 Fügen Sie einen VM-Container hinzu.

Weitere Informationen hierzu finden Sie unter „Hinzufügen von Containern“, auf Seite 44.

3 Klicken Sie auf der Seite „Dashboard“ oder „Workloads“ auf *Workload hinzufügen*.

Auf der PlateSpin Protect-Weboberfläche wird die Seite „Workload hinzufügen“ angezeigt.



4 Geben Sie die erforderlichen Workload-Details an:

- **Workload-Einstellungen:** Geben Sie den Hostnamen oder die IP-Adresse Ihres Workloads, das Betriebssystem, den Administrator-Berechtigungsnachweis und eine Sicherheitsgruppe an, der der Workload zugewiesen werden soll. Weitere Informationen hierzu finden Sie in „Verwalten von PlateSpin Protect-Sicherheitsgruppen und -Workload-Berechtigungen“, auf Seite 19.

  Verwenden Sie das erforderliche Berechtigungsnachweisformat (weitere Informationen hierzu finden Sie unter „Richtlinien für Workload- und Container-Berechtigungsnachweise“, auf Seite 62).

  Klicken Sie auf *Test-Berechtigungsnachweis*, um sicherzustellen, dass PlateSpin Protect auf den Workload zugreifen kann.

- **Reproduktionseinstellungen:** Wählen Sie die erforderlichen Reproduktionseinstellungen aus. Weitere Informationen hierzu finden Sie unter „Anfängliche Reproduktionsmethode (Vollständig und Inkrementell)“, auf Seite 65.

- **Schutzziel:** Wählen Sie das erforderliche Schutzziel aus. Dies ist entweder der Ziel-Container oder ein vorbereiteter Workload, wenn Sie *Inkrementelle Reproduktion* als anfängliche Reproduktionsmethode ausgewählt haben. Weitere Informationen hierzu finden Sie unter „Anfängliche Reproduktionsmethode (Vollständig und Inkrementell)“, auf Seite 65.

5 Klicken Sie auf *Workload hinzufügen*.

PlateSpin Protect lädt die Seite „Workloads“ neu und blendet eine Fortschrittsanzeige für den Workload ein, der hinzugefügt wird  . Warten Sie, bis der Vorgang abgeschlossen ist. Anschließend wird das Ereignis *Workload hinzugefügt* im Dashboard angezeigt.

4.4 Konfigurieren der Schutzdetails und Vorbereiten der Reproduktion

Schutzdetails steuern die Workload-Schutz- und Wiederherstellungseinstellungen sowie das Verhalten im gesamten Lebenszyklus eines geschützten Workloads. In jeder Phase des Schutz- und Wiederherstellungs-Workflows (siehe „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“, auf Seite 43) werden relevante Einstellungen aus den Schutzdetails gelesen.

So konfigurieren Sie die Schutzdetails Ihres Workloads:

1 Fügen Sie einen Workload hinzu. Weitere Informationen hierzu finden Sie unter „Hinzufügen eines Workloads für den Schutz“, auf Seite 46.

2 Wählen Sie auf der Seite „Workloads“ den erforderlichen Workload aus und klicken Sie auf *Konfigurieren*.

Auf der PlateSpin Protect-Weboberfläche wird die Seite „Schutzdetails“ des Workloads angezeigt.

3 Konfigurieren Sie die Schutzdetails in jeder Einstellungsgruppe so, wie sie für die Aufrechterhaltung Ihres ununterbrochenen Geschäftsbetriebs erforderlich sind. Weitere Informationen hierzu finden Sie unter „Workload-Schutz-Details“, auf Seite 48.

4 Korrigieren Sie alle Validierungsfehler, die eventuell auf der PlateSpin Protect-Weboberfäche angezeigt werden.

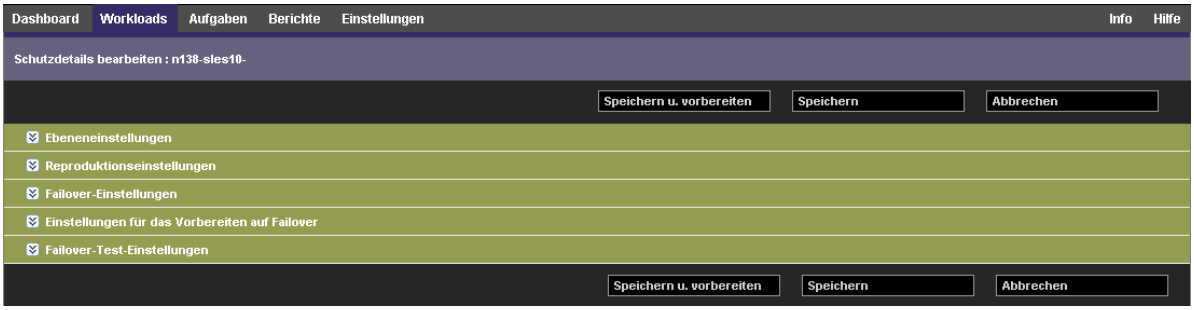
5 Klicken Sie auf *Speichern*.

Sie können alternativ auch auf *Speichern und vorbereiten* klicken. Dies speichert die Einstellungen und führt gleichzeitig den Befehl *Reproduktion vorbereiten* aus (bei Bedarf werden Datenübertragungstreiber auf dem Ursprungs-Workload installiert und die anfängliche VM-Reproduktion Ihres Workloads wird erstellt).

Warten Sie, bis der Vorgang abgeschlossen ist. Anschließend wird das Ereignis *Workload-Konfiguration abgeschlossen* im Dashboard angezeigt.

4.4.1 Workload-Schutz-Details

Workload-Schutz-Details werden in fünf Parametergruppen angegeben:



Sie können jede Parametergruppe erweitern oder komprimieren, indem Sie auf das -Symbol auf der linken Seite klicken.

Im Folgenden sind die Details der fünf Parametergruppen aufgeführt:

Tabelle 4-1 *Workload-Schutz-Details*

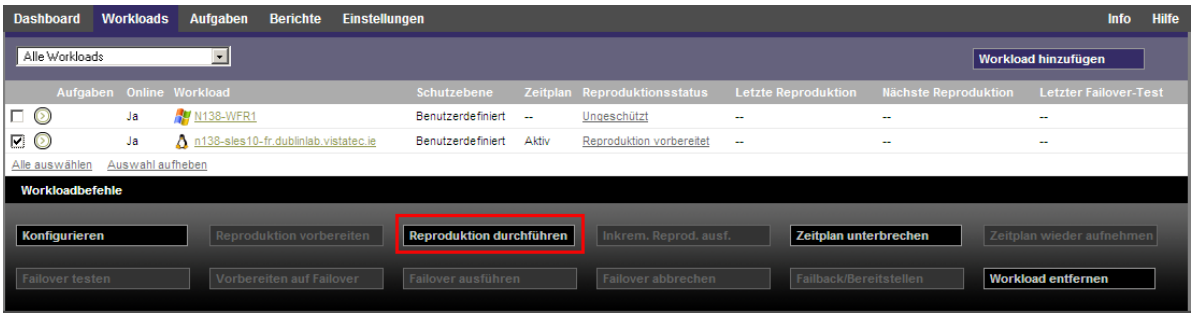
Parametergruppe (Einstellungen)	Details
Ebene	Gibt die Schutzebene des aktuellen Schutzes an. Weitere Informationen hierzu finden Sie unter „Schutzebenen“, auf Seite 63.

Parametergruppe (Einstellungen)	Details
Reproduktion	**Übertragungsverschlüsselung:** Wählen Sie zum Aktivieren der Verschlüsselung die Option *Datenübertragung verschlüsseln*. Weitere Informationen hierzu finden Sie in „Sicherheit und Datenschutz“, auf Seite 11. **Übertragungsmethode:** (Windows) Ermöglicht Ihnen, eine Datenübertragungsmethode und Sicherheit durch Verschlüsselung auszuwählen. Weitere Informationen hierzu finden Sie unter „Übertragungsmethoden“, auf Seite 62. **Ursprungsberechtigungsnachweis:** Für den Zugriff auf den Workload erforderlich. Weitere Informationen hierzu finden Sie unter „Richtlinien für Workload- und Container-Berechtigungsnachweise“, auf Seite 62. **Anzahl der CPUs:** Hier können Sie die erforderliche Anzahl der vCPUs angeben, die dem Failover-Workload zugewiesen wurden (nur zutreffend, wenn als Methode der ursprünglichen Reproduktion *Vollständig* ausgewählt wurde). **Reproduktionsnetzwerk:** Ermöglicht Ihnen die Trennung des Reproduktionsdatenverkehrs auf der Basis virtueller Netzwerke, die im VM-Container definiert sind. Weitere Informationen hierzu finden Sie unter „Netzwerke“, auf Seite 69. **Datenablage für Wiederherstellungspunkte:** Ermöglicht Ihnen die Auswahl einer mit Ihrem VM-Container verbundenen Datenablage zum Speichern von Wiederherstellungspunkten. Weitere Informationen hierzu finden Sie unter „Wiederherstellungspunkte“, auf Seite 65. **Geschützte Volumes:** Verwenden Sie diese Optionen, um Volumes für den Schutz auszuwählen und deren Reproduktionen spezifischen Datenablagen im VM-Container zuzuweisen. **Thin-Festplatten-Option:** Aktiviert die Funktion für virtuelle Thin-Provisioned-Datenträger, bei der ein virtueller Datenträger für den virtuellen Computer eine feste Größe zu haben scheint, jedoch nur die Menge an Festplattenspeicher verbraucht, die tatsächlich von den Daten auf diesem Datenträger benötigt wird. **Dienste/Daemons, die während der Reproduktion angehalten werden sollen:** Ermöglicht Ihnen die Auswahl von Windows-Diensten oder Linux-Daemonen, die während der Reproduktion automatisch angehalten werden sollen. Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“, auf Seite 66.
Failover	**VM-Arbeitsspeicher:** Ermöglicht Ihnen die Angabe der Menge an Arbeitsspeicher, der dem Failover-Workload zugeteilt werden soll. **Hostname und Domänen-/Arbeitsgruppenzugehörigkeit:** Verwenden Sie diese Optionen, um die Identität und Domänen-/Arbeitsgruppenzugehörigkeit des Failover-Workloads zu steuern, wenn dieser „live“ ist. Für die Domänenzugehörigkeit ist der Berechtigungsnachweis eines Domänenadministrators erforderlich. **Netzwerkverbindungen:** Verwenden Sie diese Optionen, um die LAN-Einstellungen des Failover-Workloads festzulegen. Weitere Informationen hierzu finden Sie unter „Netzwerke“, auf Seite 69. **Zu ändernde Dienst/Daemon-Status:** Ermöglicht Ihnen die Steuerung des Anfangsstatus spezifischer Anwendungsdienste (Windows) oder Daemons (Linux). Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“, auf Seite 66.
Vorbereiten auf Failover	Ermöglicht Ihnen die Steuerung der temporären Netzwerkeinstellungen des Failover-Workloads während des optionalen Vorgangs der Vorbereitung auf den Failover. Weitere Informationen hierzu finden Sie unter „Netzwerke“, auf Seite 69.

Parametergruppe (Einstellungen)	Details
Failover testen	**VM-Arbeitsspeicher:** Ermöglicht Ihnen das Zuweisen des erforderlichen RAM zum temporären Workload. **Hostname:** Ermöglicht Ihnen das Zuweisen eines Hostnamens zum temporären Workload. **Domäne/Arbeitsgruppe:** Ermöglicht Ihnen die Zuordnung des temporären Workloads zu einer Domäne oder Arbeitsgruppe. Für die Domänenzugehörigkeit ist der Berechtigungsnachweis eines Domänenadministrators erforderlich. **Netzwerkverbindungen:** Steuert die LAN-Einstellungen des temporären Workloads. Weitere Informationen hierzu finden Sie unter „Netzwerke“, auf Seite 69. **Zu ändernde Dienst/Daemon-Status:** Ermöglicht Ihnen die Steuerung des Anfangsstatus spezifischer Anwendungsdienste (Windows) oder Daemons (Linux). Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“, auf Seite 66.

4.5 Starten des Workload-Schutzes

Der Workload-Schutz wird durch den Befehl *Reproduktion durchführen* gestartet:



Sie können den Befehl „Reproduktion durchführen“ nach folgenden Aktionen ausführen:

- Hinzufügen eines Workloads.
- Konfigurieren der Schutzdetails eines Workloads.
- Vorbereiten der anfänglichen Reproduktion.

Wenn Sie bereit sind, fortzufahren:

1. Wählen Sie auf der Seite „Workloads“ den erforderlichen Workload aus und klicken Sie auf *Reproduktion durchführen*.
2. Klicken Sie auf *Ausführen*.

   PlateSpin Protect startet die Ausführung und zeigt eine Fortschrittsanzeige für den Schritt *Daten kopieren* an.

Hinweis: Nachdem ein Workload geschützt wurde:

- Das Ändern der Größe eines Volumes, das auf Blockebene geschützt wird, macht den Schutz ungültig. Gehen Sie wie folgt vor: 1. Entfernen Sie den Workload aus dem Schutz Ändern Sie die Größe der Volumes, wie erforderlich. 3. Bauen Sie den Schutz erneut auf, indem Sie den Workload erneut hinzufügen, dessen Schutzdetails konfigurieren und die Reproduktionen starten.
- Nach jeder signifikanten Änderung des geschützten Workloads muss der Schutz neu hergestellt werden. Dies ist zum Beispiel erforderlich, wenn Volumes oder Netzwerkkarten zu einem geschützten Workload hinzugefügt wurden.

4.6 Abbrechen von Befehlen

Auf der Seite "Befehlsdetails" eines bestimmten Befehls können sie diesen nach dessen Ausführung abbrechen, solange er noch nicht durchgeführt wurde.

So greifen Sie auf die Seite "Befehlsdetails" eines Befehls zu, der noch nicht durchgeführt wurde:

1. Wechseln Sie zur Seite „Workloads“.
2. Suchen Sie den erforderlichen Workload und klicken Sie auf den Link, der den Befehl bezeichnet, der gerade auf diesem Workload ausgeführt wird.

Auf der PlateSpin Protect-Weboberfläche wird die entsprechende Seite "Befehlsdetails" angezeigt:

3. Klicken Sie auf *Abbrechen*.

4.7 Failover

Ein *Failover* hat zur Folge, dass die Business-Funktion eines ausgefallenen Workloads von einem Failover-Workload innerhalb eines PlateSpin Protect-VM-Containers übernommen wird.

4.7.1 Erkennen von Offline-Workloads

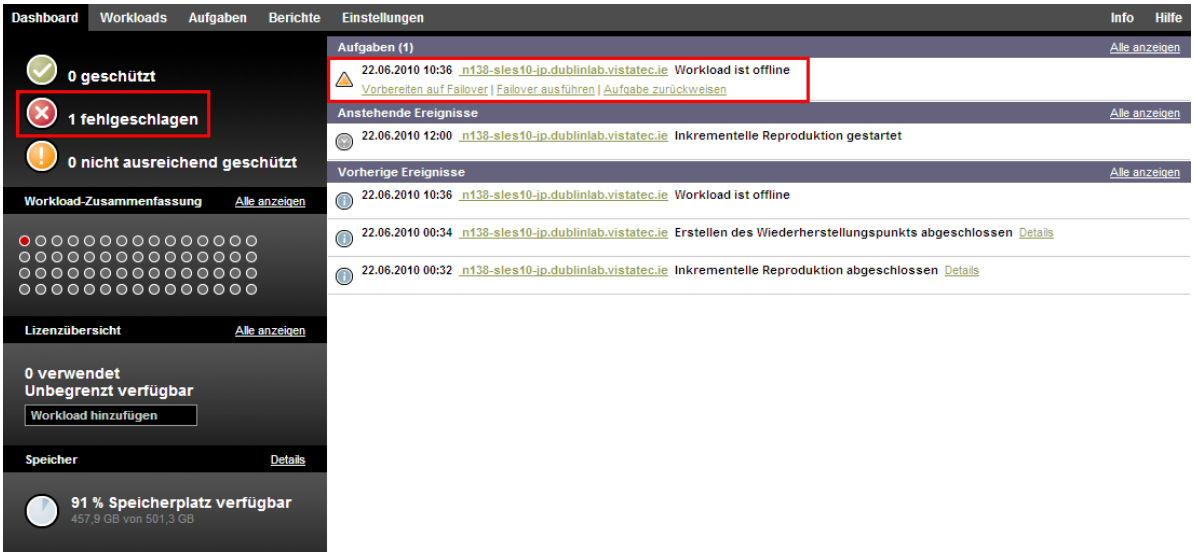
PlateSpin Protect überwacht ständig Ihre geschützten Workloads. Wenn ein Versuch zur Überwachung eines Workloads so oft wie vorher festgelegt fehlschlägt, generiert PlateSpin Protect das Ereignis *Workload ist offline*. Kriterien, anhand derer ein Workload-Fehler definiert und protokolliert wird, sind Teil der Ebeneneinstellungen eines Workload-Schutzes (Informationen hierzu finden Sie in der Zeile Ebene unter „Workload-Schutz-Details“, auf Seite 48).

Wenn zusammen mit den SMTP-Einstellungen Benachrichtigungen konfiguriert wurden, sendet PlateSpin Protect gleichzeitig eine Benachrichtigungs-Email an die angegebenen Empfänger. Weitere Informationen hierzu finden Sie in „Einrichten automatischer Email-Benachrichtigungen zu Ereignissen und Berichten“, auf Seite 26.

