MICRO FOCUS

PlateSpin® Protect 11.2 SP1

Benutzerhandbuch

December 2017

Rechtliche Hinweise

Informationen zu rechtlichen Hinweisen, Marken, Haftungsausschlüssen, Gewährleistungen, Ausfuhrbeschränkungen und sonstigen Nutzungseinschränkungen, Rechten der US-Regierung, Patentrichtlinien und Erfüllung von FIPS finden Sie unter https://www.microfocus.com/about/legal/.

Lizenzerteilung

Die für PlateSpin Protect 11 oder neuere Versionen erworbenen Lizenzen können nicht für PlateSpin Protect 10.3 oder Vorgängerversionen verwendet werden.

Inhalt

Allgemeines zu diesem Handbuch

Dieses *Benutzerhandbuch* enthält Informationen zur Verwendung von PlateSpin Protect. Dieses Handbuch bietet allgemeine Informationen, einen Überblick über die Benutzeroberfläche sowie Schritt-für-Schritt-Anweisungen für häufig anfallende Aufgaben Ferner sind Terminologiedefinitionen und Informationen zur Fehlerbehebung enthalten.

Zielgruppe

Dieses Dokument richtet sich an Administratoren und Operatoren in Rechenzentren, die PlateSpin Protect in der Workload-Schutz- und Disaster Recovery-Lösung nutzen.

Weitere Dokumentation

Die aktuelle Version dieses Handbuchs und andere Dokumentationsressourcen zu PlateSpin Protect finden Sie auf der PlateSpin Protect-Dokumentationswebsite (https://www.netiq.com/documentation/platespin-protect/).

Neben Englisch ist die Online-Dokumentation in diesen Landessprachen erhältlich: Chinesisch (vereinfacht), Chinesisch (traditionell), Deutsch, Französisch, Japanisch und Spanisch.

Kontaktangaben

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation dieses Produkts. Klicken Sie auf den Link zur **Kommentarfunktion** unten auf der Seite in der Online-Dokumentation oder senden Sie eine E-Mail an Documentation-Feedback@microfocus.com.

Bei konkreten Problemen mit einem Produkt wenden Sie sich an den Micro Focus-Kundenservice unter https://www.microfocus.com/support-and-services/.

Planung

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 (physische oder virtuelle) Infrastrukturen
- Unterstützung externer Speicherlösungen, z. B. SANs

- Kapitel 1, „Planen der PlateSpin-Umgebung“, auf Seite 13
- Kapitel 2, „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“, auf Seite 37

1 Planen der PlateSpin-Umgebung

Planen Sie die PlateSpin-Schutz- und Wiederherstellungsumgebung anhand den Informationen in diesem Abschnitt.

1.1 Unterstützte Konfigurationen

PlateSpin Protect unterstützt die meisten Hauptversionen der Betriebssysteme Microsoft Windows, SUSE Linux Enterprise Server und Red Hat Enterprise Linux. Außerdem werden ausgewählte Versionen der Betriebssysteme Novell Open Enterprise Server, Oracle Enterprise Linux und CentOS unterstützt.

In diesem Abschnitt werden alle von PlateSpin Protect unterstützten Plattformkonfigurationen beschrieben, außerdem die Software-, Hardware- und Virtualisierungsumgebungen, die für den Schutz und die Wiederherstellung der Workloads erforderlich sind. Bei einigen Konfigurationen gelten besondere Schritte für das Einrichten und Wiederherstellen der Workloads; dies ist dort jeweils vermerkt. Lesen Sie in jedem Fall die angegebenen weiterführenden Informationen in der Online-Dokumentation oder in den Knowledgebase-Artikeln, bevor Sie den Workload einrichten.

HINWEIS: Alle hier nicht erwähnten Konfigurationen werden nicht unterstützt, allerdings sind zahlreiche Verbesserungen in PlateSpin Protect eine direkte Reaktion auf die Anregungen unserer Kunden. Sie können mit dazu beitragen, dass unser Produkt Ihre Anforderungen voll und ganz erfüllt. Falls Sie an einer nicht aufgeführten Plattformkonfiguration interessiert sind, wenden Sie sich bitte an den Technischen Support. Wir freuen uns auf Ihre Rückmeldung.

1.1.1 Unterstützte Windows-Workloads

PlateSpin Protect unterstützt Workloads für die unter Tabelle 1-1 aufgeführten Versionen von Microsoft Windows-Betriebssystemen.

Sowohl die Reproduktionen auf Dateiebene als auch die auf Blockebene werden unterstützt, mit bestimmten Einschränkungen. Weitere Informationen hierzu finden Sie in Abschnitt 1.2, „Unterstützte Datenübertragungsmethoden“, auf Seite 23.

HINWEIS: Für Desktop-Workloads (Arbeitsstation-Workloads) wird der Schutz nicht unterstützt.

Tabelle 1-1 *Unterstützte Windows-Workloads*

Betriebssystem	Anmerkungen
Server	
Windows Server 2016	Für den Schutz von Windows Server 2016-Servern ist VMware 6.0 (oder höher) erforderlich.
Windows Server 2012 R2 Windows Server 2012	Umfasst Domänencontroller (DC)- und Small Business Server (SBS)-Editionen. Weitere Informationen zum Konvertieren von Active Directory-Domänencontrollern finden Sie im Knowledgebase-Artikel 7920501 (https://www.netiq.com/support/kb/doc.php?id=7920501).
Windows Server 2008 R2 (64-Bit) Windows Server 2008 (64-Bit) Windows Server 2008, aktuelles SP (32-Bit)	Umfasst Domänencontroller (DC)- und Small Business Server (SBS)-Editionen. Weitere Informationen zum Konvertieren von Active Directory-Domänencontrollern finden Sie im Knowledgebase-Artikel 7920501 (https://www.netiq.com/support/kb/doc.php?id=7920501).
Windows Server 2003 R2 (64-Bit) Windows Server 2003 R2 (32-Bit) Windows Server 2003 mit aktuellem SP (64-Bit) Windows Server 2003 mit aktuellem SP (32-Bit)	Windows 2003 erfordert SP1 oder höher für die blockbasierte Reproduktion.

Betriebssystem	Anmerkungen
Cluster	
Auf Windows Server 2016 basierender Microsoft-Failover-Cluster	Für den Schutz von Windows Server 2016-Clustern ist VMware 6.0 (oder höher) erforderlich.
Auf Windows Server 2012 R2 basierender Microsoft-Failover-Cluster	Unterstützte Modelle: *Node and Disk Majority Quorum* und *No Majority: Disk Only Quorum*.
Auf Windows Server 2008 R2 basierender Microsoft-Failover-Cluster	Die Unterstützung umfasst die blockbasierte Datenübertragung mit einem Treiber (nur Fibre Channel SANs) oder ohne einen Treiber für inkrementelle Reproduktionen für Cluster. Die dateibasierte Reproduktion wird nicht unterstützt. **WARNUNG:** Versuchen Sie nicht, den blockbasierten Treiber auf Clustern mit freigegebenen iSCSI-Laufwerken zu verwenden. Dadurch können die Cluster nicht mehr verwendet werden. Weitere Informationen hierzu finden Sie in „Vorbereiten des Windows-Cluster-Schutzes“, auf Seite 119.
Auf Windows Server 2003 R2 basierender Windows-Cluster-Server	Unterstütztes Modell: *Single-Quorum Device Cluster*. Die Unterstützung umfasst lediglich die treiberlose blockbasierte Datenübertragung für inkrementelle Reproduktionen für Cluster. Die dateibasierte Reproduktion wird nicht unterstützt. Weitere Informationen hierzu finden Sie in „Vorbereiten des Windows-Cluster-Schutzes“, auf Seite 119.
Hyper-V-Hosts	
Windows Server 2012 R2 mit Hyper-V-Rolle Windows Server 2012 mit Hyper-V-Rolle	Schutz für einen Windows-Server, der als Hyper-V-Host fungiert, und die zugehörigen Volumes. Separater Schutz der einzelnen VMs.

Konfigurationsanforderungen unter Windows

Windows-Aktualisierungen

Wenden Sie in jedem Fall die Windows-Updates auf Ihrem Quellsystem an, bevor Sie die erste vollständige Reproduktion ausführen.

Domänencontroller und Virenschutzprogramme

Wenn es sich bei dem Windows-Computer um einen Domänencontroller handelt, stellen Sie sicher, dass die Anti-Viren-Software des Systems während der Reproduktion ebenfalls deaktiviert ist.

1.1.2 Unterstützte Linux-Workloads

PlateSpin Protect unterstützt Workloads für die unter Tabelle 1-2 aufgeführten Distributionen von Linux-Betriebssystemen.

Die Reproduktion von geschützten Linux-Workloads erfolgt ausschließlich auf Blockebene. Weitere Informationen hierzu finden Sie unter „Anforderung eines `blkwatch-Treibers“, auf Seite 17`.

Tabelle 1-2 *Unterstützte Linux-Workloads*

Betriebssystem	Version	Anmerkungen
Server		
Red Hat Enterprise Linux (RHEL)	7.0 bis 7.3 6.0 bis 6.9 5.x 4.x	Eine Liste der unterstützten Linux-Kernelversionen und Architekturen für RHEL-Distributionen finden Sie in „Von Protect unterstützte Linux-Distributionen“, auf Seite 135. PlateSpin Protect bietet keine Unterstützung für das XFS-Dateisystem Version 5 (v5) unter RHEL 7.3 und unter Distributionen auf der Grundlage von RHEL 7.3. Für Red Hat Enterprise Linux 6.7, Oracle Linux 6.7- und CentOS 2.6-Workloads mit LVM-Volumes wird eine inkrementelle Reproduktion nur für den neuesten verfügbaren Kernel (Version `2.6.32-642.13.1.el6.x86_64`) für die RHEL 6.7-Distribution unterstützt. Dies ist der gleiche Kernel, der von der RHEL 6.8-Distribution verwendet wird.
SUSE Linux Enterprise Server (SLES)	11 SP1 bis 11 SP4 10.x 9.x	Eine Liste der unterstützten Linux-Kernelversionen und Architekturen für SLES-Distributionen finden Sie in „Von Protect unterstützte Linux-Distributionen“, auf Seite 135. Die Kernel-Version 3.0.13 von SLES 11 SP 3 wird nicht unterstützt. Rüsten Sie auf die Kernel-Version 3.0.27 oder höher auf, bevor Sie den Workload inventarisieren.
Open Enterprise Server (OES)	2015 SP1 11 SP1 bis 11 SP3 2 SP3 Weitere Informationen hierzu finden Sie in SUSE Linux Enterprise Server (SLES).	Für OES 2015 SP1 unterstützt Protect NSS32-Bit-Pools mit einer Größe von bis zu 8 TB; NSS64-Bit-Pools werden nicht unterstützt. Eine Liste der unterstützten Linux-Kernelversionen und Architekturen für SLES-Distributionen finden Sie in „Von Protect unterstützte Linux-Distributionen“, auf Seite 135. Die Standard-Kernel-Version 3.0.13 unter OES 11 SP2 wird nicht unterstützt. Rüsten Sie auf die Kernel-Version 3.0.27 oder höher auf, bevor Sie den Workload inventarisieren.

Betriebssystem	Version	Anmerkungen
Oracle Linux (OL) (früher Oracle Enterprise Linux (OEL))	Weitere Informationen hierzu finden Sie in Red Hat Enterprise Linux (RHEL).	Eine Liste der unterstützten Linux-Kernelversionen und Architekturen für RHEL-Distributionen finden Sie in „Von Protect unterstützte Linux-Distributionen“, auf Seite 135. blkwatch-Treiber sind für den standardmäßigen Red Hat Compatible Kernel (RHCK) und Unbreakable Enterprise Kernel (UEK) in OEL 6 U7 (oder höher) verfügbar, wie unter „Liste der Verteilungen“, auf Seite 136 angegeben. Workloads mit dem Unbreakable Enterprise Kernel werden in PlateSpin Protect 11.2 (oder früher) nicht unterstützt. Bei Oracle Linux 6 U7 bieten die blkwatch-Treiber für die Kernel-Version 2.6.32-573 keine Unterstützung für die inkrementelle Reproduktion von Workloads mit LVM-Volumes. Aktualisieren Sie den Kernel und verwenden Sie dann RHEL 6 U7-Treiber für Kernel 2.6.32-642.
CentOS	Weitere Informationen hierzu finden Sie in Red Hat Enterprise Linux (RHEL).	Eine Liste der unterstützten Linux-Kernelversionen und Architekturen für RHEL-Distributionen finden Sie in „Von Protect unterstützte Linux-Distributionen“, auf Seite 135. CentOS 7.*x* erfordert VMware 5.5 (oder höher).

Konfigurationsanforderung für Linux-Workloads

Anforderung eines `blkwatch`-Treibers

Zur blockbasierten Datenübertragung für einen Linux-Workload in `PlateSpin Protect` ist ein blkwatch-Treiber erforderlich, der speziell für die zu schützende Linux-Distribution kompiliert ist. Die PlateSpin Protect-Software umfasst vorkompilierte Versionen des `blkwatch`-Treibers für viele fehlerfreie Linux-Verteilungen (32-Bit und 64-Bit). Sie können auch einen benutzerdefinierten Treiber erstellen. Weitere Informationen finden Sie unter „Von Protect unterstützte Linux-Distributionen“, auf Seite 135.

1.1.3 Unterstützte VM-Container

Ein VM-Container ist eine Schutz-Infrastruktur, die als Host für die regelmäßig aktualisierte und bootfähige virtuelle Reproduktion eines geschützten Workloads agiert.

- „Unterstützte VMware-Plattformen“, auf Seite 18
- „Unterstützung für VMware DRS-Cluster als Container“, auf Seite 18
- „Unterstützung für VMware vCenter Site Recovery Manager“, auf Seite 19
- „Unterstützung zum Schutz der Mehrmandantenfähigkeit auf VMware“, auf Seite 19

Unterstützte VMware-Plattformen

Unter Tabelle 1-3 finden Sie eine Liste der unterstützten VMware-Plattformen. Die Plattformen werden als Schutzcontainer und Failback-Container unterstützt.

HINWEIS: Der Schutz von Workloads durch einen Ziel-VM-Container ist abhängig von der Unterstützung des Gast-Betriebssystems auf dem Ziel-Host durch den Host-Anbieter. Weitere Informationen zu Ihren Ziel-VMware-Hosts finden Sie im *VMware Compatibility Guide* (http://www.vmware.com/resources/compatibility/) (VMware-Kompatibilitätshandbuch).

Die Container-Infrastruktur kann entweder ein VMware ESXi-Server oder ein VMware DRS-Cluster sein. Weitere Informationen zu den Konfigurationsvoraussetzungen für VMware DRS-Cluster finden Sie unter „Unterstützung für VMware DRS-Cluster als Container“, auf Seite 18.

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

Container	Version	Anmerkungen
VMware vCenter oder ESXi	6.5	Als VM-Container darf der DRS-Cluster nur aus ESXi 6.5-Servern bestehen und kann nur von vCenter 6.5 verwaltet werden.
VMware vCenter oder ESXi	6.0 (GA2, U2, U3)	Als VM-Container darf der DRS-Cluster nur aus ESXi 6.0-Servern bestehen und kann nur von vCenter 6.0 verwaltet werden.
VMware vCenter oder ESXi	5.5 (GA2, U2, U3)	Als VM-Container darf der DRS-Cluster nur aus ESXi 5.5-Servern bestehen und kann nur von vCenter 5.5 verwaltet werden.
VMware vCenter oder ESXi	5.1 (GA2, U2, U3)	Als VM-Container darf der DRS-Cluster nur aus ESXi 5.1-Servern bestehen und kann nur von vCenter 5.1 verwaltet werden.
VMware vCenter oder ESXi	4.1 (GA2, U3)	Als VM-Container darf der DRS-Cluster nur aus ESXi 4.1-Servern bestehen und kann nur von vCenter 4.1 verwaltet werden.

HINWEIS: Ihre VMware ESXi-Hosts erfordern eine erworbene Lizenz. Der Schutz wird bei diesen Systemen nicht unterstützt, wenn sie mit einer kostenlosen Lizenz ausgeführt werden.

Unterstützung 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 (Schutzziele)“, auf Seite 96.

Außerdem muss Ihr VMware-Cluster die folgenden Konfigurationsanforderungen erfüllen:

- DRS muss aktiviert und auf **Teilweise automatisiert** oder auf **Vollautomatisch** gesetzt sein. (Die Einstellung **Manuell** ist nicht zulässig.)
- Mindestens eine Datenablage muss für alle VMware-Hosts im VMware-Cluster freigegeben sein.

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

Unterstützung für VMware vCenter Site Recovery Manager

PlateSpin Protect unterstützt das Kopieren von reproduzierten VMs in einen Remote-Wiederherstellungsstandort mit VMware vCenter Site Recovery Manager (SRM). Weitere Informationen hierzu finden Sie in Abschnitt 6.7, „Konfigurieren der Unterstützung für VMware vCenter Site Recovery Manager“, auf Seite 76.

Unterstützung zum Schutz der Mehrmandantenfähigkeit auf VMware

PlateSpin Protect unterstützt die Mehrmandantenfähigkeit in VMware. Mehrere Protect-Server können gemeinsam ein VMware-Cluster-Backend nutzen. Weitere Informationen hierzu finden Sie unter „Einrichten der Protect-Mehrmandantenfähigkeit auf VMWare“, auf Seite 57.

1.1.4 Unterstützte Workload-Architekturen

PlateSpin Protect unterstützt die folgenden x86-basierten Computerarchitekturen:

Prozessor und Betriebssystemarchitektur

PlateSpin Protect unterstützt den Schutz und die Wiederherstellung von x64- und x86-Architekturen für physische und virtuelle Workloads in Ihrem Rechenzentrum:

- 64 Bit
- 32 Bit

Kerne und Sockets für Ziel-VMs

Für unterstützte VM-Container mit VMware 5.1 (oder höher) und mindestens VM-Hardware-Ebene 8 können Sie in PlateSpin Protect die Anzahl der Sockets sowie die Anzahl der Kerne pro Socket für den Failover-Workload angeben. Die Gesamtzahl der Kerne wird automatisch berechnet. Dieser Parameter gilt für die anfängliche Einrichtung eines Workloads mit der anfänglichen Reproduktionseinstellung **Vollständig**.

HINWEIS: Die maximale Anzahl der Kerne, die ein Workload nutzen kann, ist abhängig von externen Faktoren, beispielsweise vom Gast-Betriebssystem, von der VM-Hardware-Version, der VMware-Lizenzierung für den ESXi-Host und den berechneten ESXi-Host-Höchstwerten für vSphere. Weitere Informationen finden Sie unter *ESXi/ESX-Konfigurationshöchstwerte* (VMware-Knowledge Base 1003497) (https://kb.vmware.com/kb/1003497).

In bestimmten Distributionen von Gast-Betriebssystemen wird die Konfiguration der Kerne und der Kerne pro Socket unter Umständen nicht berücksichtigt. Gast-Betriebssysteme mit SLES 10 SP4 und OES 2 SP3 behalten beispielsweise die ursprünglich installierten Einstellungen für Kerne und Sockets bei, während andere SLES-, RHEL- und OES-Distributionen die Konfiguration beachten.

Virtuelle CPUs für Ziel-VMs

Für VM-Container mit VMware 4.1 können Sie in PlateSpin Protect die erforderliche Anzahl von vCPUs (virtuellen CPUs) angeben, die dem Failover-Workload zugewiesen werden sollen. Dieser Parameter gilt für die anfängliche Einrichtung eines Workloads mit der anfänglichen Reproduktionseinstellung **Vollständig**. Die vCPUs werden im Gast-Betriebssystem auf dem VM-Container jeweils als CPU mit einem einzelnen Kern und einem einzelnen Socket dargestellt.

UEFI- und BIOS-Firmware

PlateSpin Protect unterstützt die UEFI- und BIOS-Firmware-Schnittstellen für Windows- und Linux-Workloads.

HINWEIS: Wenn Sie einen UEFI-basierten Workload schützen und während des gesamten Lebenszyklus des geschützten Workloads denselben Firmware-Bootmodus nutzen möchten, muss ein Container mit vSphere 5.0 (oder höher) als Ziel verwendet werden.

Die folgenden Beispiele zeigen das Protect-Verhalten beim Schutz und Failback zwischen UEFI- und BIOS-basierten Systemen:

- Wenn Sie einen UEFI-basierten Workload auf einen Container mit VMware vSphere 4 übertragen.*x* (der UEFI nicht unterstützt) führt Protect zum Zeitpunkt des Failbacks einen Übergang der UEFI-Firmware des Workloads zur BIOS-Firmware durch. Wenn dann das Failback auf einem UEFI-basierten physischen Computer ausgewählt wird, kehrt Protect den Firmware-Übergang von BIOS zu UEFI wieder um.
- Wenn Sie versuchen, ein Failback eines geschützten Windows 2003-Workloads auf einen UEFI-basierten physischen Computer durchzuführen, analysiert Protect die Auswahl und Sie werden benachrichtigt, dass dies nicht zulässig ist. Das bedeutet, dass der Firmware-Übergang von BIOS zu UEFI nicht unterstützt wird, da Windows 2003 den UEFI-Bootmodus nicht unterstützt.
- Wenn Sie einen UEFI-basierten Ursprung auf einem BIOS-basierten Ziel schützen, migriert Protect die Startlaufwerke des UEFI-Systems (bislang GPT) zu MBR-Laufwerken. Bei einem Failback dieses BIOS-Workloads auf einen UEFI-basierten physischen Computer werden die Startlaufwerke wieder zu GPT zurückkonvertiert.

Bei Windows-Workloads spiegelt PlateSpin Protect die Microsoft-Unterstützung für UEFI- oder BIOS-basierte Windows-Workloads wider. Hierbei werden Workloads vom Ursprung zum Ziel übertragen, während die unterstütze Firmware für das zugehörige Ursprungs- bzw. Zielbetriebssystem durchgesetzt wird. Sowohl blockbasierte als auch dateibasierte Übertragungen werden unterstützt. Dies gilt auch für das Failback auf einen physischen Computer. Sobald ein Übergang (Failover oder Failback) zwischen UEFI- und BIOS-Systemen eingeleitet wird, analysiert Protect diesen Übergang, und Sie erhalten eine Mitteilung über dessen Gültigkeit.

1.1.5 Unterstützter Speicher

PlateSpin Protect unterstützt die nachfolgenden Speicherkonfigurationen für Windows- und Linux-Workloads.

Speicherdatenträger

PlateSpin Protect unterstützt mehrere Arten von Ursprungsspeicherdatenträgern, darunter einfache Festplatten, dynamische Windows-Datenträger, LVM2, RAID und SAN.

Sie können angeben, ob virtuelle Datenträger auf den geschützten VM-Reproduktionen per Thin Provisioning oder Thick Provisioning bereitgestellt werden sollen.

HINWEIS: Für Speicherdatenträger gelten die folgenden Einschränkungen:

- **Dynamische Festplatten unter Windows:** PlateSpin Protect unterstützt keine dynamischen Windows-Datenträger im Ziel.

  Bei dynamischen Datenträgern befolgt der Speicher nicht die Zuordnungsstrategie „Wie Ursprung“. Sowohl einfache dynamische Volumes als auch übergreifende dynamische Volumes werden im Ziel-Workload als einfache Basis-Volume-Datenträger behandelt. Der Zieldatenträger wird mit GPT partitioniert, wenn die Gesamtgröße der Mitgliedsdatenträger im dynamischen Volume die maximal zulässige MBR-Partitionsgröße überschreitet. Weitere Informationen finden Sie unter *Microsoft TechNet: Understanding the 2 TB limit in Windows Storage* (https://blogs.technet.microsoft.com/askcore/2010/02/18/understanding-the-2-tb-limit-in-windows-storage/) (Die 2-TB-Höchstgrenze für Windows-Speicher).
- **Linux-Software-RAID:** PlateSpin Protect unterstützt keine Linux-Workloads mit Volumes auf Software-RAIDs.

Partitionierungsschemata

PlateSpin Protect unterstützt die Partitionierungsschemata MBR (Master Boot Record) und GPT (GUID-Partitionstabelle) für Windows- und Linux-Workloads. Die Workloads und der Speicher für den Schutz müssen auf Datenträgern konfiguriert sein, die mit MBR oder GPT partitioniert sind. Bei GPT sind bis zu 128 Partitionen pro Festplatte zulässig; PlateSpin Protect unterstützt jedoch nur maximal 57 GPT-Partitionen pro Festplatte.

Windows-Dateisysteme

PlateSpin Protect unterstützt auf allen unterstützten Windows-Systemen ausschließlich das NTFS-Dateisystem.

Linux-Dateisysteme

PlateSpin Protect unterstützt die Dateisysteme EXT2, EXT3, EXT4, REISERFS, XFS und NSS (nur Open Enterprise Server) jeweils nur mit blockbasierter Übertragung.

HINWEIS: Das Dateisystem XFS v5 wird für Red Hat Enterprise Linux 7.3 und die auf dieser Version basierenden Distributionen nicht unterstützt.

HINWEIS: Verschlüsselte Workload-Volumes auf dem Ursprung werden auf dem virtuellen Failover-Computer entschlüsselt.

Linux-Speicherfunktionen

Bei Linux-Workloads unterstützt PlateSpin Protect zusätzlich folgende Speicher:

- 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.
- LVM-Rohdatenträger-Volumes werden in Speicherkonfigurationen des Typs „Wie Ursprung“ in Linux-Workloads unterstützt.
- (OES-11-) NLVM-Layouts (Novell Linux Volume Management) von Ursprungs-Workloads werden beibehalten und im VM-Container neu erstellt. NSS-Pools werden vom Ursprung in die Wiederherstellungs-VM kopiert.
- (OES 2-) EVMS-Layouts von Ursprungs-Workloads werden beibehalten und im VM-Container neu erstellt. NSS-Pools werden vom Ursprung in die Wiederherstellungs-VM kopiert.

1.1.6 Unterstützte Landessprachen

Neben Englisch bietet PlateSpin Protect auch landessprachliche Unterstützung (National Language Support, NLS) für die Installation und Nutzung auf Computern, die für die folgenden internationalen Sprachen konfiguriert sind:

- Chinesisch (vereinfacht) (zh-cn)
- Chinesisch (traditionell) (zh-tw)
- Französisch (fr)
- Deutsch (de)
- Japanisch (ja)

TIPP: Weitere internationale Versionen werden eingeschränkt unterstützt; beispielweise kann die Aktualisierung von Systemdateien in anderen Sprachen erfolgen.

Für diese Sprachen sowie für Spanisch (es) steht eine lokalisierte Online-Dokumentation zur Verfügung.

Weitere Informationen zur Nutzung der Weboberfläche in einer dieser Sprachen finden Sie unter „Konfigurieren der Spracheinstellungen für internationale Versionen“, auf Seite 65.

1.1.7 Unterstützte Webbrowser

Die meisten Aktionen mit dem Produkt führen Sie über die browserbasierte Weboberfläche durch.

Die folgenden Browser werden unterstützt:

- *Google Chrome*, Version 34.0 und höher
- *Microsoft Internet Explorer*, Version 11.0 und höher
- *Mozilla Firefox*, Version 29.0 und höher

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

Informationen zur Verwendung der PlateSpin Protect-Weboberfläche in einer der unterstützten internationalen Sprachen finden Sie unter „Konfigurieren der Spracheinstellungen für internationale Versionen“, auf Seite 65.

1.2 Unterstützte Datenübertragungsmethoden

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

1.2.1 Unterstützte Übertragungsmethoden für Windows-Workloads

Für Windows-Workloads bietet PlateSpin Protect verschiedene Mechanismen, mit denen Sie die Volume-Daten des Workloads entweder auf Blockebene oder auf Dateiebene übertragen.

- **Windows-Reproduktion auf Dateiebene:** (Nur Windows) Die Daten werden dateiweise reproduziert.
- **Windows-Reproduktion auf Blockebene:** Daten werden auf dem Volume auf Blockebene reproduziert. Bei dieser Übertragungsmethode bietet PlateSpin Protect zwei Mechanismen, die sich durch ihre Auswirkungen auf die Kontinuität und durch ihre Leistungen unterscheiden. Sie können je nach Bedarf zwischen diesen beiden Mechanismen umschalten.
  - **Reproduktion mit der blockbasierten Komponente:** Bei dieser Option erfolgt die Datenübertragung auf Blockebene mit einer dedizierten Software-Komponente. Hierbei werden der Microsoft-Volumesnapshotdienst (Volume Snapshot Service VSS) sowie Anwendungen und Diensten, die VSS unterstützen, herangezogen. Die Komponente wird dabei automatisch auf dem geschützten Workload installiert.

    HINWEIS: Für die Installation und Deinstallation der blockbasierten Komponenten ist ein Neustart des geschützten Workloads erforderlich. Wenn Windows-Cluster mit einer Datenübertragung auf Blockebene geschützt werden sollen, ist kein Neustart erforderlich. Beim Konfigurieren der Details für den Workload-Schutz können Sie wahlweise angeben, dass die Komponente erst zu einem späteren Zeitpunkt installiert werden soll, so dass der erforderliche Neustart bis zur ersten Reproduktion aufgeschoben wird.

- **Reproduktion ohne die blockbasierte Komponente:** Diese Option verfolgt die Änderungen an den geschützten Volumes mithilfe eines internen „Hashing“-Mechanismus in Kombination mit Microsoft VSS. Bei der Reproduktion wird jeder Block auf dem Datenträger verglichen, und nur Änderungen werden kopiert.

  Diese Option erfordert keinen Neustart, bietet jedoch niedrigere Leistungen als die blockbasierte Komponente.

1.2.2 Unterstützte Übertragungsmethode für Linux-Workloads

Bei Linux-Workloads unterstützt PlateSpin Protect lediglich die blockbasierte Datenübertragung mit einem Blockwatch-Treiber (`blkwatch`-Treiber).

HINWEIS: Das Bereitstellen bzw. Entfernen des `blkwatch`-Treibers wird im Hintergrund ausgeführt, beeinträchtigt nicht die Kontinuität und erfordert keinen Benutzereingriff und Neustart.

Die PlateSpin Protect-Distribution umfasst vorkompilierte `blkwatch`-Treiber für Workloads mit den standardmäßigen Non-Debug-Kerneln unterstützter Linux-Distributionen. Weitere Informationen hierzu finden Sie in Abschnitt B.2, „Vorkompilierte blkwatch-Treiber für Linux-Distributionen“, auf Seite 136.

Wenn die Workloads einen nicht standardmäßigen, einen benutzerdefinierten oder einen neueren Kernel enthalten, können Sie einen benutzerdefinierten `blkwatch`-Treiber für den jeweiligen Kernel erstellen. Weitere Informationen finden Sie im Wissensdatenbankartikel 7005873 *(Erstellen eines benutzerdefinierten blockbasierten Linux-Kernel-Treibers)* (https://www.netiq.com/support/kb/doc.php?id=7005873).

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.

1.3.1 Verschlüsselung von Daten während der Übertragung

Die Übertragungsverschlüsselung sorgt für einen größeren Schutz der Workload-Daten bei der Workload-Reproduktion. Wenn die Verschlüsselung aktiviert ist, werden über das Netzwerk erfolgende Datentransfers vom Ursprung zum Ziel unter Verwendung von AES (Advanced Encryption Standard) verschlüsselt.

HINWEIS: Die Datenverschlüsselung wirkt sich auf die Leistung aus und kann die Datenübertragungsgeschwindigkeit deutlich (um bis zu 30 %) verlangsamen.

Mit der Option **Datenübertragung verschlüsseln** können Sie die Verschlüsselung einzeln für jeden Workload aktivieren oder deaktivieren. Weitere Informationen hierzu finden Sie unter „Workload-Schutz-Details“, auf Seite 149.

1.3.2 Sicherheit der Client-Server-Kommunikation

Der PlateSpin-Server aktiviert SSL auf dem PlateSpin-Server-Host und sorgt so für die sichere Datenübertragung zwischen Ihrem Webbrowser und dem PlateSpin-Server mit HTTPS (Hypertext Transfer Protocol Secure). Bei der Installation wird auch ein eigensigniertes Zertifikat hinzugefügt, falls keine gültigen Zertifikate gefunden werden.

1.3.3 Sicherheit von Berechtigungsnachweisen

PlateSpin Protect schützt den Berechtigungsnachweis mithilfe einer SSL-Verbindung für die Datenübertragung und der kryptografischen Windows-Bibliothek zum Verschlüsseln der Passwörter.

Der Berechtigungsnachweis, den Sie für den Zugriff auf verschiedene Systeme (z. B. Workloads und Failback-Ziele) verwenden, wird in der PlateSpin -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 „Konfigurieren der Benutzerautorisierung und -authentifizierung“, auf Seite 53.

1.3.5 Windows-Authentifizierung für die Microsoft SQL Server-Datenbank

PlateSpin Protect bietet die Möglichkeit, den Zugriff auf die Microsoft SQL Server-Datenbank über die Windows-Authentifizierung vorzunehmen. Weitere Informationen hierzu finden Sie unter „Anforderungen für die Windows-Authentifizierung bei der Microsoft SQL Server-Datenbank“, auf Seite 34.

1.3.6 Port-Einstellungen und Firewalls

Tabelle 1-4 zeigt eine Liste der Standard-Ports in PlateSpin Protect. Wenn Sie benutzerdefinierte Ports konfigurieren, müssen Sie entsprechend diese individuellen Ports öffnen. Für die Kommunikation zwischen dem PlateSpin Protect-Server und den verwalteten Quell- und Zielcomputern müssen außerdem die entsprechenden Ports an sämtlichen Firewalls zwischen diesen Computern geöffnet werden. Der Datenverkehr bei der Kommunikation ist bidirektional (eingehend und ausgehend). Siehe auch „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“, auf Seite 31.

Tabelle 1-4 *Standard-Ports in PlateSpin Protect*

Portnummer	Protokoll	Funktionsweise	Details
80	TCP	HTTP	(Nicht sicher) Für die HTTP-Kommunikation zwischen dem PlateSpin-Server-Host und den verwalteten Ursprungs- und Zielcomputern. Öffnen Sie diesen Port auf dem PlateSpin-Server-Host, im Ursprungs- und Ziel-Workload sowie auf den VMware-ESXi-Hosts.
443	TCP	HTTPS	(Sicher) Für die HTTPS-Kommunikation zwischen dem PlateSpin-Server-Host und den Ursprungs- und Zielcomputern, wenn SSL aktiviert ist. Öffnen Sie diesen Port auf dem PlateSpin-Server-Host, im Ursprungs- und Ziel-Workload, auf den VMware-ESXi-Hosts sowie auf dem vCenter-Hostserver.
3725	TCP	Datenübertragung	Für die Datenübertragung zwischen Ursprungs- und Zielcomputer (auch dateibasierte und blockbasierte Übertragung). Öffnen Sie diesen Port auf den Ursprungs- und Zielcomputern für alle Workloads. Jegliche Firewalls zwischen einer Quelle und dem zugehörigen Ziel müssen außerdem den TCP-Port 3725 zulassen. Weitere Informationen hierzu finden Sie unter „Unterstützte Konfigurationen“, auf Seite 13.
135 445	TCP	RPC/DCOM	Für die RPC-/DCOM-Kommunikation auf Windows-Computern während des Ermittlungsvorgangs, außerdem während die Kontrolle über den Ursprungscomputer übernommen und dieser Computer neu gestartet wird. Öffnen Sie diese Ports für die Kommunikation zwischen den Ursprungs- und Zielcomputern für alle Windows-Workloads. Weitere Informationen hierzu finden Sie unter „Unterstützte Windows-Workloads“, auf Seite 14.
137 138 139	TCP	NetBIOS	Für die NetBIOS-Kommunikation (Namensdienst, Datagrammdienst und Sitzungsdienst). Öffnen Sie diese Ports für die Kommunikation zwischen den Ursprungs- und Zielcomputern für alle Windows-Workloads. Weitere Informationen hierzu finden Sie unter „Unterstützte Windows-Workloads“, auf Seite 14.
137 138	UDP	SMB	Für die SMB-Kommunikation zur Dateiübertragung des Take-Control-Ordners und der zugehörigen Dateien vom PlateSpin-Server auf den Ursprungscomputer. Öffnen Sie diese Ports auf dem PlateSpin-Server-Host und in den Quell-Workloads.
139 445	TCP	SMB	

Portnummer	Protokoll	Funktionsweise	Details
22	TCP		Für die SSH- und SCP-Kommunikation auf Linux-Computern während des Ermittlungsvorgangs. Öffnen Sie diesen Port auf den Ursprungs- und Zielcomputern für alle Linux-Workloads. Weitere Informationen hierzu finden Sie unter „Unterstützte Linux-Workloads“, auf Seite 15.
25	TCP	SMTP	Für den SMTP-Datenverkehr, wenn die E-Mail-Benachrichtigung deaktiviert ist. Öffnen Sie diesen Port auf dem PlateSpin-Server-Host und dem Mail-Relay-Host.
25	UDP	SMTP	
1433	TCP	SQL	Für die Microsoft SQL Server-Kommunikation zur Authentifizierung und Datenübertragung an einen Remote-SQL-Server. Öffnen Sie die SQL-Ports auf dem PlateSpin-Server-Host und dem SQL Server-Remote-Host sowie in allen dazwischenliegenden Firewalls. Weitere Informationen zu den Port-Anforderungen für SQL Server finden Sie unter *Konfigurieren der Firewall für den Server-Zugriff* im Microsoft Developers Network.
1434	TCP	SQL	Für die dedizierte Administratorverbindung zu Microsoft SQL Server.
1434	UDP	SQL	Für die benannten Instanzen in Microsoft SQL Server. Dieser Port ist ggf. erforderlich, wenn Sie benannte Instanzen auf einem Remote-SQL-Server nutzen.
49152 bis 65535	TCP	SQL	Für Microsoft SQL Server oder RPC für LSA, SAM und Netlogon. Wenn Sie Microsoft SQL Server für einen bestimmten TCP-Port konfigurieren, müssen Sie diesen Port in der Firewall öffnen. Weitere Informationen hierzu finden Sie in „Anforderungen für die Windows-Authentifizierung bei der Microsoft SQL Server-Datenbank“, auf Seite 34.

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-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 RPO-, RTO- und TTO-Spezifikationen

In Ihrer Schutzumgebung sind unterschiedliche Wiederherstellungspunkte und -zeitpunkte für die verschiedensten Workloads erforderlich.

- **Angestrebter Wiederherstellungszeitpunkt (RPO):** Die RPO-Einstellung beschreibt das in Zeit gemessene tolerierbare Ausmaß eines Datenverlusts im Fall eines weitreichenden IT-Ausfalls. Sie definieren den RPO mit einem konfigurierbaren Intervall zwischen den inkrementellen Reproduktionen eines geschützten Workloads.

  Der RPO 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):** Die RTO-Einstellung beschreibt die tolerierbare Ausfallzeit eines Workloads, gemessen als die Zeitspanne bis zum Abschluss eines Failover-Vorgangs. Mit dem Failover-Vorgang wird ein Failover-Workload online geschaltet, der dann vorübergehend einen geschützten Produktions-Workload ersetzt.

  Die 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 unter „Failover“, auf Seite 153.
- **Angestrebte Testzeit (TTO):** Die TTO-Einstellung beschreibt die Zeit, die zum Testen des Wiederherstellungsplans benötigt wird, damit der Dienst erfolgreich wiederhergestellt werden kann. Es entspricht weitgehend der RTO, umfasst jedoch auch die Zeit, die ein Benutzer zum Testen des Failover-Workloads benötigt.

  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 155.

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.

Beim Testen der Failover-Antwort beachten Sie die Istwerte für die konfigurierten RPO-, RTO- und TTO-Werte:

- **RPA (Recovery Point Actual):** Der RPA ist der in Zeit gemessene tatsächliche Datenverlust, der durch das tatsächlich gemessene Intervall zwischen inkrementellen Reproduktionen eines geschützten Workloads während eines Failover-Tests definiert wird. Der RPA wird auch als *tatsächlicher angestrebter Wiederherstellungszeitpunkt* (tatsächlicher RPO) bezeichnet.
- **RTA (Recovery Time Actual):** Der RTA ist ein Wert für die tatsächliche Ausfallzeit eines Workloads, definiert durch die Zeit, die für einen Failover-Vorgang erforderlich ist. Der RTA wird auch als *tatsächliche angestrebte Wiederherstellungszeit* (tatsächliche RTO) bezeichnet.
- **Tatsächliche Testzeit (TTA):** Die TTA ist ein Maß für den tatsächlichen Zeitraum, in dem sich ein Wiederherstellungsplan für den Katastrophenfall testen lässt. Es entspricht weitgehend der tatsächlichen RTO, umfasst jedoch auch die Zeit, die ein Benutzer zum Testen des Failover-Workloads benötigt. Die TTA wird auch als *tatsächliche angestrebte Testzeit* (tatsächliche TTO) bezeichnet.

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 unter „Generieren von Workload- und Workload-Schutz-Berichten“, auf Seite 173.

1.4.3 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 unter „Schutzebenen“, auf Seite 162.

1.4.4 Bandbreitendrosselung

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

Die Bandbreitendrosselung kann für jeden Workload einzeln konfiguriert werden oder auf einer Schutzebene. Weitere Informationen hierzu finden Sie unter „Schutzebenen“, auf Seite 162.

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-Server kann zwischen 10 und 50 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 ESXi-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.

1.4.6 Datenbankserver

PlateSpin Protect enthält die Microsoft SQL Server Express Edition. Die Funktionen von SQL Server Express reichen für einen einzelnen PlateSpin-Server aus, der bis zu 50 Workloads schützt (siehe Abschnitt 1.4.5, „Skalierbarkeit“, auf Seite 30).

HINWEIS: Microsoft SQL Server Express verfügt über eine Größenbeschränkung bei Datenbanken von 10 GB und kann jeweils nur einen CPU-Kern nutzen. Weitere Informationen zu Anforderungen und Einschränkungen bei SQL Server Express finden Sie in der Dokumentation zu Microsoft SQL Server 2014 Express (https://www.microsoft.com/en-us/download/details.aspx?id=42299).

Die PlateSpin-Server-Datenbankinstanz kann monatlich um bis zu 0,5 GB pro Workload anwachsen, abhängig von der Anzahl der geplanten inkrementellen Reproduktionen. Es wird empfohlen, die älteren Berichtsdaten regelmäßig zu archivieren oder zu verwerfen, damit genügend Platz für neue Berichtsdaten bereitsteht.

In einem VMware-DRS-Cluster müssen die Schutzziele über mehrere Hosts im Cluster hinweg ausgeglichen werden, sodass die optimale Leistung erzielt wird.

Außerdem wird empfohlen, in den folgenden Umgebungen den PlateSpin-Server zur Verwendung einer Datenbankinstanz auf dem bestehenden Microsoft SQL Server Standard Edition- oder Enterprise Edition-Datenbankserver konfigurieren:

- Bereitstellungen von mehreren PlateSpin-Servern, die denselben Remote-Datenbankserver mit Microsoft SQL Server für ihre Datenbankinstanzen verwenden
- Bereitstellungen, bei denen die Aufbewahrung des gesamten Berichtsdatenverlaufs wichtig ist

Mehrere PlateSpin-Server können auf denselben Remote-Datenbankserver zugreifen, wobei jedoch jeder Server eine eigene Datenbankinstanz benötigt.

Weitere Informationen zum Einrichten einer Remote-Datenbankinstanz für den PlateSpin-Server finden Sie unter „Konfigurieren des Microsoft SQL Server-Remote-Datenbankservers“ im *PlateSpin Protect-Installations- und Aufrüstungshandbuch*.

1.5 Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk

Bevor Sie Workloads für den Schutz und die Reproduktion einrichten, konfigurieren Sie das Netzwerk mit den Zugriffs- und Kommunikationseinstellungen in diesem Abschnitt.

1.5.1 Netzwerkanforderungen für die Weboberfläche des PlateSpin-Server-Hosts

Tabelle 1-5 zeigt die Ports, die auf dem PlateSpin-Server-Host geöffnet sein müssen, damit der Zugriff auf die Weboberfläche zugelassen wird.

Tabelle 1-5 *Erforderliche geöffnete Ports für den PlateSpin-Server-Host*

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

1.5.2 Netzwerkanforderungen für Container

Tabelle 1-6 zeigt die Software-, Netzwerk- und Firewall-Anforderungen für die unterstützten Workload-Container.

Tabelle 1-6 *Zugriffs- und Kommunikationsanforderungen für Container*

System	Voraussetzungen	Erforderliche Ports (Standards)
Alle Container	Ping-Funktion (ICMP-Echoanfrage und -antwort).	
Alle VMware-Container. Weitere Informationen hierzu finden Sie unter „Unterstützte VM-Container“, auf Seite 17.	◆ VMware-Konto mit Administratorrolle ◆ VMware Web-Services-API und Dateiverwaltungs-API	HTTPS (TCP 443)

System	Voraussetzungen	Erforderliche Ports (Standards)
vCenter Server	Dem zugreifenden Benutzer müssen die erforderlichen Rollen und Berechtigungen zugewiesen sein. Weitere Informationen hierzu finden Sie in der entsprechenden VMware-Dokumentation.	HTTPS (TCP 443)

1.5.3 Netzwerkanforderungen für Workloads

Tabelle 1-7 zeigt die Software-, Netzwerk- und Firewall-Anforderungen für Workloads, die mithilfe von PlateSpin Protect geschützt werden sollen.