Wenn ein Workload-Fehler erkannt wird, während der Status der Reproduktion *Im Leerlauf* lautet, können Sie mit dem Befehl *Failover ausführen* fortfahren. Wenn ein Workload-Fehler auftritt, während eine inkrementelle Reproduktion stattfindet, bleibt der Vorgang hängen. Brechen Sie in diesem Fall den Vorgang ab (weitere Informationen hierzu finden Sie unter „Abbrechen von Befehlen“, auf Seite 51) und fahren Sie dann mit dem Befehl *Failover ausführen* fort. Weitere Informationen hierzu finden Sie unter „Durchführen eines Failovers“, auf Seite 53.

Die folgende Abbildung zeigt die Dashboard-Seite der PlateSpin Protect-Weboberfläche beim Erkennen eines Workload-Fehlers. Beachten Sie die anwendbaren Aufgaben im Teilfenster mit den Aufgaben und Ereignissen:

Abbildung 4-1 *Die Dashboard-Seite bei Erkennen eines Workload-Fehlers ("Workload offline")*



4.7.2 Durchführen eines Failovers

Failover-Einstellungen, einschließlich der Netzwerkidentitäts- und LAN-Einstellungen des Failover-Workloads, werden zum Zeitpunkt der Konfiguration zusammen mit den Schutzdetails gespeichert. Informationen hierzu finden Sie in der Zeile Failover unter „Workload-Schutz-Details“, auf Seite 48.

Sie können folgende Methoden zur Durchführung eines Failovers verwenden:

- Wählen Sie den erforderlichen Workload auf der Seite „Workloads“ aus und klicken Sie auf *Failover ausführen*.
- Klicken Sie auf den entsprechenden Befehls-Hyperlink im Ereignis *Workload ist offline* im Teilfenster mit den Aufgaben und Ereignissen. Weitere Informationen hierzu finden Sie unter Abbildung 4-1.
- Führen Sie einen Befehl *Auf Failover vorbereiten* aus, um den virtuellen Failover-Computer rechtzeitig vorher zu booten. Sie können den Failover danach auch immer wieder abbrechen (was bei stufenweisen Failovers nützlich ist).

Verwenden Sie eine dieser Methoden, um den Failover-Vorgang zu starten, und wählen Sie einen Wiederherstellungspunkt aus, der auf den Failover-Workload angewendet werden soll (Informationen hierzu finden Sie unter „Wiederherstellungspunkte“, auf Seite 65). Klicken Sie auf *Ausführen* und überwachen Sie den Vorgang. Wenn der Vorgang abgeschlossen ist, sollte der Reproduktionsstatus des Workloads *Live* lauten.

Informationen zum Testen des Failover-Workloads oder des Failover-Vorgangs im Rahmen einer geplanten Übung zur Wiederherstellung im Katastrophenfall finden Sie unter „Verwenden der Funktion "Failover testen"“, auf Seite 54.

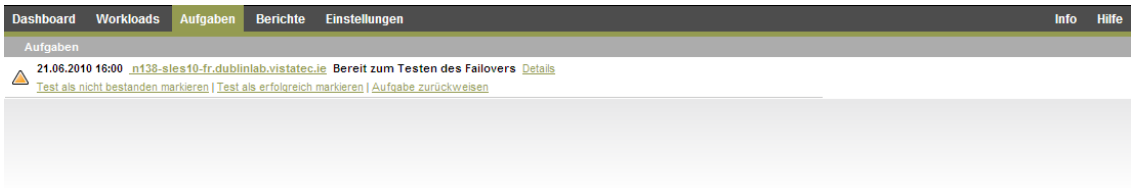
4.7.3 Verwenden der Funktion "Failover testen"

PlateSpin Protect ermöglicht es Ihnen, die Failover-Funktionalität und die Integrität des Failover-Workloads zu testen. Dies geschieht unter Verwendung des Befehls *Failover testen*, der den Failover-Workload zu Testzwecken in einer eingeschränkten Netzwerkumgebung bootet.

Wenn Sie diesen Befehl ausführen, wendet PlateSpin Protect die Failover-Test-Einstellungen, die in den Workload-Schutz-Details gespeichert sind, auf den Failover-Workload an (siehe Zeile Failover testen in „Workload-Schutz-Details“, auf Seite 48.

1. Definieren Sie ein angemessenes Zeitfenster für das Testen und stellen Sie sicher, dass keine Reproduktionen im Gange sind. Der Reproduktionsstatus des Workload muss *Im Leerlauf* sein.
2. Wählen Sie auf der Seite „Workloads“ den erforderlichen Workload aus, klicken Sie auf *Failover testen*, wählen Sie einen Wiederherstellungspunkt aus (siehe „Wiederherstellungspunkte“, auf Seite 65) und klicken Sie anschließend auf *Ausführen*.

   Anschließend generiert PlateSpin Protect ein entsprechendes Ereignis sowie eine Aufgabe mit einem Satz von anwendbaren Befehlen:



3. Überprüfen Sie die Integrität und die Betriebsfunktionen des Failover-Workloads. Verwenden Sie den VMware vSphere-Client, um auf den Failover-Workload im VM-Container zuzugreifen.
4. Markieren Sie den Test als *nicht bestanden* oder *erfolgreich bestanden*. Verwenden Sie die entsprechenden Befehle in der Aufgabe (*Test als nicht bestanden markieren*, *Test als erfolgreich markieren*). Die ausgewählte Aktion wird im Verlauf der Ereignisse gespeichert, die mit dem Workload verknüpft sind und kann über Berichte abgerufen werden. *Aufgabe zurückweisen* verwirft die Aufgabe und das Ereignis.

   Nach Abschluss der Aufgaben *Test als nicht bestanden markieren* oder *Test als erfolgreich markieren* verwirft PlateSpin Protect die temporären Einstellungen, die auf den Failover-Workload angewendet wurden. Der Schutz wird in den Zustand versetzt, den er vor dem Test hatte.

4.8 Failback

Der nächste logische Schritt, der einem Failover folgt, ist ein Failback-Vorgang. Er überträgt den Failover-Workload an seine ursprüngliche oder, falls erforderlich, auf eine neue Infrastruktur.

Failback-Methoden unterscheiden sich je nach Ziel-Infrastrukturtyp und dem Grad der Automatisierung des Failback-Vorgangs:

- **Automatischer Failback auf eine virtuelle Maschine:** Unterstützt für VMware ESX-Plattformen und VMware DRS-Cluster.
- **Halbautomatischer Failback auf einen physischen Computer:** Wird für alle physischen Computer unterstützt.
- **Halbautomatischer Failback auf eine virtuelle Maschine:** Wird für Xen auf SLES- und Microsoft Hyper-V-Plattformen unterstützt.

Die folgenden Abschnitte enthalten weitere Informationen:

- Abschnitt 4.8.1, „Automatischer Failback auf eine virtuelle Maschine“, auf Seite 55
- Abschnitt 4.8.2, „Halbautomatischer Failback auf einen physischen Computer“, auf Seite 58
- Abschnitt 4.8.3, „Halbautomatischer Failback auf eine virtuelle Maschine“, auf Seite 59

4.8.1 Automatischer Failback auf eine virtuelle Maschine

Die folgenden Container werden als Ziele für automatische Failbacks unterstützt:

Plattform	Hinweise
VMware DRS-Cluster in vSphere 5.0	◆ Die DRS-Konfiguration muss entweder **Teilweise automatisiert** oder **Vollautomatisch** sein (sie darf nicht auf **Manuell** gesetzt sein) ◆ Der Cluster darf nur aus ESXi 5.0-Servern bestehen und darf nur von vCenter 5.0 verwaltet werden
VMware DRS-Cluster in vSphere 4.1	◆ Die DRS-Konfiguration muss entweder **Teilweise automatisiert** oder **Vollautomatisch** sein (sie darf nicht auf **Manuell** gesetzt sein) ◆ Der Cluster kann eine Kombination aus ESX 4.1- und ESX**i** 4.1-Servern verwenden und darf nur von vCenter 4.1 verwaltet werden
VMware ESX**i** 4.1, 5.0	ESX**i**-Versionen erfordern eine erworbene Lizenz. Der Schutz wird bei diesen Systemen nicht unterstützt, wenn sie mit einer kostenlosen Lizenz ausgeführt werden.
VMware ESX 4.1	

Führen Sie folgende Schritte aus, um einen automatischen Failback eines Failover-Workloads auf einen Ziel-VMware-Container durchzuführen.

1. Wählen Sie im Anschluss an einen Failover den Workload auf der Seite „Workloads“ aus und klicken Sie auf *Failback durchführen*.
2. Legen Sie die folgenden Parametergruppen fest:
   - **Workload-Einstellungen:** Geben Sie den Hostnamen oder die IP-Adresse Ihres Failover-Workloads und den Berechtigungsnachweis eines Administrators an. Verwenden Sie das erforderliche Berechtigungsnachweisformat (weitere Informationen hierzu finden Sie unter „Richtlinien für Workload- und Container-Berechtigungsnachweise“, auf Seite 62).
   - **Failback-Zieleinstellungen:** Geben Sie die folgenden Parameter an:
     - **Reproduktionsmethode:** Wählen Sie den Umfang der Datenreproduktion aus. Wenn Sie *Inkrementell* auswählen, müssen Sie ein Ziel vorbereiten. Weitere Informationen hierzu finden Sie unter „Anfängliche Reproduktionsmethode (Vollständig und Inkrementell)“, auf Seite 65.
     - **Zieltyp:** Wählen Sie *Virtuelles Ziel* aus. Falls Sie nicht über einen Failback-Container verfügen, klicken Sie auf *Container hinzufügen* und inventarisieren Sie einen unterstützten VM-Host. Verwenden Sie dazu einen Administrator-Berechtigungsnachweis.
3. Klicken Sie auf *Speichern und vorbereiten* und überwachen Sie den Fortschritt auf dem Bildschirm „Befehlsdetails“.

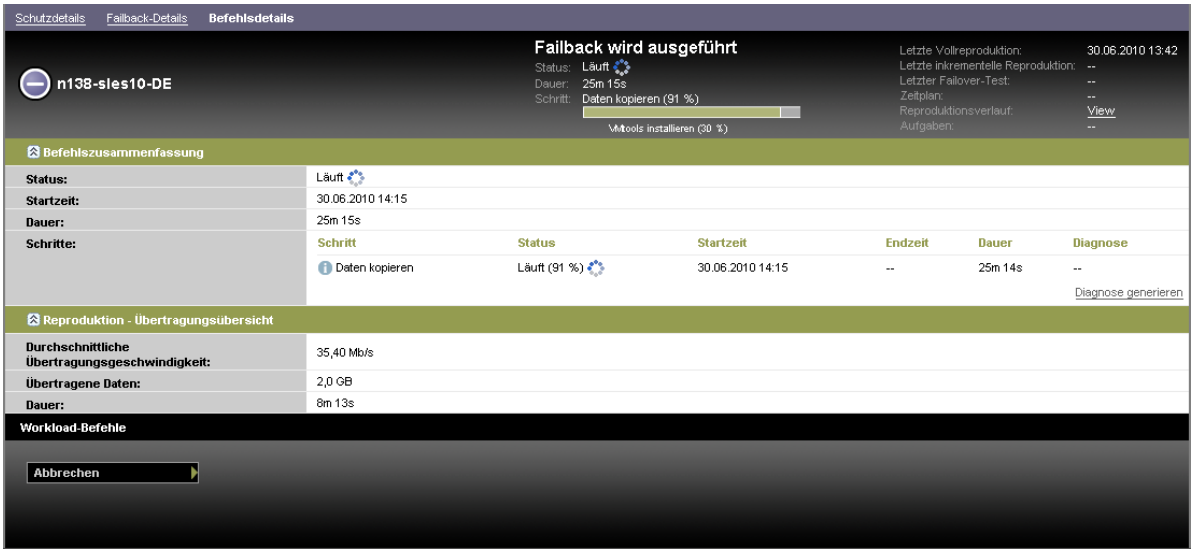
   Nach erfolgreichem Abschluss lädt PlateSpin Protect den Bildschirm „Bereit für Failback“ und fordert Sie auf, die Details des Failback-Vorgangs anzugeben.

4 Konfigurieren Sie die Failback-Details. Weitere Informationen hierzu finden Sie unter „Failback-Details (Workload an VM)“, auf Seite 57.

5 Klicken Sie auf *Speichern und Failback durchführen* und überwachen Sie den Fortschritt auf der Seite „Befehlsdetails“. Weitere Informationen hierzu finden Sie unter Abbildung 4-2.

PlateSpin Protect führt den Befehl aus. Wenn Sie in der Parametergruppe „Post-Failback“ die Option *Erneut schützen nach Failback* ausgewählt haben, wird der Befehl *Erneut schützen* auf der PlateSpin Protect-Weboberfläche angezeigt.

Abbildung 4-2 *Failback-Befehlsdetails*



Failback-Details (Workload an VM)

Failback-Details werden durch drei Parametergruppen dargestellt, die Sie konfigurieren, wenn Sie einen Workload-Failback an eine virtuelle Maschine durchführen.

Tabelle 4-2 *Failback-Details (VM)*

Parametergruppe (Einstellungen)	Details
Failback	**Übertragungsmethode:**) Ermöglicht Ihnen, eine Datenübertragungsmethode und Sicherheit durch Verschlüsselung auszuwählen. Weitere Informationen hierzu finden Sie unter „Übertragungsmethoden“, auf Seite 62.
	Failback-Netzwerk: Ermöglicht Ihnen, den Failback-Datenverkehr über ein dediziertes Netzwerk zu leiten, das zu den in Ihrem VM-Container definierten Netzwerken gehört. Weitere Informationen hierzu finden Sie unter „Netzwerke“, auf Seite 69.
	VM-Datenablage: Ermöglicht Ihnen die Auswahl einer Datenablage, die Ihrem Failback-Container für den Ziel-Workload zugeordnet ist.
	Zu kopierende Volumes: Ermöglicht Ihnen die Auswahl der Volumes für die Neuerstellung auf dem Ziel und die Zuweisung zu einer bestimmten Datenablage.
	Anzuhaltende Dienste/Daemonen: Ermöglicht Ihnen die Auswahl von Windows-Diensten oder Linux-Daemons, die während des Failbacks automatisch angehalten werden sollen. Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“, auf Seite 66.
	Alternative Adresse für Ursprung: Hier kann ggf. eine zusätzliche IP-Adresse für den virtuellen Failover-Computer eingegeben werden. Weitere Informationen hierzu finden Sie unter „Schutz über öffentliche und private Netzwerke durch NAT“, auf Seite 23.
Workload	***Anzahl der CPUs:*** Ermöglicht Ihnen die Angabe der erforderlichen Anzahl der dem Ziel-Workload zugewiesenen vCPUs.
	VM-Arbeitsspeicher: Ermöglicht Ihnen das Zuweisen des erforderlichen RAM zum Ziel-Workload.
	Hostname, Domäne/Arbeitsgruppe: Verwenden Sie diese Optionen, um die Identität und die Domänen-/Arbeitsgruppenzugehörigkeit des Ziel-Workloads zu steuern. Für die Domänenzugehörigkeit ist der Berechtigungsnachweis eines Domänenadministrators erforderlich.
	Netzwerkverbindungen: Verwenden Sie diese Optionen, um die Netzwerkzuordnung des Ziel-Workloads basierend auf den virtuellen Netzwerken des zugrunde liegenden VM-Containers anzugeben.
	Zu ändernde Dienststatus: Ermöglicht Ihnen die Steuerung des Anfangsstatus spezifischer Anwendungsdienste (Windows) oder Daemons (Linux). Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“, auf Seite 66.

Parametergruppe (Einstellungen)	Details
Post-Failback	**Workload erneut schützen:** Verwenden Sie diese Option, wenn Sie planen, den Schutzvertrag für den Ziel-Workload nach der Bereitstellung neu zu erstellen. Dadurch kann der Ereignisverlauf für den Workload kontinuierlich geführt und eine Workload-Lizenz automatisch zugewiesen/festgelegt werden. ◆ ***Erneut schützen nach Failback:*** Wählen Sie diese Option, wenn Sie planen, den Schutzvertrag für den Ziel-Workload neu zu erstellen. Wenn der Failback abgeschlossen ist, steht für den Failback-Workload der Befehl *Erneut schützen* auf der PlateSpin Protect-Weboberfläche zur Verfügung. ◆ ***Kein erneutes Schützen:*** Wählen Sie diese Option, wenn Sie den Schutzvertrag für den Ziel-Workload nicht neu erstellen möchten. Zum Schützen des Failback-Workload nach dessen Abschluss müssen Sie diesen Workload neu inventarisieren und dessen Schutzdetails neu konfigurieren.

4.8.2 Halbautomatischer Failback auf einen physischen Computer

Gehen Sie folgendermaßen vor, um nach einem Failover den Failback eines Workloads an einen physischen Computer durchzuführen. Bei dem physischen Computer kann es sich um die ursprüngliche oder eine neue Infrastruktur handeln.

1. Registrieren Sie den erforderlichen physischen Computer bei Ihrem PlateSpin Protect-Server. Weitere Informationen hierzu finden Sie in „Registrieren von physischen Computern mit PlateSpin Protect für Failback“, auf Seite 69.
2. (Optional: Windows-Plattformen) Führen Sie das PS-Analyseprogramm aus, um festzustellen, ob Treiber fehlen. Weitere Informationen hierzu finden Sie in „Analysieren von Gerätetreibern mit PlateSpin Analyzer (Windows)“, auf Seite 79.
3. Falls das PS-Analyseprogramm fehlende oder nicht kompatible Treiber meldet, laden Sie die erforderlichen Treiber in die Gerätetreiberdatenbank von PlateSpin Protect hoch. Weitere Informationen hierzu finden Sie unter „Verwalten der Gerätetreiber“, auf Seite 81.
4. Wählen Sie im Anschluss an einen Failover den Workload auf der Seite „Workloads“ aus und klicken Sie auf *Failback durchführen*.
5. Legen Sie die folgenden Parametergruppen fest:
   - **Workload-Einstellungen:** Geben Sie den Hostnamen oder die IP-Adresse Ihres Failover-Workloads und den Berechtigungsnachweis eines Administrators an. Verwenden Sie das erforderliche Berechtigungsnachweisformat (weitere Informationen hierzu finden Sie unter „Richtlinien für Workload- und Container-Berechtigungsnachweise“, auf Seite 62).
   - **Failback-Zieleinstellungen:** Geben Sie die folgenden Parameter an:
     - ***Reproduktionsmethode:*** Wählen Sie den Umfang der Datenreproduktion aus.

       Weitere Informationen hierzu finden Sie unter „Anfängliche Reproduktionsmethode (Vollständig und Inkrementell)“, auf Seite 65.
     - ***Zieltyp:*** Wählen Sie die Option *Physische Ziele* und wählen Sie anschließend den physischen Computer aus, den Sie in Schritt 1 registriert haben.

6 Klicken Sie auf *Speichern und vorbereiten* und überwachen Sie den Fortschritt auf dem Bildschirm „Befehlsdetails“.

   Nach erfolgreichem Abschluss lädt PlateSpin Protect den Bildschirm „Bereit für Failback“ und fordert Sie auf, die Details des Failback-Vorgangs anzugeben.

7 Konfigurieren Sie die Failback-Details und klicken Sie anschließend auf *Speichern und Failback durchführen*.

   Überwachen Sie den Fortschritt auf dem Bildschirm „Befehlsdetails“.

4.8.3 Halbautomatischer Failback auf eine virtuelle Maschine

Bei diesem Failback-Typ wird ein Prozess ähnlich dem Halbautomatischer Failback auf einen physischen Computer für ein VM-Ziel durchgeführt, das kein nativ unterstützter VMware-Container ist. Während dieses Prozesses weisen Sie das System an, ein VM-Ziel als physischen Computer zu betrachten.

Ein halbautomatischer Failback auf eine VM wird für folgende Ziel-VM-Plattformen unterstützt:

- XEN unter SLES 10 SP2
- Microsoft Hyper-V Server 2008 (*nicht* R2)

Hinweis: Sie können auch einen halbautomatischen Failback an einem Container vornehmen, der einen vollautomatischen Failback unterstützt (VMware ESX- und DRS-Cluster-Ziele).

4.9 Erneutes Schützen eines Workloads

Durch den Vorgang *Erneut schützen*, dem logischen nächsten Schritt nach einem *Failback* wird der Workload-Schutz-Lebenszyklus abgeschlossen und neu gestartet. Nach einem erfolgreichen Failback-Vorgang wird ein Befehl *Erneut schützen* auf der PlateSpin Protect-Weboberfläche zur Verfügung gestellt und das System wendet die gleichen Schutzdetails an wie bereits bei der ursprünglichen Konfiguration des Schutzvertrags angegeben.

Hinweis: Der Befehl *Erneut schützen* ist nur verfügbar, wenn Sie die Option *Erneut schützen* in den Failback-Details ausgewählt haben. Weitere Informationen hierzu finden Sie unter „Failback“, auf Seite 54.

Der restliche Workflow im Schutz-Lebenszyklus ist der gleiche wie der bei normalen Vorgängen zum Workload-Schutz. Sie können ihn so oft wie erforderlich wiederholen.

5 Grundlagen des Workload-Schutzes

Dieser Abschnitt bietet Informationen zu den verschiedenen funktionalen Bereichen eines Workload-Schutzvertrags.

5.1 Workload-Lizenzverbrauch

Die PlateSpin Protect-Produktlizenz berechtigt Sie für eine bestimmte Anzahl von Workloads zum Schutz durch die Workload-Lizenzierung. Jedesmal, wenn Sie einen zu schützenden Workload hinzufügen, verbraucht das System eine einzelne Workload-Lizenz aus Ihrem Lizenzpool. Sie können eine verbrauchte Lizenz durch Entfernen eines Workloads bis zu maximal fünf Mal wiederherstellen.

Informationen über die Produktlizenzierung und die Lizenzaktivierung finden Sie unter „Produktlizenzierung“, auf Seite 15.

5.2 Richtlinien für Workload- und Container-Berechtigungsnachweise

PlateSpin Protect muss Administratorrechte für Workloads und Container haben. Während des gesamten Workload-Schutz- und -Wiederherstellungs-Workflows werden Sie von PlateSpin Protect aufgefordert, Berechtigungsnachweise in einem bestimmten Format einzugeben.

Tabelle 5-1 *Workload- und Container-Berechtigungsnachweise*

Ermitteln von	Berechtigungsnachweis	Anmerkungen
Alle Windows-Workloads	Berechtigungsnachweise eines lokalen oder Domänen-Administrators.	Verwenden Sie für den Benutzernamen das folgende Format: ◆ Bei Domänenmitgliedscomputern: *Autorität\Prinzipal* ◆ Bei Arbeitsgruppenmitgliedscomputern: *Hostname\Prinzipal*
Windows-Cluster	Berechtigungsnachweis eines Domänen-Administrators.	
Alle Linux-Workloads	Root-äquivalenter Benutzername und Passwort	Andere Konten als das Root-Konto müssen für die Verwendung von `sudo` konfiguriert werden. Weitere Informationen hierzu finden Sie im KB-Artikel 7920711 (http://www.novell.com/support/viewContent.do?externalId=7920711).
VMware ESX 4.1, ESXi 5.0	ESX-Konto mit Administrator-Rolle.	Wenn ESX für die Windows-Domänenauthentifizierung konfiguriert ist, können Sie auch Ihren Berechtigungsnachweis für die Windows-Domäne verwenden.

5.3 Übertragungsmethoden

Eine Übertragungsmethode legt fest, wie Daten eines Ursprungs-Workloads auf einem Ziel reproduziert werden. PlateSpin Protect bietet unterschiedliche Datenübertragungsmöglichkeiten, die vom Betriebssystem des geschützten Workloads abhängen:

- **Blockebene:** Daten werden auf dem Volume auf Blockebene reproduziert. Bei dieser Übertragungsmethode verwendet PlateSpin Protect einen Treiber zum Überwachen von Änderungen auf dem Ursprungs-Workload.
  - **Windows-Systeme:** Für Windows-Systeme verwendet PlateSpin Protect eine blockbasierte Komponente und nutzt den Microsoft Volume Snapshot Service (VSS) mit Anwendungen und Diensten, die VSS unterstützen. Bei der automatischen Installation der blockbasierten Komponente ist ein Neustart des Ursprungs-Workloads erforderlich. Dies ist nicht der Fall, wenn Sie Windows-Cluster mit einem Datentransfer auf Blockebene schützen. Wenn Sie die

Details zum Workload-Schutz konfigurieren, können Sie den Zeitpunkt der Komponenteninstallation auswählen. Wie beim Entfernen eines Workloads ist auch bei der Deinstallation der blockbasierten Komponente ein Neustart erforderlich.

- **Linux-Systeme:** Transfers auf Blockebene auf Linux-Systemen werden von PlateSpin Protect mithilfe einer Datentransferkomponente auf Blockebene durchgeführt und nutzen die LVM-Snapshots, sofern vorhanden (die standardmäßige und empfohlene Option). Weitere Informationen hierzu finden Sie im KB-Artikel 7005872 (http://www.novell.com/support/viewContent.do?externalId=7005872).

  Die im Lieferumfang von PlateSpin Protect enthaltene blockbasierte Linux-Komponente ist für Standard- und Nicht-Debug-Kernels der unterstützen Linux-Distributionen vorkompiliert. Wenn Sie einen nicht-standardmäßigen, benutzerdefinierten oder neueren Kernel haben, können Sie die blockbasierte Komponente gemäß den Spezifikationen Ihres Kernels neu aufbauen. Weitere Informationen hierzu finden Sie im KB-Artikel 7005873 (http://www.novell.com/support/viewContent.do?externalId=7005873).

  Das Bereitstellen bzw. Entfernen der Komponente wird im Hintergrund ausgeführt, beeinträchtigt nicht die Kontinuität und erfordert keinen Benutzereingriff und Neustart.

- **Dateiebene:** Die Daten werden dateiweise reproduziert (nur Windows). Unterstützt mit oder ohne VSS, doch die Verwendung von VSS wird dringend empfohlen.

PlateSpin Protect ermöglicht Ihnen, die Datenreproduktion zu verschlüsseln, um die Übertragung Ihrer Workload-Daten sicherer zu machen. Wenn die Verschlüsselung aktiviert ist, werden über das Netzwerk erfolgende Datentransfers vom Ursprung zum Ziel unter Verwendung von AES (Advanced Encryption Standard) oder 3DES, falls eine FIPS-konforme Verschlüsselung aktiviert ist.

Hinweis: Die Verschlüsselung wirkt sich auf die Leistung aus und kann die Datenübertragungsgeschwindigkeit erheblich beeinträchtigen.

5.4 Schutzebenen

Bei einer Schutzebene handelt es sich um eine benutzerdefinierbare Sammlung von Workload-Schutz-Parametern, die Folgendes definieren:

- Die Häufigkeit und das Wiederholungsmuster von Reproduktionen
- Ob die Datenübertragung verschlüsselt werden soll
- Ob und wie eine Datenkomprimierung durchgeführt werden soll
- Ob die verfügbare Bandbreite während des Datentransfers auf eine bestimmte Durchsatzrate gedrosselt werden soll
- Kriterien, anhand deren das System einen Workload als offline (fehlgeschlagen) erachtet

Eine Schutzebene ist ein wesentlicher Bestandteil jedes Workload-Schutzvertrages. In der Konfigurationsphase eines Workload-Schutzvertrages können Sie eine von mehreren integrierten Schutzebenen auswählen und ihre Attribute entsprechend den Anforderungen des spezifischen Schutzvertrages anpassen.

Sie können benutzerdefinierte Schutzebenen auch vorab erstellen:

1. Klicken Sie auf Ihrer PlateSpin Protect-Weboberfläche auf *Einstellungen* > *Schutzebenen* > *Schutzebene erstellen*.
2. Geben Sie die Parameter für die neue Schutzebene ein:

Name	Geben Sie einen Namen für die Ebene ein.
Inkrementelle Wiederholung	Geben Sie die Häufigkeit der inkrementellen Reproduktionen und das inkrementelle Wiederholungsmuster an. Sie können das Datum direkt in das Feld *Beginn der Wiederholung* eingeben oder auf das Kalendersymbol klicken, um ein Datum auszuwählen. Wählen Sie *Keine* als Wiederholungsmuster, wenn nie eine inkrementelle Reproduktion durchgeführt werden soll.
Vollständige Wiederholung	Geben Sie die Häufigkeit der Vollreproduktionen und das Muster der vollständigen Wiederholung an.
Sperrzeit:	Verwenden Sie diese Einstellungen, um eine Wiederherstellungs-Sperrzeit durchzusetzen (um geplante Wiederherstellungen bei Spitzenauslastungszeiten auszusetzen oder um Konflikte zwischen VSS-bewusster Software und der PlateSpin-Komponente für den VSS-Datentransfer auf Blockebene zu vermeiden). Klicken Sie zum Festlegen einer Sperrzeit auf *Bearbeiten* und wählen Sie ein Wiederholungsmuster (Täglich, Wöchentlich etc.) sowie die Anfangs- und Endzeit der Sperrzeit. **Hinweis**: Die Anfangs- und Endzeiten für die Sperrzeit hängt von der Systemuhr an Ihrem PlateSpin Protect-Server ab.
Komprimierungsgrad	Diese Einstellungen legen fest, ob und wie Workload-Daten vor der Übertragung komprimiert werden. Weitere Informationen hierzu finden Sie in „Datenkomprimierung“, auf Seite 13. Wählen Sie eine der verfügbaren Optionen aus.*Schnell* verbraucht die wenigsten CPU-Ressourcen auf dem Ursprung, geht jedoch mit einer geringeren Komprimierung einher. *Maximal* verbraucht die meisten Ressourcen, erzielt aber auch eine höhere Komprimierung. *Optimal* liegt dazwischen und ist die empfohlene Option.
Bandbreitendrosselung	Diese Einstellungen steuern die Bandbreitendrosselung. Weitere Informationen hierzu finden Sie in „Bandbreitendrosselung“, auf Seite 13. Um die Bandbreite bei Reproduktionen auf eine bestimmte Rate zu drosseln, geben Sie den erforderlichen Durchsatzwert in Mb/s sowie das Zeitmuster ein.
Beizubehaltende Wiederherstellungspunkte	Geben Sie die Anzahl der beizubehaltenden Wiederherstellungspunkte für Workloads an, die diese Schutzebene verwenden. Weitere Informationen hierzu finden Sie unter „Wiederherstellungspunkte“, auf Seite 65.
Workload-Fehler	Geben Sie an, wie viele Versuche zur Workload-Erkennung durchgeführt werden sollen, bis der Workload als fehlgeschlagen erachtet wird.
Workload-Erkennung	Geben Sie das Zeitintervall (in Sekunden) zwischen den Workload-Erkennungsversuchen an.

5.5 Wiederherstellungspunkte

Ein Wiederherstellungspunkt ist ein zu einem bestimmten Zeitpunkt erstellter Snapshot eines Workloads. Er ermöglicht es, einen reproduzierten Workload in einem bestimmten Zustand wiederherzustellen.

Sie können für jeden geschützten Workload bis zu 32 Wiederherstellungspunkte verwenden.

Warnung: Wiederherstellungspunkte, die sich im Laufe der Zeit anhäufen, können dazu führen, dass der Speicherplatz von PlateSpin Protect nicht mehr ausreicht.

5.6 Anfängliche Reproduktionsmethode (Vollständig und Inkrementell)

Bei Workload-Schutz- und Failback-Vorgängen bestimmt der Parameter „Anfängliche Reproduktion“ den Umfang der Daten, die von einem Ursprung auf ein Ziel übertragen werden.

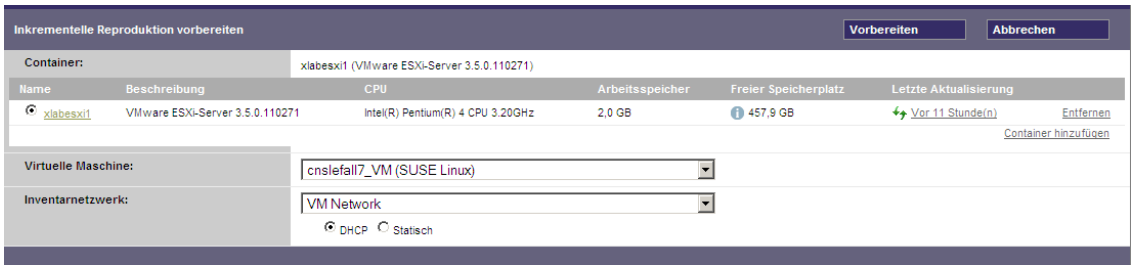
- **Vollständig:** Eine vollständige Volume-Übertragung erfolgt von einem Produktions-Workload auf dessen Reproduktion (der Failover-Workload) oder von einem Failover-Workload auf seine ursprüngliche virtuelle oder physische Infrastruktur.
- **Inkrementell:** Es werden nur Unterschiede vom Ursprung auf dessen Ziel übertragen, vorausgesetzt, sie verfügen über ähnliche Betriebssysteme und Volume-Profile.
  - Beim Schutz: Der Produktions-Workload wird mit einer vorhandenen VM im VM-Container verglichen. Bei der vorhandenen VM kann es sich um eine der folgenden VMs handeln:
    - Die Wiederherstellungs-VM eines bereits geschützten Workloads (wenn die Option *VM löschen* des Befehls *Workload entfernen* deaktiviert wurde).
    - Ein virtueller Computer (VM), der manuell in den VM-Container importiert wurde, wie z. B. ein Workload-VM, der auf einem Wechseldatenträger physisch vom Produktionsstandort auf einen Remote-Wiederherstellungsstandort verschoben wird.

      Weitere Informationen hierzu finden Sie in der VMware-Dokumentation.
  - Während des Failbacks auf eine virtuelle Maschine wird der Failover-Workload mit einer vorhandenen VM in einem Failback-Container verglichen.
  - Während des Failbacks auf einen physischen Computer wird der Failover-Workload mit einem Workload auf der physischen Zielmaschine verglichen, sofern der physische Computer bei PlateSpin Protect registriert ist (siehe „Halbautomatischer Failback auf einen physischen Computer“, auf Seite 58).

Wenn Sie während des Workload-Schutzes und Failbacks auf einen VM-Host *Inkrementell* als anfängliche Reproduktionsmethode wählen, müssen Sie zur Ziel-VM navigieren und diese für eine Synchronisierung mit dem Ursprung des ausgewählten Vorgangs vorbereiten.

1. Fahren Sie mit dem erforderlichen Workload-Befehl fort, z. B. *Workload hinzufügen* oder *Failback.*
2. Wählen Sie für *Anfängliche Reproduktionsmethode* die Option *Inkrementelle Reproduktion*.
3. Klicken Sie auf *Workload vorbereiten*.