Tabelle 1-7 *Zugriffs- und Kommunikationsanforderungen für Workloads*

Workload-Typ	Voraussetzungen	Erforderliche Ports (Standards)
Alle Workloads	Ping-Unterstützung (ICMP-Echoanfrage und -antwort)	
Alle Windows-Workloads. Weitere Informationen hierzu finden Sie unter „Unterstützte Windows-Workloads“, auf Seite 14.	◆ Microsoft .NET Framework 3.5 Service Pack 1 ◆ Microsoft .NET Framework 4.0 Zur Ermittlung muss auf den Ursprungs-Workloads Microsoft .NET Framework 2 SP2 (oder höher) ausgeführt werden.	
Alle Workloads in Windows-Server-Clustern. Siehe Cluster unter „Unterstützte Windows-Workloads“, auf Seite 14.	Der PlateSpin-Server muss die DNS-Auflösung beim Nachschlagen und beim rekursiven Nachschlagen der IP-Adressen für den Windows-Server-Cluster und dessen Knoten vornehmen können. Aktualisieren Sie den DNS-Server bzw. die lokale `hosts`-Datei (`%systemroot%\system32\drivers\etc\hosts`) auf der Forge-VM.	

Workload-Typ	Voraussetzungen	Erforderliche Ports (Standards)
Alle Windows-Workloads. Weitere Informationen hierzu finden Sie unter „Unterstützte Windows-Workloads“, auf Seite 14.	◆ Integrierter `Administrator`- oder Domänen-Administrator-Kontoberechtigungsnachweis (die Mitgliedschaft in der lokalen Administratorgruppe reicht nicht aus). ◆ 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** (`firewall.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 Alt+0150 ICMPv4In)** ◆ **Datei- und Druckerfreigabe (Echoanforderung Alt+0150 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 Alt+0150 RPC)** ◆ **Datei- und Druckerfreigabe (Spoolerdienst – RPC-EPMAP)**	TCP 3725 NetBIOS (TCP 137 bis 139) SMB (TCP 139, 445 und UDP 137, 138) RPC (TCP 135, 445)
Windows Server 2003 (mit SP1 Standard, SP2 Enterprise und R2 SP2 Enterprise).	**HINWEIS:** Nach dem Aktivieren der erforderlichen Anschlüsse aktivieren Sie die PlateSpin-Remote-Verwaltung mit dem folgenden Befehl an der Server-Eingabeaufforderung: `netsh firewall set service RemoteAdmin enable` Weitere Informationen zum Befehl „netsh“ finden Sie im Microsoft TechNet-Artikel *Das Befehlszeilenprogramm „Netsh“* (http://technet.microsoft.com/en-us/library/cc785383%28v=ws.10%29.aspx).	TCP 3725, 135, 139, 445 UDP 137, 138, 139

Workload-Typ	Voraussetzungen	Erforderliche Ports (Standards)
Alle Linux-Workloads. Weitere Informationen hierzu finden Sie unter „Unterstützte Linux-Workloads“, auf Seite 15.	Secure Shell (SSH)-Server	TCP 22, 3725

1.5.4 Anforderungen für die Windows-Authentifizierung bei der Microsoft SQL Server-Datenbank

PlateSpin Protect bietet die Möglichkeit, den Zugriff auf die Microsoft SQL Server-Datenbank über die Windows-Authentifizierung vorzunehmen. Für die Authentifizierung müssen Sie die Active Directory-Einstellungen konfigurieren und Ports in der Firewall öffnen.

So aktivieren Sie die Windows-Authentifizierung bei der SQL-Datenbank:

1. Konfigurieren Sie Microsoft SQL Server so, dass sowohl TCP/IP-Verbindungen als auch Named-Pipe-Verbindungen zugelassen werden.
2. (Bedingt) Falls der Zugriff auf die Microsoft SQL Server-Datenbank über die Windows-Authentifizierung erfolgen soll, müssen Sie Folgendes in Active Directory konfigurieren:
   - Sie müssen den Microsoft SQL Server-Datenbankserver in die Domäne aufnehmen.
   - Sie benötigen zwei Domänenbenutzerkonten für die PlateSpin Protect-Installation.
     - **Ein Domänenbenutzer mit dem `sysadmin`-Rollensatz:** Mit diesem Benutzer mit SQL Admin-Rechten werden Datenbanken, Tabellen und andere Schemaobjekte erstellt.
     - **PlateSpin-Service-Benutzer:** Der Servicebenutzer kann ein Domänenbenutzer mit niedrigen Rechten in der Domäne sein. Allerdings muss der Servicebenutzer als lokaler Administrator des PlateSpin Protect-Servers fungieren und diese Berechtigung vor Beginn der Installation erhalten.

       Wenn das Passwort des Windows-Benutzers geändert wird, müssen Sie das Passwort für den PlateSpin-Service-Benutzer und für den IIS-Anwendungspool aktualisieren. Verwenden Sie daher nach Möglichkeit einen Windows-Benutzer, dessen Passwort niemals ausläuft.

   HINWEIS: Bei der Windows-Authentifizierung müssen Sie sich als Domänenbenutzer mit SQL Admin-Rechten anmelden, wenn Sie den PlateSpin-Server aufrüsten oder aktualisieren.

3. Zur Unterstützung der Authentifizierung auf dem SQL-Server öffnen Sie die folgenden Ports in der Firewall:
   - **Ports 49152-65535/TCP:** Datenverkehr für RPC für LSA, SAM, Netlogon zulassen.
   - **Port 1433/TCP:** Datenverkehr für Microsoft SQL Server zulassen.
   - **Benutzerdefinierte Ports:** Wenn Sie SQL Server für einen benutzerdefinierten TCP-P konfigurieren, müssen Sie diesen Port in der Firewall öffnen.

   HINWEIS: Falls Sie keine dynamischen Ports nutzen, müssen Sie den dedizierten Port im Feld **Datenbankserver** angeben.

4 (Bedingt) Sollen dedizierte Ports für PlateSpin Protect verwendet werden, müssen Sie die Ports in der Firewall öffnen:

4a Legen Sie auf dem Datenbankserver fest, welche Ports geöffnet werden müssen:

4a1 Wählen Sie im SQL Server-Konfigurationsmanager die Option **Protokolle für SQLExpress > TCP/IP**, klicken Sie mit der rechten Maustaste, und wählen Sie **Eigenschaften**.

4a2 Wählen Sie im Dialogfeld die Registerkarte **IP-Adressen**.

4a3 Wenn für **TCP-Port** oder **Dynamische TCP-Ports** ein Wert ungleich 0 festgelegt ist, öffnen Sie unter **IP/Alle** (oder unter dem gewünschten Protokoll) die gewünschten Ports in der Firewall. Über diese Ports stellen Sie eine Verbindung zum SQL-Server her.

Wenn für das Feld **Dynamische TCP-Ports** beispielsweise der Wert 60664 festgelegt ist und für das Feld **TCP-Port** der Wert 1555, müssen Sie entsprechend die Ports 60664 und 1555 in den Firewall-Regeln auf dem SQL-Server aktivieren.

4b Öffnen Sie die Ports in der Firewall.

HINWEIS: Falls eine Wertemenge für dynamische Ports vorliegt, wird Ihr Server unter Umständen nicht in der Liste der SQL-Server aufgeführt, wenn Sie auf **Durchsuchen** klicken. In diesem Fall müssen Sie den Server manuell im Eingabefeld **Datenbankserver** der PlateSpin Protect-Installation angeben.

Wenn der Servername beispielsweise `MYSQLSERVER` und der Name der Datenbankinstanz `SQLEXPRESS` lautet und für den dynamischen Port der dedizierte Port `60664` festgelegt ist, geben Sie den folgenden Text ein, und wählen Sie dann den gewünschten Authentifizierungstyp aus:

`MEINSQLSERVER\SQLEXPRESS,60664.`

Sie müssen die Ports in der Firewall öffnen.

1.5.5 Anforderungen zum 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-Server:** Tragen Sie die zusätzlichen IP-Adressen, die dem PlateSpin-Server-Host zugewiesen sind, in das PlateSpin-Konfigurationswerkzeug Ihres Servers ein. Weitere Informationen hierzu finden Sie in „Anforderungen für den Betrieb des PlateSpin-Servers durch NAT“, auf Seite 36.
- **Ziel-Container:** Wenn Sie versuchen, einen Container zu ermitteln, z. B. VMware ESX, geben Sie die öffentlichen (externen) IP-Adressen dieses Hosts in den Parametern für die Ermittlung an.
- **Workload:** Geben Sie bei dem Versuch, einen Workload hinzuzufügen, die öffentliche (externe) 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 157) 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 PlateSpin-Server-Hosts angeben oder eine seiner öffentlichen (externen) Adressen, die in der PlateSpin Configuration-Datenbank des Servers aufgezeichnet wurden. Weitere Informationen hierzu finden Sie in „Anforderungen für den Betrieb des PlateSpin-Servers durch NAT“, auf Seite 36.

1.5.6 Anforderungen für den Betrieb des PlateSpin-Servers durch NAT

Für den Betrieb in Umgebungen, in denen die Netzwerkadressübersetzung (Network Address Translation, NAT) aktiviert ist, benötigt der PlateSpin-Server zusätzliche IP-Adressen. Weitere Informationen hierzu finden Sie in „Anforderungen für den Betrieb des PlateSpin-Servers durch NAT“, auf Seite 36.

1.5.7 Außerkraftsetzen der Standard-Bash-Shell zum Ausführen von Befehlen auf Linux-Workloads

Standardmäßig verwendet der PlateSpin-Server bei der Ausführung von Befehlen auf einem Linux-basierten Workload die `/bin/bash`-Shell.

Falls erforderlich, können Sie die Standard-Shell außer Kraft setzen, indem Sie den entsprechenden Registry-Schlüssel auf dem PlateSpin-Server ändern. Siehe Knowledgebase-Artikel 7010676 *Verfahren zum Übergehen der Linux-Standard-Shell* (https://www.netiq.com/support/kb/doc.php?id=7010676).

2 Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung

PlateSpin Protect definiert folgenden Workflow für den Workload-Schutz und die Wiederherstellung. Der Großteil dieser Schritte kann über Workload-Befehle auf der Seite „Workloads“ durchgeführt werden. Weitere Informationen hierzu finden Sie in „Workload-Schutz- und Wiederherstellungsbefehle“, auf Seite 45.

Tabelle 2-1 *Schutz- und Wiederherstellungslebenszyklus*

Job	Aktion	Anmerkungen
Vorbereitung Die Workloads, die Container und die Umgebung müssen die erforderlichen Kriterien erfüllen.		
	1. Stellen Sie sicher, dass PlateSpin Protect Ihren Workload unterstützt.	Weitere Informationen hierzu finden Sie unter „Unterstützte Konfigurationen“, auf Seite 13.
	2. Stellen Sie sicher, dass Ihre Workloads und VM-Container die Zugriffs- und Netzwerkvoraussetzungen erfüllen.	Weitere Informationen hierzu finden Sie unter „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“, auf Seite 31.
Inventar Workloads, die Sie schützen möchten, sowie Container, auf denen Failover-Workloads gehostet werden, müssen ordnungsgemäß inventarisiert werden. Sie können Workloads und Container jedem beliebigen Ordner hinzufügen, doch jeder Schutzvertrag erfordert einen definierten Workload und Container, der vom PlateSpin-Server inventarisiert wurde.		
	3. Ergänzen Sie den PlateSpin-Server mit Ziel-Containern.	Weitere Informationen hierzu finden Sie in „Hinzufügen von Containern (Schutzziele)“, auf Seite 96.
	4. Ergänzen Sie den PlateSpin-Server mit Ursprungs-Workloads.	Weitere Informationen hierzu finden Sie in „Hinzufügen von Workloads (Schutzursprünge)“, auf Seite 100.
	5. Bei einem physischen Schutzziel bereiten Sie Gerätetreiber vor.	Weitere Informationen hierzu finden Sie in Kapitel 11, „Vorbereiten der Gerätetreiber für physische Failback-Ziele“, auf Seite 105.
	6. Bei einem Linux-Workload bereiten Sie den Workload-Schutz vor:	Weitere Informationen hierzu finden Sie in Kapitel 12, „Vorbereiten von Linux-Workloads für den Schutz“, auf Seite 115.
	7. Bei Windows-Server-Cluster-Workloads bereiten Sie den Cluster-Workload-Schutz vor.	Weitere Informationen hierzu finden Sie in Kapitel 13, „Vorbereiten des Windows-Cluster-Schutzes“, auf Seite 119.

Job	Aktion	Anmerkungen
Schutzvertrag definieren		
	8. Definieren Sie die Details und Spezifikationen für einen Schutzvertrag.	Weitere Informationen hierzu finden Sie in „Konfigurieren der Schutzdetails und Vorbereiten der Reproduktion“, auf Seite 147.
	9. Bereiten Sie die Reproduktion vor.	
Schutz einleiten		
	10. Starten Sie den Schutzvertrag gemäß Ihren Anforderungen.	Weitere Informationen hierzu finden Sie in „Starten des Workload-Schutzes“, auf Seite 152.
Schutzlebenszyklusjobs (optional) Diese Schritte gehören nicht zum automatisierten Reproduktionsplan, sind jedoch in verschiedenen Situationen von Nutzen oder auch aufgrund Ihrer Strategie zur Aufrechterhaltung des ununterbrochenen Geschäftsbetriebs unerlässlich.		
	11. *Manuell/inkrementell*. Sie können eine inkrementelle Reproduktion manuell ausführen, also außerhalb des Workload-Schutzvertrags.	Wählen Sie den Workload aus und klicken Sie auf **Inkrementellen Vorgang ausführen**.
	12. *Testbetrieb*. Die Failover-Funktion lässt sich auf kontrollierte Weise in einer kontrollierten Umgebung testen.	Weitere Informationen hierzu finden Sie unter Verwenden der Funktion „Failover testen“.
Failover		
	13. Mit diesem Schritt wird ein Failover des geschützten Workloads auf die Reproduktion vorgenommen, die in Ihrem VM-Container ausgeführt wird.	Weitere Informationen hierzu finden Sie in „Failover“, auf Seite 153.
Failback		
	14. Dieser Schritt entspricht der Phase der Wiederaufnahme des Betriebs, nachdem Sie die Probleme mit dem Produktions-Workload behoben haben.	Weitere Informationen hierzu finden Sie in „Failback“, auf Seite 155.
Erneuter Schutz		
	15. In diesem Schritt definieren Sie den ursprünglichen Schutzvertrag für den Workload neu.	Weitere Informationen hierzu finden Sie in „Erneutes Schützen eines Workloads“, auf Seite 160. Der Befehl **Erneut schützen** steht nach einem erfolgreichen Failback zur Verfügung.

Verwalten des PlateSpin-Servers

In diesem Abschnitt erfahren Sie, wie Sie Ihre PlateSpin Protect-Lizenz aktivieren und das PlateSpin-Produkt für Ihre Umgebung anpassen. Machen Sie sich mit den PlateSpin-Werkzeugen und den Konfigurationsoptionen vertraut. Schlagen Sie in diesem Abschnitt nach, wenn Sie Lizenzen oder Benutzer verwalten oder Einstellungen anpassen.

3 Verwenden der PlateSpin-Werkzeuge

Die meisten Aktionen mit dem Produkt führen Sie über die browserbasierte Weboberfläche durch. Auf der webbasierten PlateSpin-Konfigurationsseite können Sie auch globale Parameter für die PlateSpin-Server-Anwendung konfigurieren.

3.1 Starten der Weboberfläche

1. (Optional) Konfigurieren Sie PlateSpin-Server und Ihren Webbrowser für eine der unterstützten internationalen Sprachen (statt Englisch). Weitere Informationen hierzu finden Sie in „Konfigurieren der Spracheinstellungen für internationale Versionen“, auf Seite 65.
2. Öffnen Sie einen unterstützten Webbrowser und wechseln Sie zu folgender Adresse:

   `https://Ihr_PlateSpin_Server/Protect`

   Ersetzen Sie *`Ihr_PlateSpin_Server`* durch den DNS-Hostnamen oder die IP-Adresse Ihres PlateSpin-Server-Hosts.

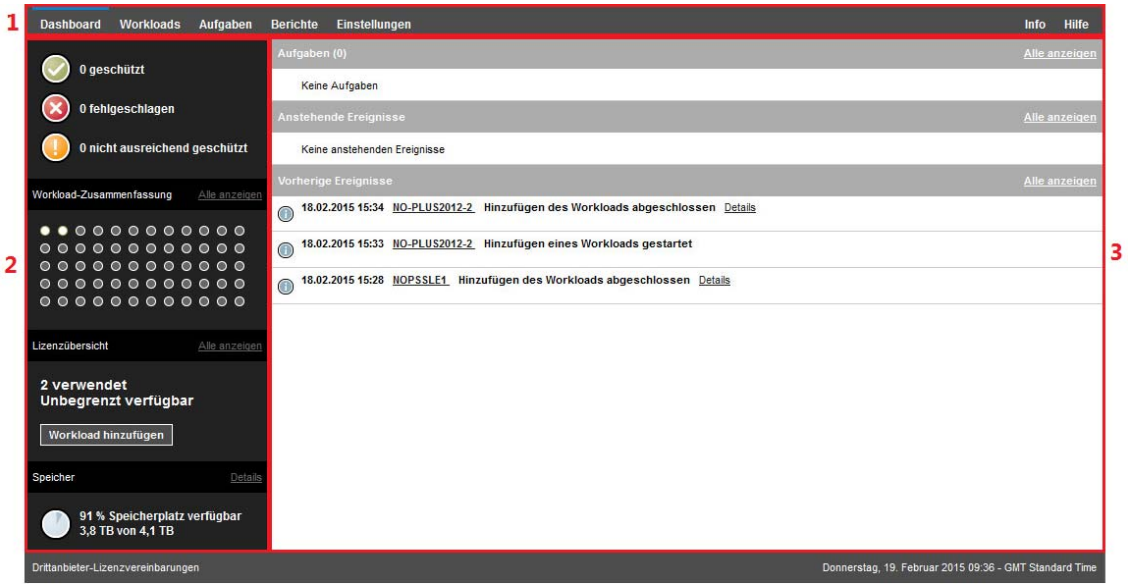
   Wenn SSL nicht aktiviert ist, verwenden Sie `http` in der URL.
3. Melden Sie sich mit den standardmäßigen Berechtigungsnachweisen für den PlateSpin-Server-Host an.

   Weitere Informationen zum Einrichten zusätzlicher Benutzer für PlateSpin finden Sie unter Kapitel 5, „Konfigurieren der Benutzerautorisierung und -authentifizierung“, auf Seite 53.

3.2 Überblick über das Dashboard

Die Dashboard-Seite der PlateSpin Protect-Weboberfläche enthält Elemente, mit denen Sie zu verschiedenen Funktionsbereichen der Oberfläche navigieren und Workload-Schutz- und Wiederherstellungsaufgaben durchführen.

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.

Die folgenden Abschnitte enthalten weitere Informationen.

- Abschnitt 3.2.1, „Navigationsleiste“, auf Seite 43
- Abschnitt 3.2.2, „Teilfenster mit visueller Zusammenfassung“, auf Seite 43
- Abschnitt 3.2.3, „Teilfenster mit Aufgaben und Ereignissen“, auf Seite 44

HINWEIS: Sie können bestimmte Elemente der Weboberfläche an das Markenbild Ihres Unternehmens anpassen. Weitere Informationen finden Sie unter „Anpassen der PlateSpin Protect-Weboberfläche an das Markenbild“, auf Seite 87.

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 „Überblick über Workloads“, auf Seite 45.
- **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 173.
- **Einstellungen:** Zeigt die Seite „Einstellungen“ an, die Zugriff auf die folgenden Konfigurationsoptionen bietet:
  - **Schutzebenen:** Weitere Informationen hierzu finden Sie unter „Schutzebenen“, auf Seite 162.
  - **Workload-Tags:** Weitere Informationen hierzu finden Sie unter „Erstellen und Verwenden von Workload-Tags“, auf Seite 79.
  - **Berechtigungen:** Weitere Informationen hierzu finden Sie in „Konfigurieren der Benutzerautorisierung und -authentifizierung“, auf Seite 53.
  - **Container:** Weitere Informationen hierzu finden Sie unter „Hinzufügen von Containern (Schutzziele)“, auf Seite 96.
  - **Benachrichtigungseinstellungen:** „Aktivieren von Ereignisbenachrichtigungen“, auf Seite 68.
  - **Einstellungen für Reproduktionsberichte:** „Aktivieren von Reproduktionsberichten“, auf Seite 69
  - **SMTP:** Weitere Informationen hierzu finden Sie unter „Konfigurieren von SMTP für den E-Mail-Benachrichtigungsdienst“, auf Seite 67.
  - **Lizenzen:** Weitere Informationen hierzu finden Sie unter „Aktivieren Ihrer Produktlizenz“, auf Seite 49.

3.2.2 Teilfenster mit visueller Zusammenfassung

Das Teilfenster mit visueller Zusammenfassung zeigt den allgemeinen Schutzstatus der Workloads im Inventar, den Status der einzelnen lizenzierten Workloads, eine Übersicht über die Lizenznutzung sowie den freien Speicherplatz.

Schutzstatus

Der allgemeine Schutzstatus der Workloads im Inventar wird mit 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.

Workload-Übersicht

Die Workload-Übersicht zeigt den Integritätsstatus der einzelnen Workloads, die auf der Seite „Workloads“ aufgeführt sind. Die maximale Anzahl der Punktsymbole für die den Workload-Status entspricht der Anzahl der installierten Workload-Lizenzen auf dem PlateSpin-Server. Bei einer unbegrenzten Lizenz zeigt die Übersicht 96 Punktsymbole. Tabelle 3-1 zeigt die verschiedenen Möglichkeiten für den Workload-Status, die durch die Punktsymbole dargestellt werden.

Die Symbole stellen die Workloads in alphabetischer Reihenfolge gemäß dem Workload-Namen dar. 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.

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

Geschützt	Ungeschützt
Fehlgeschlagen	Ungeschützt – Fehler
Nicht ausreichend geschützt	Abgelaufen
	Nicht verwendet

Lizenzübersicht

Die Lizenzübersicht zeigt die Anzahl der installierten Lizenzen sowie die Anzahl der Lizenzen, die derzeit durch die Workloads genutzt werden.

Speicher

Unter **Speicher** finden Sie den insgesamt für PlateSpin Protect verfügbaren Container-Speicherplatz sowie den derzeit belegten 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 unter „Konfigurieren der E-Mail-Benachrichtigungsdienste für Ereignisse und Reproduktionsberichte“, auf Seite 67.

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: `Mark. 'Test erfolgr.'` und `Mark. 'Test n. best.'`. Wenn

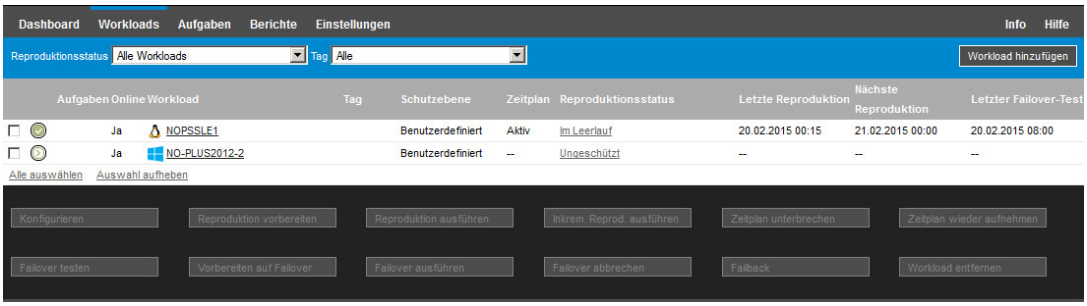
Sie auf eine der Aufgaben klicken, wird der Failover-Test abgebrochen und es wird ein entsprechendes Ereignis in das Protokoll geschrieben. Ein weiteres Beispiel ist das Ereignis `FullReplicationFailed`, das zusammen mit einer `StartFull`-Aufgabe gezeigt wird. Sie finden eine vollständige Liste der aktuellen 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 Überblick über Workloads

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. Die Workloads-Liste zeigt Informationen zu Verfügbarkeit (online oder offline), Tag, Schutzebene, Status und Ausführungszeitpunkte der Reproduktionen sowie Zeitpunkt des letzten Test-Failovers.

Abbildung 3-2 *Die Seite „Workloads“*

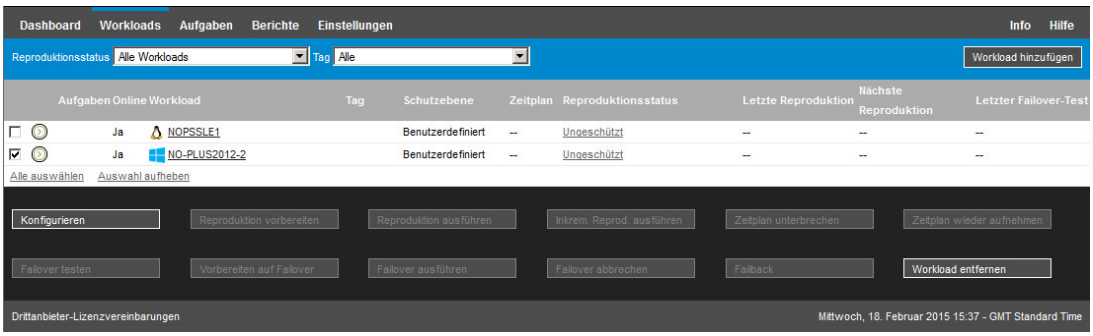


HINWEIS: Alle Zeitstempel entsprechen der Zeitzone des PlateSpin Server-Hosts. Diese kann sich von der Zeitzone des geschützten Workloads oder der Zeitzone des Hosts, auf dem Sie die Weboberfläche ausführen, unterscheiden. Unten rechts im Client-Fenster werden das Serverdatum und die Serveruhrzeit angezeigt.

3.4 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 Tabelle 3-2 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 ausführen	Startet die Reproduktion des Workloads entsprechend der angegebenen Parameter (vollständige Reproduktion).
Inkrementell ausführen	Führt eine inkrementelle Übertragung von geänderten Daten vom Ursprung zum Ziel außerhalb der im Vertrag 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.
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).
Erneut schützen	Nach einem erfolgreichen Failback-Vorgang steht die Option „Erneut schützen“ zur Verfügung.
Workload entfernen	Entfernt einen Workload aus dem Inventar.

3.5 Andere PlateSpin-Server-Verwaltungstools

3.5.1 PlateSpin-Konfiguration

Bestimmte Aspekte des Verhaltens des PlateSpin-Servers werden anhand von Konfigurationsparametern gesteuert, die Sie auf einer Konfigurations-Webseite mit Ihrem PlateSpin-Server-Host festlegen:

`https://Ihr_PlateSpin_Server/platespinconfiguration/`

HINWEIS: Normalerweise brauchen Sie diese Einstellungen nicht zu ändern, es sei denn, der PlateSpin-Support rät Ihnen dazu.

So ändern Sie Konfigurationsparameter und wenden sie an:

1. Öffnen Sie folgende Seite in einem beliebigen Webbrowser:

   `https://Ihr_PlateSpin_Server/platespinconfiguration/`
2. Suchen Sie den gewünschten Serverparameter und ändern Sie dessen Wert.
3. Speichern Sie die Einstellungen und schließen Sie die Seite.

   Die Änderungen treten ohne Neubooten und ohne Neustarten der PlateSpin-Dienste in Kraft.

In den nachfolgenden Themen finden Sie Informationen zu verschiedenen Situationen, in denen Sie das Produktverhalten mithilfe von PlateSpin-Konfigurationsparametern ändern müssen:

- „Anforderungen für den Betrieb des PlateSpin-Servers durch NAT“, auf Seite 36
- „Optimieren des Datentransfers über WAN-Verbindungen“, auf Seite 71
- „Optimieren der Leistung der Reproduktionsumgebung“, auf Seite 74
- „Einstellen der Methode für erneutes Booten des Konfigurationsdiensts“, auf Seite 75
- „Konfigurieren der Unterstützung für VMware vCenter Site Recovery Manager“, auf Seite 76
- „Anpassen der Weboberfläche an das Markenbild mithilfe von Konfigurationsparametern“, auf Seite 87
- „Konfigurieren der Ermittlung des aktiven Windows-Knotens“, auf Seite 125
- „Fehlersuche beim Konfigurationsdienst“, auf Seite 176

3.5.2 Protect Agent-Dienstprogramm

Mit dem Protect Agent-Dienstprogramm (ProtectAgent.cli.exe) können Sie die Treiber für die blockbasierte Übertragung installieren, aufrüsten, abfragen und deinstallieren. Beim Installieren, Deinstallieren und Aufrüsten von Treibern muss in jedem Fall neu gebootet werden; mit Protect Agent können Sie jedoch präzise steuern, wann diese Aktionen ausgeführt werden, und somit, wann der Server neu gebootet wird. Mit dem Protect Agent-Dienstprogramm ist es beispielsweise möglich, die Treiber während einer geplanten Ausfallzeit statt während der ersten Reproduktion zu installieren. Weitere Informationen hierzu finden Sie in Anhang D, „Protect Agent-Dienstprogramm“, auf Seite 141.

3.5.3 VMware-Rollenwerkzeug

Das VMware-Rollenwerkzeug (PlateSpin.VMwareRoleTool.exe) ist ein Befehlszeilenprogramm, mit dem Sie eindeutige Benutzerrollen in einem VMware-Rechenzentrum zur Unterstützung der Mehrmandantenfähigkeit erstellen. Mit den Rollen geben Sie VMware-Benutzern ohne Administratorrechte (oder „aktivierten Benutzern“) die Möglichkeit, Protect-Lebenszyklusvorgänge in der VMware-Umgebung auszuführen. Weitere Informationen hierzu finden Sie in Abschnitt 5.4, „Einrichten der Protect-Mehrmandantenfähigkeit auf VMWare“, auf Seite 57.

4 Lizenzverwaltung

Sobald Sie eine Lizenz für das Produkt aktiviert haben, können Sie die Verfügbarkeit der Workload-Lizenzen überwachen, neue Lizenzen hinzufügen und abgelaufene Lizenzen entfernen.

4.1 Aktivieren Ihrer Produktlizenz

Die PlateSpin Protect-Produktlizenz berechtigt Sie zu einer bestimmten oder auch unbegrenzten Anzahl von Workloads zum Schutz durch die Workload-Lizenzierung.

Für die Produktlizenzierung von PlateSpin Protect benötigen Sie einen Lizenzaktivierungscode. Falls Sie nicht über einen Lizenzaktivierungscode verfügen, können Sie diesen beim Customer Center (http://www.netiq.com/customercenter/) anfordern. Ein Kundenservicemitarbeiter wird sich mit Ihnen in Verbindung setzen und Ihnen den Lizenzaktivierungscode mitteilen.

HINWEIS: Wenn Sie bereits PlateSpin-Kunde sind und kein Customer Center-Konto haben, müssen Sie zunächst eins mit derselben Email-Adresse erstellen, die in Ihrer Bestellung angegeben ist. Siehe Konto erstellen (https://www.netiq.com/selfreg/jsp/createAccount.jsp).

Sie können Ihre Produktlizenz entweder online oder offline aktivieren.

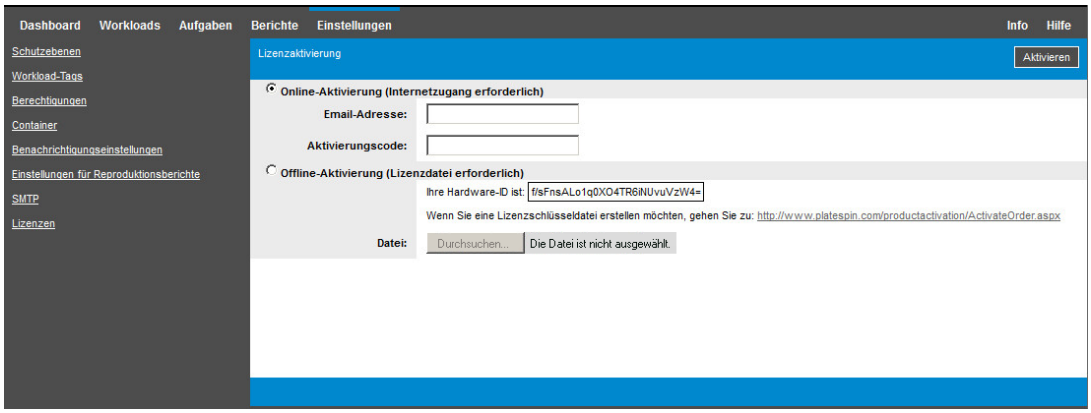
4.1.1 Online-Lizenzaktivierung

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.

So richten Sie die Online-Lizenzaktivierung ein:

1 Klicken Sie in der Weboberfläche auf **Einstellungen > Lizenzen** und dann auf **Lizenz hinzufügen**.



2 Wählen Sie **Online-Aktivierung**.

3 Geben Sie die Email-Adresse, die Sie auch bei der Auftragserteilung angegeben haben, sowie den erhaltenen Aktivierungscode an, und klicken Sie auf **Aktivieren**.

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

4.1.2 Offline-Lizenzaktivierung

Für die Offline-Aktivierung erhalten Sie einen PlateSpin Protect-Lizenzschlüssel über das Internet. Dazu müssen Sie einen Computer mit Internetzugang verwenden.

1 Klicken Sie in der Weboberfläche auf **Einstellungen > Lizenzen** und dann auf **Lizenz hinzufügen**.

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 Customer Center-Benutzernamen und Ihrem Passwort an.

4 Erstellen Sie anhand der Hardware-ID eine Lizenzschlüsseldatei. Für diesen Vorgang sind die folgenden Angaben erforderlich:

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

5 Speichern Sie die generierte Lizenzschlüsseldatei, übertragen Sie sie zum Produkt-Host, der über keine Internet-Konnektivität verfügt, und aktivieren Sie damit das Produkt.

6 Geben Sie in der Weboberfläche auf der Seite „Lizenzaktivierung“ den Pfad der Datei an, oder wechseln Sie in das entsprechende Verzeichnis, und klicken Sie auf **Aktivieren**.

   Die Lizenzschlüsseldatei wird gespeichert und das Produkt wird basierend auf dieser Datei aktiviert.

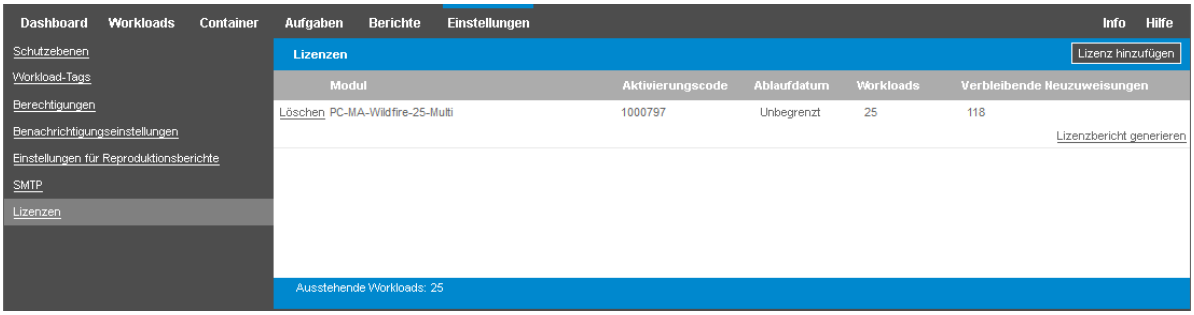
4.2 Informationen zum Workload-Lizenzverbrauch

Die PlateSpin Protect-Produktlizenz berechtigt Sie zu einer bestimmten oder auch unbegrenzten Anzahl von Workloads zum Schutz durch die Workload-Lizenzierung. Jedes Mal, 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.

Auf der Seite „Dashboard“ der PlateSpin Protect-Weboberfläche wird unter „Lizenzübersicht“ die aktuelle Anzahl der installierten und verbrauchten Lizenzen angezeigt.

Auf der Seite „Lizenzen“ (**Einstellungen** > **Lizenz**) werden alle installierten Lizenzen mit der aktuellen Anzahl der verbrauchten Workload-Lizenzen und der verbleibenden Neuzuweisungen für diese Lizenzen angezeigt. Die Seite zeigt außerdem die Gesamtzahl der verbleibenden, nicht verwendeten Workload-Lizenzen für den PlateSpin-Server.

Abbildung 4-1 *Lizenzanzahl und verbleibende Neuzuweisungen*



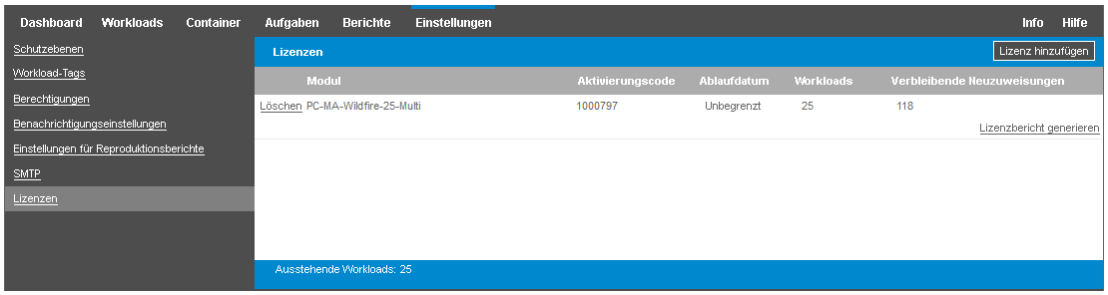
4.3 Anzeigen der Lizenzinformationen

Das Produkt-Dashboard umfasst eine Lizenzübersicht mit der Gesamtzahl der installierten Lizenzen und der aktuellen Anzahl der verbrauchten Lizenzen.

Auf der Seite „Lizenzen“ finden Sie Informationen zu den Workload-Lizenzen, die auf einem PlateSpin-Server installiert sind. Für die einzelnen Lizenzen werden jeweils die aktuelle Anzahl der verwendeten Workload-Lizenzen sowie die aktuelle Anzahl der verbleibenden Neuzuweisungen für verwendete Lizenzen angezeigt.

So rufen Sie Lizenzinformationen ab:

1. Wählen Sie in der Weboberfläche die Option **Einstellungen > Lizenzen**.



2. Lesen Sie die Lizenzinformationen:
   - Aktivierungscode
   - Ablaufdatum
   - Workloads
   - Verbleibende Neuzuweisungen
3. Beachten Sie die Angabe unter **Ausstehende Workloads** für die Anzahl der verfügbaren nicht verwendeten Lizenzen.

4.4 Hinzufügen einer Lizenz

Neue Lizenzen werden mit demselben Verfahren hinzugefügt, mit dem die erste Lizenz aktiviert wurde. Informationen hierzu finden Sie hier:

- Abschnitt 4.1.1, „Online-Lizenzaktivierung“, auf Seite 49
- Abschnitt 4.1.2, „Offline-Lizenzaktivierung“, auf Seite 50

4.5 Löschen einer Lizenz

Sie können eine abgelaufene Lizenz auf der Seite „Lizenzen“ löschen.

1. Wählen Sie in der Weboberfläche die Option **Einstellungen > Lizenzen**.
2. Lesen Sie die Lizenzinformationen.
3. Klicken Sie neben der abgelaufenen Lizenz auf **Löschen** und bestätigen Sie den Löschvorgang.

4.6 Erzeugen eines Lizenzberichts für den technischen Support

Bei Lizenzproblemen bittet Sie der technische Support unter Umständen, einen Lizenzbericht zu erzeugen. Dieser Diagnosebericht enthält verschlüsselte Produktinformationen zu den Lizenzen, die Sie für Ihren PlateSpin-Server aktiviert haben.

1. Wählen Sie in der Weboberfläche die Option **Einstellungen > Lizenzen**.
2. Klicken Sie unterhalb der Lizenzliste auf **Lizenzbericht anzeigen**.

   Die Datei `LicenseReport.txt` wird in einer neuen Browser-Registerkarte oder einem neuen Browser-Fenster geöffnet, je nach Browser-Einstellungen.
3. Speichern Sie die Datei `LicenseReport.txt` unter dem Namen `LicenseReport.psl` auf Ihrem lokalen Computer.

5 Konfigurieren der Benutzerautorisierung und -authentifizierung

Der Abschnitt enthält folgende Informationen:

5.1 Informationen zum rollenbasierten Zugriff in 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 5-1 *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 ausführen	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.

So richten Sie den ordnungsgemäßen rollenbasierten Zugriff auf PlateSpin Protect ein:

1. Fügen Sie Benutzer zu den erforderlichen, in Tabelle 5-1 aufgeführten Benutzergruppen hinzu. Weitere Informationen finden Sie in der Windows-Dokumentation.
2. Erstellen Sie Sicherheitsgruppen auf Anwendungsebene, die diese Benutzer bestimmten Workloads zuordnen. Weitere Informationen hierzu finden Sie unter „Verwalten von PlateSpin Protect-Sicherheitsgruppen und -Workload-Berechtigungen“, auf Seite 56.

5.2 Verwalten von PlateSpin Protect-Zugriff und -Berechtigungen

Die folgenden Abschnitte enthalten weitere Informationen:

- Abschnitt 5.2.1, „Hinzufügen von PlateSpin Protect-Benutzern“, auf Seite 55
- Abschnitt 5.2.2, „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Protect-Benutzer“, auf Seite 55

5.2.1 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 Server-Host vorhandenen Benutzern bestimmte Rollenberechtigungen gewähren möchten, lesen Sie bitte unter „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Protect-Benutzer“, auf Seite 55 weiter.

1. Öffnen Sie auf dem PlateSpin-Server-Host die Systemkonsole „Lokale Benutzer und Gruppen“ (**Start** > **Ausführen** > `lusrmgr.msc` > **Eingabetaste**).
2. Klicken Sie mit der rechten Maustaste auf den Knoten **Benutzer** und wählen Sie **Neuer Benutzer**.
3. 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 55.

5.2.2 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 5-1, „Details zu Workload-Schutz-Rollen und -Berechtigungen“, auf Seite 54.

1. Öffnen Sie auf dem PlateSpin-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 auf der Registerkarte **Mitglied von** auf **Hinzufügen**.
4. Suchen Sie die gewünschte Workload-Schutzgruppe und weisen Sie sie dem Benutzer zu.

Es kann einige Minuten dauern, bis die Änderung wirksam wird. Zur manuellen Anwendung der Änderungen müssen Sie den Server mit der ausführbaren Datei `RestartPlateSpinServer.exe` neu starten.

So starten Sie den Webserver neu:

1. Bevor Sie den PlateSpin-Server neu starten, halten Sie alle Verträge an, oder stellen Sie sicher, dass derzeit keine Reproduktion, kein Failover und kein Failback ausgeführt wird. Setzen Sie den Vorgang erst dann fort, wenn alle Workloads im Leerlauf sind.
2. Navigieren Sie auf dem PlateSpin-Server-Host zum Unterverzeichnis `..\bin\RestartPlateSpinServer`.
3. Doppelklicken Sie auf die Programmdatei `RestartPlateSpinServer.exe`.

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

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 56.

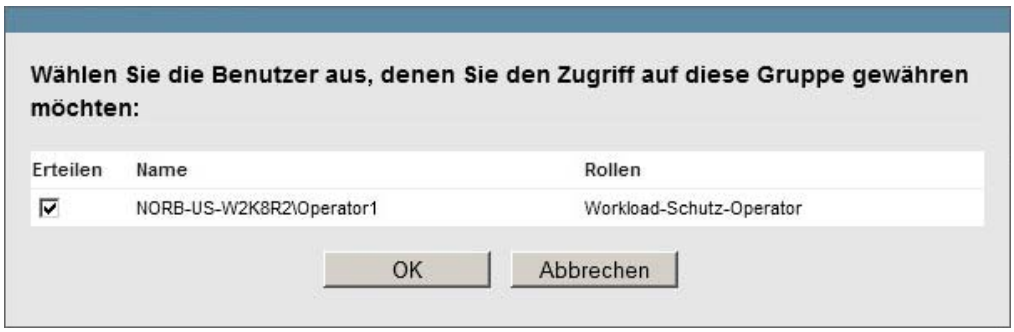
5.3 Verwalten von PlateSpin Protect-Sicherheitsgruppen und -Workload-Berechtigungen

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.

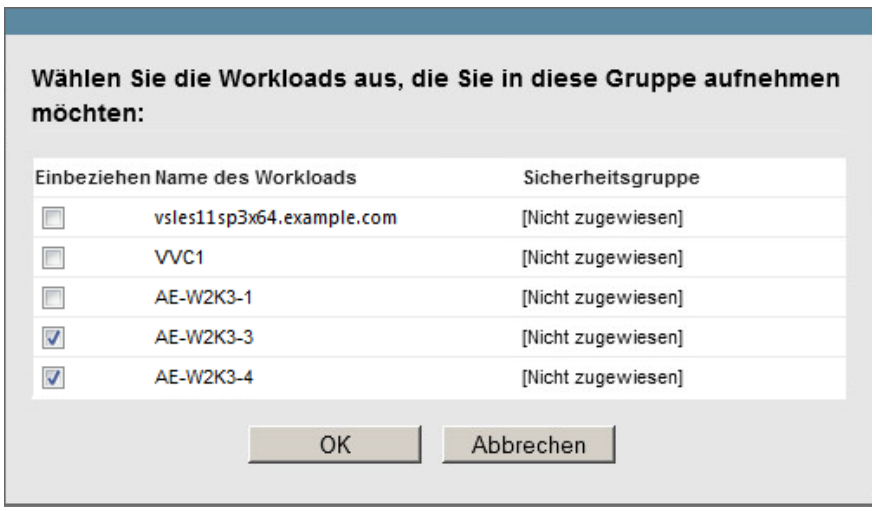
1. Weisen Sie einem PlateSpin Protect-Benutzer die Workload-Schutz-Rolle zu, deren Berechtigungen am besten für die Rolle dieses Benutzers in Ihrer Organisation geeignet sind. Weitere Informationen hierzu finden Sie unter „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Protect-Benutzer“, auf Seite 55.
2. Greifen Sie als Administrator auf der PlateSpin Protect-Weboberfläche auf PlateSpin Protect zu, und klicken Sie 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.