   Auf der PlateSpin Protect-Weboberfläche wird die Seite „Inkrementelle Reproduktion vorbereiten“ angezeigt.



4 Wählen Sie den erforderlichen Container, die virtuelle Maschine und das Inventarnetzwerk aus, das für die Kommunikation mit der VM verwendet werden soll.

5 Klicken Sie auf *Vorbereiten*.

Warten Sie, bis der Prozess abgeschlossen wurde und darauf, dass die Benutzerschnittstelle zum ursprünglichen Befehl zurückkehrt, und wählen Sie den vorbereiteten Workload aus.

Hinweis: (Nur Datenreproduktionen auf Blockebene) Die erste inkrementelle Reproduktion dauert deutlich länger als nachfolgende Reproduktionen. Dies liegt daran, dass das System die Volumes auf dem Ursprung und dem Ziel Block für Block miteinander vergleichen muss. Alle nachfolgenden Reproduktionen verlassen sich auf die Änderungen, die bei der Ausführung eines aktiven Workloads von der blockbasierten Komponente erkannt wurden.

5.7 Steuerung von Diensten und Daemons

PlateSpin Protect ermöglicht Ihnen die Steuerung von Diensten und Daemons:

- **Steuerung des Diensts/Daemons:** Während des Datentransfers können Sie Windows-Dienste oder Linux-Daemons, die auf dem Ursprungs-Workload ausgeführt werden, automatisch anhalten. Dadurch wird sichergestellt, dass der Workload in einem stabileren Zustand reproduziert wird als wenn er weiterhin ausgeführt werden würden.

  Beispielsweise sollten Sie bei Windows-Workloads Dienste von Virenschutz-Software oder von VSS-Backup-Software anderer Hersteller anhalten.

  Um mehr Kontrolle über die Linux-Ursprünge während der Reproduktion zu haben, können Sie während jeder Reproduktion benutzerdefinierte Skripte über Ihre Linux-Workloads ausführen. Weitere Informationen hierzu finden Sie unter „Verwenden von Freeze- und Thaw-Skripts für alle Reproduktionen (Linux)“, auf Seite 67.

- **Steuerung des Startstatus/der Ausführungsebene des Ziels:** Sie können den Startstatus (Windows) oder die Ausführungsebene (Linux) von Diensten/Daemons auf dem virtuellen Failover-Computer auswählen. Wenn Sie einen Failover-Vorgang oder einen Failover-Testvorgang ausführen, können Sie angeben, welche Dienste oder Daemons ausgeführt oder gestoppt werden sollen, wenn der Failover-Workload in den Live-Modus wechselt.

  Zu den allgemeinen Diensten, denen Sie den Startstatus () `Deaktiviert` zuweisen sollten, gehören herstellerspezifische Dienste, die an die ihnen zugrunde liegende physische Infrastruktur gebunden und in einer virtuellen Maschine nicht erforderlich sind.

5.8 Verwenden von Freeze- und Thaw-Skripts für alle Reproduktionen (Linux)

Bei Linux-Systemen bietet PlateSpin Protect die Möglichkeit, die benutzerdefinierten Skripts `freeze` und `thaw` automatisch auszuführen. Diese Skripts ergänzen die automatische Daemon-Steuerungsfunktion. `freeze` wird zu Beginn einer Reproduktion ausgeführt, `thaw` am Ende.

Sie sollten diese Funktion in Ergänzung der automatisierten Daemon-Steuerungsfunktion verwenden, die über die Benutzeroberfläche zur Verfügung steht (siehe „Steuerung des Diensts/ Daemons:“, auf Seite 66). Beispielsweise können Sie diese Funktion verwenden, um bestimmte Daemons während der Reproduktion temporär anzuhalten, statt sie herunterzufahren.

Führen Sie zur Implementierung der Funktion folgende Schritte aus, bevor Sie den Linux-Workload-Schutz einrichten:

1. Erstellen Sie die folgenden Dateien:
   - `platespin.freeze.sh`: Ein zu Beginn einer Reproduktion auszuführendes Shell-Skript
   - `platespin.thaw.sh`: Ein zum Abschluss einer Reproduktion auszuführendes Shell-Skript
   - `platespin.conf`: Eine Textdatei, die alle erforderlichen Argumente sowie einen Zeitüberschreitungswert definiert.

     Der Inhalt der Datei `platespin.conf` muss in folgender Syntax angegeben werden:

     ```
     [ServiceControl]
     FreezeArguments=<Argumente>
     ThawArguments=<Argumente>
     TimeOut=<Zeitüberschreitung>
     ```

     Ersetzen Sie *<Argumente>* durch die erforderlichen Befehlsargumente, getrennt durch ein Leerzeichen, und *<Zeitüberschreitung>* durch einen Zeitüberschreitungswert in Sekunden. Wenn kein Wert angegeben wurde, wird die Standard-Zeitüberschreitung (60 Sekunden) verwendet.
2. Speichern Sie die Skripte sowie die `.conf`-Datei auf dem Linux-Ursprungs-Workload in folgendem Verzeichnis:

   `/etc/platespin`

5.9 Volumes

Beim Hinzufügen eines Workloads für den Schutz inventarisiert PlateSpin Protect die Speichermedien Ihres Ursprungs-Workloads und richtet automatisch Optionen auf der PlateSpin Protect-Weboberfläche ein, über die Sie die für den Schutz benötigten Volumes angeben können.

PlateSpin Protect unterstützt mehrere Speichertypen, darunter dynamische Windows-Datenträger, LVM, RAID und SAN.

Bei Linux-Workloads bietet PlateSpin Protect folgende zusätzlichen Funktionen:

- Nicht-Volume-Speicher wie eine Swap-Partition, die mit dem Ursprungs-Workload verknüpft ist, werden im Failover-Workload neu erstellt.

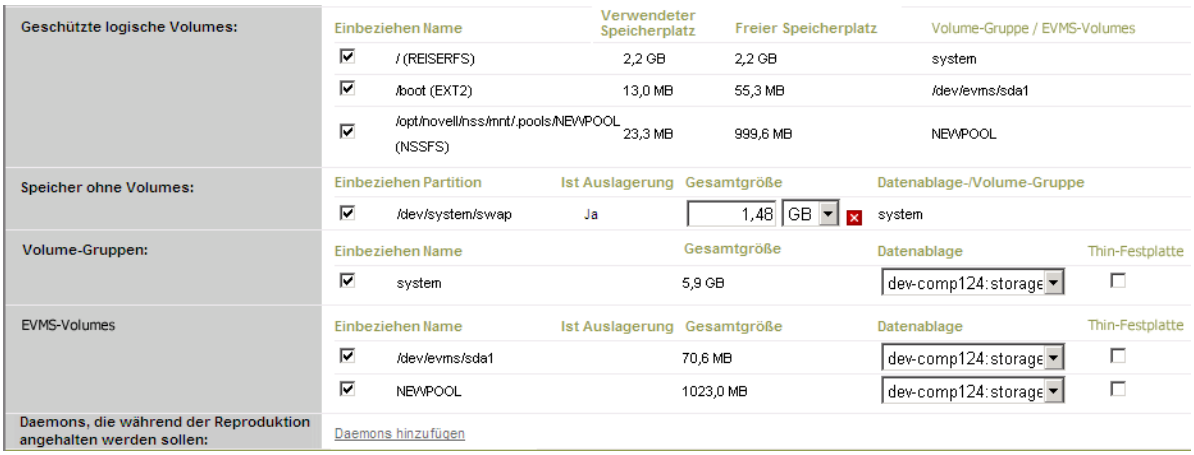
- Das Layout der Volume-Gruppen und logischen Volumes wird beibehalten, sodass Sie es während des Failbacks neu erstellen können.
- (OES 2-Workloads) EVMS-Layouts von Ursprungs-Workloads werden beibehalten und im VM-Container neu erstellt. NSS-Pools werden vom Ursprung in die Wiederherstellungs-VM kopiert.

Die folgenden Abbildungen zeigen die unter „Reproduktionseinstellungen“ festgelegten Parameter für einen Linux-Workload mit mehreren Volumes und zwei logischen Volumes in einer Volume-Gruppe.

Abbildung 5-1 *Volumes, logische Volumes und Volume-Gruppen eines geschützten Linux-Workloads*

Die folgende Abbildung zeigt Volume-Schutz-Optionen eines OES 2-Workloads mit Optionen, die angeben, dass das EVMS-Layout beibehalten und für den Failover-Workload neu erstellt werden soll:

Abbildung 5-2 *Reproduktionseinstellungen, Volume-bezogene Optionen (OES 2-Workload)*



5.10 Netzwerke

PlateSpin Protect ermöglicht Ihnen die Steuerung der Netzwerkidentität Ihres Failover-Workloads und der LAN-Einstellungen, sodass Sie verhindern können, dass der Reproduktionsdatenverkehr den LAN- oder WAN-Datenverkehr beeinträchtigt.

Sie können spezifische Netzwerkeinstellungen in den Details für den Workload-Schutz festlegen, die in unterschiedlichen Phasen des Workload-Schutz- und -Wiederherstellungs-Workflows verwendet werden:

- **Reproduktion:** (Reproduktion-Parameter festgelegt) Zur Trennung des regulären Reproduktionsdatenverkehrs vom Produktionsdatenverkehr.
- **Failover:** (Failover-Parameter festgelegt) Definiert, dass der Failover-Workload beim Wechsel in den Live-Modus Teil des Produktionsnetzwerks wird.
- **Vorbereiten auf Failover:** (Vorbereiten auf Failover-Netzwerkparameter) Für Netzwerkeinstellungen während der optionalen Failover-Vorbereitungsphase.
- **Failover testen:** (Failover testen-Parameter festgelegt) Definiert, dass Netzwerkeinstellungen während einer Failover-Testphase für den Failover-Workload gelten.

5.11 Registrieren von physischen Computern mit PlateSpin Protect für Failback

Wenn die erforderliche Zielinfrastruktur für einen Failback-Vorgang ein physischer Computer ist, müssen Sie ihn in PlateSpin Protect registrieren.

Die Registrierung eines physischen Computers erfolgt durch das Booten des physischen Zielcomputers mit dem entsprechenden PlateSpin-Boot-Image (ISO-Image).

Um ein Boot-ISO-Image zu verwenden, müssen Sie es vom PlateSpin Protect-Bereich unter Novell Downloads (http://download.novell.com) herunterladen, indem Sie eine Suche mit den folgenden Parametern durchführen:

- *Produkt oder Technologie:* `PlateSpin Protect`
- *Version auswählen:* `PlateSpin Protect 10.2`
- *Datumsbereich:* `Alle Datumsangaben`

Verwenden Sie das für Ihren Zielcomputer passende Image:

Tabelle 5-2 *Boot-ISO-Images für physische Zielcomputer*

Dateiname	Anmerkungen
`WindowsFailback.zip` (enthält `WindowsFailback.iso`)	Windows
`WindowsFailback-WinPE3.zip` (enthält `WindowsFailback-WinPE3.iso`)	Zur Verwendung mit einer Hardware, die nicht von `WindowsFailback.zip` unterstützt wird.
`LinuxFailback.zip` (enthält `LinuxFailback.iso`)	Linux-Systeme
`WindowsFailback-Cisco.zip` (enthält `WindowsFailback-Cisco.iso`)	Windows-Systeme auf Cisco-Hardware
`WindowsFailback-Dell.zip` (enthält `WindowsFailback-Dell.iso`)	Windows-Systeme auf Dell-Hardware
`WindowsFailback-Fujitsu.zip` (enthält `WindowsFailback-Fujitsu.iso`)	Windows-Systeme auf Fujitsu-Hardware

Nachdem Sie die erforderliche Datei heruntergeladen haben, dekomprimieren Sie diese und speichern Sie die extrahierte ISO-Datei.

- Abschnitt 5.11.1, „Registrieren physischer Zielcomputer“, auf Seite 70

5.11.1 Registrieren physischer Zielcomputer

1. Brennen Sie das entsprechende Image auf eine CD oder speichern Sie es auf einem Medium, von dem Ihr Ziel booten kann.
2. Stellen Sie sicher, dass der Netzwerk-Switch-Anschluss, der mit dem Ziel verbunden ist, auf *Autom. Vollduplex* eingestellt ist.

   Da die Windows-Version des Boot-CD-Images nur die Funktion *Vollduplex automatisch aushandeln* unterstützt, wird hierdurch sichergestellt, dass keine Konflikte in den Duplexeinstellungen bestehen.
3. Verwenden Sie die Boot-CD zum Booten des physischen Zielcomputers und warten Sie, bis das Befehlszeilenfenster geöffnet wird.

   (Nur Windows) Warten Sie, bis die Befehlszeilenfenster *REGISTERMACHINE* und *Recovery Console* geöffnet sind. Verwenden Sie das Befehlszeilenfenster von REGISTERMACHINE. Weitere Informationen zum Befehlszeilenprogramm „Recovery Console“ finden Sie unter „Verwenden des Befehlszeilenprogramms „Recovery Console“ (Windows)“, auf Seite 71.
4. (Nur Linux) Geben Sie bei 64-Bit-Systemen im anfänglichen Bootprompt Folgendes ein:
   - `ps64` (für Systeme mit bis zu 512 MB RAM)
   - `ps64_512m` (für Systeme mit mehr als 512 MB RAM)
5. Drücken Sie die Eingabetaste.
6. Geben Sie nach der Eingabeaufforderung den Hostnamen oder die IP-Adresse Ihres PlateSpin Protect-Server-Hosts ein.

7 Geben Sie den Administrator-Berechtigungsnachweis für den PlateSpin Protect Server-Host einschließlich einer Zertifizierungsstelle an. Verwenden Sie für das Benutzerkonto das folgende Format:

*Domäne**Benutzername* oder *Hostname**Benutzername*

Verfügbare Netzwerkkarten werden anhand ihrer MAC-Adressen erkannt und angezeigt.

8 Wenn DHCP auf der zu verwendenden NIC verfügbar ist, drücken Sie die Eingabetaste, um fortzufahren. Wenn DHCP nicht verfügbar ist, geben Sie an, dass die erforderliche NIC mit einer statischen IP-Adresse konfiguriert werden soll.

9 Geben Sie einen Hostnamen für den physischen Computer ein oder drücken Sie die Eingabetaste, um die Standardwerte zu übernehmen.

10 Wenn Sie dazu aufgefordert werden, anzugeben, ob Sie HTTPS verwenden möchten, müssen Sie `J` eingeben, wenn Sie SSL aktiviert haben, oder `N`, wenn dies nicht der Fall ist.

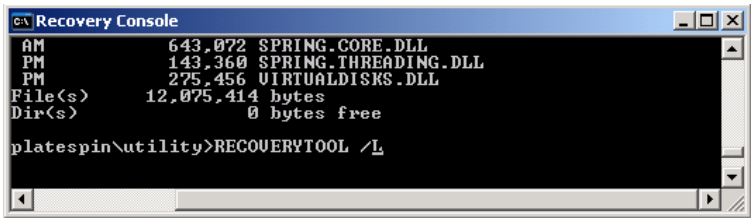
Nach kurzer Zeit sollte der physische Computer in den Failback-Einstellungen der PlateSpin Protect-Weboberfläche verfügbar sein.

Verwenden des Befehlszeilenprogramms „Recovery Console“ (Windows)

Das Befehlszeilenprogramm „Recovery Console“ ermöglicht es Ihnen, Windows-Gerätetreiber dynamisch auf dem Zielcomputer einzubinden, ohne den gesamten Registrierungsprozess für das physische Ziel neu starten zu müssen.

Das Dienstprogramm wird beim ersten Versuch, vom Windows-Boot-Image zu starten, in einem zweiten Befehlszeilenfenster geladen (siehe Schritt 3 auf Seite 70).

Geben Sie zur Verwendung des Recovery-Tools den Befehlsnamen `RECOVERYTOOL`, gefolgt vom anwendbaren Parameter, im Recovery Console-Fenster ein.



Sie können folgende Parameter verwenden:

- `/L` - zum Auflisten aller auf dem Ziel-Betriebssystem installierten Treiberdienste
- `/J` - zum Einbinden von Treibern in das Ziel-Betriebssystem

Sie können angeben, ob die Treiber vom PlateSpin Protect-Server oder von einem lokalen Pfad heruntergeladen werden sollen. Wenn Sie einen lokalen Pfad verwenden möchten, sollten Sie mehrere Treiber für dasselbe Gerät gruppieren. Wenn Sie Treiber vom PlateSpin Protect-Server herunterladen möchten, fordert das Dienstprogramm Sie auf anzugeben, welchen Treiber Sie verwenden möchten (falls es mehrere gibt).

Einfügen von Treibern in das PlateSpin-Boot-Image (Linux)

Sie können mithilfe eines benutzerdefinierten Dienstprogramms weitere Linux-Gerätetreiber zu einem Paket zusammenstellen und in das PlateSpin-Boot-Image einfügen, bevor Sie es auf eine CD brennen:

1 Besorgen Sie die erforderlichen `*.ko`-Treiberdateien oder kompilieren Sie sie.

Wichtig: Stellen Sie sicher, dass die Treiber mit dem in der ISO-Datei (`2.6.16.21-0.8-default`) enthaltenen Kernel kompatibel sind und zur Architektur des Zielcomputers passen.

2 Mounten Sie das Image in einem Linux-Computer (`root`-Berechtigungsnachweis erforderlich). Verwenden Sie die folgende Befehlssyntax:

```
mount –o loop <Pfad-zu-ISO> <Mount-Punkt>
```

3 Kopieren Sie das Skript `rebuildiso.sh`, das sich im Unterverzeichnis `/tools` der gemounteten ISO-Datei befindet, in ein temporäres Arbeitsverzeichnis. Wenn Sie fertig sind, entladen Sie die ISO-Datei. (Führen Sie dazu den Befehl `unmount <Mount-Punkt>` aus.)

4 Erstellen Sie ein weiteres Arbeitsverzeichnis für die erforderlichen Treiberdateien und speichern Sie diese in diesem Verzeichnis.

5 Führen Sie in dem Verzeichnis, in dem Sie das Skript `rebuildiso.sh` gespeichert haben, folgenden Befehl als `Root`-Benutzer aus:

```
./rebuildiso.sh –i <ISO-Datei> -d <Treiber-Verzeichnis> -m i586|x86_64
```

Wenn der Vorgang abgeschlossen ist, enthält die ISO-Datei die zusätzlichen Treiber.

5.12 Themen zu erweitertem Workload-Schutz

- Abschnitt 5.12.1, „Schützen von Windows-Clustern“, auf Seite 72
- Abschnitt 5.12.2, „Linux-Failback auf einen paravirtualisierten virtuellen Computer in XEN auf SLES“, auf Seite 73
- Abschnitt 5.12.3, „Verwenden von Workload-Schutz-Funktionen über die PlateSpin Protect-Web-Services-API“, auf Seite 77

5.12.1 Schützen von Windows-Clustern

PlateSpin Protect unterstützt den Schutz der Geschäftsdienste eines Microsoft Windows-Clusters. Folgende Cluster-Technologien werden unterstützt:

- Auf Windows 2003 Server basierender Windows-Cluster-Server (*Single-Quorum Device Cluster*-Modell)
- Auf Windows 2008 Server basierendes Microsoft-Failover-Cluster (Modelle *Knoten- und Datenträgermehrheit* und *Keine Mehrheit: Nur Datenträger*)

Der Schutz eines Clusters wird durch inkrementelle Reproduktionen der Änderungen auf dem aktiven Knoten erreicht, die an ein virtuelles Einzelknoten-Cluster übertragen werden, das Sie während der Fehlerbehebung an der Ursprungsinfrastruktur verwenden können.

Der Umfang der Unterstützung von Cluster-Migrationen in der aktuellen Version ist von folgenden Bedingungen abhängig:

- Wenn Sie einen Vorgang des Typs *Workload hinzufügen* durchführen, müssen Sie über die IP-Adresse des Clusters (*Virtuelle IP-Adresse*) den aktiven Knoten identifizieren, d. h. den Knoten, der zurzeit die Quorum-Ressource des Clusters besitzt. Wenn Sie die IP-Adresse eines einzelnen Knotens angeben, wird dieser Knoten als regulärer Windows-Workload inventarisiert (das Cluster bleibt unerkannt).
- Eine Quorum-Ressource eines Clusters muss zu der Ressourcengruppe (Dienst) des Clusters gehören, die geschützt wird.

Wenn ein Knoten-Failover zwischen zwei inkrementellen Reproduktionen eines geschützten Clusters auftritt, generiert PlateSpin Protect ein Schutzereignis. Falls das Profil des neuen aktiven Knotens dem des ausgefallenen aktiven Knotens entspricht, wird der Zeitplan für den Schutz fortgesetzt, anderenfalls schlägt der Befehl fehl. Die Profile der Clusterknoten werden als ähnlich erachtet, wenn:

- sie dieselbe Anzahl an Volumes haben
- alle Volumes auf allen Knoten exakt dieselbe Größe haben
- sie eine identische Anzahl an Netzwerkverbindungen haben

Um ein Windows-Cluster zu schützen, gehen Sie nach dem gleichen Ablaufplan wie für den normalen Workload-Schutz vor (siehe „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“, auf Seite 43).

Beim Failback bietet PlateSpin Protect eine Validierung, die Ihnen hilft, sicherzustellen, dass auf dem Ziel freigegebene Volume-Layouts beibehalten werden. Stellen Sie sicher, dass Sie die Volumes ordnungsgemäß zuordnen.

5.12.2 Linux-Failback auf einen paravirtualisierten virtuellen Computer in XEN auf SLES

Sie können ein Failback auf einen paravirtualisierten virtuellen Computer in XEN auf SLES (nur Version 10) durchführen. Diese Migration erfolgt indirekt in zwei Phasen. Die paravirtualisierte VM muss zuerst in eine vollständig virtualisierte VM umgewandelt und später wieder zurückverwandelt werden. Zur Umwandlung des virtuellen Computers wird ein im PlateSpin Boot-ISO-Image enthaltenes Dienstprogramm (`xmpsadministrator`-) verwendet.

Das Verfahren variiert leicht, je nachdem, ob das Ziel eine neue oder eine vorhandene paravirtualisierte VM ist.

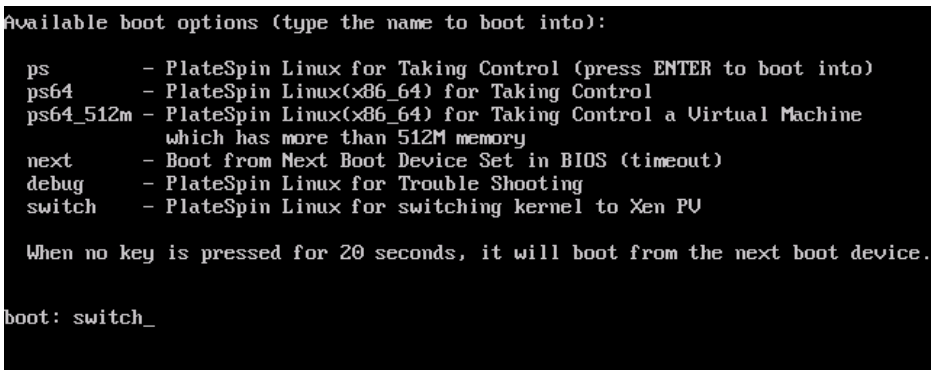
- „Linux-Failback auf eine neue paravirtualisierte VM“, auf Seite 74
- „Linux-Failback auf eine vorhandene paravirtualisierte VM“, auf Seite 76

Linux-Failback auf eine neue paravirtualisierte VM

1. Kopieren Sie das PlateSpin Linux Boot-ISO-Image in XEN am SLES-Zielserver. Weitere Informationen hierzu finden Sie unter Tabelle 5-2, „Boot-ISO-Images für physische Zielcomputer“, auf Seite 70.
2. Starten Sie den Virtual Machine Manager und erstellen Sie eine vollständig virtualisierte VM:
   - **2a** Wählen Sie die Option *I need to install an operating system* (Ich muss ein Betriebssystem installieren).
   - **2b** Wählen Sie eine geeignete Größe für das Datenträger-Image (die Datenträgergröße sollte größer oder gleich der Datenträgergröße des virtuellen Failover-Computers sein).
   - **2c** Wählen Sie das Boot-ISO-Image als Installationsquelle.

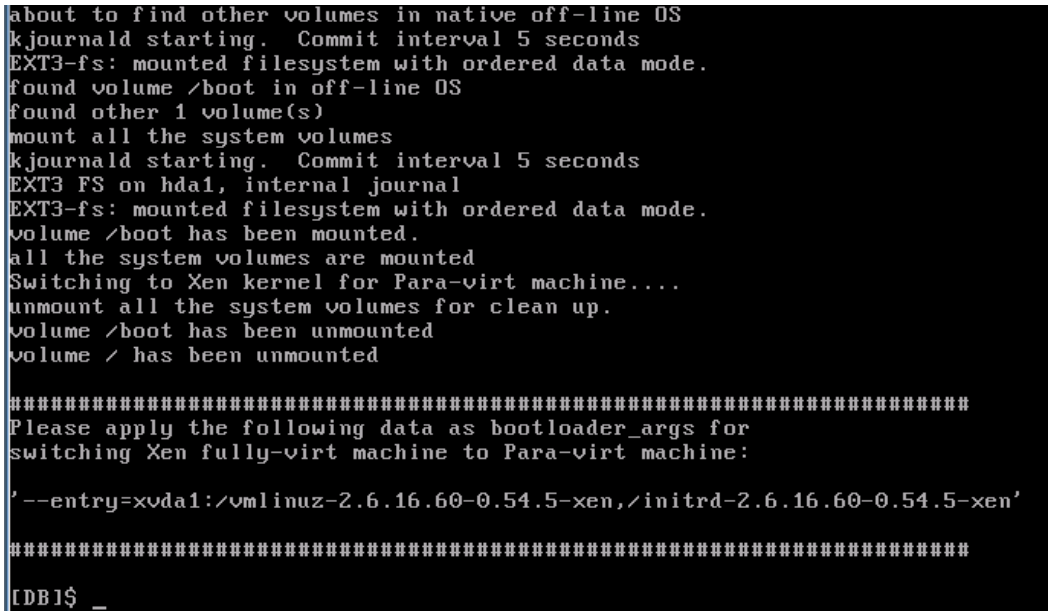
     Die VM bootet in der PlateSpin-Betriebssystemumgebung, die in den Einstellungen für das *Failback auf den physischen Computer* angegeben ist.
3. Führen Sie die Failback-Prozedur durch. Weitere Informationen hierzu finden Sie in „Halbautomatischer Failback auf einen physischen Computer“, auf Seite 58.

   Wenn der Vorgang abgeschlossen ist, sollte die VM als vollständig virtualisierter Computer voll funktionsfähig sein.
4. Starten Sie die VM neu und achten Sie darauf, dass sie immer noch in die PlateSpin-Betriebssystemumgebung startet.



5. Geben Sie an der `boot:`-Eingabeaufforderung `switch` ein und drücken Sie die Eingabetaste.

   Dadurch wird das Betriebssystem wieder als bootfähige paravirtualisierte Maschine konfiguriert. Wenn der Vorgang abgeschlossen ist, sollte die Ausgabe ähnlich wie die folgende aussehen:



Beachten Sie die Bootloader-Argumente im letzten Abschnitt der Ausgabe:

```
Please apply the following data as bootloader_args for
switching Xen fully-virt machine to Para-virt machine:

'-entry=xvda1:/vmlinuz-2.6.16.60-0.54.5-xen, /initrd-2.6.16.60-0.54.5-xen'
```

Diese werden vom `xmps`-Dienstprogramm verwendet, um den Speicherort des Kernels und des `initrd`-Images einzurichten, von dem aus die paravirtualisierte Maschine startet.

6 Schalten Sie die virtuelle Maschine aus:

```
[DB]$ poweroff
```

7 Melden Sie sich bei XEN am SLES-Server als `root` an und hängen Sie das PlateSpin Linux Boot-ISO-Image ein (das Befehlsbeispiel geht davon aus, dass das ISO-Image in das Verzeichnis `/root` kopiert wurde):

```
# mkdir /mnt/ps
# mount -o loop /root/linuxfailback.iso /mnt/ps
```

8 Führen Sie das `xmps`-Dienstprogramm aus, um eine paravirtualisierte VM auf der Basis der Konfiguration der vollständig virtualisierten VM zu erstellen:

```
# /mnt/ps/tools/xmps --pv --vm_name=SLES10-FV --new_vm_name=SLES10-PV --
bootloader_args="--entry=xvda1:/vmlinuz-2.6.16.60-0.54.5-xen, /initrd-
2.6.16.60-0.54.5-xen"
```

Geben Sie folgendes im Dienstprogramm ein:

- den Namen der vollständig virtualisierten VM, auf der die Konfiguration der paravirtualisierten Maschine basieren soll (`SLES10-FV`)
- den Namen der zu erstellenden virtuellen Maschine (`SLES10-PV`)
- die Bootloader-Argumente der paravirtualisierten Maschine `"--bootloader_args"` (dargestellt unter Schritt 5)

Wenn bereits eine VM mit demselben Namen wie der unter `new_vm_name` angegebene vorhanden ist, schlägt das `xmps`-Dienstprogramm fehl.

Die neu erstellte paravirtualisierte VM (SLES10-PV) sollte nun im Virtual Machine Manager verfügbar und bereit zum Einschalten sein. Die entsprechende vollständig virtualisierte Maschine ist deaktiviert und kann nicht gebootet werden. Diese VM kann sicher gelöscht werden (nur die VM-Konfiguration wird entfernt).

9 Entladen Sie das PlateSpin Linux Boot-ISO-Image:

```
# umount /mnt/ps
```

Linux-Failback auf eine vorhandene paravirtualisierte VM

1 Kopieren Sie das PlateSpin Linux Boot-ISO-Image in XEN am SLES-Zielserver. Weitere Informationen hierzu finden Sie unter Tabelle 5-2, „Boot-ISO-Images für physische Zielcomputer“, auf Seite 70.

2 Melden Sie sich bei XEN am SLES-Server als root an und hängen Sie das PlateSpin Linux Boot-ISO-Image ein:

```
# mkdir /mnt/ps
# mount -o loop /root/linuxfailback.iso /mnt/ps
```

3 Führen Sie das xmps-Dienstprogramm aus, um eine vollständig virtualisierte VM auf der Basis der Konfiguration der paravirtualisierten VM (dem beabsichtigten Failback-Ziel) zu erstellen:

```
# /mnt/ps/tools/xmps --fv --vm_name=SLES10-PV --new_vm_name=SLES10-FV --
bootiso=/root/linuxfailback.iso
```

Geben Sie folgendes im Dienstprogramm ein:

- den Namen der vorhandenen paravirtualisierten Maschine (SLES10-PV), die das beabsichtigte Failback-Ziel ist
- den Namen der vorübergehend vollständig virtualisierte Maschine (SLES10-FV), die für den zweistufigen Failback-Vorgang erstellt werden soll
- den vollständigen Pfad des Boot-ISO-Images (unter der Annahme, dass sich die ISO-Datei unter /root: /root/linuxfailback.iso befindet)

Wenn bereits eine VM mit demselben Namen wie der unter new_vm_name angegebene vorhanden ist, schlägt das xmps-Dienstprogramm fehl.

Die neu erstellte vollständig virtualisierte VM (SLES10-FV) sollte nun im Virtual Machine Manager verfügbar sein.

4 Schalten Sie die neu erstellte vollständig virtualisierte Maschine (SLES10-FV) ein.

Die VM bootet in der PlateSpin-Betriebssystemumgebung, die in den Einstellungen für das *Failback auf den physischen Computer* angegeben ist.

5 Führen Sie die Failback-Prozedur durch. Weitere Informationen hierzu finden Sie in „Halbautomatischer Failback auf einen physischen Computer“, auf Seite 58.

6 Starten Sie die VM neu, führen Sie switch aus und konfigurieren Sie den Workload erneut, wie unter „Linux-Failback auf eine neue paravirtualisierte VM“, auf Seite 74 beschrieben (nur von Schritt 4 bis Schritt 9).

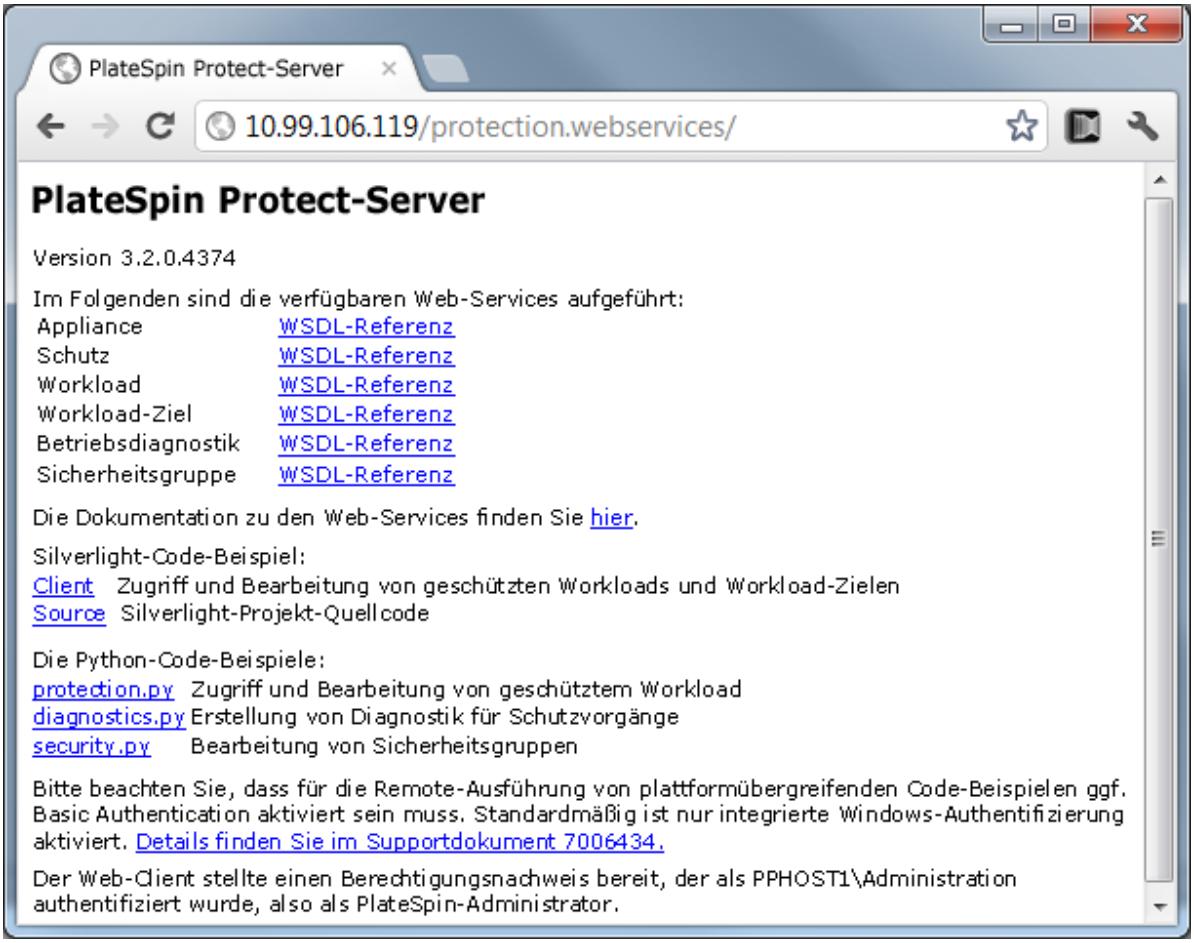
5.12.3 Verwenden von Workload-Schutz-Funktionen über die PlateSpin Protect-Web-Services-API

Mithilfe der `protection.webservices`-API können Sie Workload-Schutz-Funktionen programmatisch von Ihren Anwendungen aus verwenden. Sie können alle Programmier- oder Skriptsprachen verwenden, die Web-Services unterstützen.