5.4 Einrichten der Protect-Mehrmandantenfähigkeit auf VMWare

PlateSpin Protect enthält eindeutige Benutzerrollen (und ein Werkzeug für deren Erstellung in einem VMware-Rechenzentrum), die es VMware-Benutzern ohne Administratorrechte (oder „aktivierten Benutzern“) ermöglicht, Protect-Lebenszyklusvorgänge in der VMware-Umgebung auszuführen. Anhand dieser Rollen können Sie als Dienstanbieter Ihren VMware-Cluster für eine Mehrfachmandantenfähigkeit segmentieren. Dies bedeutet, dass mehrere Protect-Container in Ihrem Rechenzentrum instanziiert werden und Protect-Kunden oder „Mandanten“ aufnehmen können, die ihre Daten und den Nachweis über deren Vorhandensein von anderen Kunden, die ebenfalls Ihr Rechenzentrum nutzen, getrennt halten und den Zugriff durch diese Kunden verhindern möchten.

Dieser Abschnitt enthält folgende Informationen:

5.4.1 Definieren von VMware-Rollen für Mehrfachmandantenfähigkeit

PlateSpin Protect erfordert bestimmte Berechtigungen für den Zugriff auf und die Durchführung von Aufgaben in der VMware-Infrastruktur (also VMware-„Container“), die den Protect-Workflow und die Protect-Funktionen in dieser Umgebung ermöglichen. Die Datei `PlateSpinRole.xml` definiert die mindestens erforderlichen Berechtigungen und verbindet sie in den drei benutzerdefinierten VMware-Rollen:

- PlateSpin-Manager für virtuelle Maschinen
- PlateSpin-Infrastruktur-Manager
- PlateSpin-Benutzer

Diese Datei ist in der Installation des PlateSpin Protect-Servers enthalten. Über eine zusätzliche ausführbare Datei (`PlateSpin.VMware.Role.Tool.exe`) kann auf die Datei zugegriffen werden, um die Erstellung dieser benutzerdefinierten PlateSpin-Rollen in einer vCenter-Zielumgebung zu ermöglichen.

Standardmäßig befinden sich die Rollendefinitionsdatei (`PlateSpinRole.xml`) und das Rollendefinitionswerkzeug (`PlateSpin.VMwareRoleTool.exe`) im Ordner `\VMwareRolesTool:`

`<Installationsverzeichnis>\PlateSpin Protect Server\bin\VMwareRolesTool`

Dieser Abschnitt enthält folgende Informationen:

- „(Optional) Manuelle Definition der PlateSpin-Rollen in vCenter“, auf Seite 59
- „Anzeigen von Berechtigungen für benutzerdefinierte PlateSpin-Rollen in vCenter“, auf Seite 59

Grundlegende Befehlszeilensyntax

Führen Sie an dem Ort, an dem das Rollenwerkzeug installiert ist, das Werkzeug an der Befehlszeile aus und verwenden Sie dazu diese grundlegende Syntax:

```
PlateSpin.VMware.Role.Tool.exe /host=[host name or IP address of vCenter or ESX host] /user=[user name] /role=[PlateSpinRole.xml] /create
```

`PlateSpinRole.xml` bezeichnet den Namen der Rollendefinitionsdatei.

HINWEIS: Die Datei mit der Rollendefinition befindet sich standardmäßig im Ordner mit dem Rollendefinitionswerkzeug.

Zusätzliche Befehlszeilenparameter und -flaggen

Wenden Sie nach Bedarf die folgenden Parameter an, wenn Sie die `PlateSpin.VMwareRole.Tool.exe` zur Erstellung oder Aktualisierung in vCenter verwenden:

Parameter

`/Erstellen`	(Obligatorisch) Erstellt die Rollen, die durch den Parameter `/role` definiert wurden
`/Alle_Berechtigungen_abrufen`	Zeigt alle vom Server definierten Berechtigungen an
`/get_compatible_roles`	Zeigt alle Rollen an, die mit der durch `/role` definierten Rolle kompatibel sind
`/check_role=[`*`Rollenname`*`]`	Prüft die Kompatibilität der angegebenen Rolle mit der durch `/role` definierten Rolle

Optionale Flaggen

`/Interaktiv`	Führen Sie das Werkzeug mit interaktiven Optionen aus, anhand deren Sie einzelne Rollen wählen, die Rollenkompatibilität überprüfen oder alle kompatiblen Rollen auflisten können. Weitere Informationen zur Verwendung des Werkzeugs im interaktiven Modus finden Sie unter *VMware-Rollenwerkzeug zum Verifizieren von Berechtigungen für Rollen* (KB 7018547) (https://www.netiq.com/support/kb/doc.php?id=7018547).
`/password=[passwort]`	Gibt das VMware-Passwort an (umgeht die Aufforderung zur Eingabe des Passworts)
`/verbose`	Zeigt detaillierte Informationen an

Beispiel für die Verwendung des Werkzeugs

Verwendung: `PlateSpin.VMwareRole.Tool.exe /Host=Houston_Vertrieb /Benutzer=pedrom / Rolle=PlateSpinRole.xml /create`

Resultierende Aktionen:

1. Das Werkzeug für die Rollendefinition wird auf dem vCenter-Server `Houston_Vertrieb` ausgeführt, auf dem ein Administrator mit dem Benutzernamen `pedrom` vorhanden ist.
2. Wenn der Parameter `/password` nicht vorhanden ist, fordert das Werkzeug zur Eingabe des Benutzerpassworts auf, das Sie daraufhin eingeben.
3. Das Werkzeug greift auf die Rollendefinitionsdatei (`PlateSpinRole.xml`) zu, die sich im selben Verzeichnis befindet wie die ausführbare Datei für das Werkzeug (der Pfad dazu musste nicht näher definiert werden).
4. Das Werkzeug findet die Definitionsdatei und wird angewiesen (`/Erstellen`), die im Inhalt dieser Datei definierten Rollen in der vCenter-Umgebung zu erstellen.
5. Das Werkzeug greift auf die Definitionsdatei zu und erstellt die neuen Rollen (einschließlich der entsprechenden Mindestberechtigungen für den definierten, eingeschränkten Zugriff) innerhalb von vCenter.

   Die neuen benutzerdefinierten Rollen müssen später Benutzern in vCenter zugewiesen werden.

(Optional) Manuelle Definition der PlateSpin-Rollen in vCenter

Sie können den vCenter-Client verwenden, um die benutzerdefinierten PlateSpin-Rollen zu erstellen und zuzuweisen. Dazu ist es erforderlich, die Rollen mit den aufgeführten Berechtigungen wie in `PlateSpinRole.xml` definiert zu erstellen. Wenn Sie die Rollen manuell erstellen, gibt es für den Namen der Rollen keine Beschränkungen. Die einzige Beschränkung besteht darin, dass die Rollennamen, die Sie entsprechend der Rollen in der Definitionsdatei erstellen, über alle Mindestberechtigungen verfügen, die in der Definitionsdatei aufgeführt sind.

Weitere Informationen zur Erstellung von benutzerdefinierten Rollen in vCenter finden Sie unter *Verwalten der VMWare VirtualCenter-Rollen und -Berechtigungen* (http://www.vmware.com/pdf/vi3_vc_roles.pdf) im technischen Ressourcen-Center von VMware.

Anzeigen von Berechtigungen für benutzerdefinierte PlateSpin-Rollen in vCenter

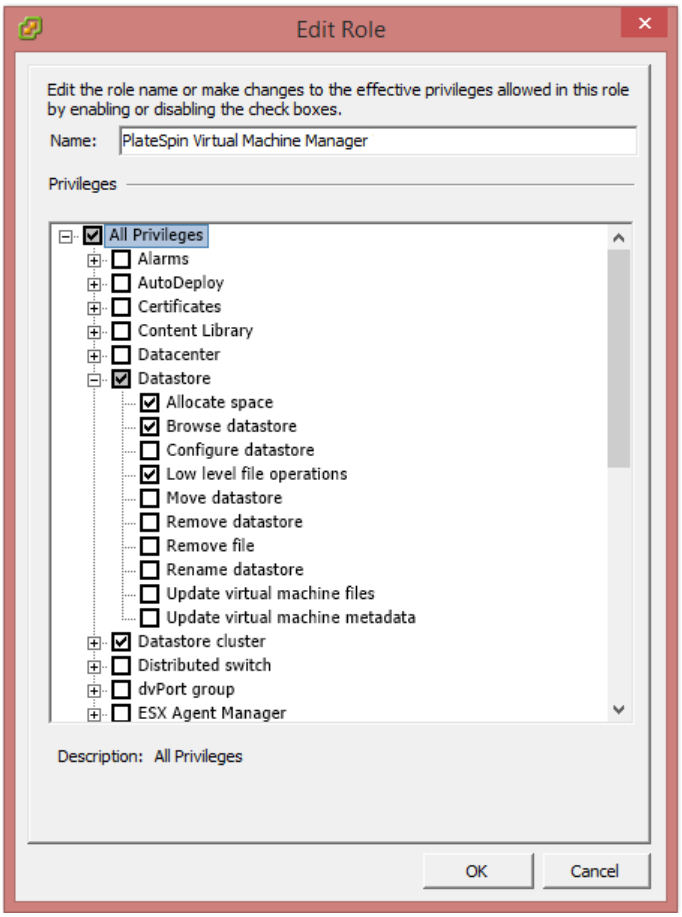
Im vCenter-Client zeigen Sie die Mindestberechtigungen an, die für benutzerdefinierte PlateSpin-Rollen festgelegt sind.

1 Wählen Sie eine benutzerdefinierte Rolle in vCenter aus:

- PlateSpin-Manager für virtuelle Maschinen
- PlateSpin-Infrastruktur-Manager
- PlateSpin-Benutzer

2 Klicken Sie auf **Bearbeiten**, um die Berechtigungseinstellungen im Dialogfeld zum Bearbeiten der Rolle anzuzeigen.

Die folgende Abbildung zeigt beispielsweise einige der für die Rolle „PlateSpin-Manager für virtuelle Maschinen“ festgelegten Berechtigungen.



5.4.2 Zuweisen von Rollen in vCenter

Beim Einrichten einer Mehrmandantenumgebung müssen Sie pro Kunde oder „Mandant“ einen einzelnen Protect-Server bereitstellen. Sie weisen diesem Protect-Server einen aktivierten Benutzer mit bestimmten Protect-VMware-Rollen zu. Dieser aktivierte Benutzer erstellt den Protect-Container. Als Service-Anbieter bewahren Sie den Berechtigungsnachweis dieses Benutzers auf und geben ihn Ihrem Mandantenkunden nicht bekannt.

In der folgenden Tabelle sind die Rollen aufgeführt, die Sie benötigen, um den aktivierten Benutzer zu definieren. Sie enthält auch weitere Informationen über den Zweck der Rolle:

vCenter-Container für die Rollenzuweisung	**Details zur Rollenzuweisung**	**Anweisungen für die Übertragung**	**Weitere Informationen**
Stamm des vCenter-Inventarbaums	Weisen Sie dem aktivierten Benutzer die *PlateSpin-Infrastruktur-Manager*-Rolle (oder eine entsprechende Rolle) zu.	Aus Sicherheitsgründen müssen Sie die Berechtigung als nicht übertragbar definieren.	Diese Rolle ist erforderlich, um Aufgaben zu überwachen, die von der Protect-Software ausgeführt werden, und um abgelaufene WMware-Sitzungen zu beenden.
Alle Rechenzentrum-objekte, auf die der aktivierte Benutzer zugreifen muss	Weisen Sie dem aktivierten Benutzer die *PlateSpin-Infrastruktur-Manager*-Rolle (oder eine entsprechende Rolle) zu.	Aus Sicherheitsgründen müssen Sie die Berechtigung als nicht übertragbar definieren.	Diese Rolle ist erforderlich, um den Zugriff auf die Datenspeicher des Rechenzentrums für den Datei-Upload/Download zuzulassen. Definieren Sie die Berechtigung als nicht übertragbar.
Jeder Cluster, der als Container zu Protect hinzugefügt werden soll, und jeder Host, der im Cluster enthalten ist	Weisen Sie dem aktivierten Benutzer die *PlateSpin-Infrastruktur-Manager*-Rolle (oder eine entsprechende Rolle) zu.	Die Übertragung liegt im Ermessen des VMware-Administrators.	Für die Zuweisung zu einem Host müssen Sie die Berechtigung vom Cluster-Objekt übertragen oder eine zusätzliche Berechtigung an jedem Cluster-Host erstellen. Wenn die Rolle am Cluster-Objekt zugewiesen und übertragen wird, sind keine weiteren Änderungen beim Hinzufügen eines neuen Hosts zum Cluster erforderlich. Die Übertragung dieser Berechtigung bringt jedoch Auswirkungen auf die Sicherheit mit sich.
Jeder Ressourcen-Pool, auf den der aktivierte Benutzer zugreifen muss	Weisen Sie dem aktivierten Benutzer die Rolle des *PlateSpin-Managers für virtuelle Maschinen* (oder eine entsprechende Rolle) zu.	Die Übertragung liegt im Ermessen des VMware-Administrators.	Obwohl Sie den Zugriff auf eine beliebige Anzahl von Ressourcen-Pools an einem Standort im Baum zuweisen können, müssen Sie dem aktivierten Benutzer diese Rolle an mindestens einem Ressourcen-Pool zuweisen.

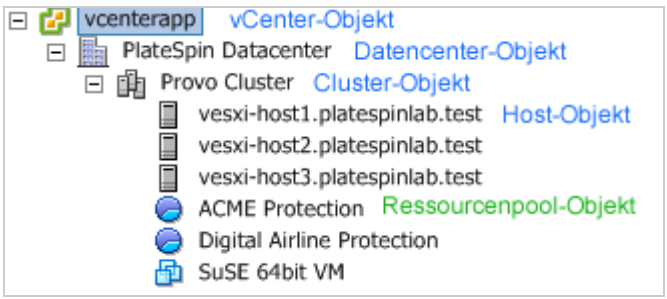
vCenter-Container für die Rollenzuweisung	Details zur Rollenzuweisung	Anweisungen für die Übertragung	Weitere Informationen
Jeder VM-Ordner, auf den der aktivierte Benutzer zugreifen muss	Weisen Sie dem aktivierten Benutzer die Rolle des *PlateSpin-Managers für virtuelle Maschinen* (oder eine entsprechende Rolle) zu.	Die Übertragung liegt im Ermessen des VMware-Administrators.	Obwohl Sie den Zugriff auf eine beliebige Anzahl von VM-Ordnern an einem beliebigen Standort im Baum zuweisen können, müssen Sie dem aktivierten Benutzer diese Rolle an mindestens einem Ordner zuweisen.
Jedes Netzwerk, auf das der aktivierte Benutzer zugreifen muss Verteilte virtuelle Netzwerke mit einem dvSwitch und einer dvPortgroup	Weisen Sie dem aktivierten Benutzer die Rolle des *PlateSpin-Managers für virtuelle Maschinen* (oder eine entsprechende Rolle) zu.	Die Übertragung liegt im Ermessen des VMware-Administrators.	Obwohl Sie den Zugriff auf eine beliebige Anzahl von Netzwerken an einem beliebigen Standort im Baum zuweisen können, müssen Sie dem aktivierten Benutzer diese Rolle an mindestens einem Ordner zuweisen. ◆ Um dem dvSwitch die richtige Rolle zuzuweisen, müssen Sie die Rolle auf das Rechenzentrum übertragen (wodurch ein weiteres Objekt erstellt wird, das die Rolle erhält) oder den dvSwitch in einen Ordner stellen und die Rolle an diesem Ordner zuweisen. ◆ Damit eine Standard-Portgruppe als verfügbares Netzwerk an der Protect-Oberfläche aufgeführt wird, müssen Sie dafür an jedem Host im Cluster eine Definition erstellen.
Jeder Datenspeicher und Datenspeicher-Cluster, auf den der aktivierte Benutzer zugreifen muss	Weisen Sie dem aktivierten Benutzer die Rolle des *PlateSpin-Managers für virtuelle Maschinen* (oder eine entsprechende Rolle) zu.	Die Übertragung liegt im Ermessen des VMware-Administrators.	Dem aktivierten Benutzer muss diese Rolle an mindestens einem Datenspeicher oder Datenspeicher-Cluster zugewiesen worden sein. Bei Datenspeicher-Clustern muss die Berechtigung an die darin enthaltenen Datenspeicher übertragen werden. Wenn für ein einzelnes Mitglied des Clusters kein Zugriff bereitgestellt wurde, treten bei vorbereiteten und vollständigen Reproduktionen Fehler auf..

In der folgenden Tabelle sehen Sie die Rolle, die Sie dem Kunden oder Mandantenbenutzer zuweisen können.

vCenter-Container für die Rollenzuweisung	Details zur Rollenzuweisung	Anweisungen für die Übertragung	Weitere Informationen
Alle Ressourcen-Pools und Ordner, in denen die virtuellen Maschinen des Kunden erstellt werden	Weisen Sie dem Mandantenbenutzer die *PlateSpin-Benutzer*-Rolle (oder eine entsprechende Rolle) zu.	Die Übertragung liegt im Ermessen des VMware-Administrators.	Dieser Mandant ist Mitglied der PlateSpin-Administratorgruppe am PlateSpin Protect-Server und ist auch am vCenter-Server vorhanden. Wenn der Mandant die von der virtuellen Maschine verwendeten Ressourcen (also die Netzwerke, ISO-Images etc.) ändern darf, müssen Sie diesem Benutzer dazu die nötigen Berechtigungen an diesen Ressourcen erteilen. Wenn Sie dem Kunden beispielsweise erlauben möchten, das Netzwerk zu ändern, in das seine virtuelle Maschine eingebunden ist, dann sollten Sie diesem Benutzer (mindestens) die schreibgeschützte Rolle (oder eine höhere Rolle) an allen Netzwerken zuweisen, auf die der Kunde zugreifen darf.

In der folgenden Abbildung ist eine virtuelle Infrastruktur in der vCenter-Konsole dargestellt. Den blau gekennzeichneten vCenter-, Rechenzentrums-, Cluster- und Hostobjekten wird die Rolle des Infrastruktur-Managers zugewiesen. Den grün gekennzeichneten Ressourcenpoolobjekten wird die Rolle des Managers für virtuelle Maschinen zugewiesen. Der Baum zeigt keine VM-Ordner, Netzwerke und Datenspeicher. Diesen Objekten wird die Rolle des *PlateSpin-Managers für virtuelle Maschinen* zugewiesen.

Abbildung 5-1 *In vCenter zugewiesene Rollen*



Auswirkungen auf die Sicherheit durch Zuweisen von VMware-Rollen

Die PlateSpin-Software verwendet einen aktivierten Benutzer nur zur Durchführung von Schutzmaßnahmen für Lebenszyklusvorgängen. Aus Ihrer Sicht als Service-Anbieter hat ein Endbenutzer niemals Zugriff auf den Berechtigungsnachweis des aktivierten Benutzers und kann nicht auf denselben Satz von VMware-Ressourcen zugreifen. In einer Umgebung, in der mehrere

Protect-Server für die Verwendung derselben vCenter-Umgebung konfiguriert sind, verhindert Protect die Möglichkeit für den Zugriff über mehrere Clients hinweg. Die wichtigsten Auswirkungen auf die Sicherheit sind wie folgt:

- Wenn die Rolle des *PlateSpin-Infrastruktur-Managers* dem vCenter-Objekt zugewiesen wurde, kann jeder aktivierte Benutzer die von jedem anderen Benutzer ausgeführten Aufgaben sehen (doch diese nicht bearbeiten).
- Da es keine Möglichkeit gibt, Berechtigungen an Datenspeicherordnern oder -unterordnern festzulegen, haben alle aktivierten Benutzer mit Berechtigungen an einem Datenspeicher Zugriff auf die Festplatten aller anderen aktivierten Benutzer, die im Datenspeicher gespeichert sind.
- Wenn die Rolle des *PlateSpin-Infrastruktur-Managers* dem Cluster-Objekt zugewiesen wurde, kann jeder aktivierte Benutzer HA oder DRS am gesamten Cluster aus- oder einschalten.
- Wenn die *PlateSpin-Benutzer*-Rolle am Speicher-Cluster-Objekt zugewiesen wurde, kann jeder aktivierte Benutzer SDRS für den gesamten Cluster aus- oder einschalten.
- Durch Festlegen der Rolle des *PlateSpin-Infrastruktur-Managers* am DRS-Cluster-Objekt und Übertragen dieser Rolle kann der aktivierte Benutzer alle virtuelle Maschinen sehen, die sich im Standard-Ressourcen-Pool und/oder Standard-VM-Ordner befinden. Für die Übertragung ist es außerdem erforderlich, dass der Administrator ausdrücklich für den aktivierten Benutzer festlegt, dass dieser eine „Nicht-Zugriff“-Rolle an jedem Ressourcen-Pool/VM-Ordner erhält, auf die dieser aktivierte Benutzer nicht zugreifen sollte.
- Durch Festlegen der Rolle des *PlateSpin-Infrastruktur-Managers* am vCenter-Objekt darf der aktivierte Benutzer Sitzungen von anderen Benutzern beenden, die mit dem vCenter verbunden sind.

HINWEIS: Denken Sie daran, dass in diesen Szenarien die unterschiedlichen aktivierten Benutzer tatsächlich verschiedene Instanzen der PlateSpin-Software darstellen.

---

6 Konfigurieren der PlateSpin-Server-Anwendung

In diesem Abschnitt werden die Konfigurationsvoraussetzungen und die Einrichtung für PlateSpin Protect beschrieben.

6.1 Konfigurieren der Spracheinstellungen für internationale Versionen

Neben Englisch bietet PlateSpin Protect auch landessprachliche Unterstützung (National Language Support, NLS) für die folgenden internationalen Sprachen:

- Chinesisch-vereinfacht
- Chinesisch-traditionell
- Französisch
- Deutsch
- Japanisch

Zum Verwalten Ihres PlateSpin-Servers in einer der unterstützten Sprachen konfigurieren Sie den Sprachencode für das Betriebssystem auf dem PlateSpin-Server-Host und in Ihrem Webbrowser.

6.1.1 Einstellen der Sprache im Betriebssystem

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

So ändern Sie die Sprache des Betriebssystems:

1. Rufen Sie Ihren PlateSpin 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.

6.1.2 Einstellen der Sprache im Webbrowser

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

1. Rufen Sie im Webbrowser die Spracheinstellung auf:
   - **Chrome:**
     1. Wählen Sie im Chrome-Menü den Befehl **Einstellungen**, blättern Sie zum Link **Erweiterte Einstellungen anzeigen** und klicken Sie darauf.
     2. Blättern Sie zu **Sprachen**, und klicken Sie auf **Sprach- und Eingabeeinstellungen**.
   - **Firefox:**
     1. Wählen Sie im Menü **Extras** den Befehl **Optionen**, und wählen Sie die Registerkarte **Inhalt**.
     2. Klicken Sie unter **Sprachen** auf **Wählen**.
   - **Internet Explorer:**
     1. Wählen Sie im Menü **Extras** den Befehl **Internetoptionen**, und wählen Sie die Registerkarte **Allgemein**.
     2. Klicken Sie unter **Darstellung** auf **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-Server herstellen. Weitere Informationen hierzu finden Sie unter „Starten der Weboberfläche“, auf Seite 41.

HINWEIS: (Für Benutzer der chinesischen Sprachversionen) Der Versuch, über einen Browser ohne spezifische chinesische Version eine Verbindung zum PlateSpin 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.

6.2 Konfigurieren der E-Mail-Benachrichtigungsdienste für Ereignisse und Reproduktionsberichte

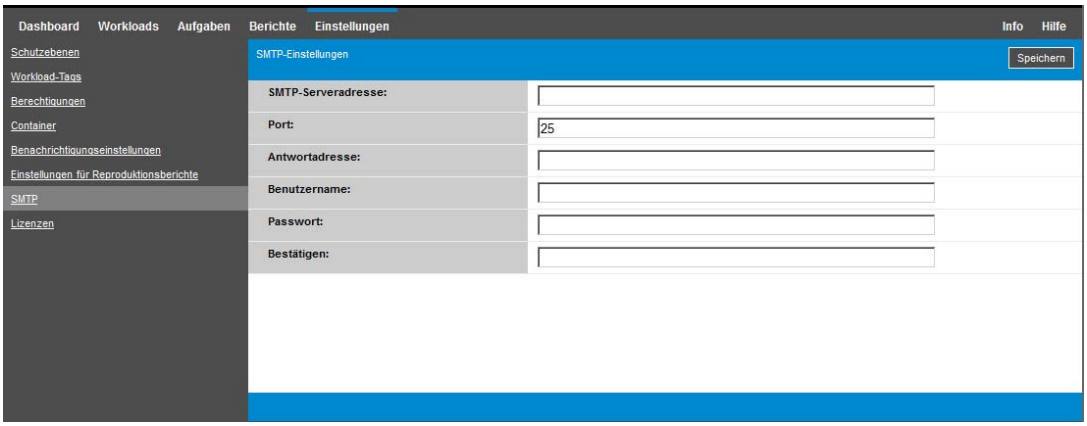
Sie können PlateSpin Protect so konfigurieren, dass automatische E-Mail-Benachrichtigungen zu Ereignissen und zum Fortschritt an angegebene E-Mail-Adressen zuständiger Empfänger versendet werden. Für diese Funktion ist es erforderlich, dass Sie zuerst einen gültigen SMTP-Server für PlateSpin Protect angeben.

- Abschnitt 6.2.1, „Konfigurieren von SMTP für den E-Mail-Benachrichtigungsdienst“, auf Seite 67
- Abschnitt 6.2.2, „Aktivieren von Ereignisbenachrichtigungen“, auf Seite 68
- Abschnitt 6.2.3, „Aktivieren von Reproduktionsberichten“, auf Seite 69

6.2.1 Konfigurieren von SMTP für den E-Mail-Benachrichtigungsdienst

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

Abbildung 6-1 *SMTP-Einstellungen (Simple Mail Transfer Protocol)*



So konfigurieren Sie die SMTP-Einstellungen:

1. Klicken Sie auf Ihrer PlateSpin Protect-Weboberfläche auf **Einstellungen > SMTP**.
2. Legen Sie die SMTP-Servereinstellungen zum Empfangen von E-Mail-Benachrichtigungen zu Ereignissen und zu Fortschritten fest:
   - **Adresse**
   - **Port** (standardmäßig 25)
   - **Antwortadresse**
3. Geben Sie den Benutzernamen und das Passwort ein. Bestätigen Sie anschließend das Passwort.
4. Klicken Sie auf **Speichern**.

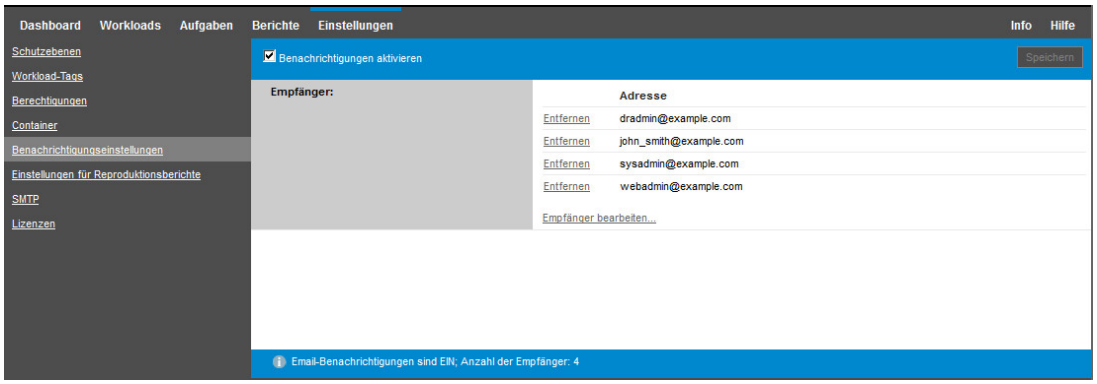
6.2.2 Aktivieren von Ereignisbenachrichtigungen

Ereignisse werden stets in das Systemanwendungs-Ereignisprotokoll mit den Protokolleintragsarten „Warnmeldung“, „Fehler“ und „Informationen“ eingetragen. Sie können auch festlegen, dass automatisch Ereignisbenachrichtigungen an zuständige Empfänger gesendet werden.

1. Richten Sie einen SMTP-Server für PlateSpin Protect ein.

   Weitere Informationen hierzu finden Sie in „Konfigurieren von SMTP für den E-Mail-Benachrichtigungsdienst“, auf Seite 67.

2. Klicken Sie auf der PlateSpin Protect-Weboberfläche auf **Einstellungen > 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**.

   Wenn Sie eine E-Mail-Adresse löschen möchten, klicken Sie neben der Adresse auf **Entfernen**.

Die in Tabelle 6-1 genannten Ereignisarten können E-Mail-Benachrichtigungen auslösen, wenn die E-Mail-Benachrichtigung aktiviert ist.

HINWEIS: Die Ereignisprotokolleinträge besitzen eindeutige IDs, die sich jedoch in künftigen Hauptversionen durchaus ändern können.

Tabelle 6-1 *Ereignistypen nach Protokolleintragsarten*

Ereignisarten	Anmerkungen
Protokolleintragsart: Warnmeldung	
`FullReplicationMissed`	Ähnlich dem Ereignis `Inkrementelle Reproduktion verpasst`.

Ereignisarten	Anmerkungen
`IncrementalReplicationMissed`	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.
`WorkloadOfflineDetected`	Wird generiert, wenn das System erkennt, dass ein Workload, der zuvor online war, nun offline ist. Betrifft Workloads, deren Schutzvertragsstatus nicht **Unterbrochen** lautet.
Protokolleintragsart: Fehler	
`FailoverFailed`	
`FullReplicationFailed`	
`IncrementalReplicationFailed`	
`PrepareFailoverFailed`	
Protokolleintragsart: Informationen	
`FailoverCompleted`	
`FullReplicationCompleted`	
`IncrementalReplicationCompleted`	
`PrepareFailoverCompleted`	
`TestFailoverCompleted`	Wird generiert, wenn ein Failover-Test-Vorgang manuell als ordnungsgemäß durchgeführt oder als Fehler gekennzeichnet wird.
`WorkloadOnlineDetected`	Wird generiert, wenn das System erkennt, dass ein Workload, der zuvor offline war, nun online ist. Betrifft Workloads, deren Schutzvertragsstatus nicht **Unterbrochen** lautet.

6.2.3 Aktivieren von Reproduktionsberichten

Sie können festlegen, dass Reproduktionsberichte automatisch an zuständige Empfänger gesendet werden.

1 Richten Sie einen SMTP-Server für PlateSpin Protect ein.

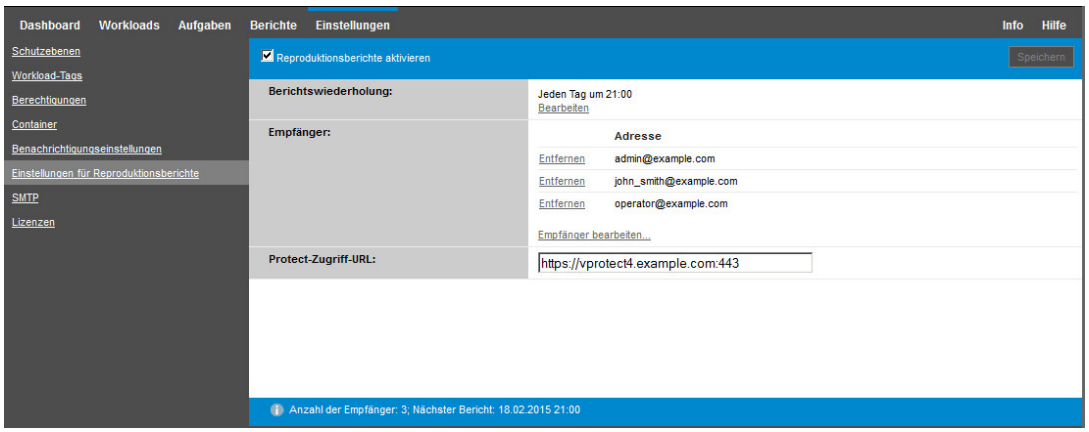
Weitere Informationen hierzu finden Sie in „Konfigurieren von SMTP für den E-Mail-Benachrichtigungsdienst“, auf Seite 67.

2 Klicken Sie auf der PlateSpin Protect-Weboberfläche auf **Einstellungen > Einstellungen für Reproduktionsberichte**.

3 Wählen Sie die Option **Reproduktionsberichte aktivieren**.

4 Klicken Sie im Abschnitt **Berichtswiederholung** auf **Bearbeiten**, und geben Sie das entsprechende Wiederholungsmuster für die Berichte an. Mit **Schließen** können Sie den Abschnitt wieder komprimieren.

5 Klicken Sie im Abschnitt **Empfänger** auf **Empfänger bearbeiten**, geben Sie die entsprechenden E-Mail-Adressen getrennt durch Kommas ein und klicken Sie anschließend auf **OK**. Mit **Entfernen** neben einer E-Mail-Adresse können Sie den Empfänger aus der Liste löschen.



6 (Optional) Geben Sie im Abschnitt **Protect-Zugriff-URL** eine nicht standardmäßige URL für Ihren PlateSpin-Server ein (z. B. wenn Ihr PlateSpin-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 173.

6.3 Konfigurieren von alternativen IP-Adressen für den PlateSpin-Server

Sie können alternative IP-Adressen in den PlateSpin-Konfigurationsparameter `AlternateServerAddresses` eintragen, sodass der PlateSpin-Server über NAT-fähige Umgebungen genutzt werden kann.

So tragen Sie alternative IP-Adressen für den PlateSpin-Server ein:

1 Öffnen Sie folgende Seite in einem beliebigen Webbrowser:

`https://`*`Ihr_PlateSpin_Server`*`/platespinconfiguration/`

2 Suchen Sie den Parameter `AlternateServerAddresses` und tragen Sie IP-Adressen für den PlateSpin-Server ein.

3 Speichern Sie die Einstellungen und schließen Sie die Seite.

Die Änderungen treten ohne Neubooten und ohne Neustarten der PlateSpin-Dienste in Kraft.

6.4 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 anhand der Einstellungen im Konfigurationswerkzeug auf Ihrem PlateSpin-Server-Host liest. Weitere Informationen finden Sie unter Abschnitt 3.5.1, „PlateSpin-Konfiguration“, auf Seite 46.

6.4.1 Feinabstimmung der Parameter

Mit den Parametern für die Konfiguration der Dateiübertragung optimieren Sie die Datenübertragung über ein WAN. Diese globalen Einstellungen gelten für alle dateibasierten und VSS-Reproduktionen.

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.

Tabelle 6-2 zeigt die Konfigurationsparameter auf der PlateSpin-Konfigurationsseite (`https://`*`Ihr_PlateSpin-Server`*`/platespinconfiguration/`), die die Datenübertragungsgeschwindigkeit steuern; hier sind jeweils die Standardwerte und die maximal zulässigen Werte angegeben. Zum Optimieren der Funktionsfähigkeit in einer WAN-Umgebung mit hoher Latenz können Sie diese Werte nach dem Prinzip von Versuch und Irrtum bearbeiten.

Tabelle 6-2 *Standardparameter und optimierte Konfigurationsparameter für die Datenübertragung*

Parameter	Standardwert	Höchstwert
`AlwaysUseNonVSSFileTransferForWindows2003`	Falsch	
`FileTransferCompressionThreadsCount` Steuert die Anzahl der Threads, die für die Datenkomprimierung auf Paketebene verwendet werden. Diese Einstellung wird ignoriert, wenn die Komprimierung deaktiviert ist. Da die Komprimierung CPU-abhängig ist, kann sich diese Einstellung auf die Arbeitsgeschwindigkeit auswirken.	2	nicht zutreffend
`FileTransferBufferThresholdPercentage` Bestimmt die Mindestdatenmenge, die im Puffer gespeichert wird, bevor neue Netzwerkpakete erstellt und gesendet werden.	10	
`FileTransferKeepAliveTimeOutMilliSec` Gibt an, wie lange mit dem Absenden von Keep-Alive-Meldungen gewartet werden soll, wenn eine TCP-Zeitüberschreitung eingetreten ist.	120000	

Parameter	Standardwert	Höchstwert
`FileTransferLongerThan24HoursSupport`	Wahr	
`FileTransferLowMemoryThresholdInBytes` Bestimmt die Untergrenze für die Speichermenge auf dem Server. (Unterhalb dieser Mindestmenge treten bestimmte Netzwerkverhaltensweisen stärker auf.)	536870912	
`FileTransferMaxBufferSizeForLowMemoryInBytes` Bestimmt die Größe des internen Puffers bei mangelndem Speicherplatz.	5242880	
`FileTransferMaxBufferSizeInBytes` Bestimmt die Größe des internen Puffers für die Speicherung von Paketdaten.	31457280	
`FileTransferMaxPacketSizeInButes` Bestimmt die Größe der größten noch versendbaren Pakete.	1048576	
`FileTransferMinCompressionLimit` Gibt den Schwellwert für die Komprimierung auf Paketebene in Byte an.	0 (deaktiviert)	Max. 65536 (64 KB)
`FileTransferPort`	3725	

`FileTransferSendReceiveBufferSize`
 	
Definiert die maximal zulässige Größe (in Byte) des Sende- und Empfangspuffers für TCP-Verbindungen im Reproduktionsnetzwerk. Die Puffergröße wirkt sich auf die Größe des TCP-Emfangsfensters (RWIN) aus, mit der wiederum die Datenmenge (in Byte) bestimmt wird, die ohne TCP-Bestätigung gesendet werden kann. Diese Einstellung ist sowohl für dateibasierte als auch für blockbasierte Übertragungen relevant. Wenn Sie die Puffergröße gemäß der Bandbreite und der Latenz des Netzwerks anpassen, wird der Durchsatz erhöht und die CPU-Tätigkeit wird vermindert.
 	
Wenn der Wert auf 0 (aus) 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 in MBit/s / 8) * VERZÖGERUNG in Sekunden)) * 1.000 * 1.024
 	
Beispielsweise wäre die geeignete Puffergröße bei einer 100-Mb/s-Verbindung mit 10 ms Latenz wie folgt:
 	
`(100/8)*0,01 * 1024 * 1000 = 128000 Byte`
 	
Weitere Informationen zur Feinabstimmung finden Sie unter Abschnitt 6.4.2, „Feinabstimmung für FileTransferSendReceiveBufferSize“, auf Seite 73.
	0 (8192 Byte)	Max. 5242880 (5 MB)

Parameter	Standardwert	Höchstwert
`FileTransferSendReceiveBufferSizeLinux` Gibt die Einstellung der TCP/IP-Empfangsfenstergröße (RWIN) für Dateiübertragungsverbindungen unter Linux an. Sie steuert die Anzahl der Byte, die ohne TCP-Acknowledgement gesendet werden. Angabe in Byte. Wenn der Wert auf 0 (aus) gesetzt ist, wird die TCP/IP-Fenstergröße für Linux automatisch anhand der Einstellung für `FileTransferSendReceiveBufferSize` berechnet. Sind beide Parameter auf 0 (aus) gesetzt, gilt der Standardwert 248 KB. Geben Sie bei benutzerdefinierten Größen die Größe in Byte an. **HINWEIS:** In früheren Versionen mussten Sie diesen Parameter auf die Hälfte des gewünschten Werts einstellen; dies ist nicht mehr erforderlich.	0 (253952 Byte)	
`FileTransferShutDownTimeOutInMinutes`	1090	
`FileTransferTCPTimeOutMilliSec` Legt den Zeitraum für die Zeitüberschreitung für TCP-Senden und TCP-Empfang fest.	30.000	
`PostFileTransferActionsRequiredTimeInMinutes`	60	

6.4.2 Feinabstimmung für FileTransferSendReceiveBufferSize

Der Parameter „FileTransferSendReceiveBufferSize“ definiert die maximal zulässige Größe (in Byte) des Sende- und Empfangspuffers für TCP-Verbindungen im Reproduktionsnetzwerk. Die Puffergröße wirkt sich auf die Größe des TCP-Emfangsfensters (RWIN) aus, mit der wiederum die Datenmenge (in Byte) bestimmt wird, die ohne TCP-Bestätigung gesendet werden kann. Diese Einstellung ist sowohl für dateibasierte als auch für blockbasierte Übertragungen relevant. Wenn Sie die Puffergröße gemäß der Bandbreite und der Latenz des Netzwerks anpassen, wird der Durchsatz erhöht und die CPU-Tätigkeit wird vermindert.

Durch Feinabstimmung des Parameters „FileTransferSendReceiveBufferSize“ optimieren Sie die Übertragung von Blöcken oder Dateien von den Ursprungsservern auf die Zielserver in der Reproduktionsumgebung. Legen Sie den Parameter auf der PlateSpin-Konfigurationsseite (`https://Ihr_PlateSpin-Server/platespinconfiguration/`) fest.

So berechnen Sie die optimale Puffergröße:

1. Ermitteln Sie die Latenz (Verzögerung) zwischen dem Ursprungsserver und dem Zielserver.

   Letztlich soll die Latenz für eine Paketgröße festgestellt werden, die der MTU so nahe wie möglich kommt.

   1a Melden Sie sich als Administratorbenutzer beim Ursprungsserver an.

   1b Geben Sie bei einer Eingabeaufforderung Folgendes ein:

   ```
   # ping <target-server-ip-address> -f -l <MTU_minus_28> -n 10
   ```

   In der Regel erweitert die Option `-l` für `ping` die Header der angegebenen Nutzlast für die *IP-Adresse des Zielservers* um 28 Byte. Eine Größe von `MTU minus 28` (in Byte) ist damit ein geeigneter Ausgangswert.

1c Ändern Sie die Nutzlast schrittweise und geben Sie den Befehl jeweils erneut in Schritt 1b ein, bis die folgende Meldung angezeigt wird:

```
Das Paket muss fragmentiert werden.
```

1d Notieren Sie die Latenz (in Sekunden)

Liegt die Latenz beispielsweise bei 35 ms (Millisekunden), dann notieren Sie den Wert 0,035 für die Latenz.

2 Berechnen Sie einen Wert (in Byte) für die anfängliche Puffergröße:

```
Puffergröße = (Bandbreite in MBit/s / 8) * Latenz in Sekunden * 1.000 * 1.024
```

Geben Sie die Netzwerkbandbreite in Binärwerten an. Das bedeutet: 10 GBit/s = 10.240 MBit/s und 1 GBit/s = 1.024 MBit/s.

Für ein 10-GBit/s-Netzwerk mit einer Latenz von 35 ms gilt beispielsweise die folgende Berechnung:

```
Buffergröße = (10.240 / 8) * 0,035 * 1.000 * 1.024 = 45.875.200 Byte
```

3 (Optional) Berechnen Sie die optimale Puffergröße durch Aufrunden auf ein Vielfaches der maximalen Segmentgröße (Maximum Segment Size, MSS).

3a Ermitteln Sie die MSS:

```
MSS = MTU-Größe in Bytes – (Größe des IP-Headers + Größe des TCP-Headers)
```

Der IP-Header umfasst 20 Byte. Der TCP-Header umfasst 20 Byte plus zusätzliche Byte für Optionen wie den Zeitstempel.

Bei einer MTU-Größe von 1.470 liegt die MSS in der Regel bei 1430.

```
MSS = 1.470 Byte – (20 Byte + 20Byte) = 1.430 Byte
```

3b Berechnen Sie die optimale Puffergröße:

```
Optimale Puffergröße = (Runden(Puffergröße / MSS)) * MSS
```

Im obigen Beispiel also:

```
Optimale Puffergröße = (Runden(45.875.200 / 1.430)) * 1.430 = 32.081
* 1.430 = 45.875.830
```

In diesem Fall muss aufgerundet werden, da das Abrunden ein Vielfaches der MSS ergibt, das unter der Puffergröße 45.875.200 liegt:

```
Nicht optimale Puffergröße = 32.080 * 1.430 = 45.874.400
```

6.5 Optimieren der Leistung der Reproduktionsumgebung

Mit den Konfigurationsparametern für Kontrollübernahme und Snapshots optimieren Sie die Reproduktionsleistung. Diese Einstellungen sind global und gelten für alle Reproduktionen.

Tabelle 6-3 zeigt die Konfigurationsparameter auf der PlateSpin-Konfigurationsseite (`https://` *`Ihr_PlateSpin-Server`*`/platespinconfiguration/`), die die Reproduktionsumgebung steuern; hier sind jeweils die Standardwerte angegeben.

Tabelle 6-3 Standardmäßige Konfigurationsparameter für die Reproduktionsumgebung

Parameter	Standardwert
`TakeControlMemorySizeInMB` Die Größe des Arbeitsspeichers (in MB), die bei der Übernahme der Kontrolle für die Reproduktion festgelegt werden soll.	768
`TakeControlCoresPerSocket` Die Anzahl der virtuellen Kerne pro Socket für die Übernahme der Kontrolle, wenn das Ziel in LRD oder `bootofx.iso` gebootet wird.	1
`TakeControlSockets` Die Anzahl der virtuellen Sockets für die Übernahme der Kontrolle, wenn das Ziel in LRD oder `bootofx.iso` gebootet wird.	1
`MaximumConcurrentReplications` Die Anzahl der Reproduktionen, die gleichzeitig ausgeführt werden können.	25
`VssSnapshotCreationDelay` Der Zeitraum (in Sekunden) für die Verzögerung zwischen den einzelnen Versuchen, wenn ein VSS-Snapshot im Rahmen der Reproduktion erstellt wird.	120
`VssSnapshotCreationRetryCount` Die maximale Anzahl an Versuchen, einen VSS-Snapshot bei der Reproduktion zu erstellen, bevor der Reproduktionsversuch fehlschlägt.	5

6.6 Einstellen der Methode für erneutes Booten des Konfigurationsdiensts

Bei einer Failover-Aktion optimiert der Konfigurationsdienst das erneute Booten, indem er veranlasst, dass es auf ein Minimum reduziert wird, und steuert, wann es stattfindet. Wenn ein Konfigurationsdienst für einen Windows-Workload während einer Failover-Aktion mit dem Fehler `Konfigurationsdienst nicht gestartet` hängt, müssen Sie möglicherweise zulassen, dass das erneute Booten wie während der Konfiguration angefordert durchgeführt wird. Sie können konfigurieren, dass ein einzelner betroffener Workload die Optimierung für erneutes Booten überspringt, oder eine globale `SkipRebootOptimization`-Einstellung auf dem PlateSpin-Server konfigurieren, damit die Optimierung für erneutes Booten für alle Windows-Workloads übersprungen wird.