`http://`*<Hostname | IP-Adresse>*`/protection.webservices`

Ersetzen Sie *<Hostname | IP-Adresse>* durch den Hostnamen oder die IP-Adresse Ihres PlateSpin Protect Server-Hosts.

Abbildung 5-3 *Die erste Seite der API der Schutz-Webdienste*



Wenn Sie Skripte für häufige Workload-Schutz-Vorgänge schreiben möchten, verwenden Sie die in Python geschriebenen Referenzbeispiele als Orientierungshilfe. Eine Microsoft Silverlight-Anwendung wird zusammen mit dem Quellcode ebenfalls zu Referenzzwecken bereitgestellt.

6 Hilfswerkzeuge für die Arbeit mit physischen Computern

Im Lieferumfang von PlateSpin Protect sind Werkzeuge enthalten, die für die Verwendung bei der Arbeit mit physischen Computern als Failback-Ziele vorgesehen sind.

6.1 Analysieren von Gerätetreibern mit PlateSpin Analyzer (Windows)

Verwenden Sie PlateSpin Analyzer, um potenzielle Treiberprobleme zu ermitteln, und beheben Sie sie, bevor Sie auf einem physischen Computer ein Workload-Failback durchführen.

Hinweis: PlateSpin Analyzer unterstützt zurzeit nur Windows-Workloads.

1. Starten Sie auf dem PlateSpin Protect Server-Host das Programm `Analyzer.Client.exe`, das sich in folgendem Verzeichnis befindet:

   `\Programme\PlateSpin Protect Server\PlateSpin Analyzer`

2. Stellen Sie sicher, dass als Netzwerk *Standard* ausgewählt ist, und wählen Sie den erforderlichen Computer in der Dropdown-Liste *Alle Computer* aus.
3. (Optional) Beschränken Sie den Umfang der Computer auf eine bestimmte Sprache, um die Analysedauer zu verkürzen.
4. Klicken Sie auf *Analysieren*.

   Je nach Anzahl der inventarisierten Workloads, die Sie ausgewählt haben, kann die Analyse zwischen wenigen Sekunden und mehreren Minuten dauern.

Analysierte Server werden im linken Teilfenster aufgeführt. Wählen Sie einen Server aus, um die Testergebnisse im rechten Teilfenster anzuzeigen. Die Testergebnisse können sich aus allen oder einigen der folgenden Elemente zusammensetzen:

Tabelle 6-1 *Statusmeldungen in PlateSpin Analyzer-Testergebnissen*

Ergebnis	Beschreibung
Bestanden	Der Computer hat die PlateSpin Analyzer-Tests bestanden.
Warnhinweis	Ein oder mehrere Tests haben Warnmeldungen für den Computer zurückgegeben, die auf potenzielle Migrationsprobleme hinweisen. Klicken Sie auf den Hostnamen, um die Details dazu anzuzeigen.
Fehlgeschlagen	Ein oder mehrere Tests für diesen Computer sind fehlgeschlagen. Klicken Sie auf den Hostnamen, um die Details anzuzeigen und weitere Informationen zu erhalten.

Die Registerkarte *Zusammenfassung* enthält eine Liste mit den analysierten und nicht analysierten Computern sowie den Computern, die den Test bestanden oder nicht bestanden haben bzw. bei denen eine Fehlermeldung ausgegeben wurde.

Die Registerkarte *Testergebnisse* bietet folgende Informationen:

Tabelle 6-2 *Registerkarte „Testergebnisse“ von PlateSpin Analyzer*

Abschnitt	Details
System Test	Bestätigt, dass der Computer die Mindestanforderungen an Hardware und Betriebssystem erfüllt.
Hardware-Unterstützung	Prüft die Hardware-Kompatibilität des Workloads.
Zielhardware-Unterstützung	Prüft die Hardware-Kompatibilität bezüglich der Verwendung als physischen Zielcomputer.
Softwaretest	Sucht nach Anwendungen und Datenbanken, die für den Live-Transfer geschlossen werden müssen, um die Transaktionsintegrität zu gewährleisten.
Test auf inkompatible Anwendungen	Stellt sicher, dass Anwendungen, die den Migrationsprozess bekanntermaßen stören, nicht auf dem System installiert sind. Diese Anwendungen werden in der Datenbank für inkompatible Anwendungen gespeichert. Wählen Sie zum Hinzufügen, Löschen oder Bearbeiten von Einträgen in dieser Datenbank *Inkompatible Anwendung* im Menü *Werkzeuge*.

Die Registerkarte *Eigenschaften* enthält detaillierte Informationen über einen ausgewählten Computer.

6.2 Verwalten der Gerätetreiber

PlateSpin Protect wird mit einer Bibliothek an Gerätetreibern ausgeliefert. Die passenden Treiber werden automatisch auf den Ziel-Workloads installiert. Verwenden Sie das Dienstprogramm PlateSpin Analyzer, um zu prüfen, ob die erforderlichen Treiber verfügbar sind. Weitere Informationen hierzu finden Sie unter „Analysieren von Gerätetreibern mit PlateSpin Analyzer (Windows)“, auf Seite 79.

Falls PlateSpin Analyzer feststellt, dass Treiber fehlen oder nicht kompatibel sind, oder falls Sie für Ihre Zielinfrastruktur bestimmte Treiber benötigen, müssen Sie möglicherweise Treiber zur PlateSpin Protect-Treiberdatenbank hinzufügen (heraufladen).

6.2.1 Verpacken von Gerätetreibern für Windows-Systeme

So verpacken Sie Ihre Windows-Gerätetreiber zum Heraufladen in die PlateSpin Protect-Treiberdatenbank:

1. Bereiten Sie alle abhängigen Gerätetreiberdateien (`*.sys`, `*.inf`, `*.dll` usw.) für Ihre Zielinfrastruktur und Ihr Zielgerät vor. Wenn Sie herstellerspezifische Treiber als `.zip`-Archiv oder als Programmdatei erhalten haben, extrahieren Sie diese zuerst.
2. Speichern Sie die Treiberdateien in separaten Ordnern mit einem eigenen Ordner pro Gerät.

Die Treiber können nun hochgeladen werden. Weitere Informationen hierzu finden Sie in „Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin Protect“, auf Seite 82.

Hinweis: Damit eine problemlose Durchführung Ihres Schutzauftrags und des Ziel-Workloads gewährleistet ist, sollten Sie nur digital signierte Treiber für die folgenden Systeme hochladen:

- Alle 64-Bit-Windows-Systeme
- 32-Bit-Versionen von Windows Vista- und Windows Server 2008 und Windows 7-Systemen

---

6.2.2 Verpacken von Gerätetreibern für Linux-Systeme

Wenn Sie ein Paket Ihrer Linux-Gerätetreiber erstellen möchten, um sie in die PlateSpin Protect-Treiberdatenbank heraufzuladen, können Sie hierfür ein benutzerdefiniertes Dienstprogramm verwenden, das in Ihrem Linux ISO-Boot-Image enthalten ist. Weitere Informationen hierzu finden Sie unter Tabelle 5-2, „Boot-ISO-Images für physische Zielcomputer“, auf Seite 70.

1. Erstellen Sie auf einer Linux-Workstation ein Verzeichnis für Ihre Gerätetreiberdateien. Alle Treiber in dem Verzeichnis müssen für denselben Kernel und dieselbe Architektur sein.
2. Laden Sie das Boot-Image herunter und mounten Sie es.

   Geben Sie beispielsweise in der Annahme, dass das ISO-Image in das Verzeichnis `/root` kopiert wurde, folgende Befehle ein:

   ```
   # mkdir /mnt/ps
   # mount -o loop /root/linuxfailback.iso /mnt/ps
   ```

3 Kopieren Sie vom Unterverzeichnis `/tools` des gemounteten ISO-Images das Archiv `packageModules.tar.gz` in ein anderes Arbeitsverzeichnis und extrahieren Sie es.

   Wenn sich beispielsweise die `.gz`-Datei in Ihrem aktuellen Arbeitsverzeichnis befindet, geben Sie folgenden Befehl ein:

   ```
   tar -xvzf packageModules.tar.gz
   ```

4 Wechseln Sie zum Arbeitsverzeichnis und führen Sie folgenden Befehl aus:

   `./PackageModules.sh –d <Pfad-zum-Treiberverzeichnis> -o <Paketname>`

   Ersetzen Sie *<Pfad-zum-Treiberverzeichnis>* mit dem aktuellen Pfad zum Verzeichnis, in dem Sie Ihre Treiberdateien gespeichert haben, und *<Paketname>* mit dem aktuellen Paketnamen im folgenden Format:

   `Treibername-Treiberversion-Dist-Kernelversion-Arch``.pkg`

   Beispiel: `bnx2x-1.48.107-RHEL4-2.6.9-11.EL-i686.pkg`

Das Paket kann nun hochgeladen werden. Weitere Informationen hierzu finden Sie unter „Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin Protect“, auf Seite 82.

6.2.3 Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin Protect

Verwenden Sie den PlateSpin Treibermanager zum Hochladen von Gerätetreibern in die Treiberdatenbank.

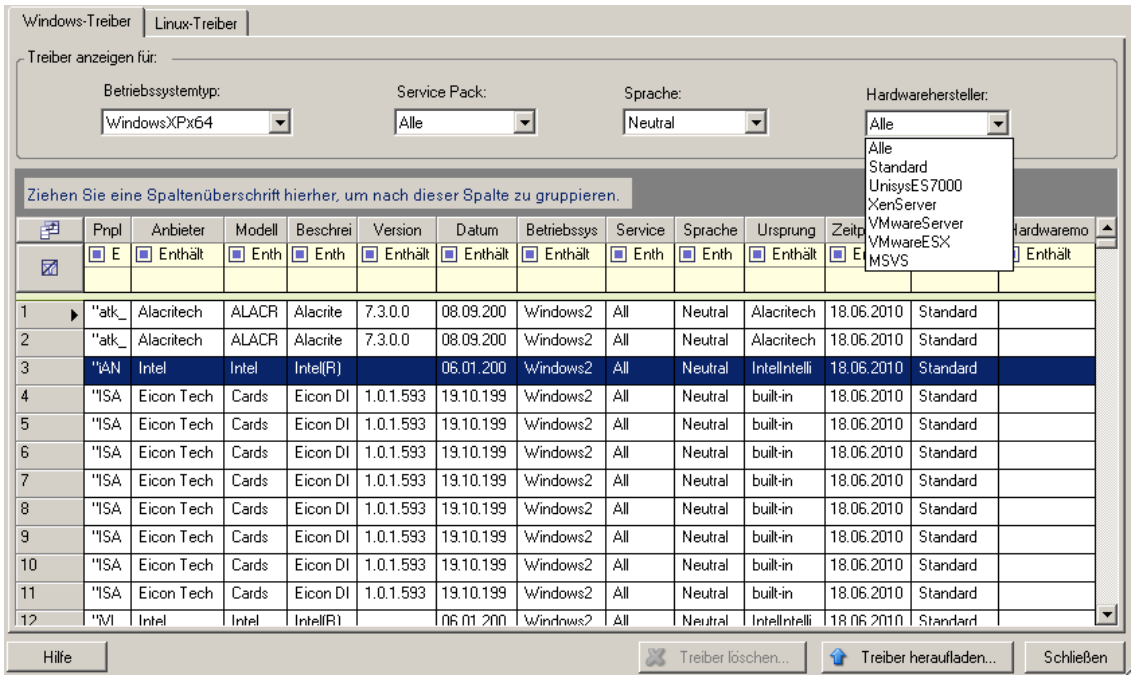
Hinweis: Beim Hochladen von Treibern überprüft PlateSpin Protect nicht, ob der Treiber zum ausgewählten Betriebssystem bzw. den Bit-Spezifikationen passt. Laden Sie nur Treiber hoch, die für Ihre Zielinfrastruktur geeignet sind.

- „Upload-Prozedur für Gerätetreiber (Windows)“, auf Seite 82
- „Upload-Prozedur für Gerätetreiber (Linux)“, auf Seite 84

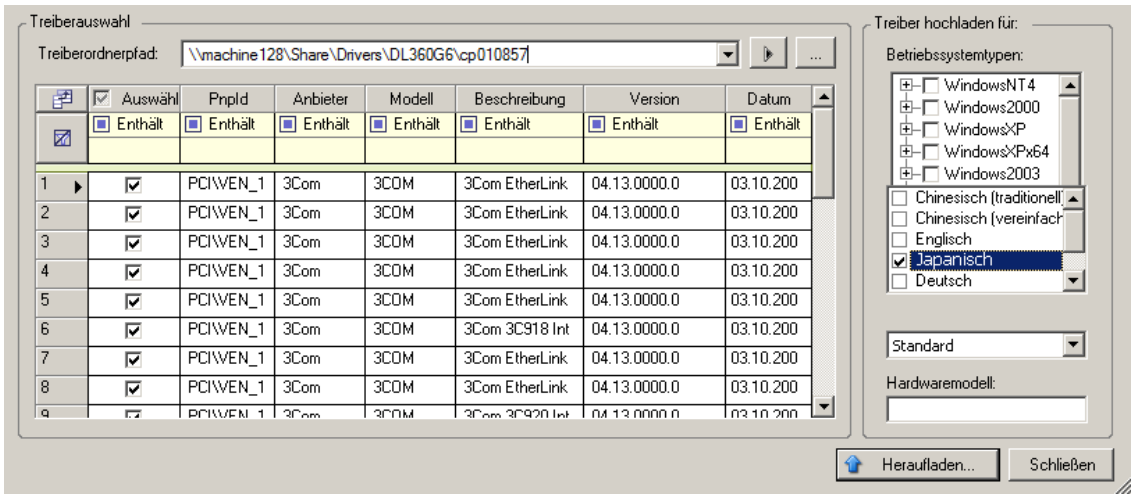
Upload-Prozedur für Gerätetreiber (Windows)

1 Beziehen Sie die erforderlichen Gerätetreiber und bereiten Sie diese vor. Weitere Informationen hierzu finden Sie in Verpacken von Gerätetreibern für Windows-Systeme.

2 Starten Sie auf dem PlateSpin Protect Server-Host unter `Programme\PlateSpin Protect Server\DriverManager` das Programm `DriverManager.exe` und wählen Sie die Registerkarte *Windows-Treiber* aus.



3 Klicken Sie auf *Treiber hochladen*, navigieren Sie zu dem Ordner, der die erforderlichen Treiberdateien enthält, und wählen Sie den zutreffenden Betriebssystemtyp, die Sprache und die Hardwarehersteller-Optionen aus.



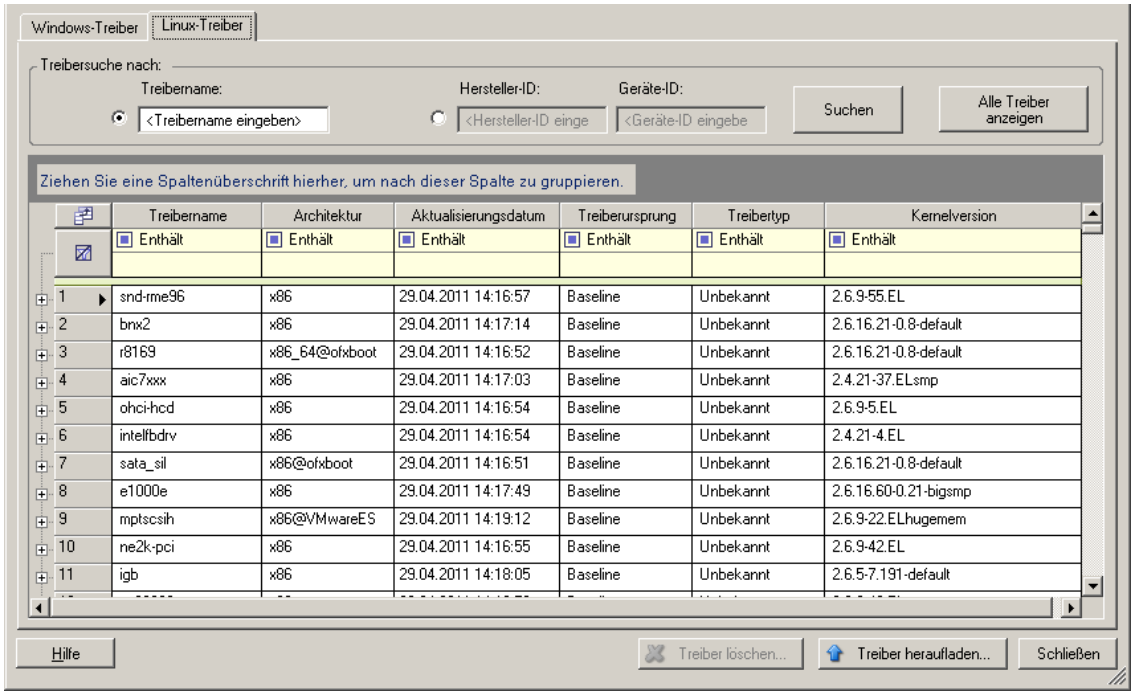
Wählen Sie *Standard* als Option für *Hardwarehersteller* aus, es sei denn, Ihre Treiber sind speziell für eine der aufgeführten Zielumgebungen vorgesehen.

4 Klicken Sie auf *Heraufladen* und bestätigen Sie Ihre Auswahl.

Das System lädt die ausgewählten Treiber in die Treiberdatenbank.

Upload-Prozedur für Gerätetreiber (Linux)

1. Beziehen Sie die erforderlichen Gerätetreiber und bereiten Sie diese vor. Weitere Informationen hierzu finden Sie in Verpacken von Gerätetreibern für Linux-Systeme.
2. Klicken Sie auf *Werkzeuge* > *Gerätetreiber verwalten* und wählen Sie die Registerkarte *Linux-Treiber* aus:



3. Klicken Sie auf *Treiber hochladen*, navigieren Sie zu dem Ordner, der das erforderliche Treiberpaket (`*.pkg`) enthält, und klicken Sie auf *Alle Treiber hochladen*.

   Das System lädt die ausgewählten Treiber in die Treiberdatenbank.

7 Fehlersuche

7.1 Fehlerbehebung bei der Workload-Inventarisierung (Windows)

Möglicherweise müssen Sie die folgenden typischen Probleme während der Workload-Inventarisierung beheben.

Probleme oder Meldungen	Lösungen
`The domain in the credentials is invalid or blank`	Dieser Fehler tritt auf, wenn das Format des Berechtigungsnachweises falsch ist. Versuchen Sie, die Ermittlung unter Verwendung eines lokalen Administratorkontos mit dem Berechtigungsnachweisformat `Hostname\LocalAdmin` durchzuführen. Sie können auch versuchen, die Ermittlung unter Verwendung eines Domänen-Administratorkontos mit dem Berechtigungsnachweisformat `Domäne\DomainAdmin` durchzuführen.
`Unable to connect to Windows server...Access is denied`	Bei dem Versuch, einen Workload hinzuzufügen, wurde ein Nicht-Administratorkonto verwendet. Verwenden Sie ein Administratorkonto oder fügen Sie den Benutzer zur Administratorgruppe hinzu und versuchen Sie es erneut. Diese Meldung kann auch auf einen WMI-Verbindungsfehler hinweisen. Probieren Sie die nachfolgend aufgeführten Lösungsmöglichkeiten aus und führen Sie dann den „WMI-Verbindungstest“, auf Seite 87 erneut durch. Wenn der Test erfolgreich ist, versuchen Sie erneut, den Workload hinzuzufügen. ◆ „Fehlerbehebung bei DCOM-Verbindungen“, auf Seite 87 ◆ „Fehlerbehebung bei der RPC-Dienst-Verbindung“, auf Seite 88

Probleme oder Meldungen	Lösungen
`Unable to connect to Windows server...The network path was not found`	Netzwerk-Verbindungsfehler. Führen Sie die Tests in „Durchführen von Verbindungstests“, auf Seite 86 durch. Falls ein Test fehlschlägt, stellen Sie sicher, dass sich PlateSpin Protect und der Workload im selben Netzwerk befinden. Konfigurieren Sie das Netzwerk neu und versuchen Sie es erneut.
`“Discover Server Details {hostname}” Failed Progress: 0% Status: NotStarted`	Dieser Fehler kann aus verschiedenen Gründen auftreten. Es gibt für jede Ursache eine eigene Lösung: ◆ Bei Umgebungen, die einen lokalen Proxy mit Authentifizierung verwenden: Umgehen Sie den Proxy oder fügen Sie die richtigen Berechtigungen hinzu. Weitere Informationen hierzu finden Sie im KB-Beitrag 7920339 (http://www.novell.com/support/viewContent.do?externalId=7920339). ◆ Wenn lokale oder Domänenrichtlinien die erforderlichen Berechtigungen einschränken, führen Sie die im KB-Artikel 7920862 (http://www.novell.com/support/viewContent.do?externalId=7920862) beschriebenen Schritte aus.

Workload-Ermittlungsfehler mit Fehlermeldung
`Could not find file output.xml`
oder
`Network path not found`
oder (beim Versuch, einen Windows-Cluster zu ermitteln)
`Inventory failed to discover. Inventory result returned nothing.`
	Es gibt mehrere mögliche Gründe für den Fehler `Datei output.xml wurde nicht gefunden`:
	◆ Virenschutz-Software auf dem Ursprung könnte die Ermittlung beeinträchtigen. Deaktivieren Sie die Virenschutz-Software, um festzustellen, ob sie die Ursache für das Problem ist. Weitere Informationen hierzu finden Sie unter „Deaktivieren der Virenschutz-Software“, auf Seite 88.
	◆ Die Datei- und Drucker-Freigabe für Microsoft-Netzwerke ist möglicherweise nicht aktiviert. Aktivieren Sie die Freigabe in den Eigenschaften der Netzwerkschnittstellenkarte.
	◆ Die Admin$-Freigaben auf dem Ursprung sind möglicherweise nicht zugänglich. Stellen Sie sicher, dass PlateSpin Protect auf diese Freigaben zugreifen kann. Weitere Informationen hierzu finden Sie unter „Aktivieren von Datei-/Freigabe-Berechtigungen und -Zugriff“, auf Seite 88.
	◆ Der Server- oder der Arbeitsstationsdienst läuft möglicherweise nicht. Wenn dies der Fall ist, aktivieren Sie den Dienst und stellen Sie den Startmodus auf `Automatisch` ein.
	◆ Der Remoteregistrierungsdienst von Windows ist deaktiviert. Starten Sie den Dienst und stellen Sie den Starttyp auf „Automatisch“ ein.

7.1.1 Durchführen von Verbindungstests

Netzwerk-Verbindungstest

Führen Sie diesen allgemeinen Netzwerk-Verbindungstest durch, um festzustellen, ob PlateSpin Protect mit dem Workload kommunizieren kann, den Sie zu schützen versuchen.

1. Wechseln Sie zu Ihrem PlateSpin Protect Server-Host.
2. Öffnen Sie ein Befehlszeilenfenster und senden Sie einen Ping-Befehl an Ihren Workload:

   ```
   ping workload_ip
   ```

WMI-Verbindungstest

1. Wechseln Sie zu Ihrem PlateSpin Protect Server-Host.
2. Klicken Sie auf *Start* > *Ausführen*, geben Sie `Wbemtest` ein und drücken Sie die `Eingabetaste`.
3. Klicken Sie auf *Verbinden*.
4. Geben Sie unter *Namespace* den Namen des Workloads ein, den Sie zu ermitteln versuchen, und hängen Sie `\root\cimv2` an den Namen an. Wenn der Hostname beispielsweise `win2k` lautet, geben Sie Folgendes ein:

   ```
   \\win2k\root\cimv2
   ```

5. Geben Sie den entsprechenden Berechtigungsnachweis ein. Verwenden Sie hierzu entweder das Format `Hostname\LocalAdmin` oder `Domäne\DomainAdmin`.
6. Klicken Sie auf *Verbinden*, um die WMI-Verbindung zu testen.

   Wenn eine Fehlermeldung zurückgegeben wird, kann keine WMI-Verbindung zwischen PlateSpin Protect und Ihrem Workload hergestellt werden.

Fehlerbehebung bei DCOM-Verbindungen

1. Melden Sie sich bei dem zu schützenden Workload an.
2. Klicken Sie auf *Start* > *Ausführen*.
3. Geben Sie `dcomcnfg` ein und drücken Sie die Eingabetaste.
4. Prüfen Sie die Verbindung:
   - Bei Windows-Systemen (XP/Vista/2003/2008/7) wird das Fenster "Komponentendienste" angezeigt. Klicken Sie im Ordner *Computer* des Konsolenbaums im Verwaltungstool „Komponentendienste“ mit der rechten Maustaste auf den Computer, den Sie hinsichtlich der DCOM-Verbindung prüfen möchten, und klicken Sie anschließend auf *Eigenschaften*. Klicken Sie auf die Registerkarte *Standardeigenschaften* und stellen Sie sicher, dass *DCOM (Distributed COM) auf diesem Computer aktivieren* ausgewählt ist.
   - Auf einem Computer am Windows 2000-Server wird das Dialogfeld „DCOM-Konfiguration“ angezeigt. Klicken Sie auf die Registerkarte *Standardeigenschaften* und stellen Sie sicher, dass *DCOM (Distributed COM) auf diesem Computer aktivieren* ausgewählt ist.
5. Wenn DCOM nicht aktiviert ist, aktivieren Sie es und booten Sie entweder den Server neu oder starten Sie den Windows-Verwaltungsinstrumentation-Dienst neu. Versuchen Sie nun nochmals, den Workload hinzuzufügen.

Fehlerbehebung bei der RPC-Dienst-Verbindung

Es gibt drei potenzielle Blockaden beim RPC-Dienst:

- Der Windows-Dienst
- Eine Windows-Firewall
- Eine Netzwerk-Firewall

Stellen Sie für den Windows-Dienst sicher, dass der RPC-Dienst auf dem Workload ausgeführt wird. Führen Sie `services.msc` von einem Befehlszeilenfenster aus, um das Dienstefenster zu öffnen. Fügen Sie für eine Windows-Firewall eine RPC-Ausnahme hinzu. Bei Hardware-Firewalls können Sie folgende Strategien probieren:

- PlateSpin Protect und der Workload müssen sich auf derselben Seite der Firewall befinden
- Öffnen spezifischer Ports zwischen PlateSpin Protect und dem Workload (siehe „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“, auf Seite 21)

7.1.2 Deaktivieren der Virenschutz-Software

Virenschutz-Software kann gelegentlich einige der mit WMI und der Remoteregistrierung zusammenhängenden PlateSpin Protect-Funktionen blockieren. Um sicherzustellen, dass die Workload-Inventarisierung erfolgreich durchgeführt wird, muss gegebenenfalls zuerst der Virenschutzdienst auf einem Workload deaktiviert werden. Darüber hinaus kann Virenschutz-Software mitunter auch den Zugriff auf bestimmte Dateien sperren und nur den Zugriff auf bestimmte Prozesse oder Programmdateien zulassen. Dies kann mitunter die dateibasierte Datenreproduktion verhindern. Wenn Sie den Workload-Schutz konfigurieren, können Sie in diesem Fall die zu deaktivierenden Dienste auswählen, z. B. Dienste, die von Virenschutz-Software installiert und verwendet werden. Diese Dienste werden nur für die Dauer der Dateiübertragung deaktiviert. Sobald der Prozess abgeschlossen ist, werden sie wieder gestartet. Bei einer Datenreproduktion auf Blockebene ist dies nicht erforderlich.

7.1.3 Aktivieren von Datei-/Freigabe-Berechtigungen und -Zugriff

Für den zuverlässigen Schutz eines Workloads muss PlateSpin Protect erfolgreich Software innerhalb des Workloads bereitstellen und installieren. Bei der Bereitstellung dieser Komponenten auf einem Workload sowie während des Hinzufügens eines Workloads verwendet PlateSpin Protect die administrativen Freigaben des Workloads. PlateSpin Protect benötigt Administratorzugriff auf die Freigaben und verwendet dazu ein lokales Administratorkonto oder ein Domänen-Administratorkonto.

So stellen Sie sicher, dass die administrativen Freigaben aktiviert sind:

1. Klicken Sie mit der rechten Maustaste auf *Arbeitsplatz* auf dem Desktop und wählen Sie *Verwalten*.
2. Erweitern Sie *System* > *Freigegebene Ordner* > *Freigaben*.
3. Im Verzeichnis `Freigegebene Ordner` müsste neben anderen die Freigabe Admin$ vorhanden sein.

Nachdem Sie sich vergewissert haben, dass die Freigaben aktiviert sind, stellen Sie sicher, dass sie vom PlateSpin Protect Server-Host aus zugänglich sind:

1. Wechseln Sie zu Ihrem PlateSpin Protect Server-Host.
2. Klicken Sie auf *Start* > *Ausführen*, geben Sie `\\<Server-Host>\Admin$` ein und klicken Sie anschließend auf *OK*.
3. Verwenden Sie bei Aufforderung denselben Berechtigungsnachweis wie für das Hinzufügen des Workloads zum PlateSpin Protect-Workload-Inventar.

   Das Verzeichnis wird geöffnet und Sie sollten in der Lage sein, darin zu navigieren und seinen Inhalt zu ändern.
4. Wiederholen Sie diesen Vorgang für alle Freigaben außer der IPC$-Freigabe.

   Windows verwendet die IPC$-Freigabe für die Berechtigungsnachweisvalidierung und Authentifizierung. Sie ist nicht einem Ordner oder einer Datei im Workload zugeordnet, der Test schlägt daher immer fehl. Die Freigabe sollte aber weiterhin sichtbar sein.

PlateSpin Protect ändert den vorhandenen Inhalt des Volumes nicht. Es erstellt jedoch ein eigenes Verzeichnis, für das es Zugriff und Berechtigungen benötigt.

7.2 Fehlerbehebung bei der Workload-Inventarisierung (Linux)

Probleme oder Meldungen	Lösungen
`Es konnte weder eine Verbindung zum SSH-Server, der auf <IP-Adresse> läuft, noch zu den VMware Virtual Infrastructure-Webdiensten unter <IP-Adresse>/sdk hergestellt werden`	Diese Meldung wird aufgrund mehrerer möglicher Ursachen ausgegeben: ◆ Der Workload ist nicht erreichbar. ◆ Auf dem Workload wird SSH nicht ausgeführt. ◆ Die Firewall ist aktiv und die erforderlichen Ports wurden nicht geöffnet. ◆ Das spezifische Betriebssystem des Workloads wird nicht unterstützt Informationen zu Netzwerk- und Zugriffsanforderungen für einen Workload finden Sie unter „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“, auf Seite 21.
`Access denied`	Dieses Authentifizierungsproblem weist auf einen ungültigen Benutzernamen oder ein ungültiges Passwort hin. Weitere Informationen über den richtigen Berechtigungsnachweis für den Workload-Zugriff finden Sie unter „Richtlinien für Workload- und Container-Berechtigungsnachweise“, auf Seite 62.

7.3 Beheben von Problemen während der Ausführung des Befehls „Reproduktion vorbereiten“ (Windows)

Probleme oder Meldungen	Lösungen
Authentifizierungsfehler beim Überprüfen der Controller-Verbindung während der Einrichtung des Controllers auf dem Ursprung.	Das für das Hinzufügen eines Workloads verwendete Konto muss von dieser Richtlinie zugelassen sein. Weitere Informationen hierzu finden Sie unter „Gruppenrichtlinie und Benutzerrechte“, auf Seite 90.
Es konnte nicht festgestellt werden, ob .NET Framework installiert ist (mit Ausnahme `Die vertrauenswürdige Beziehung zwischen dieser Arbeitsstation und der primären Domäne ist fehlgeschlagen`).	Überprüfen Sie, ob der Remoteregistrierungsdienst auf dem Ursprung aktiviert ist und ausgeführt wird. Siehe auch „Fehlerbehebung bei der Workload-Inventarisierung (Windows)“, auf Seite 85.

7.3.1 Gruppenrichtlinie und Benutzerrechte

Aufgrund der Art und Weise, wie PlateSpin Protect mit dem Betriebssystem des Ursprungs-Workloads interagiert, muss das zum Hinzufügen des Workloads verwendete Administratorkonto über bestimmte Benutzerrechte auf dem Ursprungscomputer verfügen. In den meisten Fällen sind diese Einstellungen Standardwerte der Gruppenrichtlinie. Wenn die Umgebung jedoch gesperrt wurde, wurden folgende Benutzerrechte-Zuweisungen möglicherweise entfernt:

- Traverse Checking umgehen
- Token auf Prozessebene ersetzen
- Als Teil des Betriebssystems agieren

Um zu überprüfen, ob diese Gruppenrichtlinien-Einstellungen festgelegt wurden, können Sie `gpresult /v` von der Befehlszeile auf dem Ursprungscomputer oder alternativ `RSOP.msc` ausführen. Wenn die Richtlinie nicht festgelegt oder wenn sie deaktiviert wurde, kann sie über die lokale Sicherheitsrichtlinie des Computers oder über eine der für den Computer geltenden Domänengruppenrichtlinien aktiviert werden.

Sie können die Richtlinie sofort mithilfe von `gpudate /force` (bei Windows 2003/XP) oder `secedit /refreshpolicy machine_policy /enforce` (bei Windows 2000) aktualisieren.

7.4 Fehlerbehebung bei der Workload-Reproduktion

Probleme oder Meldungen	Lösungen
Behebbarer Fehler bei der Reproduktion während des Vorgangs *Erstellen eines Snapshots der virtuellen Maschine planen* oder *Planen des Zurücksetzens der virtuellen Maschine auf Snapshot vor dem Start*.	Dieses Problem tritt auf, wenn der Server ausgelastet ist und der Vorgang länger als erwartet dauert. Warten Sie bis die Reproduktion abgeschlossen ist.