So überspringen Sie die Optimierung für erneutes Booten bei einem einzelnen Windows-Workload:

1. Melden Sie sich als Administratorbenutzer beim Ursprungs-Workload an.
2. Fügen Sie im Stammverzeichnis des Systemlaufwerks (normalerweise `C:`) eine Datei mit der Bezeichnung `PlateSpin.ConfigService.LegacyReboot` ohne Dateierweiterung hinzu. Geben Sie an der Eingabeaufforderung Folgendes ein:

   ```
   echo $null >> %SYSTEMDRIVE%\PlateSpin.ConfigService.LegacyReboot
   ```

3. Führen Sie die fehlgeschlagene Test-Failover- oder Failover-Aktion erneut aus.

So überspringen Sie die Optimierung für alle Windows-Workloads:

1. Melden Sie sich beim PlateSpin-Server an und öffnen Sie die Konfigurationsseite für den PlateSpin-Server unter:

   `https://Ihr_PlateSpin_Server/platespinconfiguration/`

2. Suchen Sie den Konfigurationsparameter **ConfigurationServiceValues** und klicken Sie dann für den Parameter auf **Bearbeiten**.
3. Ändern Sie die Einstellung **SkipRebootOptimization** von `false` zu `true`.
4. Klicken Sie auf **Speichern**.
5. Führen Sie eine inkrementelle oder Vollreproduktion aus.

   Die Reproduktion überträgt die geänderten Konfigurationseinstellungen auf die Ziel-VM.
6. Führen Sie den fehlgeschlagenen Test-Failover oder Failover für die betroffenen Windows-Workloads erneut aus.

6.7 Konfigurieren der Unterstützung für VMware vCenter Site Recovery Manager

Mit PlateSpin Protect können Sie ihre Workloads lokal schützen und sie mithilfe einer zusätzlichen Methode an einem Remotestandort, wie einem SAN, reproduzieren. Sie können beispielsweise mit VMware vCenter Site Recovery Manager (SRM) eine komplette Datenablage reproduzierter Ziel-VMs an einem Remotestandort reproduzieren. In diesem Fall sind spezifische Konfigurationsschritte erforderlich, um sicherzustellen, dass die Ziel-VMs reproduziert werden können und ordnungsgemäß funktionieren, sobald sie am Remotestandort eingeschaltet werden.

Workloads, die von PlateSpin Protect reproduziert und vom VMware vCenter (SRM) verwaltet werden, funktionieren nahtlos, wenn Sie PlateSpin Protect wie folgt für die Unterstützung für SRM konfigurieren:

- Konfigurieren Sie eine Einstellung, damit die PlateSpin Protect-ISO und -Datenträger in derselben Datenablage gespeichert werden wie die VMware `.vmx`- und `.vmdk`-Dateien.
- Bereiten Sie die PlateSpin Protect-Umgebung auf das Kopieren der VMware Tools auf das Failover-Ziel vor. Dazu müssen einige Dateien manuell erstellt und kopiert werden. Außerdem müssen Konfigurationseinstellungen vorgenommen werden, um den Installationsprozess der VMware Tools zu beschleunigen.

- Abschnitt 6.7.1, „Einrichten von Workload-Dateien in derselben Datenablage“, auf Seite 76
- Abschnitt 6.7.2, „Einrichten der VMware-Tools für Failover-Ziele“, auf Seite 77
- Abschnitt 6.7.3, „Beschleunigen des Konfigurationsprozesses“, auf Seite 78

6.7.1 Einrichten von Workload-Dateien in derselben Datenablage

So stellen Sie sicher, dass die Workload-Dateien in derselben Datenablage gespeichert sind:

1. Öffnen Sie die Webseite für die Konfiguration. Rufen Sie hierzu in einem Webbrowser die URL `https://Your_PlateSpin_Server/platespinconfiguration/` auf.
2. Navigieren Sie auf der Webseite für die Konfiguration zum Serverparameter `CreatePSFilesInVmDatastore`, und ändern Sie den Wert in `wahr`.

HINWEIS: Die für das Konfigurieren des Reproduktionsvertrags verantwortliche Person muss sicherstellen, dass für alle VM-Zieldatenträgerdateien dieselbe Datenablage angegeben ist.

3 Speichern Sie die Einstellungen und schließen Sie die Seite.

6.7.2 Einrichten der VMware-Tools für Failover-Ziele

Die Setup-Pakete für die VMware Tools können während der Reproduktion auf das Failover-Ziel kopiert werden, sodass sie beim Start der VM vom Konfigurationsdienst installiert werden können. Dieser Vorgang wird automatisch ausgeführt, wenn das Failover-Ziel eine Verbindung zum PlateSpin Server herstellen kann. Wird der Vorgang nicht ausgeführt, müssen Sie die Umgebung vor der Reproduktion entsprechend vorbereiten.

So bereiten Sie Ihre Umgebung vor:

1 Rufen Sie die VMware Tools-Pakete von einem ESX-Host ab:

1a Kopieren Sie mit `scp` das Image `windows.iso` aus dem Verzeichnis `/usr/lib/vmware/isoimages` auf einem zugänglichen VMware-Host in einen lokalen temporären Ordner.

1b Öffnen Sie das ISO-Image, extrahieren Sie die Setup-Pakete und speichern Sie sie an einem verfügbaren Speicherort:

- **VMware 5.*x* (oder höher):** Die Setup-Pakete bestehen aus den Dateien `setup.exe` und `setup64.exe`.
- **VMware 4.*x*:** Die Setup-Pakete bestehen aus den Dateien `VMware Tools.msi` und `VMware Tools64.msi`.

2 Erstellen Sie OFX-Pakete aus den extrahierten Setup-Paketen:

2a Komprimieren Sie das gewünschte Paket. Stellen Sie dabei sicher, dass sich die Setup-Installationsdatei auf der Root-Ebene des `.zip`-Archivs befindet.

2b Benennen Sie das `.zip`-Archiv in `1.package` um, sodass es als OFX-Paket verwendet werden kann.

HINWEIS: Wenn Sie ein OFX-Paket von mehr als einem Setup-Paket erstellen möchten, beachten Sie, dass für jedes Setup-Paket ein eigenes eindeutiges `.zip`-Archiv erforderlich ist.

Da jedes Paket den gleichen Namen (`1.package`) hat, müssen Sie beim Speichern mehrerer `.zip`-Archive als OFX-Paket für jedes Paket ein eigenes Unterverzeichnis anlegen.

3 Kopieren Sie das entsprechende OFX-Paket (`1.package`) in das Verzeichnis `%Programme (x86)%\PlateSpin\Packages\%GUID%` auf dem PlateSpin-Server.

Der Wert `%GUID%` hängt von der Version Ihres VMware-Servers und der Architektur der VMware Tools ab (siehe Tabelle 6-4). Kopieren Sie das Paket mit dem entsprechenden GUID-Wert in das richtige Verzeichnis.

Tabelle 6-4 *GUIDs für die VMware Tools-Verzeichnisnamen*

VMware Server Version	VMware Tools-Architektur	GUID
6.5	x86	`D61C0FCA-058B-42C3-9F02-898F568A3071`
6.5	x64	`5D3947B7-BE73-4A00-A549-B15E84B98803`

VMware Server Version	VMware Tools-Architektur	GUID
6.0	x86	311E672E-05BA-4CAF-A948-B26DF0C6C5A6
6.0	x64	D7F55AED-DA64-423F-BBBE-F1215529AD03
5.5	x86	660C345A-7A91-458b-BC47-6A3914723EF7
5.5	x64	8546D4EF-8CA5-4a51-A3A3-6240171BE278
5.1	x86	34DD2CBE-183E-492f-9B36-7A8326080755
5.1	x64	AD4FDE1D-DE86-4d05-B147-071F4E1D0326
5,0	x86	AD4FDE1D-DE86-4d05-B147-071F4E1D0326
5,0	x64	F7C9BC91-7733-4790-B7AF-62E074B73882
4.1	x86	F2957064-65D7-4bda-A52B-3F5859624602
4.1	x64	80B1C53C-6B43-4843-9D63-E9911E9A15D5
4.0	x86	D052CBAC-0A98-4880-8BCC-FE0608F0930F
4.0	x64	80B50267-B30C-4001-ABDF-EA288D1FD09C

6.7.3 Beschleunigen des Konfigurationsprozesses

Nach dem Booten des Failover-Ziels wird der Konfigurationsdienst gestartet, um die Verwendung der VM vorzubereiten. Er bleibt jedoch einige Minuten inaktiv und wartet auf Daten vom PlateSpin Server bzw. sucht auf der CD ROM nach VMware Tools.

So verkürzen Sie die Wartezeit:

1. Navigieren Sie auf der Webseite für die Konfiguration zur Konfigurationseinstellung `ConfigurationServiceValues`, und ändern Sie den Wert der untergeordneten Einstellung `WaitForFloppyTimeoutInSecs` in null (0).
2. Navigieren Sie auf der Webseite für die Konfiguration zum Parameter `ForceInstallVMToolsCustomPackage`, und ändern Sie den Wert in `wahr`.

Mit diesen Einstellungen dauert der Konfigurationsprozess weniger als 15 Minuten: Der Zielcomputer wird (maximal zweimal) neu gestartet, die VMware Tools werden installiert, und SRM greift auf die Tools zu, um das Konfigurieren von Networking am Remotestandort zu unterstützen.

7 Konfigurieren der PlateSpin-Weboberfläche

In der PlateSpin-Weboberfläche können Sie Tags konfigurieren, mit denen logische Verknüpfungen zwischen Workloads verfolgt werden. Darüber hinaus können Sie die Bildschirmaktualisierungsraten für verschiedene Seiten steuern. Konfigurieren Sie die Weboberfläche anhand der Angaben in diesem Abschnitt.

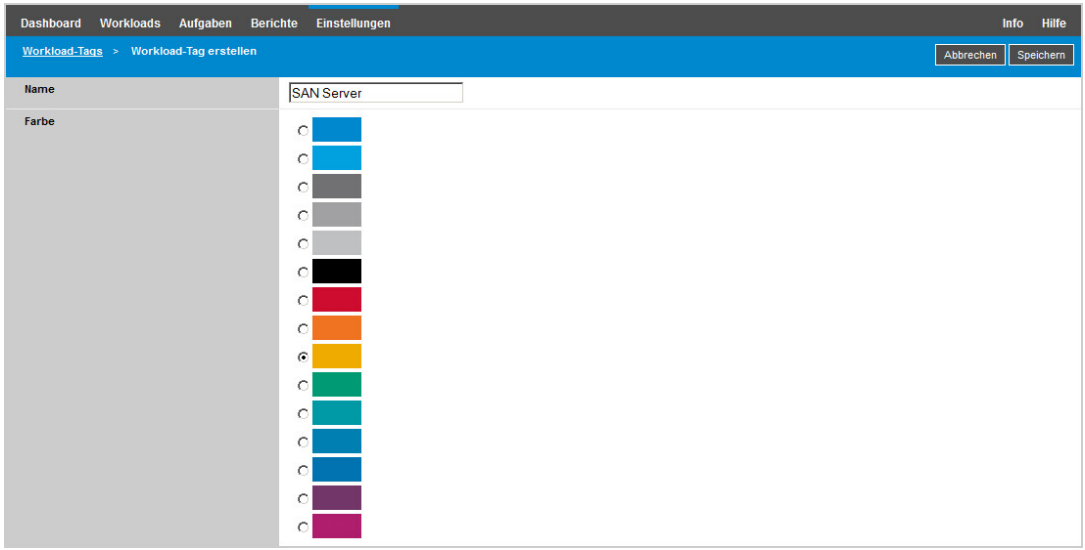
7.1 Erstellen und Verwenden von Workload-Tags

Wenn Sie zahlreiche Workloads verwalten und eine Aktion auf mehrere Workloads gleichzeitig anwenden möchten, kann das Durchsuchen der Liste und das Auswählen ähnlicher Workloads unter Umständen sehr zeitaufwändig sein. In diesem Fall können Sie die Liste nach Name oder Funktion sortieren. Alternativ können Sie mithilfe eines Tags eine benutzerdefinierte Verknüpfung zwischen den Workloads anlegen, die als Gruppe verwaltet werden sollen. Sie können die Workloads schnell und einfach nach der Spalte „Tag“ sortieren, die gewünschten getaggten Workload auswählen und verfügbare Aktionen gleichzeitig für diese Workloads ausführen.

Ein Tag kann eine logische oder physische Verknüpfung für einen Workload darstellen, die für Sie sinnvoll ist. Den Tags weisen Sie jeweils eine eindeutige Farbe und einen eindeutigen Namen zu. Sie können beliebig viele eindeutige Tags anlegen; die Auswahl an Farben ist allerdings begrenzt. Jedem Workload kann jeweils mit einem einzelnen Tag verknüpft werden. Wenn Sie einen Workload auf einen neuen Server exportieren, bleibt seine Tag-Einstellung erhalten.

7.1.1 Erstellen eines Workload-Tags

1 Klicken Sie auf der PlateSpin Protect-Weboberfläche auf **Einstellungen > Workload-Tags > Workload-Tag erstellen**.



2 Geben Sie einen eindeutigen Tag-Namen (max. 25 Zeichen) ein, und weisen Sie dieser Beschreibung eine Farbe zu.

3 Klicken Sie auf **Speichern**. Das neue Tag wird auf der Seite „Einstellungen“ in der Ansicht „Workload-Tags“ in die Liste der verfügbaren Workload-Tags aufgenommen.

7.1.2 Bearbeiten eines Workload-Tags

1 Klicken Sie auf der PlateSpin Protect-Weboberfläche auf **Einstellungen** > **Workload-Tags**.

2 Bearbeiten Sie die verfügbaren Tags nach Bedarf. Klicken Sie auf den Tag-Namen, ändern Sie den Namen oder die zugewiesene Farbe, und klicken Sie auf **Speichern**.

7.1.3 Hinzufügen eines Tags zu einem Workload

1 Wählen Sie in der Liste der Workloads den zu taggenden aktiven Workload aus, und klicken Sie auf **Konfigurieren**. Die Konfigurationsseite für diesen Workload wird geöffnet.

2 Klappen Sie den Abschnitt **Tag** auf. Das Dropdown-Feld **Tag** wird angezeigt.

3 Wählen Sie den Namen des Tags aus, das dem Workload zugewiesen werden soll, und klicken Sie auf **Speichern**.

7.1.4 Entfernen eines Tags von einem Workload

1 Wählen Sie in der Liste der Workloads den Workload aus, und klicken Sie auf **Konfigurieren**. Die Konfigurationsseite für diesen Workload wird geöffnet.

2 Klappen Sie den Abschnitt **Tag** auf. Das Dropdown-Feld **Tag** wird angezeigt.

3 Wählen Sie die „leere“ Zeile in der Liste der verfügbaren Tag-Namen aus, und klicken Sie auf **Speichern**.

7.1.5 Löschen eines Workload-Tags

Sie können die nicht mehr benötigten Tags löschen. Sie können ein Tag nicht löschen, wenn es noch mindestens einem Workload zugewiesen ist.

1 Klicken Sie auf der PlateSpin Protect-Weboberfläche auf **Einstellungen** > **Workload-Tags**.

2 Heben Sie die Verknüpfung des gewünschten Tags zu den Workloads auf.

3 Klicken Sie neben dem Tag auf **Löschen**, und bestätigen Sie mit **OK.**

7.2 Konfigurieren der Aktualisierungsraten für die Weboberfläche

Bei mehreren Seiten in der Weboberfläche ist das Aktualisierungsintervall konfigurierbar (siehe Tabelle 7-1). Sie können die Intervalleinstellung an die Anforderungen in Ihrer PlateSpin-Umgebung anpassen.

Tabelle 7-1 *Standardmäßige Aktualisierungsintervalle der Weboberfläche*

Parameter der Weboberfläche	Standardmäßiges Aktualisierungsintervall (in Sekunden)
DashboardUpdateIntervalSeconds	60
WorkloadsUpdateIntervalSeconds	60
WorkloadTargetsUpdateIntervalSeconds	30
WorkloadDetailsUpdateIntervalSeconds	15
TasksUpdateIntervalSeconds	15

1 Öffnen Sie die folgende Datei in einem Texteditor:

```
\Programme\PlateSpin Protect Server\Platespin Forge\web\web.config
```

2 Passen Sie den Wert für die folgenden Intervalleinstellungen individuell an Ihre PlateSpin-Umgebung an:

```
<add key="DashboardUpdateIntervalSeconds" value="60" /> <add
key="WorkloadsUpdateIntervalSeconds" value="60" /> <add
key="WorkloadTargetsUpdateIntervalSeconds" value="30" /> <add
key="WorkloadDetailsUpdateIntervalSeconds" value="15" /> <add
key="TasksUpdateIntervalSeconds" value="15" />
```

3 Speichern Sie die Datei.

Die neuen Einstellungen treten in der nächsten Weboberflächen-Sitzung in Kraft. Der PlateSpin-Server-Dienst und der Server müssen nicht neu gestartet werden.

7.3 Anpassen der Benutzeroberfläche für die Weboberfläche

Sie können das Erscheinungsbild der PlateSpin-Weboberfläche an das Markenbild Ihres Unternehmens anpassen. (z. B. Farben, Logo und Produktname). Weitere Informationen finden Sie unter Anhang A, „Anpassen der PlateSpin Protect-Weboberfläche an das Markenbild“, auf Seite 87.

8 Verwalten mehrerer PlateSpin-Server in der Verwaltungskonsole

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

In einem Rechenzentrum mit mehreren Instanzen von PlateSpin Protect und PlateSpin Forge 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.

8.1 Verwenden der PlateSpin Protect-Verwaltungskonsole

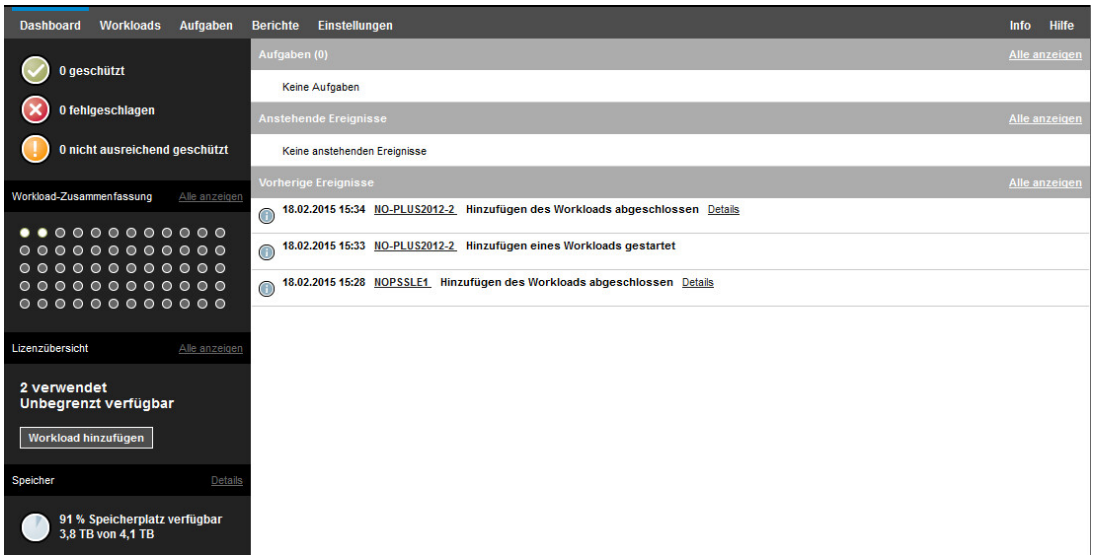
So verwenden Sie die Verwaltungskonsole:

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

   `https://`*Ihr_PlateSpin_Server*`/console`

   Ersetzen Sie *Ihr_PlateSpin_Server* durch die IP-Adresse oder den DNS-Hostnamen des PlateSpin-Server-Hosts, der als Manager festgelegt wurde.
2. Melden Sie sich mit Ihrem Benutzernamen und Ihrem Passwort an.
3. (Erste Anmeldung) Klicken Sie im Begrüßungsbildschirm auf **PlateSpin-Server hinzufügen** und richten Sie eine PlateSpin-Server-Instanz nach den Anweisungen unter Abschnitt 8.3, „Hinzufügen von Instanzen von PlateSpin Protect und PlateSpin Forge zur Verwaltungskonsole“, auf Seite 85 ein.

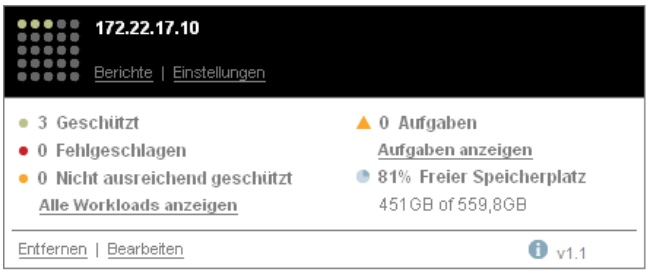
4 (Nachfolgende Anmeldungen) Öffnen Sie das Dashboard.



8.2 Informationen zu PlateSpin Protect-Verwaltungskonsolenkarten

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

Abbildung 8-1 *PlateSpin Protect-Instanzkarte*



Eine Karte zeigt grundlegende Informationen über die spezifische Instanz von PlateSpin Protect und PlateSpin Forge an, beispielsweise:

- 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.

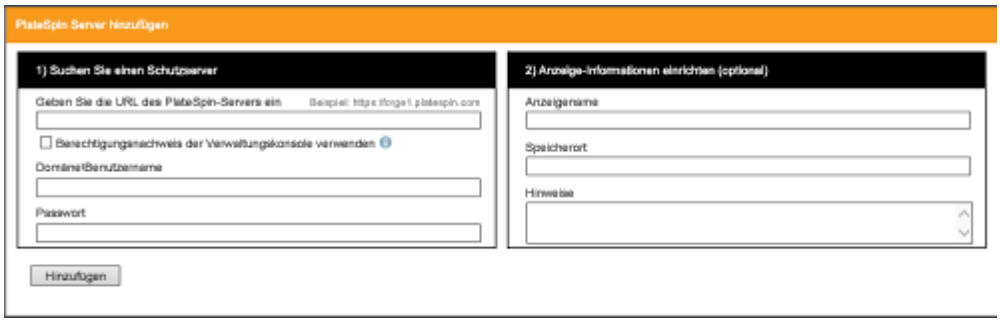
8.3 Hinzufügen von Instanzen von PlateSpin Protect und PlateSpin Forge zur Verwaltungskonsole

Beim Hinzufügen einer PlateSpin Protect- oder PlateSpin Forge-Instanz zur Verwaltungskonsole wird eine neue Karte in das Dashboard der Verwaltungskonsole aufgenommen.

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 PlateSpin Forge-Instanz zur Konsole hinzu:

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



2 Geben Sie die URL des PlateSpin-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 hinzugefügte PlateSpin Protect- oder Plate Spin Forge-Instanz gültig sind. Geben Sie im Feld **Passwort** das entsprechende Passwort ein.

5 (Optional) Geben Sie einen eindeutigen, aussagekräftigen **Anzeigenamen** (max. 15 Zeichen) für den PlateSpin-Server, den **Speicherort** (max. 20 Zeichen) und ggf. erforderliche **Hinweise** (max. 400 Zeichen) an.

6 Klicken Sie auf **Hinzufügen**.

Es wird eine neue Karte zum Dashboard hinzugefügt.

8.4 Bearbeiten von Karten auf der Verwaltungskonsole

So können Sie die Details einer Karte auf der Verwaltungskonsole ändern:

1. Suchen Sie in der Verwaltungskonsole die Karteninstanz für den zu ändernden PlateSpin Protect-Server oder PlateSpin Forge-Server.
2. Klicken Sie auf der Karte auf den Hyperlink **Bearbeiten**.

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

   Das aktualisierte Konsolen-Dashboard wird angezeigt.

8.5 Entfernen von Karten aus der Verwaltungskonsole

So entfernen Sie eine Karte von der Verwaltungskonsole:

1. Suchen Sie in der Verwaltungskonsole die Karteninstanz für den zu entfernenden PlateSpin Protect-Server oder PlateSpin Forge-Server.
2. Klicken Sie auf der Karte auf den Hyperlink **Entfernen**.

   Es wird eine Bestätigungsaufforderung angezeigt.
3. Klicken Sie zur Bestätigung auf **OK**.

   Die Karteninstanz wird vom Dashboard entfernt.

A Anpassen der PlateSpin Protect-Weboberfläche an das Markenbild

Sie können das Erscheinungsbild der Weboberfläche an das Markenbild Ihres Unternehmens anpassen (z. B. Farben, Logo und Produktname). Hierbei können Sie sogar die Links zu den Registerkarten **Info** und **Hilfe** aus der Produktbenutzeroberfläche entfernen.

In diesem Abschnitt finden Sie weitere Informationen zur Bearbeitung des Markenbilds für das Produkt:

A.1 Anpassen der Weboberfläche an das Markenbild mithilfe von Konfigurationsparametern

Sie können das Erscheinungsbild der Weboberfläche an die unternehmenseigene Gestaltung Ihrer Websites anpassen. Zum Anpassen der Weboberfläche an das Markenbild bearbeiten Sie die Konfigurationsparameter für den PlateSpin-Server-Host.

So bearbeiten Sie die Markenbildparameter der Weboberfläche:

1. Öffnen Sie `https://Ihr_PlateSpin-Server/platespinconfiguration/` in einem beliebigen Webbrowser, und melden Sie sich als Administrator an.
2. Suchen Sie den gewünschten Serverparameter, klicken Sie auf **Bearbeiten**, und ändern Sie den Wert dieses Parameters.

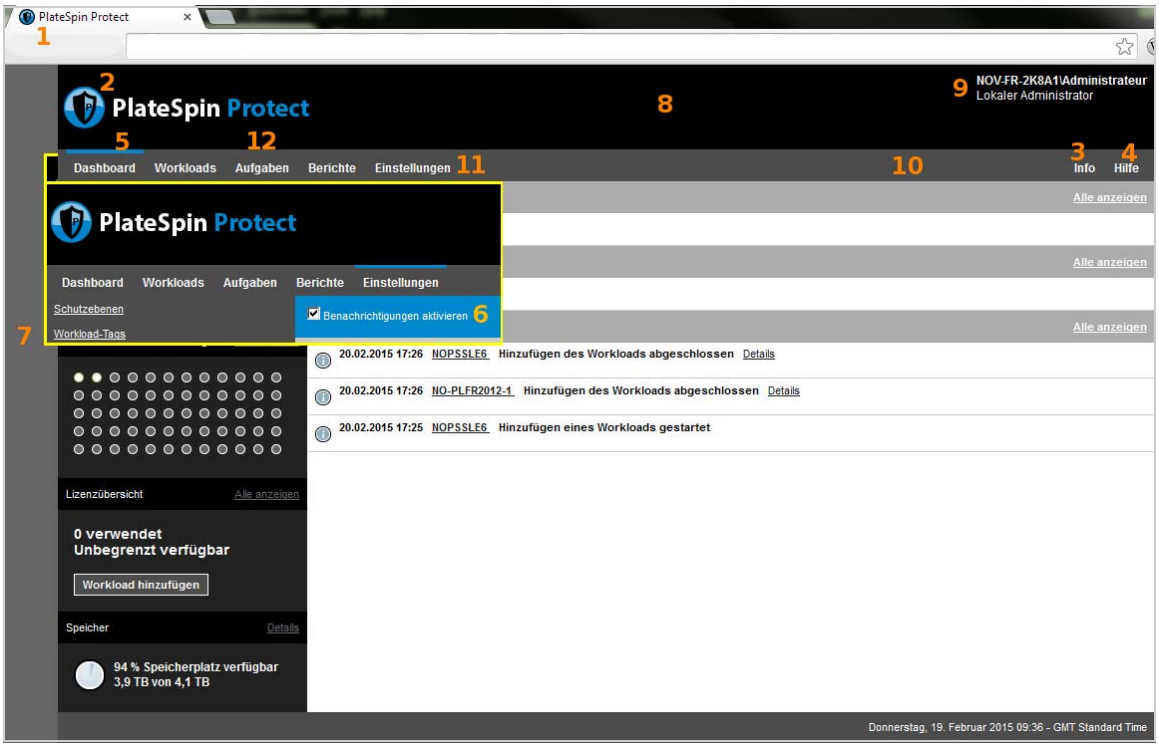
   Weitere Informationen finden Sie in Abbildung A-1 mit den konfigurierbaren Elementen der Benutzeroberfläche. Tabelle A-1 zeigt die Einstellungsnamen, Beschreibungen und Standardwerte der einzelnen konfigurierbaren Elemente.
3. Speichern Sie die Einstellungen und schließen Sie die Seite.

   Ein Neustart des Systems oder der Services ist nach einer Änderung im Konfigurationsprogramm nicht erforderlich; es kann allerdings bis zu 30 Sekunden dauern, bis die Änderung in der Benutzeroberfläche in Kraft tritt.

A.1.1 Konfigurierbare Elemente in der Weboberfläche

Das Darstellungsbild der Weboberfläche ist durchgängig einheitlich. In der Darstellung des PlateSpin Protect-Dashboards in Abbildung A-1 sind die bearbeitbaren Elemente mit Zahlen gekennzeichnet. Die Einblendung zeigt die konfigurierbaren Elemente im Einstellungsbereich.

Abbildung A-1 *Protect -Weboberfläche mit gekennzeichneten konfigurierbaren Elementen*



A.1.2 Konfigurierbare Parameter in der Weboberfläche

Die nachfolgende Tabelle zeigt die Nummer („ID“) des gekennzeichneten Elements der Benutzeroberfläche im obigen Bildschirmfoto sowie den Namen, die Beschreibung und den Standardwert der jeweils zugehörigen Einstellung. Legen Sie diese Werte auf dem PlateSpin-Server auf der Seite der Konfigurationseinstellungen gemäß dem gewünschten neuen Erscheinungsbild fest. (Klicken Sie hierzu auf der Einstellungsseite bei dem gewünschten Konfigurationswert auf **Bearbeiten**.)

Tabelle A-1 *Konfigurationsparameter und Standardwerte in der Weboberfläche*

ID	Name und Beschreibung der Einstellung	Standardwert

1	`WebUIFaviconUrl`
	
	Speicherort einer gültigen `.ico`-Grafikdatei. Wählen Sie eine der folgenden Optionen aus:
	
	◆ Gültige URL zur entsprechenden `.ico`-Datei auf einem anderen Computer.
	
	Beispiel: https://meinserver.beispiel.de/dir1/dir2/icons/meinefirma_favsymbol.ico
	
	◆ Relativer Pfad unterhalb des Stammverzeichnisses des lokalen Webservers, in das Sie die entsprechende `.ico`-Datei hochgeladen haben.
	
	Sie haben beispielsweise den Pfad `\meinefirma\images\icons` im Stammverzeichnis des Webservers erstellt, in dem die Grafikdateien für die benutzerdefinierten Symbole gespeichert werden sollen:
	
	`~/\meinefirma\images\icons\meinefirma_favsymbol.ico`
	
	Der tatsächliche Dateisystempfad, in dem sich die Datei befindet, lautet in diesem Beispiel `C:\Programme (x86)\PlateSpin Protect Server\PlateSpin Forge\web\meinefirma\images\icons\meinefirma_favsymbol.ico`.
		`~/doc/de/favicon.ico` [1]

2	`WebUILogoUrl`
	
	Speicherort der Grafikdatei mit dem Produktlogo. Wählen Sie eine der folgenden Optionen aus:
	
	◆ Gültige URL zur entsprechenden Grafikdatei auf einem anderen Computer.
	
	Beispiel: https://meinserver.beispiel.de/dir1/dir2/logos/meinefirma_logo.png
	
	◆ Relativer Pfad unterhalb des Stammverzeichnisses des lokalen Webservers, in das Sie die entsprechende Grafikdatei heraufgeladen haben.
	
	Sie haben beispielsweise den Pfad `meinefirma\images\logos` im Stammverzeichnis des Webservers erstellt, in dem die benutzerdefinierten Logobilder gespeichert werden sollen:
	
	`~/meinefirma/images/logos/meinefirma_logo.png`
	
	Der tatsächliche Dateisystempfad, in dem sich die Datei befindet, lautet in diesem Beispiel `C:\Programme (x86)\PlateSpin Protect Server\PlateSpin Forge\web\meinefirma\images\logos\meinefirma_logo.png`.
		`~/Resources/protectLogo.png` [2]

ID	Name und Beschreibung der Einstellung	Standardwert
3	`WebUIShowAboutTab` Aktiviert oder deaktiviert die Anzeige der Registerkarte **Info** (**wahr** bzw. **falsch**).	Wahr
4	`WebUIShowHelpTab` Aktiviert oder deaktiviert die Anzeige der Registerkarte **Hilfe** (**wahr** bzw. **falsch**).	Wahr
5	`WebUISiteAccentColor` Akzentfarbe (hexadezimaler RGB-Wert).	#0088CE
6	`WebUISiteAccentFontColor` Schriftfarbe für die Anzeige mit der Akzentfarbe in der Weboberfläche (hexadezimaler RGB-Wert).	#FFFFFF
7	`WebUISiteBackgroundColor` Farbe für den Hintergrund der Website (hexadezimaler RGB-Wert).	#666666
8	`WebUISiteHeaderBackgroundColor` Farbe für den Hintergrund des Website-Headers (hexadezimaler RGB-Wert).	#000000
9	`WebUISiteHeaderFontColor` Schriftfarbe für den Website-Header in der Weboberfläche (hexadezimaler RGB-Wert).	#FFFFFF
10	`WebUISiteNavigationBackgroundColor` Farbe für den Hintergrund der Website-Navigation in der Weboberfläche (hexadezimaler RGB-Wert).	#4D4D4D
11	`WebUISiteNavigationFontColor` Schriftfarbe für die Links der Website-Navigation in der Weboberfläche (hexadezimaler RGB-Wert).	#FFFFFF
12	`WebUISiteNavigationLinkHoverBackgroundColor` Farbe für den Hintergrund der Links der Websitenavigation in der Weboberfläche (hexadezimaler RGB-Wert).	#808080

1 Der tatsächliche Dateipfad lautet `C:\Programme (x86)\PlateSpin Protect Server\PlateSpin Forge\web\doc\de\favicon.ico`.

2 Der tatsächliche Dateipfad lautet `C:\Programme (x86)\PlateSpin Protect Server\PlateSpin Forge\web\Resources\protectLogo.png`.

A.2 Anpassen des Produktnamens an das Markenbild in der Windows-Registrierungsdatenbank

Der Titel oben in der Produktoberfläche bietet genügend Platz für ein Unternehmenslogo und für den Namen des Produkts selbst. Mithilfe eines Konfigurationsparameters können Sie das Logo ändern, das in der Regel den Produktnamen enthält. Soll der Produktname auf einer Browser-Registerkarte geändert oder entfernt werden, müssen Sie die Windows-Registrierungsdatenbank bearbeiten.

So ändern Sie den Produktnamen:

1. Führen Sie auf dem PlateSpin-Server den Befehl `regedit` aus.
2. Navigieren Sie im Windows-Registrierungs-Editor zu folgendem Registrierungsschlüssel:

   `HKEY_LOCAL_MACHINE\SOFTWARE\PlateSpin\ProtectServer\Produktname`.

   HINWEIS: Unter Umständen finden Sie diesen Registrierungsschlüssel hier:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PlateSpin\Protect`.

   ---
3. Doppelklicken Sie auf den Schlüssel `ProductName`, ändern Sie die **Datenwerte** nach Wunsch, und klicken Sie auf **OK**.
4. Starten Sie den IIS-Server neu, damit die Änderung an der Benutzeroberfläche in Kraft tritt.

III Vorbereiten der Schutzziele und -ursprünge

Bevor Sie Schutzverträge konfigurieren können, müssen Sie die geplanten Zielcontainer und Ursprungs-Workloads festlegen. Die Details zu den Zielen und Workloads erhalten Sie über einen Inventarvorgang.

9 Vorbereiten von Containern (Schutzziele)

Ein Container ist eine Schutz-Infrastruktur, die als Host für die regelmäßig aktualisierte Reproduktion eines geschützten Workloads agiert. Wenn Sie einen Zielcontainer hinzufügen, werden ausführliche Inventardaten zum Container und dessen Ressourcen in die PlateSpin Protect-Datenbank eingetragen. Das Inventar liefert die nötigen Daten, mit denen die Nutzung des Containers bestimmt und mindestens ein Workload-Schutzvertrag für den Zielcontainer ordnungsgemäß konfiguriert werden kann.

9.1 Informationen zu Containern (Schutzziele)

Die PlateSpin-Weboberfläche bietet ein automatisches Inventar der unterstützten Zielcontainerplattformen.

9.1.1 Unterstützte Container

Bevor Sie einen Container zum PlateSpin-Server hinzufügen, überprüfen Sie, ob die VM-Containerversion unterstützt wird. Weitere Informationen hierzu finden Sie in „Unterstützte VM-Container“, auf Seite 17.

9.1.2 Netzwerkzugriffsanforderungen für Container

Stellen Sie vor dem Starten eines Inventarvorgangs sicher, dass der PlateSpin-Server mit Ihren Ursprungs-Workloads und Zielen kommunizieren kann. Weitere Informationen hierzu finden Sie in Abschnitt 1.5.2, „Netzwerkanforderungen für Container“, auf Seite 31.

9.1.3 Parameterrichtlinien für Container

Tabelle 9-1 bietet Richtlinien für die Computerauswahl, das Berechtigungsnachweisformat und die Syntax für die Inventarparameter für Ziel-Hosts in der Weboberfläche.

Tabelle 9-1 *Richtlinien für Ermittlungsparameter für Zielcontainer in der Weboberfläche*

Ermitteln	Zieltyp	Berechtigungsnachweis
VMware vCenter-Cluster	**VMware DRS-Cluster**	Berechtigungsnachweise für den VMware vCenter-Webdienst (Benutzername und Passwort)
VMware ESXi Server	**VMware ESX-Server**	ESX-Konto mit Administrator-Rolle OR Windows Domänen-Berechtigungsnachweis (nur Versionen 4 und 4.1)

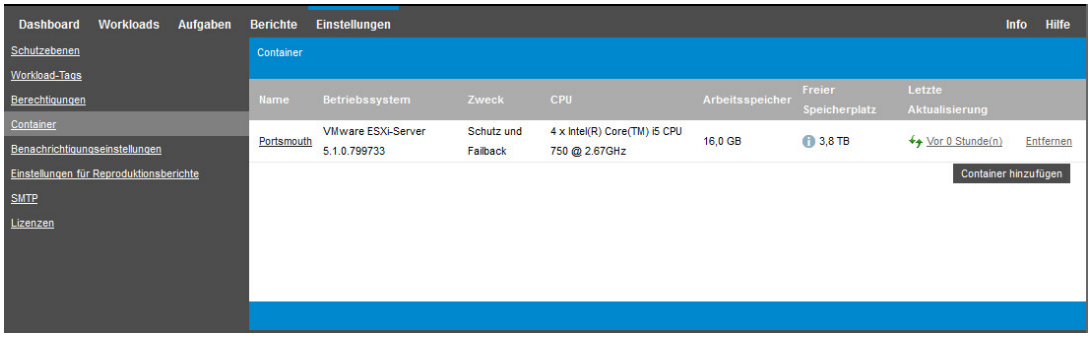
9.2 Hinzufügen von Containern (Schutzziele)

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. In PlateSpin Protect können Sie Container sowohl für den Schutz als auch für das Failback nutzen.

Um einen Workload schützen zu können, benötigen Sie einen Workload und Container, der vom PlateSpin-Server inventarisiert (oder diesem Server *hinzugefügt*) ist.

So fügen Sie einen Container hinzu:

1 Wählen Sie in der Weboberfläche die Option **Einstellungen > Container > Container hinzufügen**.



2 Geben Sie den Containertyp an:

- **VMware ESX-Server**
- **VMware DRS-Cluster**

3 Geben Sie die Zugriffsinformationen an (abhängig vom Typ der Ziele, den Sie im vorangegangenen Schritt ausgewählt haben).

Tabelle 9-2 *Optionen für VMware DRS-Cluster-Ziel*

Option	Beschreibung
vCenter-Hostname oder -IP-Adresse	Geben Sie den Hostnamen oder die IP-Adresse des vCenter-Servers an.

Option	Beschreibung
vCenter-Hostname oder -IP-Adresse	Geben Sie den Hostnamen oder die IP-Adresse des vCenter-Servers an.

- **VMware DRS-Cluster:** Weitere Informationen hierzu finden Sie in Tabelle 9-3.
- **VMware ESX-Server:** Weitere Informationen hierzu finden Sie in Tabelle 9-4.

Tabelle 9-3 *Optionen für VMware DRS-Cluster-Ziel*

Option	Beschreibung
vCenter-Hostname oder -IP-Adresse	Geben Sie den Hostnamen oder die IP-Adresse des vCenter-Servers an.

Option	Beschreibung
vCenter-Hostname oder -IP-Adresse	Geben Sie den Hostnamen oder die IP-Adresse des vCenter-Servers an.

Tabelle 9-4 *Optionen für VMware ESX-Server-Ziel*

Option	Beschreibung
Hostname oder IP-Adresse	Geben Sie den Hostnamen oder die IP-Adresse des VMware ESX-Servers an.
Benutzername und Passwort	Geben Sie den Administrator-Berechtigungsnachweis für den Zugriff auf den Zielcontainer ein. Weitere Informationen hierzu finden Sie in „Richtlinien für Workload- und Container-Berechtigungsnachweise“, auf Seite 161.

4 Validieren Sie den angegebenen Berechtigungsnachweis mit **Test-Berechtigungsnachweis**.

5 Wählen Sie den Zweck des VM-Containers aus:

- **Schutz**
- **Failback**
- **Schutz und Failback**

Wenn Sie beide Elemente auswählen (**Schutz** und **Failback**), steht dieser Container für die Auswahl als Ziel sowohl für Schutz- als auch für Failback-Vorgänge zur Verfügung.

6 Klicken Sie auf **Hinzufügen**. Hiermit werden Details zum Container hinzugefügt und ermittelt und der Container wird in die Seite „Container“ aufgenommen.

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

9.3 Aktualisieren der Containerdetails

Sie sollten die Details zu den Zielcontainern routinemäßig aktualisieren, bevor Sie einen Schutzvertrag einrichten oder ausführen. In der PlateSpin-Weboberfläche können Sie die ermittelten Ressourcen für virtuelle Zielcontainer aktualisieren.

Wenn Sie das Ziel aktualisieren, werden die zugehörigen Ressourcen automatisch erneut ermittelt und aktualisiert. Sie können nur jeweils einen Container aktualisieren, nicht mehrere Container gleichzeitig.

So aktualisieren Sie die Details für einen Zielcontainer:

1. Wählen Sie in der PlateSpin-Weboberfläche die Option **Einstellungen > Container**.
2. Klicken Sie auf das Symbol **Aktualisieren** neben dem zu aktualisierenden Container.

   Dadurch wird der Container neu inventarisiert.
3. Erweitern Sie die Bereiche auf der Seite „Containerdetails“ und lesen Sie die Informationen zu den Inventaränderungen.

9.4 Entfernen von Containern (Schutzziele)

Wenn Sie alle Schutzverträge für einen Zielcontainer entfernen, können Sie den Zielcontainer entfernen (die Ermittlung aufheben). Auch nicht verwendete Container können entfernt werden.

WICHTIG: Bevor Sie einen Container löschen, der für einen konfigurierten Workload-Schutzvertrag verwendet wird, müssen Sie alle betroffenen Verträge entfernen oder für einen anderen Zielcontainer konfigurieren.

So entfernen Sie ein Ziel über die Weboberfläche:

1. Wählen Sie in der PlateSpin-Weboberfläche die Option **Einstellungen > Container**.
2. Klicken Sie auf der Seite „Container“ auf **Entfernen** neben dem Container, der aus Protect entfernt werden soll.

10 Vorbereiten von Workloads (Schutzursprünge)

Jeder Schutzvertrag muss einen Ursprungs-Workload und einen Zielcontainer umfassen. Wenn Sie einen Workload zum PlateSpin Protect-Server hinzufügen, werden ausführliche Inventarinformationen zu diesem Computer in die PlateSpin-Datenbank eingetragen. Diese Daten sind erforderlich, um die Nutzung des Computers feststellen und ordnungsgemäß einen Schutzvertrag konfigurieren zu können.

10.1 Informationen zu Workloads (Schutzursprünge)

Die PlateSpin-Weboberfläche bietet ein automatisiertes Inventar der unterstützten Ursprungs-Workload-Konfigurationen.

10.1.1 Unterstützte Workloads

Bevor Sie einen Workload zum PlateSpin-Server hinzufügen, überprüfen Sie, ob die Betriebssystemversion und die Hardware des Workloads unterstützt wird. Weitere Informationen hierzu finden Sie in den folgenden Abschnitten in Abschnitt 1.1, „Unterstützte Konfigurationen“, auf Seite 13:

10.1.2 Netzwerkzugriffsanforderungen für Ursprungs-Workloads

Weitere Informationen zu den Netzwerkzugriffsanforderungen für das Inventar für Windows- und Linux-Workloads finden Sie unter Abschnitt 1.5.3, „Netzwerkanforderungen für Workloads“, auf Seite 32.