Probleme oder Meldungen	Lösungen
Workload-Problem erfordert Benutzereingriff	Diese Meldung kann von verschiedenen Problemen verursacht worden sein. In den meisten Fällen sollte die Meldung weitere Angaben zur Art des Problems und dem Problembereich (wie Konnektivität, Berechtigungsnachweis etc.) enthalten. Warten Sie nach der Fehlersuche einige Minuten. Wenden Sie sich an den PlateSpin-Support, falls die Meldung weiterhin angezeigt wird.
Bei allen Workloads treten behebbare Fehler auf, da kein Speicherplatz mehr vorhanden ist.	Überprüfen Sie den freien Speicherplatz. Wenn mehr Platz erforderlich ist, entfernen Sie einen Workload.
Langsame Netzwerkgeschwindigkeiten unter 1 MB.	Stellen Sie sicher, dass die Duplex-Einstellung der Netzwerkschnittstellenkarte des Ursprungscomputers aktiviert ist und dass der Switch, mit dem sie verbunden ist, eine entsprechende Einstellung hat. Wenn der Switch auf automatisch gesetzt ist, kann der Ursprung nicht auf 100 MB eingestellt werden.
Langsame Netzwerkgeschwindigkeiten über 1 MB.	Messen Sie die Latenz, indem Sie folgenden Befehl vom Ursprungs-Workload aus ausführen: `ping` *`ip`* `–t` (ersetzen Sie *ip* durch die IP-Adresse Ihres PlateSpin Protect Server-Hosts). Lassen Sie den Befehl für 50 Iterationen ausführen. Der Durchschnitt gibt dann die Latenz an. Siehe auch „Optimieren des Datentransfers über WAN-Verbindungen“, auf Seite 24.

`The file transfer cannot begin - port 3725 is already in use`
 	
oder
 	
`3725 unable to connect`
	Stellen Sie sicher, dass der Port offen ist und überwacht:
	
	Führen Sie `netstat -ano` auf dem Workload aus.
	
	Überprüfen Sie die Firewall.
	
	Wiederholen Sie die Reproduktion.

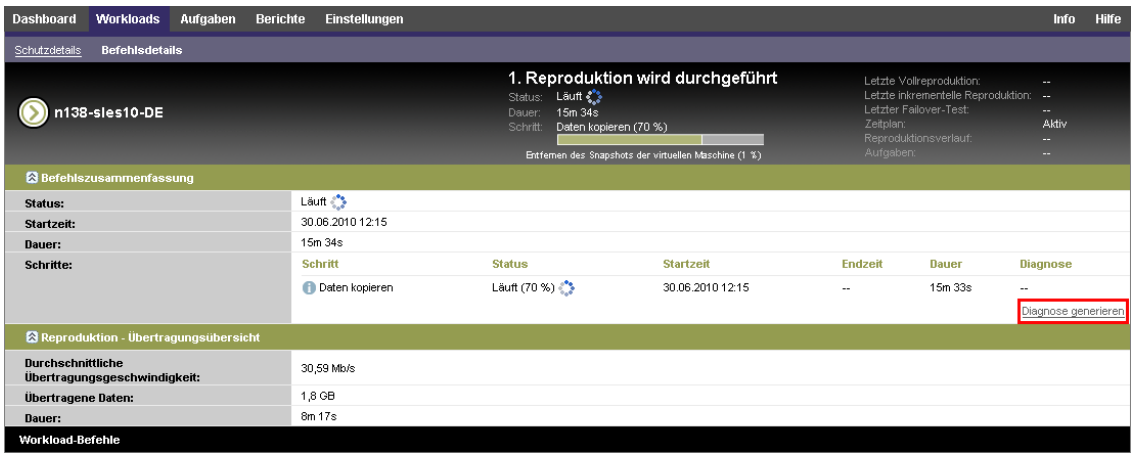
`Controller connection not established` Die Reproduktion schlägt beim Schritt *Kontrolle über die virtuelle Maschine übernehmen* fehl.	Dieser Fehler tritt auf, wenn die Reproduktionsnetzwerkinformationen ungültig sind. Entweder ist der DHCP-Server nicht verfügbar oder das virtuelle Reproduktionsnetzwerk kann keine Verbindung zum PlateSpin Protect Server-Host herstellen. Ändern Sie die Reproduktions-IP in eine statische IP oder aktivieren Sie den DHCP-Server. Stellen Sie sicher, dass das für die Reproduktion ausgewählte virtuelle Netzwerk eine Verbindung zum PlateSpin Protect Server-Host herstellen kann.

Probleme oder Meldungen	Lösungen
Der Reproduktionsauftrag startet nicht (hängt bei 0 %)	Dieser Fehler kann aus unterschiedlichen Gründen auftreten. Es gibt für jede Ursache eine eigene Lösung: ◆ Bei Umgebungen, die einen lokalen Proxy mit Authentifizierung verwenden: Umgehen Sie den Proxy oder fügen Sie die richtigen Berechtigungen hinzu, um dieses Problem zu beheben. Weitere Informationen hierzu finden Sie im KB-Beitrag 20339 (http://www.novell.com/support/viewContent.do?externalId=7920339). ◆ Wenn lokale oder Domänenrichtlinien die erforderlichen Berechtigungen einschränken, führen Sie die im KB-Artikel 7920862 (http://www.novell.com/support/viewContent.do?externalId=7920862) beschriebenen Schritte aus. Dieses Problem tritt häufig auf, wenn der PlateSpin Protect Server-Host mit einer Domäne verbunden ist und die Domänenrichtlinien mit Einschränkungen angewendet werden. Weitere Informationen hierzu finden Sie unter „Gruppenrichtlinie und Benutzerrechte“, auf Seite 90.

7.5 Generieren und Anzeigen von Diagnoseberichten

Nachdem Sie auf der PlateSpin Protect-Weboberfläche einen Befehl ausgeführt haben, können Sie detaillierte Diagnoseberichte über die Details des Befehls generieren.

1 Klicken Sie auf *Befehlsdetails* und dann auf *Diagnose generieren*.



Nach kurzer Zeit wird die Seite aktualisiert und zeigt den Link *Ansicht* oberhalb des Links *Diagnose generieren* an.

2 Klicken Sie auf *Anzeigen*.

Es wird eine neue Seite mit umfassenden Diagnoseinformationen zum aktuellen Befehl geöffnet.

3 Speichern Sie die Diagnoseseite und halten Sie sie bereit, falls Sie den technischen Support kontaktieren müssen.

7.6 Entfernen von Workloads

In einigen Situationen müssen Sie einen Workload unter Umständen vom PlateSpin Protect-Inventar entfernen und später wieder hinzufügen.

1 Wählen Sie auf der Seite „Workloads“ den zu entfernenden Workload aus und klicken Sie anschließend auf *Workload entfernen*.

(Bedingt) Bei Windows-Workloads, die zuvor durch eine Reproduktion auf Blockebene geschützt wurden, werden Sie auf der PlateSpin Protect Weboberfläche aufgefordert, anzugeben, ob Sie auch die blockbasierten Komponenten entfernen möchten. Folgenden Optionen stehen zur Auswahl:

- **Komponenten nicht entfernen:** Die Komponenten werden nicht entfernt.
- **Komponenten entfernen, Workload aber nicht neu starten:** Die Komponenten werden entfernt. Es ist jedoch ein Neustart des Workloads erforderlich, um den Deinstallationsprozess abzuschließen.
- **Komponenten entfernen und Workload neu starten:** Die Komponenten werden entfernt und der Workload wird automatisch neu gestartet. Stellen Sie sicher, dass Sie diesen Vorgang während der geplanten Ausfallzeit durchführen.

2 Klicken Sie auf auf der Seite „Befehlsbestätigung“ auf *Bestätigen*, um den Befehl auszuführen.

Warten Sie, bis der Vorgang abgeschlossen ist.

7.7 Workload-Bereinigung nach dem Schutz

Befolgen Sie dieses Schritte, um Ihren Ursprungs-Workload von allen PlateSpin-Software-Komponenten zu bereinigen, falls dies erforderlich ist, wie z. B. nach einem erfolglosen oder problematischen Schutz.

7.7.1 Bereinigen von Windows-Workloads

Komponente	Entfernungsanweisung
Blockbasierte PlateSpin-Übertragungskomponente	Weitere Informationen hierzu finden Sie im KB-Artikel 7005616 (http://www.novell.com/support/viewContent.do?externalId=7005616).
Blockbasierte Übertragungskomponente eines Drittanbieters (eingestellt)	1. Windows Software-Applet verwenden (`appwiz.cpl` ausführen) und die Komponenten entfernen. Abhängig vom Ursprung haben Sie eine der folgenden Versionen: ◆ SteelEye Data Replication for Windows v6 Update2 ◆ SteelEye DataKeeper For Windows v7 2. Booten Sie den Computer neu.

Komponente	Entfernungsanweisung
Dateibasierte Übertragungskomponente	Auf Root-Ebene für jedes geschützte Volume alle Dateien namens `PlateSpinCatalog*.dat` entfernen.
Workload-Inventarisierungssoftware	Im `Windows`-Verzeichnis des Workloads: ◆ Alle Dateien namens `machinediscovery*` entfernen. ◆ Unterverzeichnis `platespin` entfernen.
Controller-Software	1. Eine Eingabeaufforderung öffnen und das aktuelle Verzeichnis ändern in: ◆ `\Programme\platespin*` (32-Bit-Systeme) ◆ `\Programme (x86)\platespin*` (64-Bit-Systeme) 2. Führen Sie den folgenden Befehl aus: `ofxcontroller.exe /uninstall` 3. Verzeichnis `platespin*` entfernen.

7.7.2 Bereinigen von Linux-Workloads

Komponente	Entfernungsanweisung
Controller-Software	◆ Diese Prozesse stoppen: ◆ `pkill -9 ofxcontrollerd` ◆ `pkill -9 ofxjobexec` ◆ Das OFX-Controller-rpm-Package entfernen: `rpm -e ofxcontrollerd` ◆ Im Dateisystem des Workloads das Verzeichnis `/usr/lib/ofx` mit Inhalt entfernen.

Komponente	Entfernungsanweisung

Software für den Datentransfer auf Blockebene	1. Prüfen Sie, ob der Treiber aktiv ist:
	`lsmod | grep blkwatch`
	Wenn der Treiber immer noch im Arbeitsspeicher geladen ist, sollte das Ergebnis eine Zeile wie die folgende enthalten:
	`blkwatch_7616 70924 0`
	2. (Bedingt) Wenn der Treiber noch geladen ist, entfernen Sie ihn aus dem Arbeitsspeicher:
	`rmmod blkwatch_7616`
	3. Entfernen Sie den Treiber aus der Boot-Sequenz:
	`blkconfig -u`
	4. Entfernen Sie die Treiberdateien, indem Sie das folgende Verzeichnis mitsamt Inhalt löschen:
	`/lib/modules/`*`[Kernel_Version]`*`/Platespin`
	5. Löschen Sie die folgende Datei:
	`/etc/blkwatch.conf`

LVM-Snapshots	LVP-Snapshots, die bei fortlaufenden Reproduktionen verwendet werden, werden entsprechend einer *`Volume-Name`*`-PS-snapshot`-Konvention benannt. Beispiel: Ein Snapshot eines `LogVol01`-Volumes wird `LogVol01-PS-snapshot` genannt. So entfernen Sie diese LVM-Snapshots: 1. Erstellen Sie anhand einer der folgenden Methoden eine Liste der Snapshots auf dem erforderlichen Workload: ◆ Erstellen Sie auf der PlateSpin Protect-Weboberfläche einen Job-Bericht für den fehlgeschlagenen Job. Der Bericht sollte Informationen über die LVM-Snapshots und deren Namen enthalten. - ODER - ◆ Führen Sie am erforderlichen Linux-Workload den folgenden Befehl aus, um eine Liste aller Volumes und Snapshots anzuzeigen: `# lvdisplay -a` 2. Notieren Sie sich die Namen und Standorte der Snapshots, die entfernt werden sollen. 3. Entfernen Sie die Snapshots mit dem folgenden Befehl: `lvremove` *Snapshot-Name*
Bitmap-Dateien	Bei jedem geschützten Volume im Volume-Stamm die entsprechende `.blocks_bitmap`-Datei entfernen.
Werkzeuge	Im Ursprungs-Workload unter `/sbin` folgende Dateien entfernen: ◆ `bmaputil` ◆ `blkconfig`

Glossar

Container. Die Workload-Schutzinfrastruktur von PlateSpin Protect, wie beispielsweise ein VM-Host.

Ereignis. Eine PlateSpin Protect Server-Nachricht, die Informationen über wichtige Schritte während des gesamten Workload-Schutz-Lebenszyklus enthält.

Failback. Die Wiederherstellung der Geschäftsfunktion eines fehlgeschlagenen Workloads in seiner ursprünglichen Umgebung, wenn die Geschäftsfunktion eines temporären Failover-Workloads in PlateSpin Protect nicht mehr benötigt wird.

Failover. Die Übernahme der Geschäftsfunktion eines fehlgeschlagenen Workloads von einem Failover-Workload innerhalb eines PlateSpin Protect-VM-Containers.

Failover-Workload. Die bootfähige virtuelle Reproduktion eines geschützten Workloads.

Inkrementell. 1. (Substantiv) Eine einzelne geplante oder manuelle Übertragung von Unterschieden zwischen einem geschützten Workload und dessen Reproduktion (dem Failover-Workload).

2. (Adjektiv) Beschreibt den Umfang der *Reproduktion (1)*, in dem die anfängliche Reproduktion eines Workloads differentiell erstellt wird (auf der Basis von Unterschieden zwischen dem Workload und seinem vorbereiteten Gegenstück.

Vorbereiten auf Failover. Ein PlateSpin Protect-Vorgang, der den Failover-Workload in Vorbereitung eines vollständigen Failover-Vorgangs bootet.

Schutzebene. Eine benutzerdefinierbare Sammlung an Workload-Schutz-Parametern, die die Häufigkeit von Reproduktionen definiert sowie die Kriterien festlegt, anhand derer das System einen Workload als fehlgeschlagen erachtet.

Schutzvertrag. Eine Sammlung aktuell aktiver Einstellungen, die sich auf den gesamten Lebenszyklus eines Workload-Schutzes beziehen (*Inventar hinzufügen*, ursprüngliche und fortlaufende *Reproduktionen*, *Failover*, *Failback* und *Erneut schützen*).

Wiederherstellungspunkt. Ein zu einem bestimmten Zeitpunkt erstellter Snapshot, der es ermöglicht, einen reproduzierten Workload in einen früheren Zustand zurückzuversetzen.

Angestrebter Wiederherstellungszeitpunkt (RPO). In Zeit gemessener tolerierbarer Datenverlust, der durch ein konfigurierbares Intervall zwischen inkrementellen Reproduktionen eines geschützten Workloads definiert wird.

Angestrebte Wiederherstellungszeit (RTO). Ein Wert für die tolerierbare Ausfallzeit eines Workloads, definiert durch die Zeit, die für einen Failover-Vorgang erforderlich ist.

Reproduktion. 1. *Ursprüngliche Reproduktion*, die Erstellung einer ursprünglichen Basiskopie eines Workloads. Kann als *Vollständige Reproduktion* ausgeführt werden (alle Workload-Daten werden an einen "leeren" virtuellen Failover-Computer übertragen) oder als eine *Inkrementelle Reproduktion* (weitere Informationen hierzu finden Sie unter Punkt Inkrementell (2)).

2. Jegliche Übertragung geänderter Daten von einem geschützten Workload auf seine Reproduktion im Container.

Reproduktionsschema. Der zur Steuerung der Häufigkeit und des Umfangs von Reproduktionen eingerichtete Zeitplan.

Erneut schützen. Ein PlateSpin Protect-Befehl, der einen Schutzvertrag für einen Workload nach Failover- und Failback-Vorgängen wiederherstellt.

Quelle. Ein Workload oder dessen Infrastruktur, der bzw. die der Ausgangspunkt für einen PlateSpin Protect-Vorgang ist. Beispielsweise ist der Ursprung beim anfänglichen Schutz eines Workloads der Produktions-Workload. Bei einem Failback-Vorgang ist es der Failover-Workload im Container.

Siehe auch Ziel.

Ziel. Ein Workload oder dessen Infrastruktur, der bzw. die das Ergebnis eines PlateSpin Protect-Befehls ist. Beispielsweise ist das Ziel beim anfänglichen Schutz eines Workloads der Failover-Workload im Container. In einem Failback-Vorgang ist es entweder die Original-Infrastruktur des Produktions-Workloads oder ein unterstützter Container, der von PlateSpin Protect inventarisiert wurde.

Siehe auch Quelle.

Failover testen. Ein PlateSpin Protect-Vorgang, bei dem ein Failover-Workload in einer isolierten Netzwerkumgebung gebootet wird, um die Funktionalität des Failovers zu testen und um die Integrität des Wiederherstellungs-Workloads zu überprüfen.

Angestrebte Testzeit (TTO). Ein Maß dafür, wie einfach sich ein Wiederherstellungsplan für den Katastrophenfall testen lässt. Es entspricht weitgehend der RTO, umfasst jedoch auch die Zeit, die ein Benutzer zum Testen des Failover-Workloads benötigt.

Workload. Das Basis-Schutzobjekt in einer Datenablage. Ein Betriebssystem einschließlich dessen Middleware und Daten, das von der zugrunde liegenden physischen oder virtuellen Infrastruktur abgekoppelt ist.