10.1.3 Parameterrichtlinien für Ursprungs-Workloads

Tabelle 10-1 bietet Richtlinien für die Computerauswahl, das Berechtigungsnachweisformat und die Syntax für die Inventarparameter für Workloads.

Tabelle 10-1 *Richtlinien für Ermittlungsparameter für Workloads*

Ermitteln	Computertyp	Berechtigungsnachweis	Anmerkungen
Alle Windows-Workloads	**Windows**	Berechtigungsnachweis eines lokalen Administrators oder eines Domänen-Administrators.	Verwenden Sie für den Benutzernamen das folgende Format: ◆ Bei Domänenmitgliedscomputern: *Autorität\Prinzipal* ◆ Bei Arbeitsgruppenmitglieds-computern: *Hostname\Prinzipal*
Alle Linux-Workloads	**Linux**	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 (https://www.netiq.com/support/kb/doc.php?id=7920711).

10.2 Hinzufügen von Workloads (Schutzursprünge)

Ein Workload, das grundlegende Schutzobjekt in einem Datenspeicher, umfasst ein Betriebssystem, die zugehörige Middleware und die zugehörigen Daten, ist also getrennt von der zugrunde liegenden physischen oder virtuellen Infrastruktur.

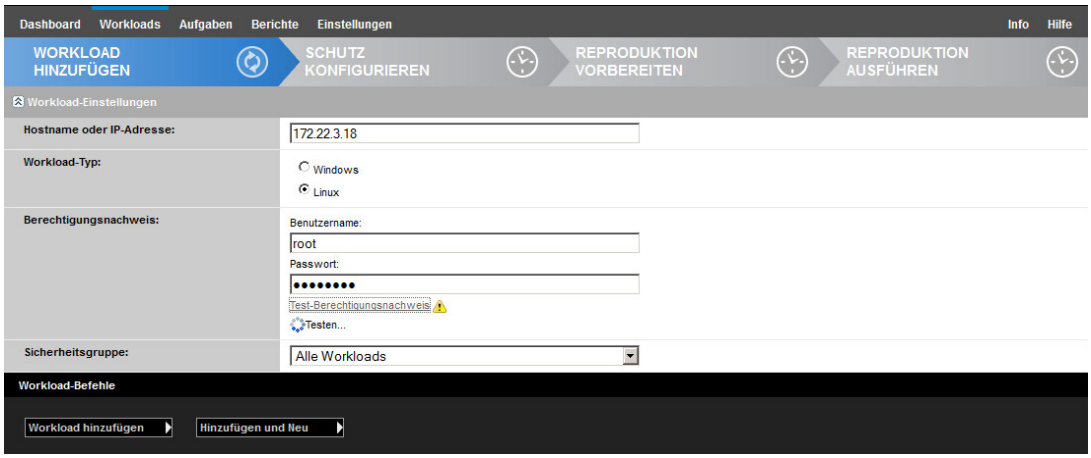
Zum Schutz eines Workloads benötigen Sie einen Workload und einen Container, der auf dem PlateSpin-Server inventarisiert (oder diesem Server *hinzugefügt*) ist.

So fügen Sie einen Workload hinzu:

1. Führen Sie die erforderlichen Vorbereitungsschritte durch.

   Weitere Informationen finden Sie unter Vorbereitung unter „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“, auf Seite 37.
2. Klicken Sie auf der Seite „Dashboard“ oder „Workloads“ auf **Workload hinzufügen**.

   In der Weboberfläche wird die Seite „Workload hinzufügen“ angezeigt.



3 Geben Sie die erforderlichen Workload-Details an:

- **Workload-Einstellungen:** Geben Sie den Hostnamen oder die IP-Adresse Ihres Workloads, das Betriebssystem und den Administrator-Berechtigungsnachweis an.

  Verwenden Sie das erforderliche Berechtigungsnachweisformat (weitere Informationen hierzu finden Sie unter „Richtlinien für Workload- und Container-Berechtigungsnachweise“, auf Seite 161).

  Überprüfen Sie, ob **PlateSpin Protect** auf den Workload zugreifen kann. Klicken Sie hierzu auf Test-Berechtigungsnachweis.

4 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. Im Dashboard wird das Ereignis **Workload hinzugefügt** angezeigt, und der neue Workload ist auf der Workload-Seite verfügbar.

5 (Bedingt) Falls Sie noch keinen Container für diesen Workload hinzugefügt haben, fügen Sie jetzt einen Container zum Schützen des Workloads hinzu. Weitere Informationen hierzu finden Sie unter „Vorbereiten von Containern (Schutzziele)“, auf Seite 95.

6 Fahren Sie mit „Konfigurieren der Schutzdetails und Vorbereiten der Reproduktion“, auf Seite 147 fort.

10.3 Tagging von Workloads

Die Seite „Workloads“ in der PlateSpin-Weboberfläche enthält unter Umständen eine lange Liste mit Workloads. Das Durchsuchen dieser Workloads zum Ausführen von Aktionen für ähnliche Workloads kann äußerst zeitaufwendig werden. Zur Behebung dieses Problems können Sie Tags für verschiedene Workload-Kategorien, Abteilungen oder andere geeignete logische Verknüpfungen für Ihre Umgebung anlegen.

Weitere Informationen zum Erstellen, Ändern oder Löschen von Workload-Tags finden Sie unter Abschnitt 7.1, „Erstellen und Verwenden von Workload-Tags“, auf Seite 79

Die erstellten Tags werden unten auf der Seite „Details zum Ziel bearbeiten“ angezeigt und können dann den entsprechenden Workloads zugewiesen werden. Auf der Seite „Workloads“ in der Spalte **Tag** wird jeweils das eindeutige Tag angezeigt, das Sie den einzelnen Workloads zugewiesen haben. Sie können nach dieser Spalte sortieren und so ähnliche Workloads gruppieren. Damit können Sie getaggte Workloads schnell und einfach auffinden und bestimmte Vorgänge auf allen getaggten Workloads gleichzeitig ausführen.

HINWEIS: Wenn Sie einen getaggten Workload auf einen neuen Server exportieren, bleiben die Tag-Einstellungen erhalten.

So weisen Sie einem Workload einen Tag beim Konfigurieren des Schutzes zu:

1. Klicken Sie in der Protect-Weboberfläche auf **Workloads**.
2. Wählen Sie in der Liste der Workloads den zu taggenden Workload aus, und klicken Sie auf **Schutz konfigurieren**.
3. Konfigurieren Sie den Workload.
4. Wählen Sie unten auf der Seite „Details zum Ziel bearbeiten“ im Abschnitt „Tag“ den Namen des Tags aus, der dem Workload zugewiesen werden soll.
5. Klicken Sie auf **Speichern**.

So können Sie einen zugewiesenen Tag für einen konfigurierten Workload hinzufügen oder ändern:

1. Klicken Sie in der Protect-Weboberfläche auf **Workloads**.
2. Klicken Sie in der Liste der Workloads auf den zu taggenden Workload. Die Seite „Details zum Ziel“ wird geöffnet.
3. Klicken Sie auf **Bearbeiten**.
4. Wählen Sie unten auf der Seite „Details zum Ziel bearbeiten“ im Abschnitt „Tag“ den Namen des Tags aus, der dem Workload zugewiesen werden soll.
5. Klicken Sie auf **Speichern**.

So heben Sie die Zuweisung eines Tags zu einem Workload auf:

1. Klicken Sie in der Protect-Weboberfläche auf **Workloads**.
2. Wählen Sie in der Liste der Workloads den Workload aus, dessen Tag entfernt werden soll, und klicken Sie auf **Schutz konfigurieren**.
3. Wählen Sie auf der Konfigurationsseite unter „Tag“ die leere Zeichenfolge aus, und klicken Sie auf **Speichern**.

10.4 Aktualisieren der Workload-Details

Die PlateSpin-Weboberfläche bietet keine Unterstützung zum Aktualisieren der Details für die ermittelten Workloads. Sollen die Details zu einem ermittelten Workload aktualisiert werden, müssen Sie den Workload entfernen und dann erneut hinzufügen und dessen Details noch einmal ermitteln. Wenn der Workload beim Entfernen bereits konfiguriert war, gehen die Konfigurationsdetails verloren. Wenn eine Schutzlizenz verwendet wird, so wird sie aus dem Workload entfernt und wieder in den Lizenzpool eingestellt. Weitere Informationen hierzu finden Sie in Abschnitt 10.5, „Entfernen von Workloads“, auf Seite 103.

10.5 Entfernen von Workloads

In einigen Situationen müssen Sie einen Workload unter Umständen vom 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**.
2. (Bedingt, Windows) Bei Windows-Workloads, die zuvor durch eine Reproduktion auf Blockebene geschützt wurden, werden Sie auf der 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. Dieser Vorgang muss während der geplanten Ausfallzeit durchgeführt werden.
3. Klicken Sie auf der Seite „Befehlsbestätigung“ auf **Bestätigen**, um den Befehl auszuführen.

   Warten Sie, bis der Vorgang abgeschlossen ist.
4. (Bedingt, Linux) Bei Linux-Workloads deinstallieren Sie den blockbasierten Treiber manuell im Ursprungs-Workload. Siehe Software für den Datentransfer auf Blockebene unter Bereinigen von Linux-Workloads.

11 Vorbereiten der Gerätetreiber für physische Failback-Ziele

PlateSpin Protect umfasst eine Bibliothek mit Gerätetreibern und PnP-IDs (Plug & Play), die immer dann zum Einsatz kommen, wenn physische Computer als Failback-Ziele fungieren. Die benutzerdefinierten Gerätetreiber und PnP-ID-Zuordnungen werden über das PlateSpin-Gerätetreiberwerkzeug (`DeviceDriver.exe`) hinzugefügt.

11.1 Verwalten der Gerätetreiber

PlateSpin Protect umfasst eine Bibliothek mit Gerätetreibern. Auf den Ziel-Workloads werden automatisch die richtigen Gerätetreiber installiert. Falls Treiber auf dem physischen Failback-Computer fehlen oder nicht kompatibel sind oder falls Sie für Ihre Zielinfrastruktur bestimmte Treiber benötigen, müssen Sie möglicherweise Treiber zur PlateSpin Protect-Treiberdatenbank hinzufügen (hochladen).

11.1.1 Packen von Gerätetreibern für Windows-Workloads

Windows-Gerätetreiber müssen als Vorbereitung zum Hochladen in die PlateSpin Protect-Treiberdatenbank gepackt werden.

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

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

So packen Sie Windows-Gerätetreiber:

1. Bereiten Sie alle voneinander abhängigen Treiberdateien (`*.sys`, `*.inf`, `*.dll` usw.) für die Zielinfrastruktur und das Gerät 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.

Das Paket kann nun hochgeladen werden. Weitere Informationen hierzu finden Sie in „Hochladen von Treiberpaketen in die Gerätetreiberdatenbank von PlateSpin“, auf Seite 106.

11.1.2 Packen von Gerätetreibern für Linux-Workloads

Linux-Gerätetreiber müssen als Vorbereitung zum Hochladen in die PlateSpin Protect-Treiberdatenbank gepackt werden. Das PlateSpin-Boot-ISO-Image (`bootofx.x2p.iso`) enthält ein benutzerdefiniertes Dienstprogramm für diesen Zweck.

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.

   Wenn das ISO-Image beispielsweise in das Verzeichnis `/root` kopiert wurde, geben Sie den folgenden Befehl für Ziele auf BIOS- bzw. UEFI-Firmware-Basis ein:

   ```
   # mkdir /mnt/ps # mount -o loop /root/bootofx.x2p.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 Treiberpaketen in die Gerätetreiberdatenbank von PlateSpin“, auf Seite 106.

11.1.3 Hochladen von Treiberpaketen in die Gerätetreiberdatenbank von PlateSpin

Verwenden Sie das PlateSpin-Treibermanager-Werkzeug zum Hochladen von Gerätetreibern in die Treiberdatenbank.

HINWEIS: Beim Hochladen validiert PlateSpin Protect die Treiber nicht anhand der ausgewählten Betriebssystemtypen oder anhand ihrer Bitspezifikationen. Laden Sie nur die Treiber hoch, die für Ihre Zielinfrastruktur geeignet und erforderlich sind.

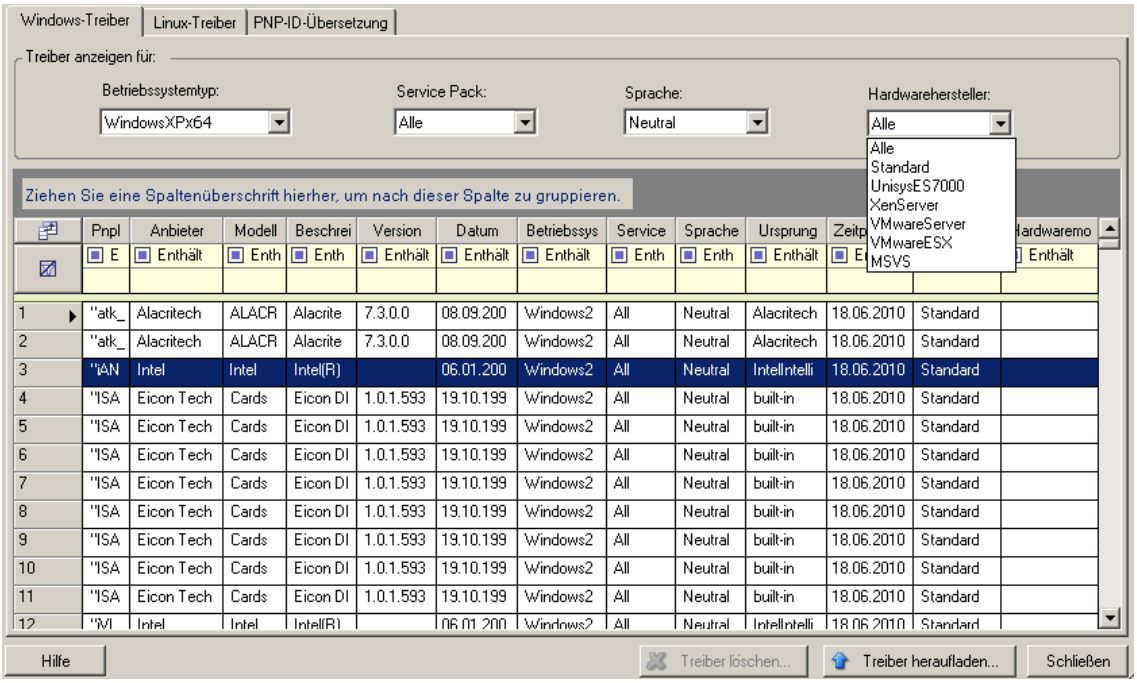
- „Upload-Prozedur für Gerätetreiber (Windows)“, auf Seite 106
- „Upload-Prozedur für Gerätetreiber (Linux)“, auf Seite 108

Upload-Prozedur für Gerätetreiber (Windows)

1. Beziehen Sie die erforderlichen Gerätetreiber und bereiten Sie diese vor. Weitere Informationen hierzu finden Sie unter „Packen von Gerätetreibern für Windows-Workloads“.
2. Melden Sie sich beim PlateSpin-Server-Host als Administratorbenutzer an.

3 Starten Sie das PlateSpin-Treibermanager-Werkzeug. Navigieren Sie zu `C:\Programme\PlateSpin Protect Server\DriverManager` und starten Sie das Programm `DriverManager.exe`.

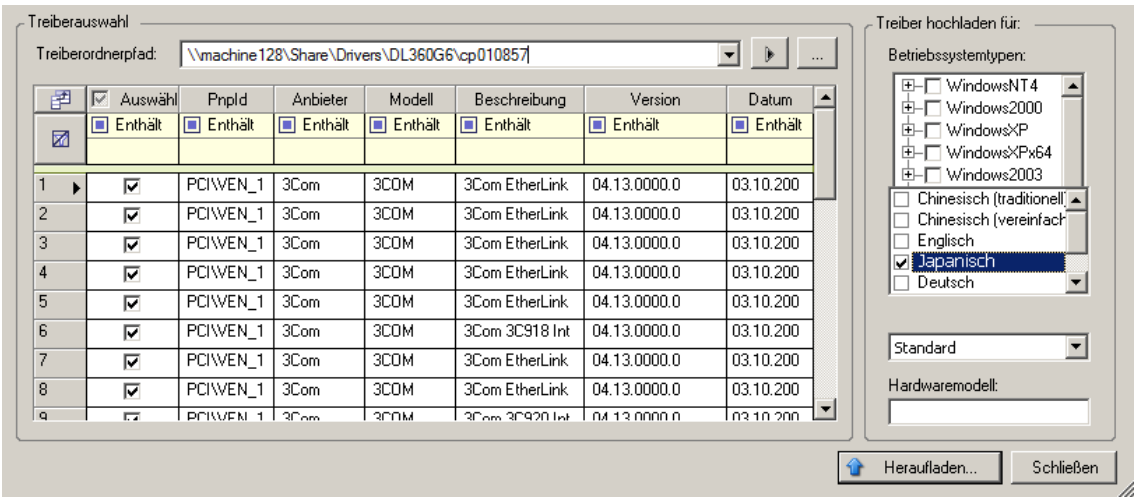
4 Klicken Sie auf **Werkzeuge** > **Gerätetreiber verwalten** und wählen Sie die Registerkarte **Windows-Treiber**.



5 Klicken Sie unten im Dialogfeld auf **Treiber heraufladen**.

6 Navigieren Sie im Dialogfeld „Treiberauswahl“ 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.

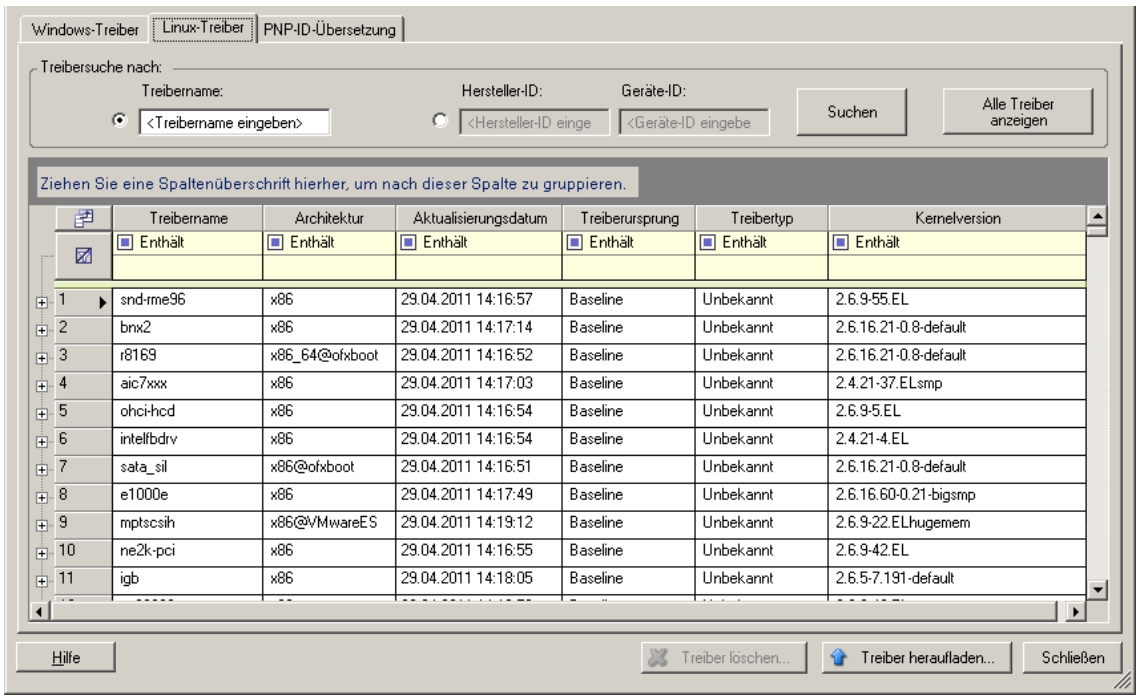


7 Klicken Sie auf **Heraufladen** und bestätigen Sie Ihre Auswahl.

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 unter „Packen von Gerätetreibern für Linux-Workloads“.
2. Melden Sie sich beim PlateSpin-Server-Host als Administratorbenutzer an.
3. Starten Sie das PlateSpin-Treibermanager-Werkzeug. Navigieren Sie zu `C:\Programme\PlateSpin Protect Server\DriverManager` und starten Sie das Programm `DriverManager.exe`.
4. Klicken Sie auf **Werkzeuge** > **Gerätetreiber verwalten** und wählen Sie die Registerkarte **Linux-Treiber**.



5. Klicken Sie unten im Dialogfeld auf **Treiber heraufladen**.
6. Navigieren Sie zu dem Ordner, der das erforderliche Treiberpaket (`*.pkg`) enthält, und klicken Sie auf **Alle Treiber heraufladen**.

   Das System lädt die ausgewählten Treiber in die Treiberdatenbank.

11.2 Verwalten der PlateSpin-PnP-ID-Zuordnungen

„Plug & Play“ (PnP) bezeichnet eine Funktion des Betriebssystems Windows, die die Konnektivität, Konfiguration und Verwaltung nativer Plug-&-Play-Geräte unterstützt. Unter Windows erleichtert diese Funktion das Auffinden von PnP-kompatiblen Hardwaregeräten, die mit einem PnP-kompatiblen Bus verbunden sind. Die Hersteller der PnP-kompatiblen Geräte weisen diesen Geräten eine Reihe von Geräteidentifikationsstrings zu. Diese Strings werden bei der Produktion in die Geräte einprogrammiert. Die Strings bilden die Grundlage der PnP-Funktionsweise: Sie sind ein Teil der Informationsquelle, mit der Windows einen geeigneten Treiber für das Gerät ermittelt.

Wenn der PlateSpin-Server die Workloads und die verfügbare Hardware ermittelt, werden diese PnP-IDs und der Speicher dieser Daten als Teil der Workload-Details festgestellt. Anhand der IDs stellt PlateSpin fest, ob und welche Treiber bei einem Failover/Failback eingefügt werden müssen. Auf

dem PlateSpin-Server wird eine Datenbank der PnP-IDs mit den Treibern für alle unterstützten Betriebssysteme geführt. Da unter Windows und Linux unterschiedliche Formate für die PnP-IDs verwendet werden, enthält ein Windows-Workload, der vom Protect-Linux-RAM-Datenträger (LRD) erkannt wird, PnP-IDs im Linux-Format.

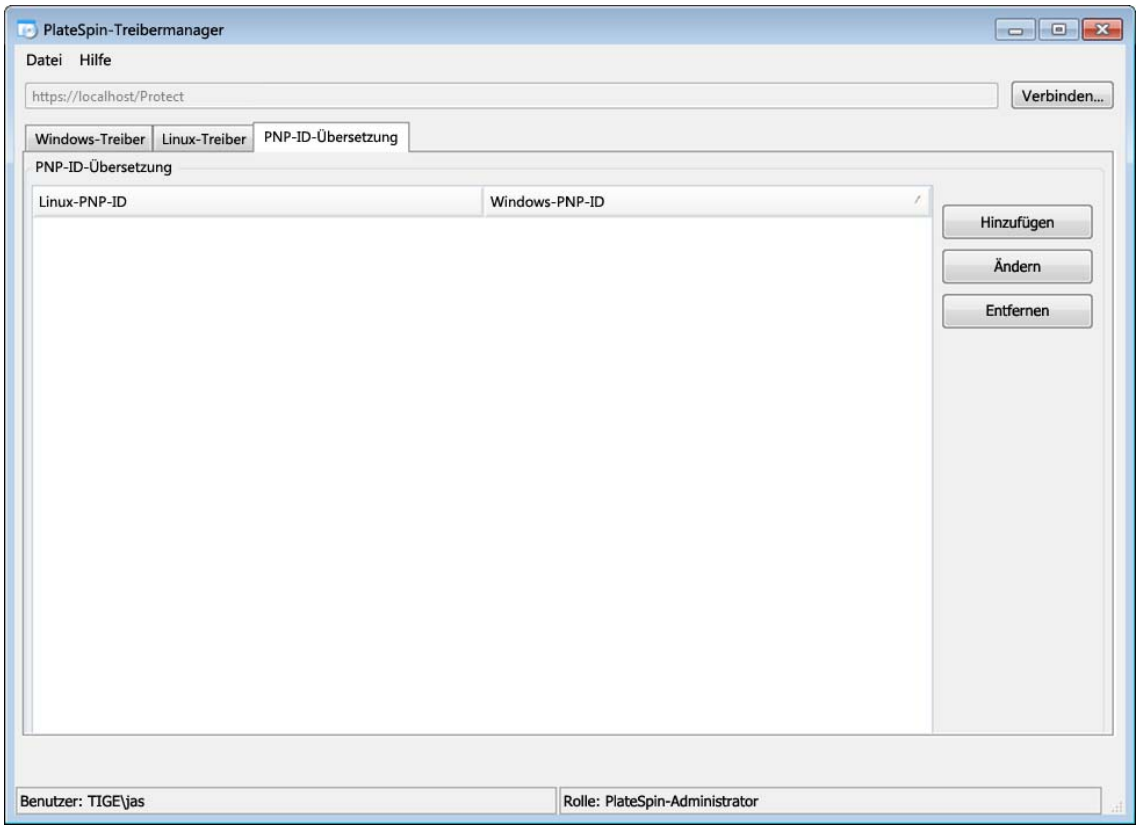
Diese IDs sind einheitlich formatiert, sodass PlateSpin die zugehörige Windows-PnP-ID anhand der Standardumwandlung feststellen kann. Die Übersetzung erfolgt automatisch im PlateSpin-Produkt.

Sie (oder ein Supporttechniker) können mit der Option „PNP-ID-Übersetzung“ im PlateSpin-Gerätetreiber-Werkzeug die PnP-ID-Zuordnungen hinzufügen, bearbeiten oder entfernen.

So fügen Sie benutzerdefinierte PnP-ID-Zuordnungen hinzu:

1. Melden Sie sich beim PlateSpin-Server-Host als Administratorbenutzer an.
2. Starten Sie das PlateSpin-Treibermanager-Werkzeug. Navigieren Sie zu `C:\Programme\PlateSpin Protect Server\DriverManager` und starten Sie das Programm `DriverManager.exe`.
3. Stellen Sie eine Verbindung zum PlateSpin-Server her.

   `https://localhost/Protect`
4. Wechseln Sie im Treibermanager-Werkzeug zur Registerkarte **PNP-ID-Übersetzung**. Die Liste **PnP-ID-Übersetzung** mit den derzeit bekannten benutzerdefinierten PnP-ID-Zuordnungen wird geöffnet.



5 Klicken Sie auf der Listenseite auf **Hinzufügen**. Das Dialogfeld „PNP-ID-Zuordnung erstellen“ wird geöffnet.

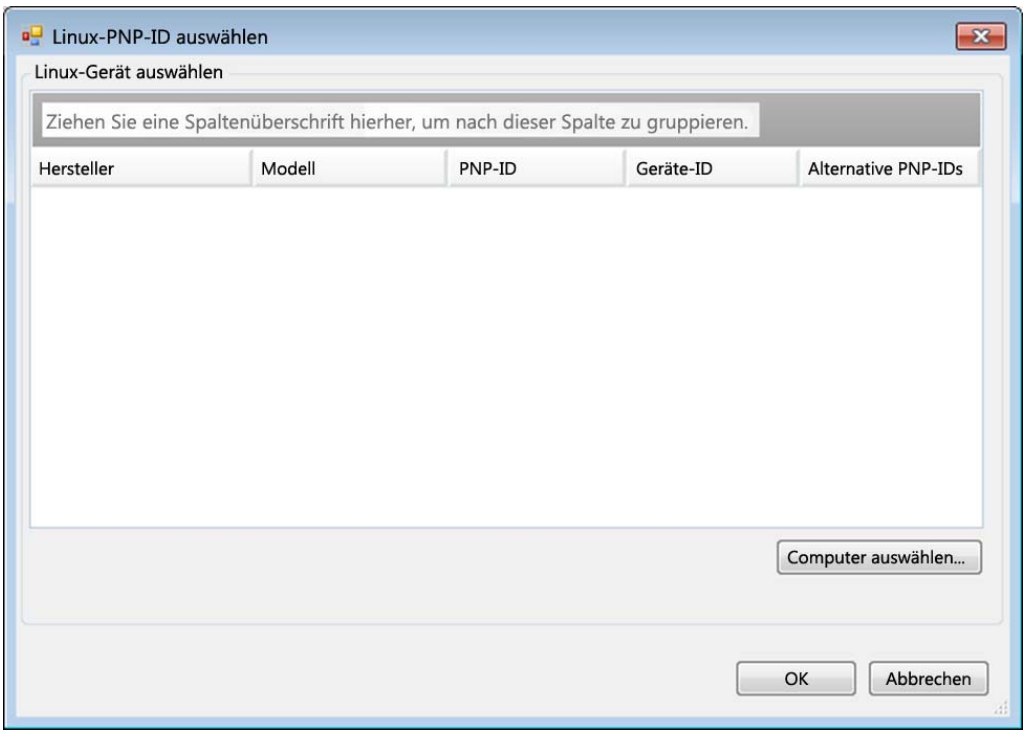
6 Fügen Sie dem Feld **Linux-PNP-ID** eine Linux-PnP-ID hinzu.

6a (Bedingt) Wenn Ihnen die Linux-PnP-ID bekannt ist, geben Sie diese ID ein.

Alternativ:

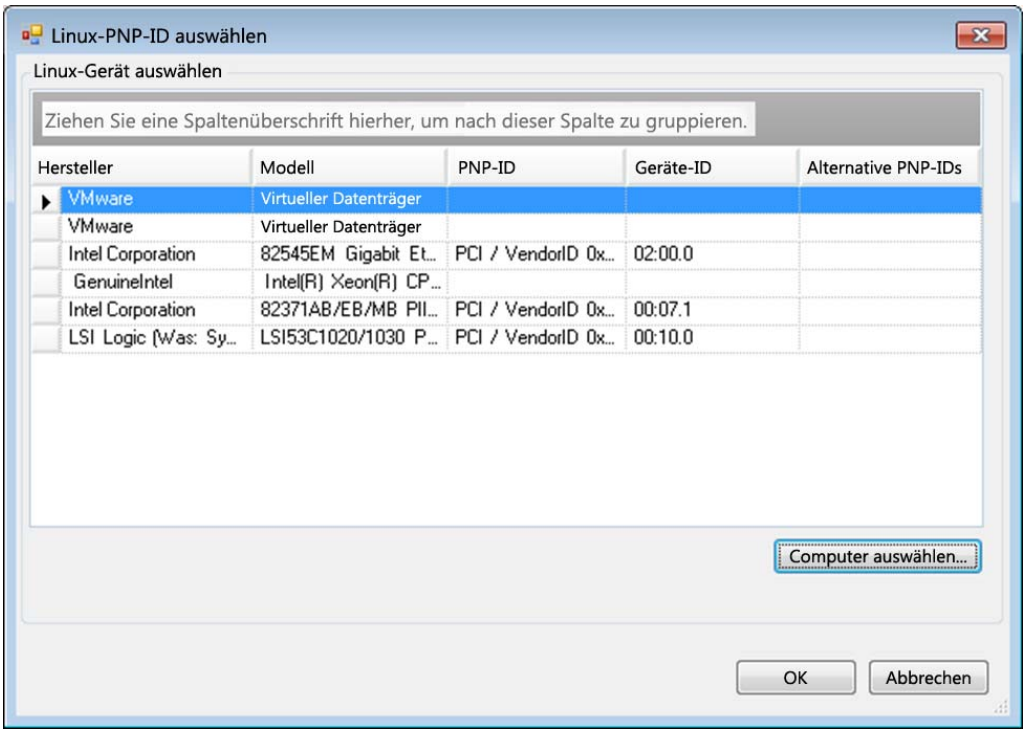
6b (Bedingt) Wählen Sie eine ID aus einem zuvor erkannten Workload aus:

6b1 Klicken Sie neben dem Feld **Linux-PNP-ID** auf **Auswählen**. Das Dialogfeld „Linux-PNP-ID auswählen“ wird geöffnet.



6b2 Klicken Sie im Dialogfeld auf **Computer auswählen**. Eine Liste der Computer, die zuvor durch den PlateSpin-Linux-RAM-Datenträger erkannt wurden, wird angezeigt.

6b3 Markieren Sie eines der Geräte in der Liste, und klicken Sie auf **Auswählen**. Das Gerät wird in die Liste im Dialogfeld „Linux-PNP-ID auswählen“ übernommen.



6b4 Wählen Sie ein Gerät in der Liste aus, und klicken Sie auf **OK**. Für die PnP-ID wird die standardmäßige Umwandlung vorgenommen und die ID wird im Dialogfeld „PnP-ID-Zuordnung erstellen“ angezeigt.

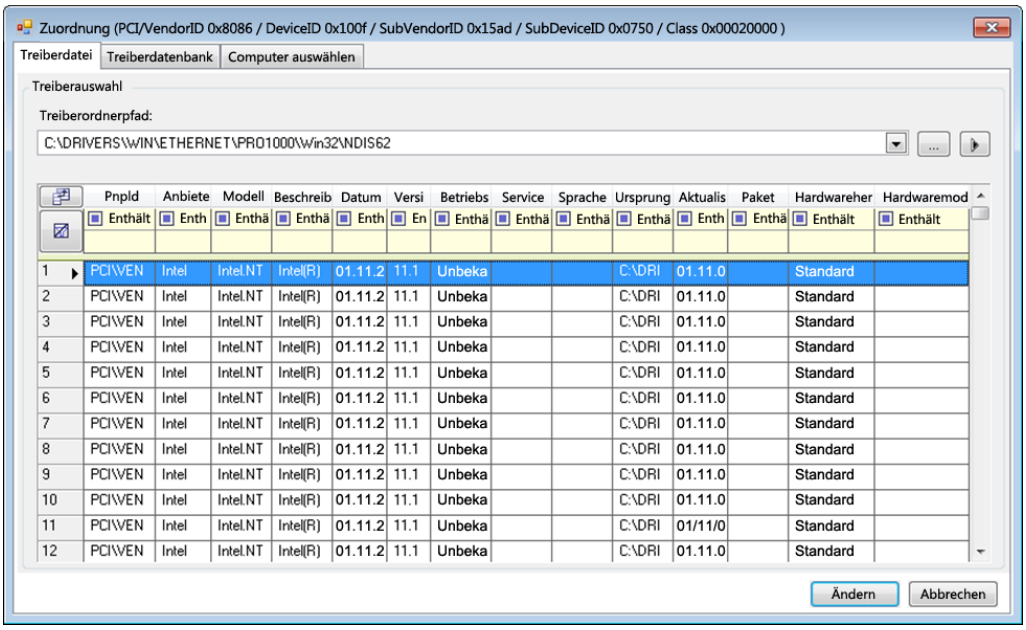
7 Fügen Sie dem Feld **Windows-PNP-ID** eine Windows-PnP-ID hinzu.

7a (Bedingt) Wenn Ihnen die Windows-PnP-ID bekannt ist, geben Sie diese ID ein.

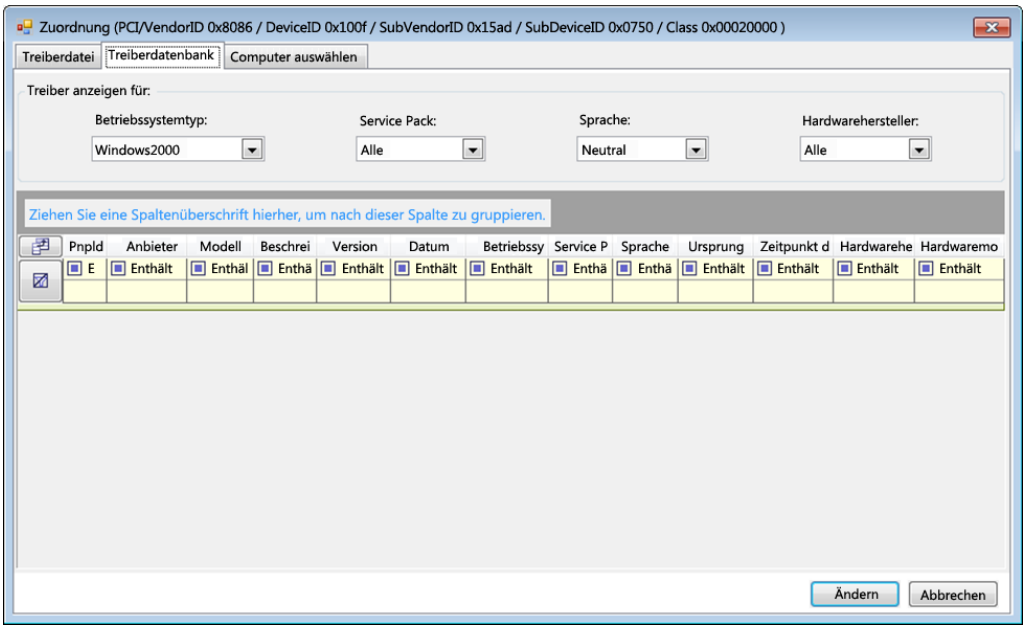
Alternativ:

7b (Bedingt) Klicken Sie neben dem Feld **Windows-PNP-ID** auf **Auswählen**. Ein Zuordnungswerkzeug wird geöffnet, in dem drei Methoden als Hilfe zum Zuordnen einer Windows-PnP-ID angeboten werden:

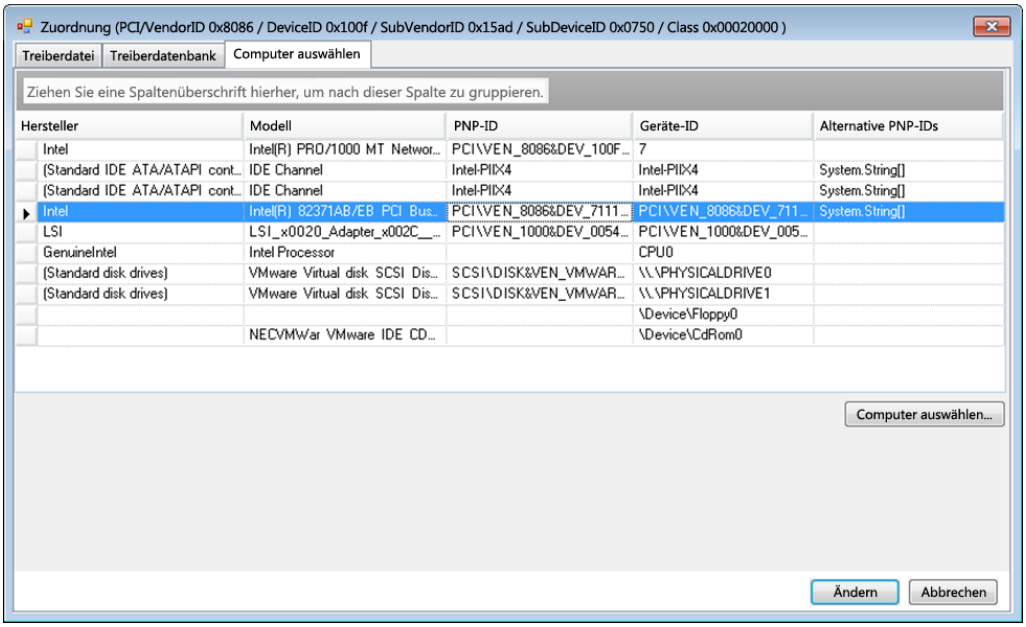
- Markieren Sie auf der Registerkarte **Treiberdatei** eine Windows-Treiberdatei (also eine Datei mit der Dateinamenerweiterung `*.inf`), wählen Sie die gewünschte PnP-ID aus, und klicken Sie auf **Ändern**.



- Markieren Sie auf der Registerkarte **Treiberdatenbank** die vorhandene Treiberdatenbank, wählen Sie die entsprechende PnP-ID aus, und klicken Sie auf **Ändern**.

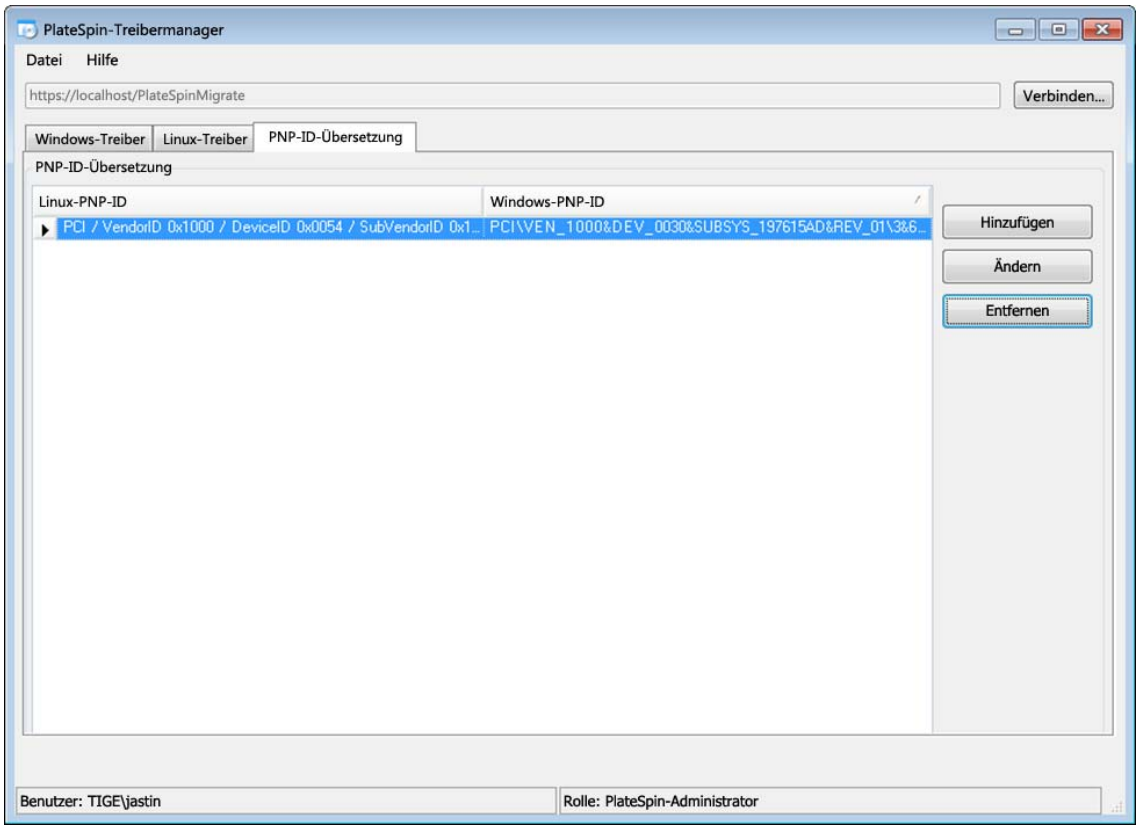


- Klicken Sie auf der Registerkarte **Computer auswählen** auf **Computer auswählen**. Wählen Sie dann in der Liste der Windows-Computer, die während der Live-Ermittlung erkannt wurden, einen Computer aus, und klicken Sie auf **OK**. Die Geräte dieses Computers werden angezeigt. Wählen Sie die gewünschte PnP-ID aus, und klicken Sie auf Ändern.



WICHTIG: Wenn Sie eine Windows-PnP-ID auswählen, die nicht mit einem Treiberpaket verknüpft ist, kann dies zum Zeitpunkt des Failover/Failback zu einem Fehler führen.

8 Bestätigen Sie im Dialogfeld „PNP-ID-Zuordnung erstellen“, dass die richtige Linux-PnP-ID und die richtige Windows-PnP-ID ausgewählt sind, und klicken Sie auf **OK**. Die Seite „PNP-ID-Übersetzung“ des PlateSpin-Treibermanagers wird geöffnet.



9 (Optional) Soll die Zuordnung in der Liste „PNP-ID-Übersetzung“ geändert oder entfernt werden, klicken Sie entsprechend auf **Entfernen** oder **Ändern**.

Mit **Entfernen** wird die Zuordnung gelöscht. (Zuvor wird allerdings ein Dialogfeld zur Bestätigung geöffnet.)

Zum Ändern gehen Sie wie folgt vor:

9a Klicken Sie auf **Ändern**. Das Dialogfeld „PnP-ID-Zuordnung erstellen“ wird geöffnet.

9b Wiederholen Sie Schritt 7 auf Seite 111, und bearbeiten Sie die Windows-PnP-ID.

HINWEIS: Die Linux-PnP-ID kann weder ausgewählt noch geändert werden.

12 Vorbereiten von Linux-Workloads für den Schutz

Mit den Aufgaben in diesem Abschnitt bereiten Sie Ihre Linux-Workloads für den Schutz in PlateSpin Protect vor.

12.1 Überprüfen der blockbasierten Treiber für Linux

Überwachen Sie, ob ein blkwatch-Modul für die Linux-Distribution des Workloads zur Verfügung steht. Eine Liste der vorkonfigurierten Treiber finden Sie unter „Von Protect unterstützte Linux-Distributionen“, auf Seite 135.

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 Knowledgebase-Artikel 7005873 (https://www.netiq.com/support/kb/doc.php?id=7005873).

12.2 Vorbereiten von Snapshots für die blockbasierte Übertragung (Linux)

Es wird empfohlen, Snapshots für die blockbasierte Datenübertragung vorzubereiten. Stellen Sie sicher, dass jede Volume-Gruppe über genügend freien Speicherplatz für Snapshots verfügt (mindestens 10 % der Summe aller Partitionen). Wenn keine Snapshots verfügbar sind, wird Protect die Blöcke im Ursprungs-Workload einzeln nacheinander zur Datenübertragung sperren und wieder freigeben.

12.2.1 Konfigurieren von LVM-Snapshots für die Linux-Volume-Reproduktion

Sind LVM-Snapshots vorhanden, greift der `blkwatch`-Treiber darauf zurück. Durch Kopieren der Blöcke aus dem Snapshot vermeiden Sie potenzielle Konflikte durch geöffnete Dateien.

Weitere Informationen zum LVM-Speicher finden Sie im Knowledgebase-Artikel 7005872 (https://www.netiq.com/support/kb/doc.php?id=7005872).

12.2.2 Konfigurieren von NSS-Snapshots für die NSS-Pool-Reproduktion

Bei Linux-Workloads mit Open Enterprise Server steht die LVM-Snapshot-Lösung für NSS-Pools nicht zur Verfügung. Bei der Reproduktion von NSS-Pools wird Protect die einzelnen Blöcke einzeln nacheinander zur Datenübertragung sperren und wieder freigeben. Damit potenzielle Konflikte mit geöffneten Dateien vermieden werden und die Leistung bei der Reproduktion erhöht wird, können Sie NSS-Pool-Snapshots für die Reproduktion heranziehen.

Sie können wahlweise einen einzigen unformatierten Datenträger für alle NSS-Pool-Snapshots hinzufügen oder je einen separaten unformatierten Datenträger pro NSS-Pool. Die beste Leistung wird erzielt, wenn Sie je einen separaten Datenträger pro Pool hinzufügen. Fügen Sie den Datenträger hinzu, bevor Sie den Workload-Schutz einrichten. Sie bereiten den zu verwendenden Datenträger vor und PlateSpin konfiguriert die NSS-Snapshots für den Pool während der Reproduktion.

HINWEIS: Standardmäßig nutzt PlateSpin den verwalteten NLVM-Datenträger mit der größten Menge an freiem Speicherplatz (unpartitionierter Speicherplatzspace) für die NSS-Pool-Snapshots. Wenn sich die NSS-Pool-Snapshots für die Reproduktion auf demselben Datenträger wie Ihr Root-Dateisystem befinden oder auf einem anderen Datenträger mit fortlaufender Datenträger-E/A, sollten Sie die NSS-Snapshots mithilfe der Datei `/etc/platespin/platespin.conf` auf einen geeigneten Datenträger leiten.

Weitere Informationen zur Funktionsweise von NSS-Snapshots auf Open Enterprise Server finden Sie unter „Richtlinien zum Verwenden und Verwalten von Pool-Snapshots“ (http://www.novell.com/documentation/oes2015/stor_nss_lx/data/br18up4.html) im *NSS-Dateisystem – Verwaltungshandbuch für Linux*.

So richten Sie einen oder mehrere Datenträger für Snapshots von NSS-Pools ein:

1. Fügen Sie auf dem OES-Ursprungs-Workload einen unformatierten Linux-Datenträger für Snapshots aller NSS-Pools hinzu. Alternativ können Sie je einen separaten Datenträger pro NSS-Pool erstellen.

   Die Größe des Datenträgers sollte etwa 20 % der Menge der verwendeten Daten im NSS-Pool entsprechen. Passen Sie die Größe gemäß der Datenänderungen oder des Datenwachstums an, die eventuell im Zeitraum einer Reproduktion auftreten können.

2. Initialisieren Sie alle in Schritt 1 erstellten Datenträger jeweils für die Verwaltung mit NLVM.

   Sie können den Datenträger mit NSSMU- oder NLVM-Befehlen initialisieren. Als Geräteformat ist wahlweise GPT oder DOS möglich.

   - So verwenden Sie NSSMU:

     1. Starten Sie NSSMU und wählen Sie **Geräte**.
     2. Wählen Sie den neuen Datenträger aus und initialisieren Sie ihn mit der Taste F3.

- So verwenden Sie NLVM-Befehle:
  1. Geben Sie in der Befehlszeile Folgendes ein:

     ```
     NLVM init <device_name> [format]
     ```

3 Unter Umständen müssen Sie angeben, welcher Datenträger für die Snapshots der einzelnen NSS-Pools verwendet werden sollen. Erstellen Sie im OES-Ursprungs-Workload eine Datei `platespin.conf` und weisen Sie die NSS-Pools den neuen Datenträgern zu:

3a Erstellen Sie in einem Texteditor die Datei `/etc/platespin/platespin.conf`.

3b Tragen Sie für die einzelnen NSS-Pools jeweils die Geräte- und Größeninformationen im Parameter `Customlocation` mit der folgenden Syntax ein:

```
[BenutzerdefinierterSpeicherort] /dev/pool/
<IhrPoolName>=<Gerät>:<maxUnpartitionierteGröße-in-MB>
```

Für den Pool `NSSPOOL`, mit dem Snapshots auf dem Gerät `sdc` mit einer maximalen Größe von 12.228 MB hinzugefügt werden sollen, geben Sie beispielsweise den nachfolgenden Eintrag an.

```
[BenutzerdefinierterSpeicherort] /dev/pool/NSSPOOL=sdc:12288
```

4 Speichern Sie die Datei.

5 Richten Sie den Workload-Schutz für den OES-Ursprungs-Workload ein.

12.3 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.

Das Skript `freeze` wird zu Beginn einer Reproduktion ausgeführt, das Skript `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 165). 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`

13 Vorbereiten des Windows-Cluster-Schutzes

PlateSpin Protect unterstützt den Schutz der Geschäftsdienste eines Microsoft Windows-Clusters. Die folgenden Microsoft Windows-Cluster-Betriebssysteme werden unterstützt:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2008 R2
- Windows Server 2003 R2

Weitere Informationen hierzu finden Sie in „Cluster“ in Abschnitt 1.1.1, „Unterstützte Windows-Workloads“, auf Seite 14.

HINWEIS: Die Windows-Cluster-Management-Software bietet die Failover- und Failback-Steuerung für die Ressourcen, die auf den Clusterknoten ausgeführt werden. Dieser Vorgang wird in diesem Dokument als *Clusterknoten-Failover* oder *Clusterknoten-Failback* bezeichnet.

Der PlateSpin-Server bietet die Failover- und Failback-Steuerung für den geschützten Workload, der für den Cluster steht. Dieser Vorgang wird in diesem Dokument als *PlateSpin-Failover* oder *PlateSpin-Failback* bezeichnet.

13.1 Planen des Cluster-Workload-Schutzes

Wenn die aktive Knotenermittlung für die PlateSpin-Umgebung aktiviert ist (Standard), werden zum Schutz eines Windows-Clusters die inkrementellen Reproduktionen der Änderungen auf dem aktiven Knoten an einen virtuellen Ein-Cluster-Knoten gestreamt, den Sie zur Fehlerbehebung der

Ursprungsinfrastruktur heranziehen können. Wenn Sie die aktive Knotenermittlung deaktivieren, kann jeder Knoten in einem Windows-Cluster als eigenständiger Knoten ermittelt und geschützt werden.

Bevor Sie Windows-Cluster für den Schutz konfigurieren können, muss die Umgebung die Voraussetzungen erfüllen, und Sie müssen sich mit den Bedingungen für den Schutz von Cluster-Workloads vertraut machen.

13.1.1 Anforderungen für den Cluster-Schutz

Der Umfang der Unterstützung des Cluster-Schutzes ist von den Bedingungen unter Tabelle 13-1 abhängig. Beachten Sie diese Anforderungen, wenn Sie den Schutz für Cluster in Ihrer PlateSpin-Umgebung konfigurieren.

Tabelle 13-1 *Cluster-Schutzanforderungen*

Anforderung	Beschreibung
Den aktiven Knoten als Windows-Cluster ermitteln	Die globale PlateSpin-Konfigurationseinstellung `DiscoverActiveNodeAsWindowsCluster` legt fest, ob Windows-Cluster als Cluster oder als separate, eigenständige Computer geschützt werden sollen: ◆ **Wahr (Standard):** Der aktive Knoten wird als Windows-Cluster ermittelt. ◆ **Falsch:** Einzelne Knoten können als eigenständige Computer ermittelt werden. Weitere Informationen hierzu finden Sie in Abschnitt 13.2, „Konfigurieren der Ermittlung des aktiven Windows-Knotens“, auf Seite 125.
Suchwerte für den Ressourcennamen	Die globale PlateSpin-Konfigurationseinstellung `MicrosoftClusterIPAddressNames` bestimmt die Cluster-Ressourcennamen, die in Ihrer PlateSpin-Umgebung ermittelt werden können. Geben Sie Suchwerte an, mit denen der Name der gemeinsam genutzten Cluster-IP-Adressressource vom Namen anderer IP-Adressressourcen im Cluster unterschieden werden kann. Weitere Informationen hierzu finden Sie in Abschnitt 13.4, „Hinzufügen von Suchwerten für den Ressourcennamen“, auf Seite 126.

Anforderung	Beschreibung
Windows-Cluster-Modus	Die globale PlateSpin-Konfigurationseinstellung `WindowsClusterMode` bestimmt die Methode für die blockbasierte Datenübertragung bei inkrementellen Reproduktionen: ◆ **Standard:** Treiberlose Synchronisierung. ◆ **SingleNodeBBT:** Treiberbasierte blockbasierte Übertragung. Informationen hierzu finden Sie in den folgenden Abschnitten: ◆ „Blockbasierte Übertragung für Cluster“, auf Seite 121 ◆ „Konfigurieren der blockbasierten Übertragungsmethode für Cluster“, auf Seite 126
Hostname oder IP-Adresse des aktiven Knotens	Beim Vorgang **Workload hinzufügen** müssen Sie den Hostnamen oder die IP-Adresse des aktiven Knotens im Cluster angeben. Aufgrund von Sicherheitsänderungen durch Microsoft können Windows-Cluster nicht mehr über den Namen des virtuellen Clusters (also über die IP-Adresse des gemeinsam genutzten Clusters) ermittelt werden.
Auflösbarer Hostname	Der PlateSpin-Server muss den Hostnamen der einzelnen Knoten im Cluster nach ihren IP-Adressen auflösen können. **HINWEIS:** Zum Auflösen des Hostnamens nach der IP-Adresse ist die DNS-Suche und die rekursive DNS-Suche erforderlich.
Quorum-Ressource	Die Quorum-Ressource eines Clusters muss in der Ressourcengruppe (Dienst) des zu schützenden Clusters koexistieren.
Ähnlichkeiten der Clusterknoten	Im standardmäßigen Windows-Cluster-Modus kann die treiberlose Synchronisierung von jedem aktiv werdenden Knoten aus fortgesetzt werden, wenn die Knoten ähnlich sind. Stimmen sie nicht überein, können die Reproduktionen nur auf dem ursprünglich ermittelten aktiven Knoten erfolgen. Weitere Informationen hierzu finden Sie in „Clusterknotenähnlichkeit“, auf Seite 125.
PowerShell 2.0	Die Windows PowerShell 2.0- muss auf allen Knoten im Cluster installiert sein.

13.1.2 Blockbasierte Übertragung für Cluster

Die blockbasierte Übertragung für Cluster unterscheidet sich von der Übertragung für eigenständige Server. Bei der ursprünglichen Reproduktion wird entweder eine vollständige Kopie angelegt (vollständige Reproduktion) oder es wird eine treiberlose Synchronisierung auf dem aktiven Knoten im Cluster ausgeführt. Bei nachfolgenden inkrementellen Reproduktionen kann eine treiberlose Methode oder eine treiberbasierte Methode für die blockbasierte Datenübertragung herangezogen werden.

HINWEIS: Protect unterstützt keine dateibasierte Übertragung für Cluster.

Die globale PlateSpin-Konfigurationseinstellung `WindowsClusterMode` bestimmt die Methode für die blockbasierte Datenübertragung bei inkrementellen Reproduktionen:

- **Standard:** Treiberlose Synchronisierung.
- **SingleNodeBBT:** Treiberbasierte blockbasierte Übertragung. Nur mit Fibre Channel SANs verwenden.

WARNUNG: Versuchen Sie nicht, SingleNodeBBT auf Clustern mit freigegebenen iSCSI-Laufwerken zu verwenden. Dadurch können die Cluster nicht mehr verwendet werden.

In Tabelle 13-2 werden die beiden Methoden beschrieben und verglichen.

Tabelle 13-2 *Vergleich der blockbasierten Datenübertragungsmethoden für inkrementelle Reproduktionen*

Überlegung	Standard-BBT	Einzelknoten-BBT
Datenübertragungs-methode	Verwendet die treiberlose Synchronisierung mit MD5-basierter Reproduktion auf dem derzeit aktiven Knoten.	Verwendet einen BBT-Treiber, der auf dem ursprünglich ermittelten aktiven Knoten installiert ist.
Leistung	Potenziell langsame inkrementelle Reproduktionen.	Erhöht die Leistung bei inkrementellen Reproduktionen erheblich.
Treiber	◆ Kein BBT-Treiber zu installieren. ◆ Kein Neubooten der Ursprungs-Clusterknoten erforderlich.	◆ Installieren Sie einen BBT-Treiber mit dem Protect Agent-Dienstprogramm auf dem ursprünglich ermittelten aktiven Knoten im Cluster. ◆ Booten Sie den Knoten neu, damit der Treiber angewendet wird. So wird ein Failover auf einen anderen Knoten im Cluster ausgelöst. Legen Sie den ursprünglich ermittelten Knoten nach dem Neubooten wieder als aktiven Knoten fest. ◆ Derselbe Knoten muss aktiv bleiben, damit Reproduktionen ausgeführt und die blockbasierte Einzelknoten-Übertragung verwendet werden kann. ◆ Nach dem Installieren des BBT-Treibers muss entweder eine vollständige Reproduktion oder eine treiberlose inkrementelle Reproduktion ausgeführt werden, bevor die treiberbasierten inkrementellen Reproduktionen beginnen können.
Unterstützte Windows-Cluster	Für alle unterstützten Windows-Server-Cluster verwendbar.	Für Cluster mit Windows Server 2008 R2 (oder höher). Andere unterstützte Windows-Cluster führen die Reproduktion mithilfe der treiberlosen Synchronisierung aus.

Überlegung	Standard-BBT	Einzelknoten-BBT
Erste inkrementelle Reproduktion	Verwendet die treiberlose Synchronisierung auf dem aktiven Knoten.	Verwendet die treiberbasierte blockbasierte Datenübertragung auf dem ursprünglich ermittelten aktiven Knoten, wenn nach der Installation des BBT-Treibers eine vollständige Reproduktion ausgeführt wurde. Ansonsten wird die treiberlose Synchronisierung auf dem ursprünglich ermittelten aktiven Knoten ausgeführt.
Nachfolgende inkrementelle Reproduktion	Verwendet die treiberlose Synchronisierung auf dem aktiven Knoten.	Verwendet die treiberbasierte blockbasierte Datenübertragung auf dem ursprünglich ermittelten aktiven Knoten. Wenn ein Cluster zu einem anderen Knoten wechselt, erfolgt die erste inkrementelle Reproduktion mit der treiberlosen Synchronisierungsmethode, sobald der ursprüngliche aktive Knoten wieder aktiv ist. Weitere Informationen hierzu finden Sie in „Auswirkungen des Clusterknoten-Failovers auf die Reproduktion“, auf Seite 123.

13.1.3 Auswirkungen des Clusterknoten-Failovers auf die Reproduktion

Tabelle 13-3 zeigt die Auswirkungen des Clusterknoten-Failovers auf die Reproduktion und die erforderlichen Maßnahmen durch den Protect-Administrator.

Tabelle 13-3 *Auswirkungen des Clusterknoten-Failovers auf die Reproduktion*

Clusterknoten-Failover oder -Failback	Standard-BBT	Einzelknoten-BBT
Clusterknoten-Failover erfolgt während der ersten vollständigen Reproduktion	Die Reproduktion schlägt fehl. Die erste vollständige Reproduktion muss erfolgreich und ohne Cluster-Failover abgeschlossen werden. 1. Entfernen Sie den Cluster aus Protect 2. (Optional) Legen Sie den ursprünglich ermittelten aktiven Knoten wieder als aktiven Knoten fest. 3. Fügen Sie den Cluster über den aktiven Knoten wieder hinzu. 4. Führen Sie die erste vollständige Reproduktion erneut aus.	

Clusterknoten-Failover oder -Failback	Standard-BBT	Einzelknoten-BBT
Clusterknoten-Failover erfolgt während einer nachfolgenden vollständigen Reproduktion oder einer nachfolgenden inkrementellen Reproduktion	Der Reproduktionsbefehl wird abgebrochen und eine Meldung wird angezeigt, dass die Reproduktion erneut ausgeführt werden muss. Falls das Profil des neuen aktiven Knotens dem des ausgefallenen aktiven Knotens entspricht, wird der Vertrag für den Schutz fortgesetzt. 1. Führen Sie die Reproduktion auf dem nunmehr aktiven Knoten erneut aus. Falls das Profil des aktiven Knotens nicht dem des fehlgeschlagenen Knotens entspricht, gilt der Schutzvertrag nur auf dem ursprünglich aktiven Knoten. 1. Legen Sie den ursprünglich ermittelten aktiven Knoten wieder als aktiven Knoten fest. 2. Führen Sie die Reproduktion auf dem aktiven Knoten erneut aus.	Der Reproduktionsbefehl wird abgebrochen und eine Meldung wird angezeigt, dass die Reproduktion erneut ausgeführt werden muss. Der Schutzvertrag gilt nur auf dem ursprünglich ermittelten aktiven Knoten. 1. Legen Sie den ursprünglich ermittelten aktiven Knoten wieder als aktiven Knoten fest. 2. Führen Sie die Reproduktion auf dem aktiven Knoten erneut aus. Bei der ersten inkrementellen Reproduktion nach einem Cluster-Failover/-Failback wird die treiberlose Synchronisierung verwendet. Bei nachfolgenden inkrementellen Reproduktionen wird der mit dem Einzelknoten-BBT festgelegte blockbasierte Treiber herangezogen.
Clusterknoten-Failover erfolgt zwischen Reproduktionen	Falls das Profil des neuen aktiven Knotens dem des fehlgeschlagenen aktiven Knotens entspricht, wird der Schutzvertrag gemäß dem Zeitplan für die nächste inkrementelle Reproduktion fortgesetzt. Andernfalls wird der Befehl für die nächste inkrementelle Reproduktion nicht ausgeführt. Wenn eine geplante inkrementelle Reproduktion fehlschlägt: 1. Legen Sie den ursprünglich ermittelten aktiven Knoten wieder als aktiven Knoten fest. 2. Führen Sie eine inkrementelle Reproduktion aus.	Die inkrementelle Reproduktion schlägt fehl, wenn der aktive Knoten zwischen den Reproduktionen wechselt. 1. Der ursprünglich ermittelte aktive Knoten muss wieder als aktiver Knoten fungieren. 2. Führen Sie eine inkrementelle Reproduktion aus. Bei der ersten inkrementellen Reproduktion nach einem Cluster-Failover/-Failback wird die treiberlose Synchronisierung verwendet. Bei nachfolgenden inkrementellen Reproduktionen wird der mit dem Einzelknoten-BBT festgelegte blockbasierte Treiber herangezogen.

13.1.4 Clusterknotenähnlichkeit

Im standardmäßigen Windows-Cluster-Modus müssen die Clusterknoten ähnliche Profile aufweisen, damit der Reproduktionsprozess nicht unterbrochen wird. Die Profile von Clusterknoten gelten als ähnlich, wenn alle folgenden Bedingungen erfüllt sind:

- Seriennummern für die lokalen Volumes der Knoten (System-Volume und reserviertes System-Volume) müssen auf allen Clusterknoten gleich sein.

  HINWEIS: Ändern Sie die Seriennummern des lokalen Volumes mit dem angepassten Dienstprogramm *Volume Manager*, damit sie mit den einzelnen Knoten des Clusters übereinstimmen. Weitere Informationen hierzu finden Sie unter „Synchronisieren von Seriennummern im lokalen Clusterknoten-Speicher“, auf Seite 139.

  Wenn die lokalen Volumes auf allen Knoten des Clusters verschiedene Seriennummern aufweisen, können Sie nach einem Clusterknoten-Failover keine Reproduktion ausführen. Beispiel: Bei einem Clusterknoten-Failover tritt ein Fehler im aktiven Knoten 1 auf und die Cluster-Software bestimmt den Knoten 2 als aktiven Knoten. Wenn die lokalen Laufwerke auf den beiden Knoten unterschiedliche Seriennummern aufweisen, wird der Befehl für die nächste Reproduktion des Workloads nicht ausgeführt.
- Die Knoten müssen dieselbe Anzahl an Volumes umfassen.
- Alle Volumes auf allen Knoten müssen exakt gleich groß sein.
- Die Knoten müssen eine identische Anzahl an Netzwerkverbindungen besitzen.

13.1.5 Einrichtung des Schutzes

Zur Konfiguration des Schutzes für einen Windows-Cluster gehen Sie nach dem gleichen Ablaufplan wie für den normalen Workload-Schutz vor. Geben Sie den Hostnamen oder die IP-Adresse für den aktiven Knoten des Clusters an. Weitere Informationen hierzu finden Sie in „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“, auf Seite 37.

13.2 Konfigurieren der Ermittlung des aktiven Windows-Knotens

Sie können Windows-Server-Cluster wahlweise als Cluster oder als eigenständige Computer ermitteln, abhängig von der globalen PlateSpin-Konfigurationseinstellung `DiscoverActiveNodeAsWindowsCluster`.

Sollen Windows-Cluster als Cluster ermittelt werden, stellen Sie den Parameter `DiscoverActiveNodeAsWindowsCluster` auf `True` (Wahr) ein. Das ist die Standardeinstellung. Die Clusterermittlung, die Inventarisierung und der Workload-Schutz erfolgen über den Hostnamen oder die IP-Adresse des aktiven Knotens im Cluster (also nicht über den virtuellen Clusternamen und eine administrative Freigabe). Für die nicht aktiven Knoten im Cluster werden keine separaten Workloads konfiguriert. Weitere Voraussetzungen für den Schutz von Cluster-Workloads finden Sie unter „Anforderungen für den Cluster-Schutz“, auf Seite 120.

Sollen alle Windows-Cluster als individuelle, eigenständige Computer ermittelt werden, stellen Sie den Parameter `DiscoverActiveNodeAsWindowsCluster` auf `False` (Falsch) ein. Mit dieser Einstellung kann der PlateSpin-Server alle Knoten in einem Windows-Failovercluster als eigenständige Computer ermitteln. Der aktive Knoten des Clusters sowie die nicht aktiven Knoten werden in diesem Fall als normale, nicht clusterfähige Windows-Workloads inventarisiert.

So aktivieren oder deaktivieren Sie die Clusterermittlung:

1. Öffnen Sie die Konfigurationsseite für den PlateSpin-Server unter

   https://<*IP-Adresse_des_PlateSpin-Servers*>/PlatespinConfiguration
2. Suchen Sie den Eintrag `DiscoverActiveNodeAsWindowsCluster`, und klicken Sie auf **Bearbeiten**.
3. Wählen Sie im Feld **Wert** die Einstellung **True** (Clusterermittlung aktivieren) bzw. **False** (Clusterermittlung deaktivieren).
4. Klicken Sie auf **Speichern**.

13.3 Konfigurieren der blockbasierten Übertragungsmethode für Cluster

Inkrementelle Reproduktionen für Windows-Cluster können mit einer treiberlosen Methode (Standard) oder einer treiberbasierten Methode (SingleNodeBBT) für die blockbasierte Datenübertragung erfolgen, abhängig von der globalen PlateSpin-Konfigurationseinstellung `WindowsClusterMode`. Weitere Informationen finden Sie unter „Blockbasierte Übertragung für Cluster“, auf Seite 121.

So konfigurieren Sie „WindowsClusterMode“:

1. Öffnen Sie die Konfigurationsseite für den PlateSpin-Server unter

   https://<*IP-Adresse_des_PlateSpin-Servers*>/PlatespinConfiguration
2. Suchen Sie den Eintrag `WindowsClusterNode` und klicken Sie auf **Bearbeiten**.
3. Wählen Sie im Feld **Wert** den Eintrag **Standard** für inkrementelle Reproduktionen mit treiberloser Synchronisierung bzw. den Eintrag **SingleNodeBBT** für inkrementelle Reproduktionen mit blockbasierten Treibern.
4. Klicken Sie auf **Speichern**.

13.4 Hinzufügen von Suchwerten für den Ressourcennamen

Damit der aktive Knoten in einem Windows-Failovercluster erkannt werden kann, muss PlateSpin Protect den Namen der gemeinsam genutzten Cluster-IP-Adressressource vom Namen anderer IP-Adressressourcen im Cluster unterscheiden können. Die gemeinsam genutzte Cluster-IP-Adressressource befindet sich auf dem aktiven Knoten im Cluster.

Der globale Parameter `MicrosoftClusterIPAddressNames` auf der Konfigurationsseite für den PlateSpin-Server enthält eine Liste der Suchwerte, mit denen Windows-Cluster-Workloads ermittelt werden. Wenn Sie einen Windows-Cluster-Workload hinzufügen, müssen Sie die IP-Adresse des derzeit aktiven Knotens im Cluster angeben. PlateSpin Protect sucht in den Namen der Cluster-IP-Adressressourcen auf dem Knoten nach dem Namen, der mit den angegebenen Zeichen *beginnt*. Jeder Suchwert muss daher so viele Zeichen enthalten, dass die gemeinsam genutzte IP-Adressressource auf einem bestimmten Cluster feststellbar ist, kann jedoch gleichzeitig so kurz sein, dass er auch für die Ermittlung in anderen Windows-Clustern genutzt werden kann.

Der Suchwert `Clust-IP-Adresse` oder `Clust-IP` ordnet beispielsweise die Ressourcennamen *Clust-IP-Adresse* für 10.10.10.201 und *Clust-IP-Adresse* für 10.10.10.101 zu.

Die gemeinsam genutzte Cluster-IP-Adressressource trägt den Standardnamen `Cluster IP Address` in englischer Sprache (bzw. eine Übersetzung dieses Namens, wenn ein Clusterknoten in einer anderen Sprache konfiguriert wurde). Die Standardsuchwerte in der Liste `MicrosoftClusterIPAddressNames` enthalten den Ressourcennamen `Cluster IP Address` auf Englisch und in allen unterstützten Sprachen.

Der Ressourcenname der gemeinsam genutzten Cluster-IP-Adressressource ist benutzerkonfigurierbar; tragen Sie daher nach Bedarf weitere Suchwerte in die Liste ein. Wenn Sie den Ressourcennamen ändern, müssen Sie die Liste `MicrosoftClusterIPAddressNames` mit dem entsprechenden Suchwert ergänzen. Wenn Sie beispielsweise den Ressourcennamen `Win2012-CLUS10-IP-ADRESSE` festlegen, fügen Sie diesen Wert zur Liste hinzu. Falls eine Namenskonvention für mehrere Cluster gilt, werden mit dem Eintrag `Win2012-CLUS` alle Ressourcennamen aufgefunden, die mit dieser Zeichenfolge beginnen.

So tragen Sie Suchwerte in die Liste `MicrosoftClusterIPAddressNames` ein:

1. Öffnen Sie die Konfigurationsseite für den PlateSpin-Server unter https://<*IP-Adresse_des_PlateSpin-Servers*>/PlatespinConfiguration
2. Suchen Sie den Eintrag `MicrosoftClusterIPAddressNames`, und klicken Sie auf **Bearbeiten**.
3. Tragen Sie im Feld **Wert** einen oder mehrere Suchwerte in die Liste ein.
4. Klicken Sie auf **Speichern**.

13.5 Zeitüberschreitung bei Quorumvermittlung

Mit dem globalen Parameter `FailoverQuorumArbitrationTimeout` auf der Konfigurationsseite für den PlateSpin-Server legen Sie den Registrierungsschlüssel „QuorumArbitrationTimeMax“ für Windows Server-Failovercluster in Ihrer PlateSpin-Umgebung fest. Die standardmäßige Zeitüberschreitung beträgt 60 Sekunden gemäß dem Microsoft-Standardwert für diese Einstellung. Weitere Informationen finden Sie unter *QuorumArbitrationTimeMax* (https://msdn.microsoft.com/en-us/library/aa369123%28v=vs.85%29.aspx?f=255&MSPPError=-2147217396) auf der Microsoft Developer Network-Website. Das angegebene Zeitüberschreitungsintervall gilt für die Quorumvermittlung bei Failover und Failback.

So legen Sie die Zeitüberschreitung für die Quorumvermittlung für alle Windows-Failovercluster fest:

1. Öffnen Sie die Konfigurationsseite für den PlateSpin-Server unter https://<*IP-Adresse_des_PlateSpin-Servers*>/PlatespinConfiguration.
2. Suchen Sie den Eintrag `FailoverQuorumArbitrationTimeout`, und klicken Sie auf **Bearbeiten**.
3. Geben Sie in das Feld **Wert** den maximalen Zeitraum (in Sekunden) für die Quorumvermittlung ein.
4. Klicken Sie auf **Speichern**.

13.6 Festlegen der Seriennummern des lokalen Volumes

Mit dem angepassten Dienstprogramm *Volume Manager* können Sie die Seriennummern des lokalen Volumes ändern, sodass sie in den einzelnen Knoten des Clusters übereinstimmen. Weitere Informationen hierzu finden Sie unter „Synchronisieren von Seriennummern im lokalen Clusterknoten-Speicher“, auf Seite 139.

13.7 PlateSpin-Failover

Wenn der PlateSpin-Failover-Vorgang abgeschlossen ist und der virtuelle Ein-Knoten-Cluster online geht, sehen Sie einen Cluster mit mehreren Knoten, bei dem ein Knoten aktiv ist (alle anderen Knoten sind nicht verfügbar).

Für ein PlateSpin-Failover (oder zum Testen des PlateSpin-Failover) auf einem Windows-Cluster muss der Cluster eine Verbindung zu einem Domänencontroller herstellen können. Zur Nutzung der Test-Failover-Funktion müssen Sie den Domänencontroller zusammen mit dem Cluster schützen. Während des Tests müssen Sie den Domänencontroller hochfahren, gefolgt vom Windows-Cluster-Workload (in einem isolierten Netzwerk).

13.8 PlateSpin-Failback

Für einen PlateSpin-Failback-Vorgang ist eine vollständige Reproduktion für Windows-Cluster-Workloads erforderlich.

Wenn Sie das PlateSpin-Failback als vollständige Reproduktion auf ein physisches Ziel konfigurieren, können Sie eine der folgenden Methoden verwenden:

- Ordnen Sie alle Festplatten auf dem virtuellen PlateSpin-Ein-Knoten-Cluster einer einzigen lokalen Festplatte auf dem Failback-Ziel zu.
- Fügen Sie dem physischen Failback-Rechner eine andere Festplatte (`Festplatte 2`) hinzu. Sie können den PlateSpin-Failback-Vorgang dann so konfigurieren, dass das System-Volume des Failover-Computers auf `Festplatte 1` und die zusätzlichen Festplatten des Failover-Computers (zuvor gemeinsam genutzte Festplatten) auf `Festplatte 2` wiederhergestellt werden. So kann die Systemfestplatte auf die Speicherfestplatte mit gleicher Größe wiederhergestellt werden wie die ursprüngliche Quelle.

Nach einem PlateSpin-Failback müssen Sie den gemeinsam genutzten Speicher wieder anschließen und die Clusterumgebung neu aufbauen, bevor Sie weitere Knoten in den wiederhergestellten Cluster aufnehmen können.

HINWEIS: Sobald der Cluster die Phase **Bereit zum erneuten Schützen** erreicht, müssen Sie zunächst das Failback-Ziel neu aufbauen und wiederherstellen, so dass es als Cluster ermittelt werden kann. Im Rahmen des Neuaufbaus müssen Sie den PlateSpin-Clustertreiber manuell deinstallieren.

Weitere Informationen zum Neuaufbauen der Cluster-Umgebung nach einem PlateSpin-Failover/-Failback finden Sie in den folgenden Ressourcen:

- **Windows Server 2012 R2 Failover-Cluster (Failback auf physischen oder virtuellen Neuaufbau):** Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7016770 (http://www.netiq.com/support/kb/doc.php?id=7016770).
- **Windows Server 2008 R2 Failover-Cluster (Failback auf physischen oder virtuellen Neuaufbau):** Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7015576 (http://www.netiq.com/support/kb/doc.php?id=7015576).

---

14 Fehlerbehebung bei der Workload-Ermittlung und der Inventarisierung

In diesem Abschnitt finden Sie Informationen zur Behebung häufiger Fehler bei der Workload-Ermittlung und der Inventarisierung.

14.1 Fehlerbehebung bei der Ermittlung von Windows-Workloads

Mit den Informationen in diesem Abschnitt können Sie Probleme bei der Workload-Inventarisierung und der Ermittlung von Windows-Workloads beheben:

14.1.1 Häufige Probleme und deren Lösung

Probleme oder Meldungen	Lösungen
`Die Domäne in dem Berechtigungsnachweis ist ungültig oder leer.`	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.

Probleme oder Meldungen	Lösungen
`Es konnte keine Verbindung zum Windows-Server hergestellt werden. Zugriff verweigert.`	Beim 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 131 erneut durch. Wenn der Test erfolgreich ist, versuchen Sie erneut, den Workload hinzuzufügen. ◆ „Fehlerbehebung bei DCOM-Verbindungen“, auf Seite 132 ◆ „Fehlerbehebung bei der RPC-Dienst-Verbindung“, auf Seite 132
`Es konnte keine Verbindung zum Windows-Server hergestellt werden. Netzwerkpfad nicht gefunden.`	Netzwerk-Verbindungsfehler. Führen Sie die Tests in „Durchführen von Verbindungstests“, auf Seite 131 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.
`„Serverdetails für {hostname} ermitteln" fehlgeschlagen. Fortschritt: 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 finden Sie im Knowledgebase-Artikel 7920339 (https://www.netiq.com/support/kb/doc.php?id=7920339). ◆ Wenn lokale Richtlinien oder Domänenrichtlinien die erforderlichen Berechtigungen einschränken, führen Sie die im Knowledgebase-Artikel 7920862 (https://www.netiq.com/support/kb/doc.php?id=7920862) beschriebenen Schritte aus.

Workload-Ermittlungsfehler mit Fehlermeldung
 	
`Die Datei output.xml wurde nicht gefunden`
 	
oder
 	
`Netzwerkpfad nicht gefunden`
 	
oder (beim Versuch, einen Windows-Cluster zu ermitteln)
 	
`Inventar konnte nicht ermitteln. Als Ergebnis wurde nichts zurückgegeben.`
	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 133.
	◆ 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 Protect auf diese Freigaben zugreifen kann. Weitere Informationen hierzu finden Sie unter „Aktivieren von Datei-/Freigabe-Berechtigungen und -Zugriff“, auf Seite 133.
	◆ 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.

14.1.2 Ändern der Heartbeat-Startverzögerung des OFX-Controllers

Damit keine Ermittlungsprobleme aufgrund von Zeitproblemen auftreten, wird eine standardmäßige Heartbeat-Startverzögerung von 15 Sekunden (15.000 ms) für den OFX-Controller eingestellt. Die Einstellung kann mit dem Registrierungsschlüssel `HeartbeatStartupDelayInMS` im Ursprungs-Workload konfiguriert werden. Dieser Registrierungsschlüssel ist standardmäßig nicht konfiguriert.

So aktivieren Sie eine kürzere oder längere Heartbeat-Verzögerung:

1. Öffnen Sie im Ursprungs-Workload den Windows-Registrierungs-Editor.
2. Wechseln Sie im Registrierungs-Editor zum folgenden Speicherort, je nach der Betriebssystemarchitektur auf dem Ursprungs-Workload:

   Pfad für einen 64-Bit-Ursprungs-Workload:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PlateSpin\OperationsFramework\Controller
   ```

   Pfad für einen 32-Bit-Ursprungs-Workload:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\PlateSpin\OperationsFramework\Controller
   ```

3. Fügen Sie einen Schlüssel mit dem Namen `HeartbeatStartupDelayInMS` und dem Typ `REG_SZ` ein und legen Sie den gewünschten Wert in Millisekunden fest. Die Standardeinstellung sollte bei 15.000 liegen.

   ```
   REG_SZ: HeartbeatStartupDelayInMS Value: "15000"
   ```

4. Starten Sie den Ursprungs-Workload neu.

14.1.3 Durchführen von Verbindungstests

- „Netzwerk-Verbindungstest“, auf Seite 131
- „WMI-Verbindungstest“, auf Seite 131
- „Fehlerbehebung bei DCOM-Verbindungen“, auf Seite 132
- „Fehlerbehebung bei der RPC-Dienst-Verbindung“, auf Seite 132

Netzwerk-Verbindungstest

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

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

   `ping` *Workload-IP-Adresse*

WMI-Verbindungstest

1. Wechseln Sie zu Ihrem PlateSpin 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 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 mit 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:

- Protect und der Workload müssen sich auf derselben Seite der Firewall befinden
- Öffnen spezifischer Ports zwischen Protect und dem Workload (siehe „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“, auf Seite 31)

14.1.4 Deaktivieren der Virenschutz-Software

Virenschutz-Software kann gelegentlich einige der Protect-Funktionen blockieren, die sich auf WMI und die Remote-Registrierung beziehen. Um sicherzustellen, dass das Workload-Inventar erfolgreich ist, kann es nötig sein, den Virenschutz-Service an einem Workload zunächst zu deaktivieren.

Darüber hinaus kann Virenschutz-Software mitunter auch den Zugriff auf bestimmte Dateien sperren und nur den Zugriff auf bestimmte Prozesse oder Programmdateien zulassen. Diese Sperre 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 müssen die Dienste nicht deaktiviert werden.

14.1.5 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 Protect die administrativen Freigaben des Workloads. 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 Server-Host aus zugänglich sind:

1. Wechseln Sie zu Ihrem PlateSpin 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 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.

14.2 Fehlerbehebung bei der Ermittlung von Linux-Workloads

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 31.
`Zugriff verweigert.`	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 161.

14.3 Fehlerbehebung bei der Ermittlung von Ziel-Hosts

Probleme oder Meldungen	Lösungen
Bei ESXi 4-1 führt die direkte Host-Ermittlung zu fehlenden VM-Portgruppen, wenn dvSwitch-Portgruppen denselben Namen haben.	Die Portgruppennamen auf dem VMware-Ziel-Host müssen eindeutig sein.

B Von Protect unterstützte Linux-Distributionen

Die PlateSpin Protect-Software umfasst vorkompilierte Versionen des `blkwatch`-Treibers für viele fehlerfreie Linux-Verteilungen (32-Bit und 64-Bit).

B.1 Analysieren Ihres Linux-Workloads

Bevor Sie feststellen können, ob PlateSpin Protect einen `blkwatch`-Treiber für Ihre Linux-Distribution umfasst, benötigen Sie weitere Informationen über den Kernel Ihres Linux-Workloads, sodass Sie ihn in der Liste der unterstützten Verteilungen als Suchbegriff verwenden können.

B.1.1 Ermitteln der Versionszeichenkette

Sie können die Versionszeichenkette des Kernels Ihres Linux-Workloads ermitteln, indem Sie auf dem Linux-Terminal des Workloads den folgenden Befehl ausführen:

```
uname -r
```

Wenn Sie beispielsweise den Befehl `uname -r` ausführen, wird die folgende Zeichenkette ausgegeben:

```
3.0.76-0.11-default
```

Wenn Sie die Liste der Verteilungen durchsuchen, werden für diese Zeichenkette zwei Übereinstimmungen angezeigt:

- `SLES11SP3-GA-3.0.76-0.11-default-x86`
- `SLES11SP3-GA-3.0.76-0.11-default-x86_64`

Die Suchergebnisse geben an, dass für das Produkt Treiber sowohl für die 32-Bit-(x86)- als auch für die 64-Bit-(x86_64)-Architektur vorhanden sind.

B.1.2 Ermitteln der Architektur

Sie können die Architektur Ihrer Linux-Workloads ermitteln, indem Sie auf dem Linux-Terminal des Workloads den folgenden Befehl ausführen:

```
uname -m
```

Wenn Sie beispielsweise den Befehl `uname -m` ausführen, wird die folgende Zeichenkette ausgegeben:

`x86-64`

Mit dieser Information können Sie festlegen, dass der Workload über eine 64-Bit-Architektur verfügt.

B.2 Vorkompilierte blkwatch-Treiber für Linux-Distributionen

PlateSpin Protect stellt vorkompilierte blkwatch-Treiber für viele fehlerfreie Linux-Distributionen bereit. Sie können die Liste der Distributionen durchsuchen, um zu ermitteln, ob die Version und Architektur des Kernels Ihres Linux-Workloads mit einer unterstützten Distribution in der Liste übereinstimmt. Wird Ihre Version und Architektur gefunden, bietet PlateSpin Protect eine vorkonfigurierte Version des `blkwatch`-Treibers.

Ist die Suche erfolglos, können Sie einen benutzerdefinierten `blkwatch`-Treiber erstellen. Führen Sie dazu die im Knowledgebase-Artikel 7005873 (https://www.netiq.com/support/kb/doc.php?id=7005873) beschriebenen Schritte aus. Selbstkompilierte Treiber werden lediglich für die Haupt- und Nebenversionen des Linux-Kernels unterstützt, die in der Liste der Distributionen aufgeführt sind, sowie für gepatchte Versionen dieser Versionen. Wenn die Haupt- und Nebenversion des Kernels in der Versionszeichenkette Ihres Linux-Workloads mit einer Haupt- und Nebenversion in der Liste übereinstimmt, wird Ihr selbstkompilierter Treiber unterstützt.

- Abschnitt B.2.1, „Liste mit Elementsyntax“, auf Seite 136
- Abschnitt B.2.2, „Liste der Verteilungen“, auf Seite 136
- Abschnitt B.2.3, „Weitere Linux-Distributionen mit Unterstützung für „blkwatch“-Treiber“, auf Seite 136

B.2.1 Liste mit Elementsyntax

Jedes Element in der Liste wird mit der folgenden Syntax formatiert:

<Distro>-<Patch>-<Kernel_Versionszeichenkette>-<Kernel_Architektur>

Für eine SLES 9 SP1-Verteilung mit einer Kernelversionszeichenkette `2.6.5-7.139-bigsmp` für die 32-Bit-(x86)-Architektur wird das Element in folgendem Format aufgeführt:

`SLES9-SP1-2.6.5-7.139-bigsmp-x86`

B.2.2 Liste der Verteilungen

Eine Liste der unterstützten Kernel-Distributionen finden Sie unter „Liste der Verteilungen“ (https://www.netiq.com/documentation/platespin-protect-11-2-1/protect_user/data/blkwatch-drivers.html#blkwatch-dist-list) im *PlateSpin Protect-Benutzerhandbuch*.

B.2.3 Weitere Linux-Distributionen mit Unterstützung für „blkwatch“-Treiber

PlateSpin Protect unterstützt die in Tabelle B-1 aufgelisteten anderen Linux-Distributionen, wenn die Distribution auf einer unterstützten Freigabeversion von Red Hat Enterprise Linux oder SUSE Linux Enterprise Server basiert. Sie können den vorkompilierten blkwatch-Treiber für die unterstützte Linux-Distribution verwenden.

Tabelle B-1 *Blkwatch-Treiberunterstützung für andere Linux-Distributionen*

Andere Linux-Distribution	Basierend auf einer unterstützten Freigabeversion für RHEL oder SLES	Anmerkungen
CentOS	Red Hat Enterprise Linux	
Open Enterprise Server (OES)	SUSE Linux Enterprise Server 11 SP1 (oder höher)	Die Standard-Kernel-Version 3.0.13 von SLES 11 SP 2 wird nicht unterstützt. Rüsten Sie auf die Kernel-Version 3.0.27 oder höher auf, bevor Sie den Workload inventarisieren.
Oracle Linux (OL) (früher Oracle Enterprise Linux (OEL))	Red Hat Enterprise Linux	Blkwatch-Treiber sind für den Standardkernel und den Unbreakable Enterprise Kernel (UEK) verfügbar wie in Abschnitt B.2.2, „Liste der Verteilungen“, auf Seite 136 angegeben. Für andere Oracle Linux-Distributionen sind vorkompilierte Treiber nur für den entsprechenden Red Hat Compatible Kernel (RHCK) verfügbar. Workloads, die den Oracle Linux Unbreakable Enterprise Kernel verwenden, werden in PlateSpin Protect 11.2 und früheren Versionen nicht unterstützt.

Eine Liste der unterstützten Kernel-Distributionen finden Sie unter „Liste der Verteilungen“ (https://www.netiq.com/documentation/platespin-protect-11-2-1/protect_user/data/blkwatch-drivers.html#blkwatch-dist-list) im *PlateSpin Protect-Benutzerhandbuch*.

C Synchronisieren von Seriennummern im lokalen Clusterknoten-Speicher

In diesem Abschnitt finden Sie detaillierte Informationen zu dem Vorgang, mit dem Sie lokale Volume-Seriennummern ändern können, damit sie mit den einzelnen Knoten des zu schützenden Windows-Clusters übereinstimmen. Die Informationen umfassen die Verwendung des Volume Manager-Programms (`VolumeManager.exe`) für die Synchronisierung von Seriennummern im lokalen Clusterknoten-Speicher.

So laden Sie das Dienstprogramm herunter und führen es aus:

1. Laden Sie die Datei `VolumeManager.exe` von der PlateSpin Protect-Download-Seite herunter:
   - **1a** Öffnen Sie Micro Focus-Downloads (https://www.microfocus.com/support-and-services/download/).
   - **1b** Wählen Sie den Eintrag PlateSpin Protect in der Liste **Nach Produkt suchen** aus oder geben Sie den Produktnamen in das Feld **Nach Produkt suchen** ein und wählen Sie dann PlateSpin Protect aus.
   - **1c** Wenn eine Versionsliste verfügbar ist, wählen Sie PlateSpin Protect 11.2.1 aus.
   - **1d** Klicken Sie auf der Seite „Download-Übersicht“ auf **Weiter zum Download** und melden Sie sich mit dem Berechtigungsnachweis für Ihr Kundenkonto an.
   - **1e** Bestätigen Sie die US-amerikanischen Exportgesetze und -bestimmungen mit **Akzeptieren**.
   - **1f** Klicken Sie auf der Download-Seite auf **Herunterladen** neben der Datei `VolumeManager.exe` und speichern Sie die Datei.
2. Kopieren Sie die heruntergeladene Datei in einen verfügbaren Speicherort auf den einzelnen Clusterknoten.
3. Öffnen Sie im aktiven Knoten des Clusters eine administrative Eingabeaufforderung, navigieren Sie zu dem Speicherort des heruntergeladenen Dienstprogramms und führen Sie folgenden Befehl aus:

   ```
   VolumeManager.exe -l
   ```

   Eine Liste mit den lokalen Volumes und deren entsprechenden Seriennummern wird angezeigt. Beispiel:

   ```
   Volume Listing: -------------------- DriveLetter (*:) VolumeId="System
   Reserved" SerialNumber: AABB-CCDD DriveLetter (C:) VolumeId=C:\ SerialNumber:
   1122-3344
   ```

   Notieren Sie sich diese Seriennummern oder lassen Sie sie angezeigt, um sie später zu vergleichen.
4. Überprüfen Sie, ob alle Seriennummern im lokalen Speicher des aktiven Knotens mit den Seriennummern im lokalen Speicher der jeweils anderen Knoten im Cluster übereinstimmen.
   - **4a** Führen Sie in jedem Clusterknoten den Befehl `VolumeManager.exe -l` aus, um dessen Volume-Seriennummern abzurufen.
   - **4b** Vergleichen Sie die Seriennummern im lokalen Speicher des aktiven Knotens (Schritt 3) mit den Seriennummern im lokalen Speicher des Knotens (Schritt 4a).

4c (Bedingt) Wenn sich die Seriennummern des aktiven Knotens von denen dieses Knotens unterscheiden, notieren Sie sich die Seriennummer, die Sie in diesem Knoten eintragen möchten und führen Sie den folgenden Befehl aus, um die Seriennummer festzulegen und anschließend zu überprüfen:

```
VolumeManager -s <VolumeId> <Seriennummer>
```

Nachfolgend sehen Sie zwei Beispiele, wie dieser Befehl verwendet werden könnte:

- `VolumeManager -s "Reserviertes System" AAAA-AAAA`
- `VolumeManager -s C:\ 1111-1111`

4d Wenn Sie alle Volume-Seriennummern im Knoten eines Clusters geändert haben, müssen Sie diesen Knoten neu starten.

4e Wiederholen Sie Schritt 4a bis Schritt 4d für jeden Knoten im Cluster.

5 (Bedingt) Wenn der Cluster bereits in einer PlateSpin-Umgebung geschützt wurde, empfehlen wir Ihnen, eine vollständige Reproduktion im aktiven Knoten durchzuführen, um sicherzustellen, dass alle Änderungen in der Datenbank eingetragen werden.

D Protect Agent-Dienstprogramm

Mit dem Protect Agent-Befehlszeilenprogramm können Sie die Treiber für die blockbasierte Übertragung installieren, aufrüsten, abfragen und deinstallieren.

Beim Installieren, Deinstallieren und Aufrüsten von Treibern muss in jedem Fall neu gebootet werden; mit Protect Agent können Sie jedoch präzise steuern, wann diese Aktionen ausgeführt werden, und somit, wann der Server neu gebootet wird. Mit Protect Agent ist es beispielsweise möglich, die Treiber während einer geplanten Ausfallzeit statt während der ersten Reproduktion zu installieren.

D.1 Verwenden des Protect Agent-Dienstprogramms für Windows

So laden Sie das Protect Agent-Dienstprogramm für Windows auf den Ursprungs-Workload herunter:

1. Melden Sie sich beim Windows-Ursprungscomputer als Administratorbenutzer an.
2. Starten Sie die Weboberfläche in einem Webbrowser und melden Sie sich an.
3. Klicken Sie auf die Registerkarte **Downloads**.
4. Klicken Sie auf den Protect Agent-Anwendungslink für die Windows-Zielplattform und speichern Sie die komprimierte Datei `ProtectAgent.cli.exe`.
5. Extrahieren Sie den Inhalt der Datei, sodass die ausführbare Datei verfügbar wird.
6. (Optional) Rufen Sie die Protect Agent-Hilfe mit dem folgenden Befehl auf:

   ```
   Protect.Agent.cli.exe -h
   ```

Das Dienstprogramm befindet sich auf dem PlateSpin-Server-Host in einer komprimierten Datei. Extrahieren Sie den Inhalt der Datei, sodass die ausführbare Datei verfügbar wird.

```
C:\Programme\PlateSpin Protect Server\bin\ProtectAgent
```

Zum Ausführen des Protect Agent-Dienstprogramms für Windows gilt die folgende Syntax:

```
ProtectAgent.cli.exe {command} [command_option] [/psserver=%IP%]
```

Tabelle D-1 beschreibt die verfügbaren Befehle, die Befehlsoption und den Switch für den Befehl `ProtectAgent.cli.exe`.

Tabelle D-1 *Protect Agent-Dienstprogramm für Windows – Befehle, Befehlsoption und Switch*

Verwendung	Beschreibung
Befehle	

Verwendung	Beschreibung
`h |? | help`	Zeigt die Nutzung und die Optionen für den Befehl.
`logs|view-logs`	Öffnet das Anwendungsprotokollverzeichnis.
`status` `/status [/psserver=%IP%]`	Zeigt den Installationsstatus für den PlateSpin-Controller und die Treiber auf diesem Workload. Wenn Sie den PlateSpin-Server angeben, werden Treiberaufrüstungen auf dem Server gesucht.
`din|driver-install` `/din [/psserver=%IP%]`	Installiert die PlateSpin-Treiber. Wenn Sie den PlateSpin-Server angeben, werden Treiberaufrüstungen auf dem Server gesucht.
`dup|driver-upgrade` `/dup [/psserver=%IP%]`	Rüstet die PlateSpin-Treiber auf. Wenn Sie den PlateSpin-Server angeben, werden Treiberaufrüstungen auf dem Server gesucht.
`dun|driver-uninstall` `[/dun /psserver=%IP%]`	Deinstalliert die PlateSpin-Treiber.

`con | config`
`/con /setting=<`*`Name_der_Einstellung`*`>:<`*`Wert`*`>`
Beispiel:
`ProtectAgent.cli.exe /config /setting=psserver:10.10.10.202`
	Gibt den Namen der Einstellung mit dem zugehörigen Wert an, die in der Konfigurationsdatei auf diesem Workload geändert werden sollen.
	Die Option `psserver` hält den OFX-Controller-Dienst (`ofxcontroller`) an, aktualisiert die Datei `OfxController.exe.config` mit der neuen IP-Adresse und startet den Dienst neu. Wenn Sie die öffentliche IP-Adresse des PlateSpin-Servers ändern, müssen Sie diesen Befehl auf jedem Ursprungs-Workload ausführen, der für den Server konfiguriert ist.

Switch	
`/psserver=%IP%`	Lädt die Treiber für die blockbasierte Übertragung vom angegebenen Server herunter, sobald Sie die Option `status`, `driver-install` oder `driver-upgrade` aufrufen.
Befehlsoption	

`setting`
`/setting=<`*`Name_der_Einstellung`*`>:<`*`Wert`*`>`
	Gibt den Namen und den Wert der zu ändernden Konfigurationseinstellung an.
	Unterstützte Einstellungsnamen:
	`psserver`
	`altAddress`
	`heartbeat`

D.2 Verwenden von Protect Agent bei Treibern für die blockbasierte Übertragung

Eine Kopie der Treiber für die blockbasierte Übertragung ist im Bundle mit dem Protect Agent-Dienstprogramm enthalten. Alternativ können Sie die Treiber mit dem Befehlszeilenschalter `/psserver=` vom PlateSpin-Server herunterladen, sobald Sie die Option `status`, `driver-install` oder `driver-upgrade` aufrufen. Dies ist insbesondere dann von Nutzen, wenn der Server mit einem neuen Treiberpaket gepatcht wurde, das Protect Agent-Befehlszeilenprogramm jedoch nicht.

HINWEIS: Zur Verdeutlichung: Bei der Verwendung von Protect Agent wird empfohlen, zunächst die Treiber zu installieren, zu deinstallieren oder aufzurüsten und dann das System vor einer Reproduktion neu zu booten.

Sie sollten den Ursprungs-Workload bei jedem Installieren, Aufrüsten oder Deinstallieren der Treiber neu starten. Hierdurch wird der derzeit ausgeführte Treiber angehalten, und beim Neustart des Systems wird der neue Treiber angewendet. Wenn Sie das System vor der Reproduktion nicht neu starten, verhält sich der Ursprung weiterhin so, als wäre die Aktion nicht ausgeführt worden. Wenn Sie beispielsweise Treiber installieren und das System dann nicht neu starten, verhält sich der Ursprung so, als wären keine Treiber während der Reproduktion installiert worden. Wenn Sie die Treiber ohne Neustart aufrüsten, verwendet der Ursprung den derzeit ausgeführten Treiber entsprechend so lange weiter, bis Sie das System neu starten.

Mit der Option `Status` wird der Benutzer daran erinnert, einen Neustart vorzunehmen, falls die Version des installierten Treibers nicht mit der Version des ausgeführten Treibers identisch ist. Beispiel:

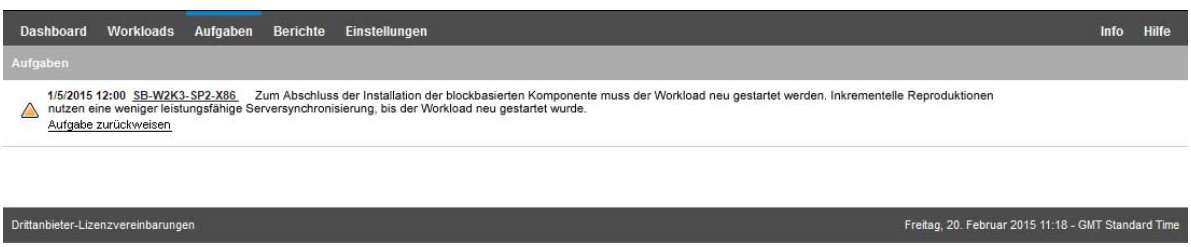
```
C:\ProtectAgent\ProtectAgent.cli.exe status
Step 1 of 2: Querying the PlateSpin controller service
   Done
Step 2 of 2: Querying the installed PlateSpin driver version
   Done

The task completed successfully
PlateSpin Controller Service Status
    Status: Running
    Version: 9.9.9.9
    Last Successful Contact: 1/5/2015 12:14:25 PM

PlateSpin Driver Status
    Installed Driver Version: 8.0.0.11
    Running Driver Version: Not running. Reboot to load the driver.
    Upgrade Available: No
```

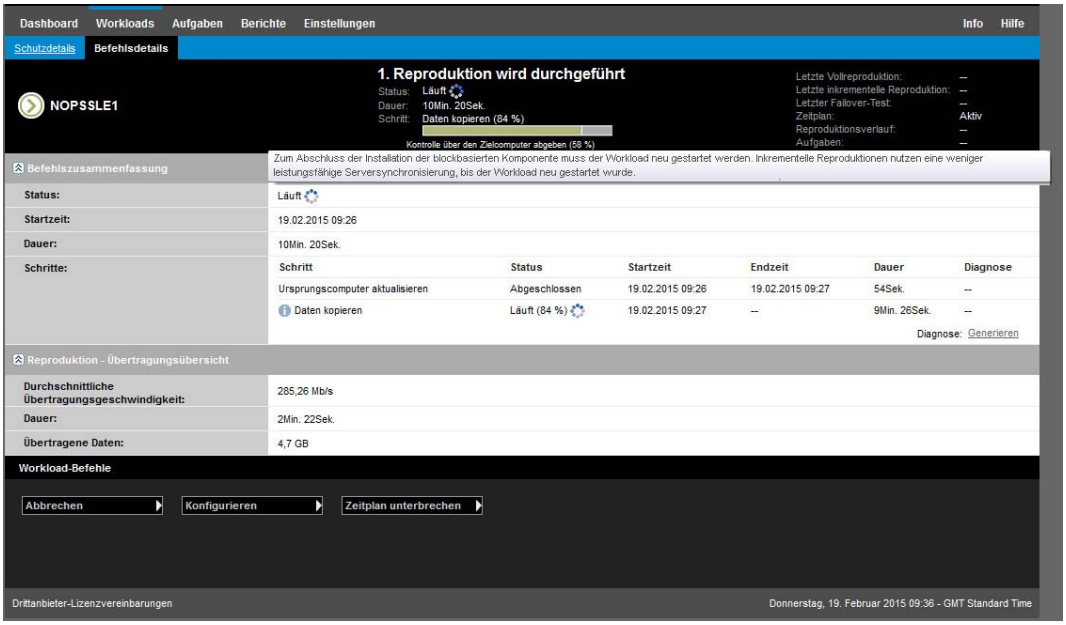
PlateSpin erstellt eine Aufgabe, mit der der Benutzer darauf hingewiesen wird, dass zum Abschluss der Treiberinstallation oder -aufrüstung ein Neustart erforderlich ist. Die Benachrichtigung wird in der Aufgabenliste angezeigt (Abbildung D-1).

Abbildung D-1 *Aufgabe für Neustart-Benachrichtigung*



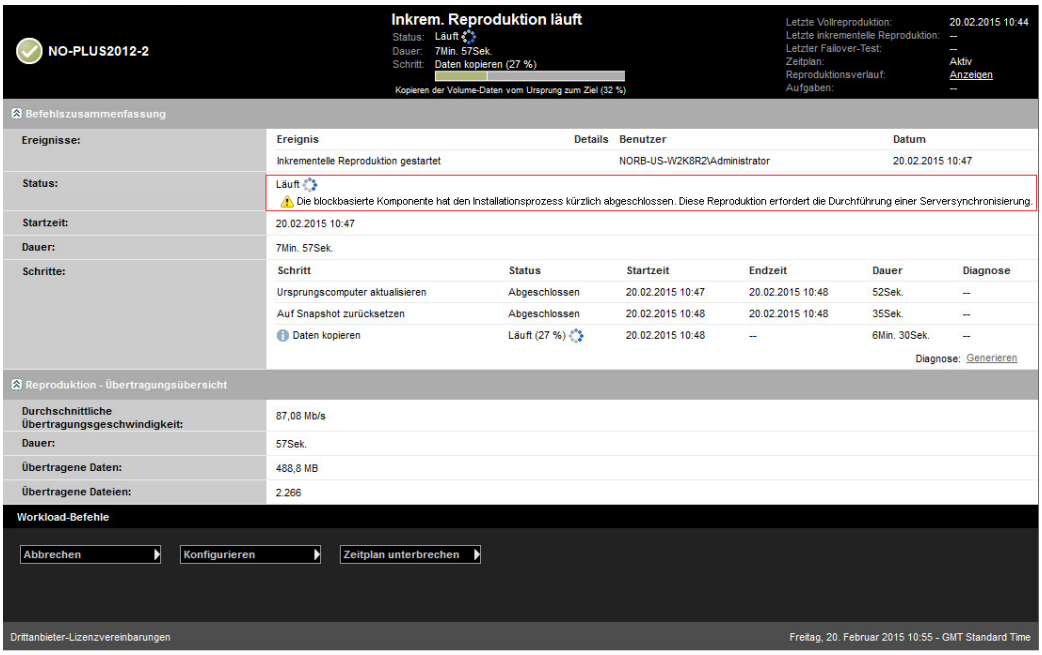
Während der Reproduktion wird die Benachrichtigung auf der Seite „Befehlsdetails“ angezeigt (Abbildung D-2).

Abbildung D-2 *Neustart-Benachrichtigung während der Reproduktion*



Beim Neustarten des Ursprungscomputers werden die installierten oder aufgerüsteten Treiber angewendet und gestartet. Wenn der Treiber erst kürzlich installiert wurde, ist nach dem Neustart eine vollständige Reproduktion bzw. eine Serversynchronisierungs-Reproduktion erforderlich, damit alle Änderungen am Ursprung erfasst werden. Diese Anforderung hinsichtlich der Serversynchronisierungs-Reproduktion wird dem Benutzer im Feld „Status“ als Warnmeldung angezeigt (siehe Abbildung D-3). Nachfolgende inkrementelle Reproduktionen werden wie geplant und ohne Warnung abgeschlossen.

Abbildung D-3 *Benachrichtigung über erforderliche Serversynchronisierung*



IV Schützen von Workloads

Sobald Sie die Ziele und Workloads ermittelt haben, können Sie die Schutzverträge für Ihre Workloads konfigurieren und so den Schutz vorbereiten.

15 Sicherung und Wiederherstellung von Workloads

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 von PlateSpin Protect verwaltete virtuelle Maschine, die die Geschäftsfunktion des Produktions-Workloads übernimmt, falls es zu einer Störung am Produktionsstandort kommt.

15.1 Voraussetzungen für den Workload-Schutz

Bereiten Sie Ihre Container und Workloads für den Schutz vor. Weitere Informationen hierzu finden Sie in Teil III, „Vorbereiten der Schutzziele und -ursprünge“, auf Seite 93.

In einer Active Directory-Domäne beachten Sie die folgenden bewährten Verfahren, bevor Sie die erste vollständige Reproduktion ausführen:

- Aktualisieren Sie in jedem Fall Windows (Windows-Update ausführen) auf dem Ursprungs-Workload, bevor Sie die erste vollständige Reproduktion ausführen.
- Richten Sie die Virenschutz-Software so ein, dass empfohlene Dateien und Ordner gemäß den Angaben in folgendem Dokument ausgeschlossen werden: *Microsoft KB-Artikel 822158: Empfehlungen zum Virenscan auf Unternehmenscomputern, auf denen unterstützte Windows-Versionen ausgeführt werden* (https://support.microsoft.com/en-us/kb/822158).
- Wenn es sich bei dem Windows-Computer um einen Domänencontroller handelt, stellen Sie sicher, dass die Virenschutz-Software des Systems während der Reproduktion deaktiviert ist.

15.2 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 (Hinzufügen/Inventarisieren, ursprüngliche und laufende Reproduktionen, Failover, Failback und erneutes Schützen) werden relevante Einstellungen aus den Schutzdetails ausgelesen. Weitere Informationen hierzu finden Sie unter „Grundlegender Workflow

für den Workload-Schutz und die Wiederherstellung“, auf Seite 37. Diese Sammlung der derzeit aktiven Einstellungen, die für den gesamten Lebenszyklus des Schutzes eines Workloads gilt, wird als *Schutzvertrag* bezeichnet.

So konfigurieren Sie die Schutzdetails Ihres Workloads:

1. Fügen Sie einen Container hinzu. Weitere Informationen hierzu finden Sie unter „Hinzufügen von Containern (Schutzziele)“, auf Seite 96.
2. Fügen Sie einen Workload hinzu. Weitere Informationen hierzu finden Sie unter „Hinzufügen von Workloads (Schutzursprünge)“, auf Seite 100.
3. Wählen Sie auf der Seite „Workloads“ den erforderlichen Workload aus und klicken Sie auf **Konfigurieren**.

   Alternativ klicken Sie auf den Namen des Workloads.

   HINWEIS: Wenn das PlateSpin Protect-Inventar noch keinen Container enthält, werden Sie vom System aufgefordert, einen Container hinzuzufügen. Klicken Sie dazu unten auf **Container hinzufügen**.

   ---
4. Wählen Sie eine **Anfängliche Reproduktionsmethode** aus. Damit geben Sie an, ob die Volume-Daten vollständig aus dem Workload auf die Failover-VM übertragen oder mit Volumes auf einer vorhandenen VM synchronisiert werden sollen. Weitere Informationen hierzu finden Sie unter „Anfängliche Reproduktionsmethode (vollständig und inkrementell)“, auf Seite 164.
5. Weisen Sie ein Schutzziel zu. Dies kann entweder ein Container oder ein **vorbereiteter** Workload sein, falls Sie *Inkrementelle Reproduktion* als anfängliche Reproduktionsmethode ausgewählt haben. Weitere Informationen hierzu finden Sie unter „Anfängliche Reproduktionsmethode (vollständig und inkrementell)“, auf Seite 164.

   HINWEIS: Wenn Ihr Inventar nur einen Container enthält, wird diesem Ihr Workload automatisch zugewiesen.

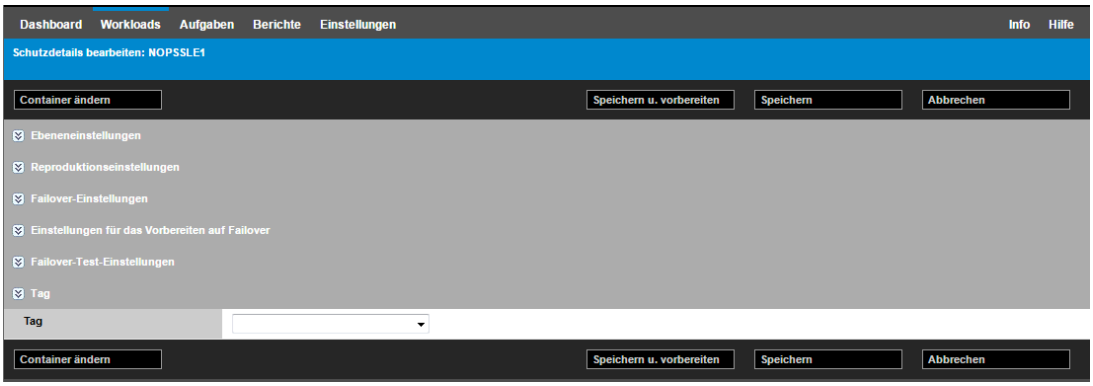
   ---
6. Konfigurieren Sie die Schutzdetails in jeder Einstellungsgruppe so, wie sie für die Aufrechterhaltung Ihres ununterbrochenen Geschäftsbetriebs erforderlich sind. Weitere Informationen hierzu finden Sie unter „Workload-Schutz-Details“, auf Seite 149.
7. Korrigieren Sie alle Validierungsfehler, die eventuell auf der PlateSpin Protect-Weboberfläche angezeigt werden.
8. 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.

15.2.1 Workload-Schutz-Details

Workload-Schutz-Details werden in fünf Parametergruppen angegeben (siehe Tabelle 15-1):



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

Tabelle 15-1 *Workload-Schutz-Details*

Parametereinstellungen	Details
Ebeneneinstellungen	
Schutzebene	Gibt die Schutzebene des aktuellen Schutzes an. Weitere Informationen hierzu finden Sie unter „Schutzebenen“, auf Seite 162.
Reproduktionseinstellungen	
Übertragungsmethode	(Windows) Wählen Sie einen dateibasierten oder einen blockbasierten Datenübertragungsmechanismus aus. Weitere Informationen zur Reproduktion auf Blockebene mit und ohne blockbasierte Komponenten finden Sie unter „Unterstützte Datenübertragungsmethoden“, auf Seite 23. Wählen Sie zum Aktivieren der Verschlüsselung die Option **Datenübertragung verschlüsseln**. Weitere Informationen hierzu finden Sie in „Verschlüsselung von Daten während der Übertragung“, auf Seite 24.
Übertragungsverschlüsselung	(Linux) Wählen Sie zum Aktivieren der Verschlüsselung die Option **Datenübertragung verschlüsseln**. Weitere Informationen hierzu finden Sie unter „Verschlüsselung von Daten während der Übertragung“, auf Seite 24.
Ursprungsberechtigungsnachweis	Geben Sie den erforderlichen Berechtigungsnachweis für den Zugriff auf den Workload an. Weitere Informationen hierzu finden Sie unter „Richtlinien für Workload- und Container-Berechtigungsnachweise“, auf Seite 161.

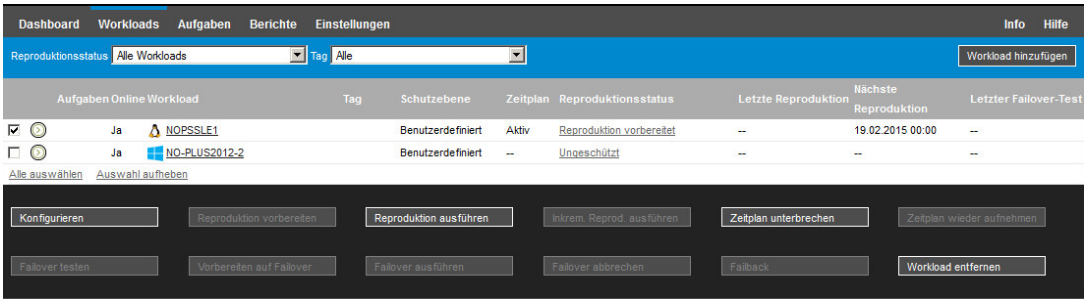
Parametereinstellungen	Details
Prozessor	(VM-Container mit VMware 5.1, 5.5 und 6.0 und mindestens VM-Hardware-Ebene 8) Geben Sie die Anzahl der Sockets sowie die Anzahl der Kerne pro Socket für den Failover-Workload an. Die Gesamtzahl der Kerne wird automatisch berechnet. Dieser Parameter gilt für die anfängliche Einrichtung eines Workloads mit der anfänglichen Reproduktionseinstellung **Vollständig**. **HINWEIS:** Die maximale Anzahl der Kerne, die ein Workload nutzen kann, ist abhängig von externen Faktoren, beispielsweise vom Gast-Betriebssystem, von der VM-Hardware-Version, der VMware-Lizenzierung für den ESXi-Host und den berechneten ESXi-Host-Höchstwerten für vSphere (siehe *vSphere 5.1-Konfigurationshöchstwerte* (http://www.vmware.com/pdf/vsphere5/r51/vsphere-51-configuration-maximums.pdf)). In bestimmten Distributionen von Gast-Betriebssystemen wird die Konfiguration der Kerne und der Kerne pro Socket unter Umständen nicht berücksichtigt. Gast-Betriebssysteme mit SLES 10 SP4 und OES 2 SP3 behalten beispielsweise die ursprünglich installierten Einstellungen für Kerne und Sockets bei, während andere SLES-, RHEL- und OES-Distributionen die Konfiguration beachten.
Anzahl der CPUs	(VM-Container mit VMware 4.1) Geben Sie die erforderliche Anzahl der vCPUs (virtuelle CPUs) an, die dem Failover-Workload zugewiesen werden sollen. Dieser Parameter gilt für die anfängliche Einrichtung eines Workloads mit der anfänglichen Reproduktionseinstellung **Vollständig**. Die vCPUs werden im Gast-Betriebssystem auf dem VM-Container jeweils als CPU mit einem einzelnen Kern und einem einzelnen Socket dargestellt.
Reproduktionsnetzwerk	Hiermit trennen Sie den Reproduktionsdatenverkehr auf der Basis virtueller Netzwerke, die in Ihrem VM-Container definiert sind. Weitere Informationen hierzu finden Sie unter „Netzwerke“, auf Seite 168. Für diese Einstellung können Sie außerdem einen MTU-Wert festlegen, der vom LRD-Reproduktionsnetzwerk (Linux-RAM-Datenträger) in PlateSpin Protect verwendet werden soll. Dieser Wert kann dazu beitragen, übermäßigen Datenverkehr über Netzwerke (z. B. VPNs) mit kleinerem MTU-Wert zu vermeiden. Der Standardwert ist eine leere Zeichenkette (kein Eintrag im Textfeld). Wenn Networking im LRD konfiguriert ist, kann das Netzwerkgerät einen eigenen Standardwert festlegen (in der Regel 1500). Wenn Sie einen Wert eingeben, passt PlateSpin Protect den MTU-Wert beim Konfigurieren der Netzwerkschnittstelle entsprechend an.
Zulässige Netzwerke	Geben Sie mindestens eine Netzwerkschnittstelle (NIC oder IP-Adresse) am Ursprung für den Reproduktionsdatenverkehr an.
Ressourcenpool für Ziel-VM	(VM-Container gehört zu einem DRS-Cluster) Geben Sie den Speicherort des Ressourcenpools an, in dem die Failover-VM erstellt werden soll.
VM-Ordner für Ziel-VM	(VM-Container gehört zu einem DRS-Cluster) Geben Sie den Speicherort des VM-Ordners an, in dem die Failover-VM erstellt werden soll.
Konfigurationsdatei-Datenablage	Wählen Sie eine mit dem VM-Container verbundene Datenablage zum Speichern von VM-Konfigurationsdateien aus. Weitere Informationen hierzu finden Sie unter „Wiederherstellungspunkte“, auf Seite 164.
Geschützte Volumes	Wählen Sie Volumes für den Schutz aus und weisen Sie deren Reproduktionen bestimmten Datenablagen auf dem VM-Container zu.

Parametereinstellungen	Details
Thin-Festplatte	Hiermit aktivieren Sie 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.
Geschützte logische Volumes	(Linux) Geben Sie mindestens ein logisches LVM-Volume an, das für einen Linux-Workload oder die NSS-Pools in einem Open Enterprise Server-Workload geschützt werden soll.
Speicher ohne Volumes	(Linux) Geben Sie einen Ablagebereich (z. B. eine Auslagerungspartition) an, der mit dem Ursprungs-Workload verbunden ist. Dieser Speicher wird im Failover-Workload erneut erstellt.
Volume-Gruppen	(Linux) Legen Sie die LVM-Volume-Gruppen fest, die mit den unter Geschützte logische Volumes in den Einstellungen angegebenen logischen LVM-Volumes geschützt werden sollen.
Dienste/Daemons, die während der Reproduktion angehalten werden sollen	Wählen Sie Windows-Dienste oder Linux-Daemons aus, die während der Reproduktion automatisch angehalten werden sollen. Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“, auf Seite 165.
Failover-Einstellungen	
VM-Arbeitsspeicher	Geben Sie die Menge an Arbeitsspeicher an, die dem Failover-Workload zugeteilt werden soll.
Hostname und Domänen-/Arbeitsgruppenzugehörigkeit	Geben Sie die Identität und die Domänen-/Arbeitsgruppenzugehörigkeit des Failover-Workloads an, wenn dieser „live“ ist. Für die Domänenzugehörigkeit ist der Berechtigungsnachweis eines Domänenadministrators erforderlich.
Netzwerkverbindungen	Legen Sie die LAN-Einstellungen für den Failover-Workload fest. Weitere Informationen hierzu finden Sie unter „Netzwerke“, auf Seite 168.
DNS-Server	Geben Sie die IP-Adresse des primären DNS-Servers und einen alternativen DNS an (optional).
Zu ändernde Dienst-/Daemon-Status	Legen Sie den Anfangsstatus für bestimmte Anwendungsdienste (Windows) oder Daemons (Linux) fest. „Steuerung von Diensten und Daemons“, auf Seite 165
Einstellungen für das Vorbereiten auf Failover	
Temporäres Failover-Netzwerk	Legen Sie die temporären LAN-Einstellungen für den Failover-Workload während der optionalen Vorbereitung auf den Failover fest. Weitere Informationen hierzu finden Sie unter „Netzwerke“, auf Seite 168.
Testen der Failover-Einstellungen	
VM-Arbeitsspeicher	Weisen Sie dem temporären Workload den erforderlichen RAM zu.
Hostname	Weisen Sie dem temporären Workload einen Hostnamen zu.
Domäne/Arbeitsgruppe	Ordnen Sie den temporären Workload einer Domäne oder Arbeitsgruppe zu. Für die Domänenzugehörigkeit ist der Berechtigungsnachweis eines Domänenadministrators erforderlich.
Netzwerkverbindungen	Legen Sie die LAN-Einstellungen für den temporären Workload fest. Weitere Informationen hierzu finden Sie unter „Netzwerke“, auf Seite 168.

Parametereinstellungen	Details
DNS-Server	Geben Sie die IP-Adresse des primären DNS-Servers und einen alternativen DNS an (optional).
Zu ändernde Dienst/Daemon-Status	Legen Sie den Anfangsstatus für bestimmte Anwendungsdienste (Windows) oder Daemons (Linux) fest. Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“, auf Seite 165.
Kennungen	
Tag	(Optional) Weisen Sie diesem Workload ein Tag zu. Weitere Informationen hierzu finden Sie unter „Tagging von Workloads“, auf Seite 101.

15.3 Starten des Workload-Schutzes

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



Sie können den Befehl „Reproduktion ausführen“ 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 ausführen**.
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.

2. Ändern Sie die Größe der Volumes nach Bedarf.
3. Bauen Sie den Schutz erneut auf. Fügen Sie hierzu den Workload erneut hinzu, konfigurieren Sie dessen Schutzdetails, und starten Sie die Reproduktionen.

- 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.

15.4 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 für den Befehl, der gerade auf diesem Workload ausgeführt wird, beispielsweise **Inkrementelle Reproduktion wird durchgeführt**.

In der Weboberfläche wird die entsprechende Seite „Befehlsdetails“ angezeigt:

3 Klicken Sie auf **Abbrechen**.

15.5 Failover

Bei einem *Failover*-Vorgang übernimmt der Failover-Workload in einem PlateSpin Protect-VM-Container die Betriebsfunktionen eines fehlgeschlagenen Produktions-Workloads.

- Abschnitt 15.5.1, „Erkennen von Offline-Workloads“, auf Seite 153
- Abschnitt 15.5.2, „Durchführen eines Failovers“, auf Seite 154
- Abschnitt 15.5.3, „Verwenden der Funktion „Failover testen““, auf Seite 155

15.5.1 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 deren ein Workload-Fehler definiert und protokolliert wird, sind Teil der Ebeneneinstellungen eines Workload-Schutzes. Weitere Informationen finden Sie in der Zeile „Ebeneneinstellungen“ unter „Workload-Schutz-Details“, auf Seite 149.

Wenn zusammen mit den SMTP-Einstellungen Benachrichtigungen konfiguriert wurden, sendet PlateSpin Protect gleichzeitig eine Benachrichtigungs-E-Mail an die angegebenen Empfänger. Weitere Informationen hierzu finden Sie unter „Konfigurieren der E-Mail-Benachrichtigungsdienste für Ereignisse und Reproduktionsberichte“, auf Seite 67.

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 153) und fahren Sie dann mit dem Befehl **Failover ausführen** fort. Weitere Informationen hierzu finden Sie unter „Durchführen eines Failovers“, auf Seite 154.

Abbildung 15-1 zeigt die Dashboard-Seite der Weboberfläche beim Erkennen eines Workload-Fehlers. Beachten Sie die anwendbaren Aufgaben im Teilfenster mit den Aufgaben und Ereignissen:

Abbildung 15-1 *Die Dashboard-Seite bei Erkennen eines Workload-Fehlers („Workload offline“)*

15.5.2 Durchführen eines Failovers

Failover-Einstellungen, einschließlich der Netzwerkidentitäts- und LAN-Einstellungen des Failover-Workloads, werden zum Zeitpunkt der Konfiguration zusammen mit den Schutzdetails gespeichert. Siehe „Failover-Einstellungen“ unter „Workload-Schutz-Details“, auf Seite 149.

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 15-1.
- 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 164). 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 155.

15.5.3 Verwenden der Funktion „Failover testen“

PlateSpin Protect ermöglicht es Ihnen, die Failover-Funktionalität und die Integrität des Failover-Workloads zu testen. Hierzu führen Sie den Befehl **Failover testen** aus. Dieser Befehl bootet den Failover-Workload in einer isolierten Netzwerkumgebung, sodass die Funktionsfähigkeit des Failovers getestet und die Integrität des Failover-Workloads überprüft werden kann.

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 „Testen der Failover-Einstellungen“ unter „Workload-Schutz-Details“, auf Seite 149.

So verwenden Sie die Funktion „Failover testen“:

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 164) 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 (**Mark. 'Test n. best.'**, **Mark. 'Test erfolgr.'**). 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 **Mark. 'Test n. best.'** oder **Mark. 'Test erfolgr.'** 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.

15.6 Failback

Bei einem *Failback*-Vorgang wird die Betriebsfunktion eines fehlgeschlagenen Produktions-Workloads in seiner ursprünglichen Umgebung wiederhergestellt, wenn die Betriebsfunktion eines temporären Failover-Workloads nicht mehr benötigt wird. Der Failback-Vorgang ist der nächste logische Schritt, der einem Failover folgt. Er überträgt den Failover-Workload an seine ursprüngliche oder, falls erforderlich, auf eine neue Infrastruktur.

Die unterstützten Failback-Methoden sind abhängig vom Typ der Zielinfrastruktur 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 Microsoft Hyper-V-Plattformen unterstützt.

Die folgenden Abschnitte enthalten weitere Informationen:

- Abschnitt 15.6.1, „Automatischer Failback auf eine VM-Plattform“, auf Seite 156
- Abschnitt 15.6.2, „Halbautomatischer Failback auf einen physischen Computer“, auf Seite 159
- Abschnitt 15.6.3, „Halbautomatischer Failback auf eine virtuelle Maschine“, auf Seite 159

15.6.1 Automatischer Failback auf eine VM-Plattform

PlateSpin Protect unterstützt das automatische Failback für Failback-Container auf einem unterstützten VMware-ESXi-Server oder einem VMware-DRS-Cluster. Weitere Informationen hierzu finden Sie unter „Unterstützte VM-Container“, auf Seite 17.

So führen Sie einen automatischen Failback eines Failover-Workloads auf einen Ziel-VMware-Container aus:

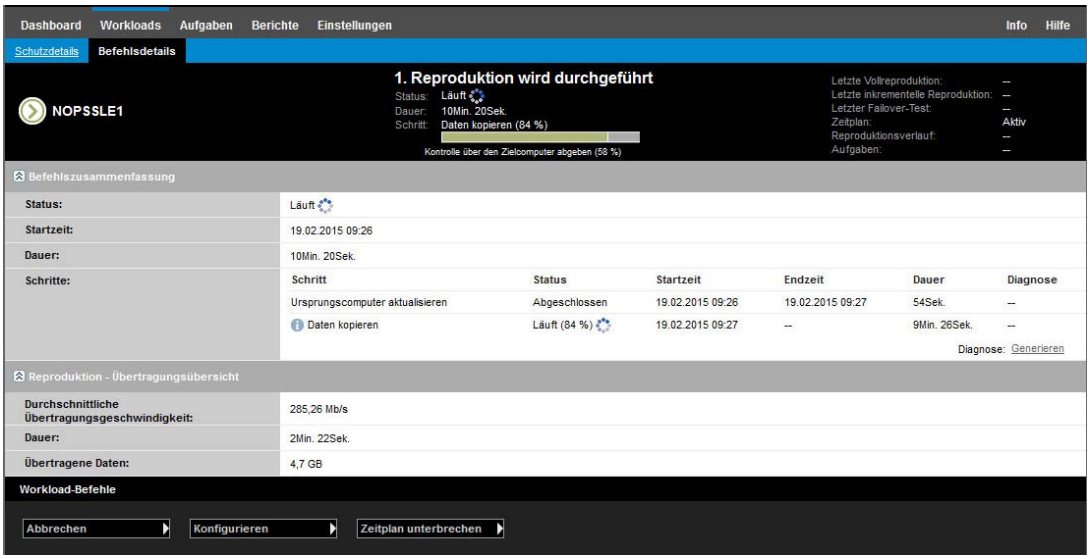
1. Wählen Sie im Anschluss an einen Failover den Workload auf der Seite „Workloads“ aus und klicken Sie auf **Failback durchführen**.

   Sie werden aufgefordert, die nachfolgenden Auswahlen zu treffen.
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 161).
   - **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 164.
     - **Zieltyp:** Wählen Sie **Virtuelles Ziel** aus. Falls Sie nicht über einen Failback-Container verfügen, klicken Sie auf **Container hinzufügen** und inventarisieren Sie einen unterstützten Container.
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 157.
5. Klicken Sie auf **Speichern und Failback durchführen** und überwachen Sie den Fortschritt auf der Seite „Befehlsdetails“. Weitere Informationen hierzu finden Sie unter Abbildung 15-2.

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

Abbildung 15-2 *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. Weitere Informationen zu den Parametereinstellungen finden Sie in Tabelle 15-2.

Tabelle 15-2 *Failback-Details (Workload an VM)*

Parametereinstellungen	Details
Failback-Einstellungen	
Übertragungsmethode	Wählen Sie eine Datenübertragungsmethode und Sicherheit durch Verschlüsselung aus. Weitere Informationen hierzu finden Sie unter „Verschlüsselung von Daten während der Übertragung“, auf Seite 24.
Failback-Netzwerk	Geben Sie das Netzwerk für den Failback-Datenverkehr an. Dies ist ein dediziertes Netzwerk, das auf den im VM-Container definierten virtuellen Netzwerken beruht. Weitere Informationen hierzu finden Sie unter „Netzwerke“, auf Seite 168.
VM-Datenablage	Wählen Sie eine Datenablage aus, die dem Failback-Container für den Ziel-Workload zugeordnet ist.
Volume-Zuordnung	Wenn Sie als anfängliche Reproduktionsmethode die Option „Inkrementell“ ausgewählt haben, wählen Sie hier die Ursprungs-Volumes aus, und ordnen Sie sie dem Failback-Ziel zur Synchronisierung zu.
Anzuhaltende Dienste/Daemons	Geben Sie die Anwendungsdienste (Windows) oder Daemons (Linux) an, die beim Failback automatisch angehalten werden sollen. Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“, auf Seite 165.
Alternative Adresse für Ursprung	Geben Sie ggf. eine zusätzliche IP-Adresse für den virtuellen Failover-Computer ein. Weitere Informationen hierzu finden Sie unter „Anforderungen zum Schutz über öffentliche und private Netzwerke durch NAT“, auf Seite 35.

Parametereinstellungen	Details
Workload-Einstellungen	
Prozessor	(VM-Container mit VMware 5.1, 5.5 und 6.0 und mindestens VM-Hardware-Ebene 8) Geben Sie die Anzahl der Sockets sowie die Anzahl der Kerne pro Socket für das Failback zum virtuellen Workload an. Die Gesamtzahl der Kerne wird automatisch berechnet. Dieser Parameter gilt für die anfängliche Einrichtung eines Workloads mit der anfänglichen Reproduktionseinstellung **Vollständig**. **HINWEIS:** Die maximale Anzahl der Kerne, die ein Workload nutzen kann, ist abhängig von externen Faktoren, beispielsweise vom Gast-Betriebssystem, von der VM-Hardware-Version, der VMware-Lizenzierung für den ESXi-Host und den berechneten ESXi-Host-Höchstwerten für vSphere (siehe *vSphere 5.1-Konfigurationshöchstwerte* (http://www.vmware.com/pdf/vsphere5/r51/vsphere-51-configuration-maximums.pdf)). In bestimmten Distributionen von Gast-Betriebssystemen wird die Konfiguration der Kerne und der Kerne pro Socket unter Umständen nicht berücksichtigt. Gast-Betriebssysteme mit SLES 10 SP4 und OES 2 SP3 behalten beispielsweise die ursprünglich installierten Einstellungen für Kerne und Sockets bei, während andere SLES-, RHEL- und OES-Distributionen die Konfiguration beachten.
Anzahl der CPUs	(VM-Container mit VMware 4.1) Geben Sie die erforderliche Anzahl der vCPUs (virtuelle CPUs) an, die dem Failback zum virtuellen Workload zugewiesen werden sollen. Dieser Parameter gilt für die anfängliche Einrichtung eines Workloads mit der anfänglichen Reproduktionseinstellung **Vollständig**. Die vCPUs werden im Gast-Betriebssystem auf dem VM-Container jeweils als CPU mit einem einzelnen Kern und einem einzelnen Socket dargestellt.
VM-Arbeitsspeicher	Weisen Sie dem Ziel-Workload den erforderlichen RAM zu.
Hostname, Domäne/Arbeitsgruppe	Geben Sie die Identität und die Domänen-/Arbeitsgruppenzugehörigkeit des Ziel-Workloads an. Für die Domänenzugehörigkeit ist der Berechtigungsnachweis eines Domänenadministrators erforderlich.
Netzwerkverbindungen	Geben Sie die Netzwerkzuordnung des Ziel-Workloads basierend auf den virtuellen Netzwerken des zugrunde liegenden VM-Containers an.
Zu ändernde Dienststatus	Legen Sie den Anfangsstatus für bestimmte Anwendungsdienste (Windows) oder Daemons (Linux) fest. Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“, auf Seite 165.
Post-Failback-Zieleinstellungen	
Workload erneut schützen	Wählen Sie diese Option, wenn Sie planen, den Schutzvertrag für den Ziel-Workload nach der Bereitstellung neu zu erstellen. Mit dieser Option 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** in der Weboberfläche zur Verfügung.

Parametereinstellungen	Details
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.

15.6.2 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-Server. Weitere Informationen hierzu finden Sie unter „Failback auf physische Computer“, auf Seite 168.
2. Falls Treiber fehlen oder nicht kompatibel sind, laden Sie die erforderlichen Treiber in die Gerätetreiberdatenbank von PlateSpin Protect hoch. Weitere Informationen hierzu finden Sie unter „Vorbereiten der Gerätetreiber für physische Failback-Ziele“, auf Seite 105.
3. Wählen Sie im Anschluss an einen Failover den Workload auf der Seite „Workloads“ aus und klicken Sie auf **Failback durchführen**.
4. 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 161).
   - **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 164.
     - **Zieltyp:** Wählen Sie die Option **Physische Ziele** und wählen Sie anschließend den physischen Computer aus, den Sie in Schritt 1 registriert haben.
5. 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.
6. Konfigurieren Sie die Failback-Details und klicken Sie anschließend auf **Speichern und Failback durchführen**.

   Überwachen Sie den Fortschritt auf dem Bildschirm „Befehlsdetails“.

15.6.3 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.

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

Sie können auch einen halbautomatischen Failback an Ziel-VM-Plattformen auf Microsoft Hyper-V-Server-Hosts vornehmen.

So starten Sie die Hyper-V-VMs bei einem Failover:

1. Fügen Sie in einem Texteditor jeweils die folgende Zeile in die Datei `/etc/vmware/config` der einzelnen Hyper-V-Hosts ein:

   ```
   vhv.allow = "TRUE"
   ```

2. Bearbeiten Sie im vSphere-Web-Client die Failover-VM-Einstellungen für die CPU:
   - **2a** Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **CPU**.
   - **2b** Wählen Sie unter **Hardware-Virtualisierung** die Option **Hardwaregestützte Virtualisierung für Gast-Betriebssystem offenlegen**.
3. Bearbeiten Sie im vSphere-Web-Client die Failover-VM-Einstellungen für die CPU-ID:
   - **3a** Erweitern Sie auf der Registerkarte **VM-Optionen** den Eintrag **Erweitert**, und wählen Sie die Option **Konfigurationsparameter bearbeiten**.
   - **3b** Überprüfen Sie die folgende Einstellung:

     ```
     hypervisor.cpuid.v0 = FALSE
     ```

15.7 Erneutes Schützen eines Workloads

Durch den Vorgang **Erneut schützen**, den 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** in der 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 155.

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.

16 Grundlagen des Workload-Schutzes

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

16.1 Richtlinien für Workload- und Container-Berechtigungsnachweise

PlateSpin Protect muss über Zugriff auf Workloads auf Administratorebene sowie eine entsprechende Rollenkonfiguration für Container verfügen. Während des gesamten Workload-Schutz- und -Wiederherstellungs-Workflows werden Sie von PlateSpin Protect aufgefordert, Berechtigungsnachweise in einem bestimmten Format einzugeben.

Tabelle 16-1 *Workload- und Container-Berechtigungsnachweise*

Ermitteln	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.	Bei Domänenmitgliedscomputern: *Autorität\Prinzipal*

Ermitteln	Berechtigungsnachweis	Anmerkungen
Alle Linux-Workloads	Benutzername und Passwort auf Root-Ebene	Andere Konten als das Root-Konto müssen für die Verwendung von sudo konfiguriert werden. Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7920711 (https://www.netiq.com/support/kb/doc.php?id=7920711).
VMware ESX- oder ESXi-Host	VMware-Konto mit einer entsprechenden Rollenkonfiguration. Weitere Informationen zum Einrichten der Mandantenfähigkeit finden Sie unter „Definieren von VMware-Rollen für Mehrfachmandantenfähigkeit“, auf Seite 57.	Wenn ESX für die Windows-Domänenauthentifizierung konfiguriert ist, können Sie auch Ihren Berechtigungsnachweis für die Windows-Domäne verwenden.
VMware vCenter Server	VMware-Konto mit einer entsprechenden Rollenkonfiguration. Weitere Informationen zum Einrichten der Mandantenfähigkeit finden Sie unter „Definieren von VMware-Rollen für Mehrfachmandantenfähigkeit“, auf Seite 57.	

16.2 Schutzebenen

Eine Schutzebene ist eine benutzerdefinierte 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.

So erstellen Sie im Vorfeld angepasste Schutzebenen:

1 Klicken Sie in der Weboberfläche auf **Einstellungen > Schutzebenen > Schutzebene erstellen**.

2 Geben Sie die Parameter für die neue Schutzebene ein:

Parameter	Aktion
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 ausgeführt 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 hängen von der Systemuhr an Ihrem PlateSpin-Server ab.
Komprimierungsgrad	Diese Einstellungen legen fest, ob und wie Workload-Daten vor der Übertragung komprimiert werden. Weitere Informationen hierzu finden Sie unter „Datenkomprimierung“, auf Seite 29. 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 unter „Bandbreitendrosselung“, auf Seite 29. 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 164.
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.

16.3 Wiederherstellungspunkte

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

Jeder geschützte Workload verfügt über mindestens einen und höchstens 32 Wiederherstellungspunkte.

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

16.4 Anfängliche Reproduktionsmethode (vollständig und inkrementell)

Die *ursprüngliche Reproduktion* ist die Erstellung einer ursprünglichen Basiskopie eines Produktions-Workloads in den Failover-Workload (virtuelle Reproduktion) in einem Schutzvorgang bzw. aus einem Failover-Workload in die ursprüngliche virtuelle oder physische Infrastruktur als Vorbereitung eines Failback-Vorgangs für den Produktions-Workload.

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

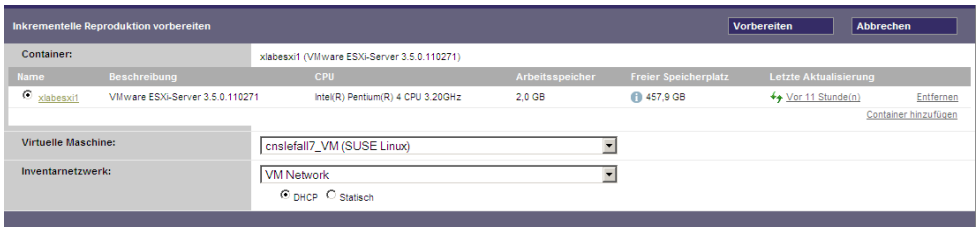
- **Vollständig:** Der Workload wird mit allen Daten vollständig übertragen.
- **Inkrementell:** Es werden nur Unterschiede vom Ursprung auf dessen Ziel übertragen, vorausgesetzt, sie verfügen über ähnliche Betriebssysteme und Volume-Profile.
  - **Beim Schutz:** Der Produktions-Workload wird mit einer 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, z. B. ein Workload-VM, der auf einem Wechseldatenträger physisch vom Produktionsstandort auf einen Remote-Wiederherstellungsstandort verschoben wird.
  - **Während des Failbacks auf eine virtuelle Maschine:** Der Failover-Workload wird mit einer vorhandenen VM in einem Failback-Container verglichen.
  - **Während des Failbacks auf einen physischen Computer:** Der Failover-Workload wird mit einem Workload auf einer physischen Zielmaschine verglichen, wenn der physische Computer in PlateSpin Protect registriert ist (siehe „Halbautomatischer Failback auf einen physischen Computer“, auf Seite 159).

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.

So richten Sie eine anfängliche Reproduktionsmethode ein:

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

In der Weboberfläche wird die Seite „Inkrementelle Reproduktion vorbereiten“ angezeigt.



4 Wählen Sie den erforderlichen Container, die virtuelle Maschine und das Netzwerk aus, das für die Kommunikation mit der VM verwendet werden soll. Wenn der angegebene Zielcontainer ein VMware DRS-Cluster ist, können Sie außerdem einen Ziel-Ressourcenpool für den Workload angeben.

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.

16.5 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 117.

- **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.

16.6 Volume-Speicher

Beim Hinzufügen eines Workloads für den Schutz inventarisiert 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. Weitere Informationen finden Sie unter Abschnitt 1.1.5, „Unterstützter Speicher“, auf Seite 21.

Abbildung 16-1 zeigt die unter „Reproduktionseinstellungen“ festgelegten Parameter für einen Linux-Workload mit mehreren Volumes und zwei logischen Volumes in einer Volume-Gruppe.

Abbildung 16-1 *Volumes, logische Volumes und Volume-Gruppen eines geschützten Linux-Workloads*

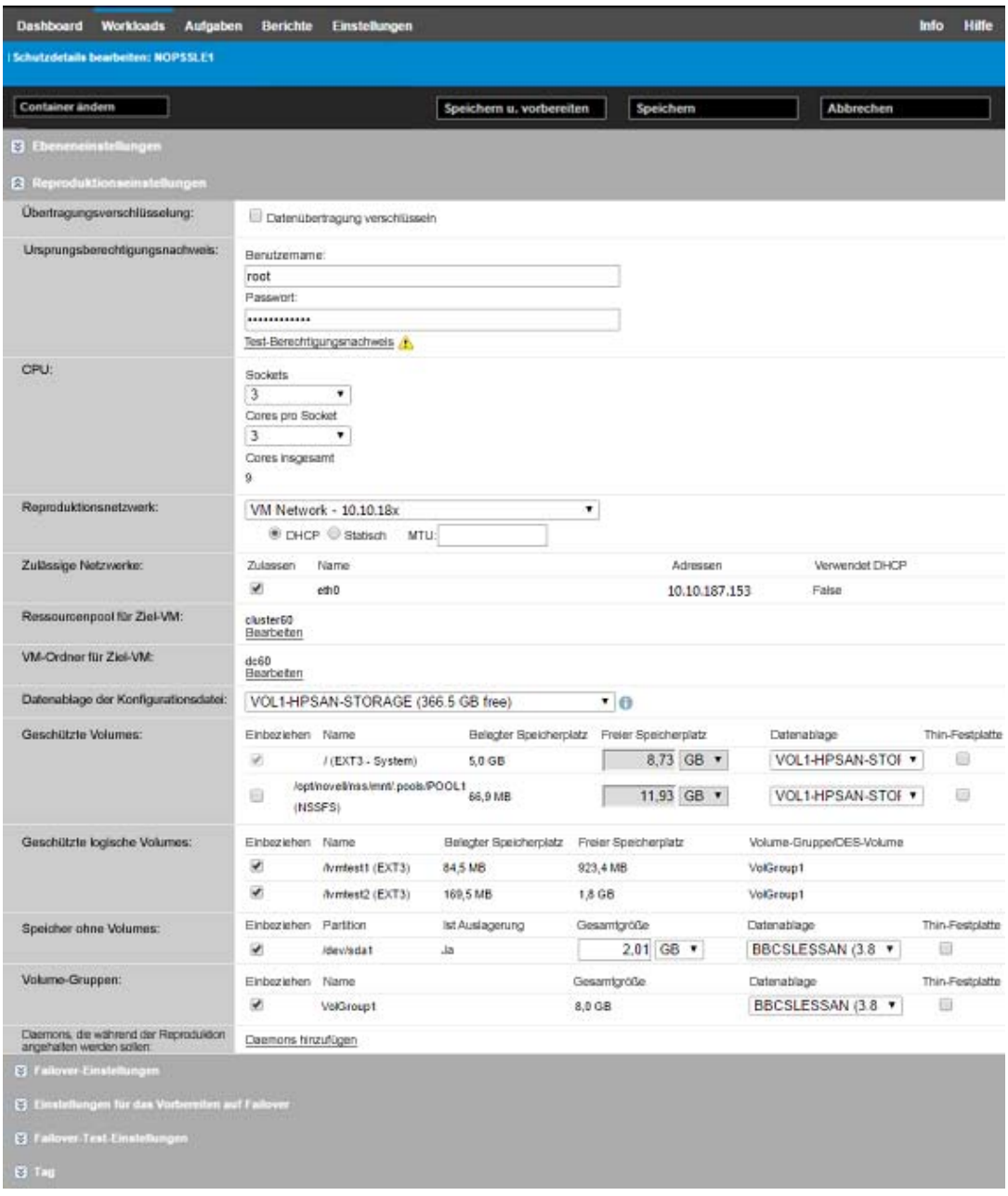
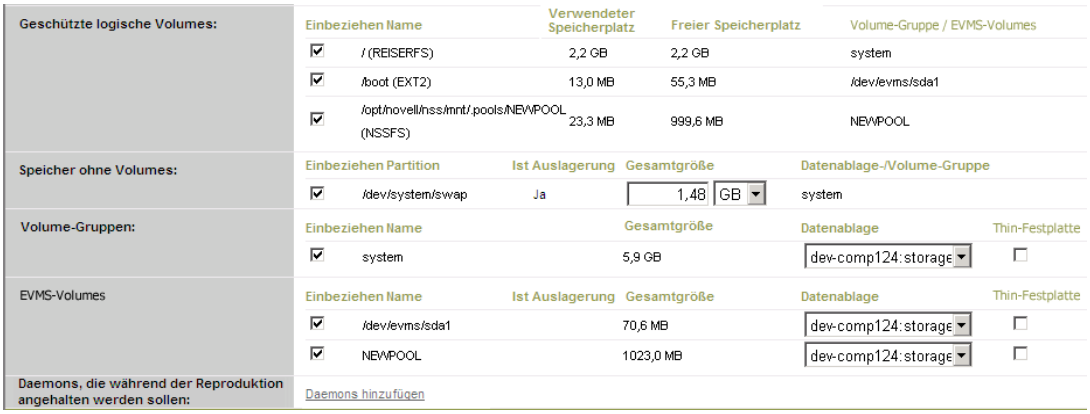


Abbildung 16-2 zeigt die Volume-Schutz-Optionen eines OES-11-Workloads, mit denen angegeben wird, dass das LVM2- und das NSS-Pool-Layout beibehalten und für den Failover-Workload neu erstellt werden soll:

Abbildung 16-2 *Reproduktionseinstellungen, Volume-bezogene Optionen (OES 11-Workload)*

Abbildung 16-3 zeigt die Volume-Schutz-Optionen eines OES-2-Workloads, mit denen angegeben wird, dass das EVMS- und das NSS-Pool-Layout beibehalten und für den Failover-Workload neu erstellt werden soll:

Abbildung 16-3 *Reproduktionseinstellungen, Volume-bezogene Optionen (OES 2-Workload)*



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

16.8 Failback auf physische Computer

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 PlateSpin-Boot-Image (OFX-ISO-Image).

- Abschnitt 16.8.1, „Herunterladen des PlateSpin-Boot-OFX-ISO-Images“, auf Seite 168
- Abschnitt 16.8.2, „Einfügen weiterer Gerätetreiber in das Boot-ISO-Image“, auf Seite 169
- Abschnitt 16.8.3, „Registrieren von physischen Computern als Failback-Ziel mit PlateSpin Protect“, auf Seite 170

16.8.1 Herunterladen des PlateSpin-Boot-OFX-ISO-Images

Die PlateSpin-Boot-OFX-ISO-Images (`bootofx.x2p.iso` für Ziele mit BIOS-Firmware und für Ziele mit UEFI-Firmware) stehen auf der PlateSpin Protect-Software-Download-Seite zum Herunterladen bereit.

1. Öffnen Sie Micro Focus-Downloads (https://www.microfocus.com/support-and-services/download/).
2. Wählen Sie den Eintrag PlateSpin Protect in der Liste **Nach Produkt suchen** aus oder geben Sie den Produktnamen in das Feld **Nach Produkt suchen** ein und wählen Sie dann PlateSpin Protect aus.
3. Klicken Sie auf der Seite „Download-Übersicht“ auf **Weiter zum Download** und melden Sie sich mit dem Berechtigungsnachweis für Ihr Kundenkonto an.
4. Bestätigen Sie die US-amerikanischen Exportgesetze und -bestimmungen mit **Akzeptieren**.
5. Klicken Sie auf der Download-Seite auf **Herunterladen** neben der Datei `bootofx.x2p.iso` und speichern Sie die Datei.

16.8.2 Einfügen weiterer Gerätetreiber in das Boot-ISO-Image

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.

So verwenden Sie das Dienstprogramm:

1 Beschaffen oder kompilieren Sie geeignete `*.ko`-Treiberdateien für den Zielhardware-Hersteller.

WICHTIG: Stellen Sie sicher, dass die Treiber mit dem in der ISO-Datei enthaltenen Kernel kompatibel sind (für x86-Systeme: `3.0.93-0.8-pae`, für x64-Systeme: `3.0.93-0.8-default`) und zur Architektur des Zielcomputers passen. Weitere Informationen finden Sie im Knowledgebase-Artikel 7005990 (https://www.netiq.com/support/kb/doc.php?id=7005990).

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 im Verzeichnis, in dem Sie das Skript `rebuildiso.sh` gespeichert haben, das Skript `rebuildiso.sh` als `Stamm` aus und verwenden Sie dazu die folgende Syntax:

```
./rebuildiso.sh <ARGS> [-v] -m32|-m64 -i <ISO-Datei>
```

In der folgenden Tabelle sind die möglichen Befehlszeilenoptionen für diesen Befehl aufgeführt:

Option	Beschreibung
`-i <ISO-Datei>`	*<ISO-Datei>* ist die ISO zum Bearbeiten, Auflisten etc.
`-v`	Falls dieser Befehl zusammen mit dem Argument `-l` verwendet wird, wird mit dieser Option der Befehl „modinfo“ zum Abrufen umfassender Treiberinformationen ausgelöst.
`-o`	Falls dieser Befehl zusammen mit dem Argument `-c` oder dem Argument `-d` verwendet wird, dann wird die alte Kopie der ISO-Datei nicht überschrieben.
`-m32`	Gibt an, dass die 32-Bit-initrd einbezogen wird.
`-m64`	Gibt an, dass die 64-Bit-initrd einbezogen wird.

In der nächsten Tabelle sind die möglichen Argumente für die Verwendung mit diesem Befehl aufgeführt. Mindestens eines dieser Argumente muss im Befehl verwendet werden:

Argument	Beschreibung
`-d <Pfad>`	*<Pfad>* gibt das Verzeichnis mit den Treibern an (d. h. `*.ko`-Dateien), die Sie einbeziehen möchten. Bei Anwendung dieses Befehls wird die ISO-Datei mit den hinzugefügten Treibern aktualisiert.
`-c <Pfad>`	*<Pfad>* gibt an, wo sich eine `ConfigureTakeControl.xml`-Datei befindet.

Argument	Beschreibung

`-l [<Typ>]`	<*Typ*> gibt eine Teilmenge von Treibern an, die Sie auflisten möchten. Standardmäßig ist „alle“ Typen festgelegt.
	
	Aufgeführte Treibertypen, die mit einem Schrägstrich (/) beginnen, befinden sich vermutlich unter <*Kernel-Modul-Verzeichnis*>/Kernel/
	
	Aufgeführte Treibertypen, die nicht mit einem Schrägstrich (/) beginnen, befinden sich vermutlich unter <*Kernel-Modul-Verzeichnis*/Kernel/Treiber/
	
	Beispiele für Treiber-Teilmengen:
	
	`-l scsi`
	`-l 'net|video'`
	`-l '/net|net'`
	
	Besondere Verwendung dieses Arguments:
	
	Wenn Sie die verfügbaren Unterverzeichnisse der einzelnen Teilmengen aufführen möchten, verwenden Sie das Argument wie folgt: `-l INDEX`

Syntax-Beispiele

- So listen Sie einen Index von 32-Bit-Treibern auf:

  ```
  # ./rebuildiso.sh -i bootofx.x2p.iso -m32 -l INDEX
  ```

- So listen Sie Treiber auf, die im Ordner „/Verschiedene“ gefunden werden:

  ```
  # ./rebuildiso.sh -i bootofx.x2p.iso -m32 -l misc
  ```

- So beziehen Sie 32-Bit-Treiber vom Ordner „/OEM-Treiber“ ein:

  ```
  # ./rebuildiso.sh -i bootofx.x2p.iso -m32 -d oem-drivers
  ```

- So beziehen Sie 64-Bit-Treiber vom Ordner „/OEM-Treiber“ sowie eine benutzerdefinierte Datei „ConfigureTakeControl.xml“ ein:

  ```
  # ./rebuildiso.sh -i bootofx.x2p.iso -m64 -c ConfigureTakeControl.xml -d
  oem-drivers
  ```

16.8.3 Registrieren von physischen Computern als Failback-Ziel mit PlateSpin Protect

1. Brennen Sie das PlateSpin-Boot-ISO-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.
3. Verwenden Sie die Boot-CD zum Booten des physischen Zielcomputers und warten Sie, bis das Befehlszeilenfenster geöffnet wird.
4. (Nur Linux) Geben Sie bei 64-Bit-Systemen im anfänglichen Bootprompt Folgendes ein:

   ```
   ps64
   ```

5. Drücken Sie die Eingabetaste.
6. Geben Sie nach der Eingabeaufforderung den Hostnamen oder die IP-Adresse Ihres PlateSpin-Server-Hosts ein.

7 Geben Sie den Administrator-Berechtigungsnachweis für den PlateSpin 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 Sie werden gefragt werden, ob HTTPS verwendet werden soll. Antworten Sie mit `J` (ja) , wenn Sie SSL aktiviert haben, bzw. mit `N` (nein), wenn dies nicht der Fall ist.

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

16.9 Schützen von Windows-Clustern

PlateSpin Protect unterstützt den Schutz der Betriebsdienste eines Microsoft Windows-Server-Clusters. Weitere Informationen zu den Anforderungen und Optionen beim Schützen der Knoten in einem Windows-Server-Cluster finden Sie unter Kapitel 13, „Vorbereiten des Windows-Cluster-Schutzes“, auf Seite 119.

16.9.1 PlateSpin-Failover

Wenn der PlateSpin-Failover-Vorgang abgeschlossen ist und der virtuelle Ein-Knoten-Cluster online geht, sehen Sie einen Cluster mit mehreren Knoten, bei dem ein Knoten aktiv ist (alle anderen Knoten sind nicht verfügbar).

Für ein PlateSpin-Failover (oder zum Testen des PlateSpin-Failover) auf einem Windows-Cluster muss der Cluster eine Verbindung zu einem Domänencontroller herstellen können. Zur Nutzung der Test-Failover-Funktion müssen Sie den Domänencontroller zusammen mit dem Cluster schützen. Während des Tests müssen Sie den Domänencontroller hochfahren, gefolgt vom Windows-Cluster-Workload (in einem isolierten Netzwerk).

16.9.2 PlateSpin-Failback

Für einen PlateSpin-Failback-Vorgang ist eine vollständige Reproduktion für Windows-Cluster-Workloads erforderlich.

Wenn Sie das PlateSpin-Failback als vollständige Reproduktion auf ein physisches Ziel konfigurieren, können Sie eine der folgenden Methoden verwenden:

- Ordnen Sie alle Festplatten auf dem virtuellen PlateSpin-Ein-Knoten-Cluster einer einzigen lokalen Festplatte auf dem Failback-Ziel zu.
- Fügen Sie dem physischen Failback-Rechner eine andere Festplatte (`Festplatte 2`) hinzu. Sie können den PlateSpin-Failback-Vorgang dann so konfigurieren, dass das System-Volume des Failover-Computers auf `Festplatte 1` und die zusätzlichen Festplatten des Failover-

Computers (zuvor gemeinsam genutzte Festplatten) auf `Festplatte 2` wiederhergestellt werden. So kann die Systemfestplatte auf die Speicherfestplatte mit gleicher Größe wiederhergestellt werden wie die ursprüngliche Quelle.

Nach einem PlateSpin-Failback müssen Sie den gemeinsam genutzten Speicher wieder anschließen und die Clusterumgebung neu aufbauen, bevor Sie weitere Knoten in den wiederhergestellten Cluster aufnehmen können.

HINWEIS: Sobald der Cluster die Phase **Bereit zum erneuten Schützen** erreicht, müssen Sie zunächst das Failback-Ziel neu aufbauen und wiederherstellen, so dass es als Cluster ermittelt werden kann. Im Rahmen des Neuaufbaus müssen Sie den PlateSpin-Clustertreiber manuell deinstallieren.

Weitere Informationen zum Neuaufbauen der Cluster-Umgebung nach einem PlateSpin-Failover/-Failback finden Sie in den folgenden Ressourcen:

- **Windows Server 2012 R2 Failover-Cluster (Failback auf physischen oder virtuellen Neuaufbau):** Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7016770 (http://www.netiq.com/support/kb/doc.php?id=7016770).
- **Windows Server 2008 R2 Failover-Cluster (Failback auf physischen oder virtuellen Neuaufbau):** Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7015576 (http://www.netiq.com/support/kb/doc.php?id=7015576).

---

17 Erzeugen von Berichten

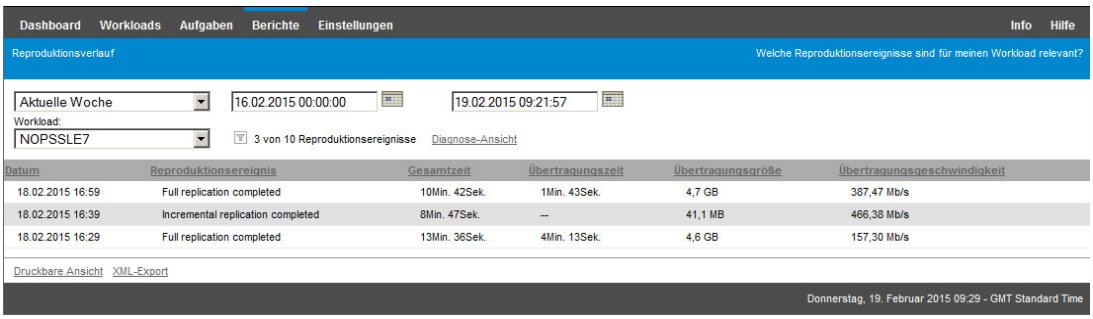
In der PlateSpin-Weboberfläche können Sie Berichte zu ermittelten Workloads und zu den Workload-Schutzverträgen erzeugen. Weitere Informationen zum Erzeugen eines Lizenzberichts finden Sie unter Abschnitt 4.6, „Erzeugen eines Lizenzberichts für den technischen Support“, auf Seite 52.

17.1 Informationen zu Protect-Berichten

Mit PlateSpin Protect können Sie die folgenden Berichte erzeugen, die einen analytischen Einblick in Ihre Workload-Schutzverträge über einen bestimmten Zeitraum hinweg eröffnen:

- **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 17-1 *Optionen für einen Reproduktionsverlaufsbericht*



17.2 Generieren von Workload- und Workload-Schutz-Berichten

So erzeugen Sie einen Bericht:

1 Klicken Sie in der Weboberfläche auf **Berichte**.

Es wird eine Liste mit Berichtstypen angezeigt.

2. Klicken Sie auf den Namen des erforderlichen Berichtstyps.
3. Wählen Sie mindestens einen Workload aus, für den ein Bericht erstellt werden soll.
4. Konfigurieren Sie den Zeitraum, für den der Bericht angezeigt werden soll.
5. Legen Sie die Parameter für den Bericht fest.
6. Führen Sie einen der folgenden Vorgänge aus:
   - Klicken Sie auf **Druckbare Ansicht**. Der Bericht wird im Webbrowser angezeigt.
   - Klicken Sie auf **XML-Export** und speichern Sie die XML-Datei auf dem Computer.

17.3 Generieren 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 unten rechts auf den Link **Generieren**.

   Nach kurzer Zeit wird die Seite aktualisiert, und der Link **Herunterladen** wird oberhalb des Links **Generieren** angezeigt.
2. Klicken Sie auf **Download** (Herunterladen).

   Die `.zip`-Datei enthält umfassende Diagnoseinformationen zum aktuellen Befehl.
3. Speichern Sie die Datei, extrahieren Sie die Diagnose und öffnen Sie sie.
4. Halten Sie die `.zip`-Datei bereit, wenn Sie sich an den Technischen Support wenden.

18 Fehlerbehebung bei Schutz und Wiederherstellung von Workloads

In diesem Abschnitt finden Sie Informationen zur Behebung häufiger Fehler beim Schutz und bei der Wiederherstellung von Workloads.

Weitere Informationen zu Problemen bei der Ermittlung und Inventarisierung für Ursprungs-Workloads und Ziel-Hosts finden Sie unter Kapitel 14, „Fehlerbehebung bei der Workload-Ermittlung und der Inventarisierung“, auf Seite 129.

18.1 Optimieren des Durchsatzes für eine Verbindung

Falls der Durchsatz zu gering ist, können Sie die Verbindung testen, ob Verbindungs- oder Bandbreitenprobleme vorliegen, und diese Probleme dann beheben. Weitere Informationen hierzu finden Sie in Anhang F, „Verwenden des iPerf-Werkzeugs zum Testen des Netzwerks und Optimieren des Netzwerkdurchsatzes für PlateSpin-Produkte“, auf Seite 195.

18.2 Fehlersuche bei Workloads, die Datenverkehr weiterleiten

In einigen Szenarien führt die Reproduktion eines Workloads, der Netzwerkverkehr weiterleitet (wenn der Zweck des Workloads beispielsweise darin liegt, als Netzwerk-Bridge für NAT, VPN oder eine Firewall zu dienen), zu einer deutlichen Verminderung der Netzwerkleistung. Dies hängt mit einem Problem mit VMXNET 2- und VMXNET 3-Adaptern zusammen, bei denen LRO (Large Receive Offload) aktiviert ist.

Zur Umgehung dieses Problems müssen Sie LRO am virtuellen Netzwerkadapter deaktivieren. Weitere Informationen finden Sie im Knowledgebase-Artikel 7005495 (https://www.netiq.com/support/kb/doc.php?id=7005495).

18.3 Fehlersuche beim Konfigurationsdienst

Nach einem Test-Failover oder Failover tritt ein Fehler auf der Ziel-VM aufgrund unspezifischer Probleme mit dem Konfigurationsdienst auf. Die allgemeine Fehlermeldung lautet:

```
Der Konfigurationsdienst auf dem Zielcomputer wurde offenbar nicht gestartet
```

In den Tipps zur Fehlersuche in diesem Abschnitt werden häufige Probleme mit dem Konfigurationsdienst und einige alternative Möglichkeiten zur Lösung erläutert.

- Abschnitt 18.3.1, „Erkennen der Ursache des Problems“, auf Seite 176
- Abschnitt 18.3.2, „Schritte, die zur Lösung des Problems unternommen werden können“, auf Seite 177
- Abschnitt 18.3.3, „Zusätzliche Tipps für die Fehlersuche“, auf Seite 180

18.3.1 Erkennen der Ursache des Problems

Der Konfigurationsdienst gibt an, dass PlateSpin-Server nicht mit dem Konfigurationsdienst auf der Ziel-VM kommunizieren kann. Analysieren Sie Ihr System, um die mögliche zugrunde liegende Ursache des Problems zu bestimmen.

- „Ziel-VM kann nicht gebootet werden“, auf Seite 176
- „Das Netzwerk ist nicht ordnungsgemäß eingerichtet“, auf Seite 176
- „Lesen oder Schreiben von Statusmeldungen auf Diskettenlaufwerke nicht möglich“, auf Seite 176

Ziel-VM kann nicht gebootet werden

Das Betriebssystem muss in der Ziel-VM geladen sein, damit der Konfigurationsdienst normal gestartet werden kann. Wenn nicht gebootet werden kann, ist dies ein Hinweis auf einen möglichen Treiberkonflikt, einen Boot-Loader-Fehler oder einen beschädigten Datenträger.

Es wird empfohlen, ein Serviceticket beim Micro Focus-Kundenservice zu öffnen, wenn das Betriebssystem auf der Ziel-VM nicht gebootet werden kann.

Das Netzwerk ist nicht ordnungsgemäß eingerichtet

Das Netzwerk muss richtig eingerichtet sein, damit der Konfigurationsdienst auf dem Ziel-Workload mit dem PlateSpin-Server kommunizieren kann.

Stellen Sie sicher, dass Sie Ihr Netzwerk so konfiguriert haben, dass der Ziel-Workload mit dem PlateSpin-Server kommunizieren kann. Weitere Informationen hierzu finden Sie unter Abschnitt 1.5, „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“, auf Seite 31.

Lesen oder Schreiben von Statusmeldungen auf Diskettenlaufwerke nicht möglich

Der Konfigurationsdienst muss mit den Diskettenlaufwerken für VMware-VMs kommunizieren können, um Statusmeldungen für den PlateSpin-Server zu lesen und zu schreiben.

Überprüfen Sie, ob die Ziel-VM mit Diskettenlaufwerken kommunizieren kann.

1. Öffnen Sie die Protokolldatei auf der VM (`C:\windows\platespin\configuration\data\log.txt`).
2. Jede der folgenden Meldungen kann ein Hinweis darauf sein, dass auf das Diskettenlaufwerk nicht zugegriffen werden kann:

   ```
   Failed (5) to write to file \\?\Volume{<guid-number>}\log.zip CopyFile \\?\Volume{<guid-number>}\windows\platespin\configuration\data\result.txt to \\?\Volume{<guid-number>}\result.txt failed The output floppy was not accessible after the timeout period
   ```

18.3.2 Schritte, die zur Lösung des Problems unternommen werden können

Versuchen Sie, Konfigurationsdienstfehler mit einer der Lösungen in diesem Abschnitt zu beheben.

- „Überspringen der Optimierung für erneutes Booten der Ziel-VM“, auf Seite 177
- „Reduzieren des Lese-/Schreibverkehrs auf Diskettenlaufwerken“, auf Seite 177
- „Ändern des Starttyps zum Verlängern der Verzögerung“, auf Seite 179
- „Konfigurieren, dass Dienste, die zu Konflikten führen, nicht automatisch beim Start ausgeführt werden“, auf Seite 180

Überspringen der Optimierung für erneutes Booten der Ziel-VM

Protect versucht standardmäßig, die Anzahl der erneuten Bootvorgänge auf der Ziel-VM auf ein Minimum zu reduzieren, um den Failover-Vorgang zu beschleunigen. Möglicherweise verbessert sich die Kommunikation zwischen Ziel-VM und PlateSpin-Server, wenn zusätzliche erneute Bootvorgänge zugelassen werden.

So überspringen Sie die Optimierung für erneutes Booten:

1. Melden Sie sich beim PlateSpin-Server an und öffnen Sie die Konfigurationsseite für den PlateSpin-Server unter:

   `https://Ihr_PlateSpin_Server/platespinconfiguration/`
2. Suchen Sie den Parameter **ConfigurationServiceValues**.
3. Bearbeiten Sie den Parameter **ConfigurationServiceValues** und legen Sie die Option **SkipRebootOptimization** auf `true` fest.
4. Klicken Sie auf **Speichern**.
5. Führen Sie eine inkrementelle oder Vollreproduktion aus.

   Die Reproduktion überträgt die geänderten Konfigurationseinstellungen auf die Ziel-VM.
6. Führen Sie den fehlgeschlagenen Test-Failover oder Failover für die betroffenen Workloads erneut aus.

Reduzieren des Lese-/Schreibverkehrs auf Diskettenlaufwerken

Sie können die Häufigkeit reduzieren, mit der der PlateSpin-Server versucht, VMware-Eingaben oder -Ausgaben auf Diskettenlaufwerken zu lesen oder zu schreiben, wenn das Diagnoseprotokoll folgenden Fehler enthält:

```
Information:1:Attempting floppy download
```

gefolgt von:

```
Verbose:1:Failed to copy file from remote URL
```

-oder-

```
Ausnahme: Der Remoteserver hat einen Fehler zurückgegeben: (500) Interner
Serverfehler
```

Dieser Fehler wird dadurch verursacht, dass VMware die Ressource sperrt. Er weist darauf hin, dass der PlateSpin-Server bei jeder Statusprüfung das Diskettenlaufwerk trennt und wieder verbindet. Die Sperrung kann dazu führen, dass die Ziel-VM keine Lese- und Schreibvorgänge auf dem Diskettenlaufwerk durchführen kann. Weitere Informationen finden Sie in dem KB-Artikel *Using the VMware vCenter Server 4.x,5.x and 6.0 Datastore Browser to Download or Copy a Powered-On Virtual Machine's .vmx and .nvram Files Fails (1019286)* (https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1019286).

Wenn Probleme beim Sperren des Diskettenlaufwerks auftreten, können Sie die Werte für die Polling-Einstellungen des Konfigurationsdiensts auf dem PlateSpin-Server erhöhen:

vmwareConfigServicePollStartDelay

Dieser Parameter bestimmt die Wartezeit, bis der PlateSpin-Server mit dem Polling für den Status des Ziel-Workloads beginnt. Der Standardwert ist 120 Sekunden (2 Minuten).

vmwareConfigServicePollIntervalInMilliseconds

Dieser Parameter bestimmt die Häufigkeit, mit der der PlateSpin-Server versucht, mit dem Ziel-Workload zu kommunizieren und auf VMware-Diskettenlaufwerken zu lesen oder zu schreiben. Das standardmäßige Polling-Intervall beträgt 30000 ms (30 Sekunden).

vmwareConfigServicePollStartTimeout

Dieser Parameter bestimmt, wie lange der PlateSpin-Server nach dem Start der Ziel-VM wartet, bevor er einen Fehler in der Weboberfläche anzeigt. Der Standardwert ist 420 Sekunden (7 Minuten).

vmwareConfigServicePollUpdateTimeout

Dieser Parameter bestimmt, wie lange der PlateSpin-Server nach jedem Polling-Intervall wartet, bevor er einen Fehler in der Weboberfläche anzeigt. Der Standardwert ist 300 Sekunden (5 Minuten).

Je höher die Werte für diese Parameter sind, desto seltener versucht der PlateSpin-Server, Lese- oder Schreibvorgänge auf den VMware-Diskettenlaufwerken der Ziel-VMs durchzuführen.

So reduzieren Sie den Lese- und Schreibverkehr für VMware-Diskettenlaufwerke:

1. Melden Sie sich beim PlateSpin-Server an und öffnen Sie die Konfigurationsseite für den PlateSpin-Server unter:

   `https://Ihr_PlateSpin_Server/platespinconfiguration/`

2. Suchen Sie die Polling-Parameter des Konfigurationsdiensts, ändern Sie die Einstellungen nach Bedarf und klicken Sie auf **Speichern**.

   Beispiel:

   ```
   vmwareConfigServicePollStartDelay = 180 (3 Minuten)
   vmwareConfigServicePollIntervalInMilliseconds = 300000 (5 Minuten)
   vmwareConfigServicePollStartTimeout = 1200 (20 Minuten)
   vmwareConfigServicePollUpdateTimeout = 900 (15 Minuten)
   ```

   Alternativ:

```
vmwareConfigServicePollStartDelay = 300 (5 Minuten)
vmwareConfigServicePollIntervalInMilliseconds = 480000 (8 Minuten)
vmwareConfigServicePollStartTimeout = 1200 (20 Minuten)
vmwareConfigServicePollUpdateTimeout = 900 (15 Minuten)
```

3. Führen Sie eine inkrementelle oder Vollreproduktion aus.

   Die Reproduktion überträgt die geänderten Konfigurationseinstellungen auf die Ziel-VM.

4. Führen Sie den fehlgeschlagenen Test-Failover oder Failover für die betroffenen Workloads erneut aus.

Ändern des Starttyps zum Verlängern der Verzögerung

Möglicherweise wird der Konfigurationsdienst gestartet, bevor die Ressourcen verfügbar sind. Sie können den Starttyp des Konfigurationsdiensts ändern, um die Verzögerung zu verlängern.

So ändern Sie den Starttyp:

1. Melden Sie sich beim PlateSpin-Server an und öffnen Sie die Konfigurationsseite für den PlateSpin-Server unter:

   `https://Ihr_PlateSpin_Server/platespinconfiguration/`

2. Suchen Sie den Parameter **windowsConfigServiceStartType**.
3. Ändern Sie den Wert von **windowsConfigServiceStartType** zu **AutoDelay**.

   Für **windowsConfigServiceStartType** sind folgende Optionen verfügbar:

   - **GroupDelay** ist der Standardwert, mit dem der Konfigurationsdienst in der Registrierung am Ende von **ServiceGroupOrder** hinzugefügt wird.
   - **AutoDelay** verlängert die Verzögerung bis zum Starten des Diensts auf das Maximum (2 Minuten nach dem Booten). Ändern Sie außerdem den Parameterwert für **ServicesPipeTimeoutForWindowsConfigService** in Schritt 4.
   - **NoDelay** ist die effizienteste Option, mit der der Dienst gestartet wird, sobald Windows dies zulässt. Diese Einstellung wird jedoch nicht empfohlen, da Probleme mit der Verbindung zu Ressourcen auftreten können.

4. (AutoDelay) Ändern Sie die Einstellung des Parameters **ServicesPipeTimeoutForWindowsConfigService** zu 180 Sekunden, um die 120 Sekunden zu berücksichtigen, die der Dienst nach dem Booten zum Starten benötigt, wenn in Schritt 3 für **windowsConfigServiceStartType** der Wert AutoDelay eingestellt wird.
5. Klicken Sie auf **Speichern**.
6. Führen Sie eine inkrementelle oder Vollreproduktion aus.

   Die Reproduktion überträgt die geänderten Konfigurationseinstellungen auf die Ziel-VM.

7. Führen Sie den fehlgeschlagenen Test-Failover oder Failover für die betroffenen Workloads erneut aus.

Konfigurieren, dass Dienste, die zu Konflikten führen, nicht automatisch beim Start ausgeführt werden

Während einer Failover-Aktion stört ein Windows-Dienst das Mounten von Diskettenlaufwerken.

Bestimmen Sie, welche Windows-Dienste so konfiguriert sind, dass sie beim erneuten Booten gestartet werden. Es ist bekannt, dass einige Dienste den Konfigurationsdienst beim Schreiben auf ein Diskettenlaufwerk stören, beispielsweise die Drahtloskonfiguration und bestimmte Virenschutz-Programme. Konfigurieren Sie diese Dienste so, dass sie nicht automatisch bei einem Test-Failover oder Failover ausgeführt werden. Wiederholen Sie dann das Test-Failover oder Failover.

Sie können auch versuchen, auf der Konfigurationsseite alle nicht wesentlichen Dienste für ein Test-Failover oder Failover zu deaktivieren, und das Test-Failover oder Failover dann wiederholen.

18.3.3 Zusätzliche Tipps für die Fehlersuche

Wenn der Konfigurationsdienst keinen Kontakt mit dem PlateSpin-Server aufnehmen kann, zeigt die Diagnose nur einen Aspekt des Problems. Sie benötigen auch die Protokolle der Ziel-VM:

- **Windows-Workloads:** Die Protokolle des Konfigurationsdiensts befinden sich im Ordner `C:\windows\platespin\configuration\data`.
  - Die Datei `log.txt` enthält alle Protokollierungsinformationen; die Datei `Config.ini` ist jedoch nützlich, um zu verstehen, welche Einstellungen konfiguriert werden müssen.
  - Die Datei `result.txt` enthält den Status des ausgeführten Konfigurationsdiensts.
  - Wenn die Ziel-VM nicht vom Eingabe-Diskettenlaufwerk lesen kann, verfügt sie nicht über die zusammengeführte Datei `Config.ini`, die benutzerdefinierte Netzwerkkonfigurationsinformationen für die Test-Failover-Netzwerkumgebung enthalten kann.
  - Wenn die Datei `Config.ini` nicht über netzwerkbezogene Informationen (wie z. B. `[NIC0]`) verfügt, könnte der Netzwerkadapter der Ziel-VM Sonderzeichen im Namen enthalten.

    Es ist ein bekanntes Problem, dass die Datei `Config.ini` erst dann richtige Werte enthält, wenn sie mit der auf dem Diskettenlaufwerk zusammengeführt wird.
  - Die Ziel-VM versucht, neu zu booten, wenn sie weder eine Verbindung zum Ausgabe-Diskettenlaufwerk noch zum Eingabe-Diskettenlaufwerk (nur einmal) herstellen kann. In diesem Fall wird eine `config.ini.floppyreboot`-Datei erstellt.
- **Linux-Workloads:** Die Protokolle des Konfigurationsdiensts befinden sich im Ordner `/tmp`.
  - Die Namen der Hauptprotokolldateien lauten `file*.platespin.fileLogger`.

    Es wird empfohlen, alle Konfigurationsordner in `/tmp` zu untersuchen. Erstellen Sie ein Tar-Paket mit den Konfigurationsordnern und den Dateien des Typs `file*.platespin.fileLogger` und senden Sie es an den Micro Focus-Kundendienst.
  - Suchen Sie außerdem folgende Konfigurationsdateien:

    ```
    /tmp/Ofx.RunCommand.Output*
    /tmp/*DiskHelper*
    /tmp/*VmTools*
    ```
  - Die Konfigurationsdatei ist `/usr/lib/psconfigservice/data/config.conf`.
  - Die Protokolldatei mit dem Endergebnis ist `/usr/lib/psconfigservice/data/result.txt`.

18.4 Fehlerbehebung beim Vorbereiten des Workloads für die Reproduktion (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 181.
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 Ermittlung von Windows-Workloads“, auf Seite 129.

18.4.1 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 `gpupdate /force` aktualisieren.

18.4.2 Mindestens zwei Volumes haben dieselbe Volume-Seriennummer

Problem: Beim Versuch, einen Schutz für einen Windows-Server einzurichten, wird der folgende Fehler angezeigt:

```
[Ursprung] Mindestens zwei Volumes haben dieselbe Seriennummer. Ändern Sie eine der Seriennummern, sodass sie eindeutig sind, und führen Sie die Ermittlung des Computers erneut durch.
```

Behelfslösung: Dieses Problem kann auftreten, wenn die Volume-Seriennummern für zwei oder mehr Volumes identisch sind. In PlateSpin Protect müssen Seriennummern eindeutig sein.

Um dieses Problem zu lösen, ändern Sie die Seriennummern für die Daten-Volumes nach Bedarf und führen Sie die Ermittlung für den Computer erneut durch. Weitere Informationen über die Verwendung von nativen Windows-Tools zum Bearbeiten von Seriennummern finden Sie in KB-Artikel 7921101.

18.5 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.
Bei aktivierter Verschlüsselung wird die inkrementelle dateibasierte Reproduktion nicht abgeschlossen	Wenn Sie die·Verschlüsselung für einen Windows-Workload aktivieren, der für die dateibasierte Übertragung konfiguriert ist, bleibt der Windows-Empfänger unter Umständen am Ende der Übertragung für inkrementelle Reproduktionen hängen. Dieser Fall tritt ein, wenn das letzte gelesene Byte der Übertragung durch den Verschlüsselungsvorgang fehlerhaft auf einen Wert ungleich null gesetzt wurde. Dieser Wert bedeutet, dass noch weitere Dateien übertragen werden, so dass weiter aus dem Stream gelesen werden soll. Wenn die Verschlüsselung für die Übertragung der Reproduktionsdaten aktiviert werden soll, nutzen Sie die blockbasierte Datenübertragung für Windows-Workloads.
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.
Der Schutz über ein WAN benötigt viel Zeit, wenn der VM-Container eine große Anzahl an Datenablagen enthält	Unter einigen Umständen kann der Prozess der Suche nach dem entsprechenden ISO-Image, das zum Booten des Ziels erforderlich ist, länger dauern als erwartet. Dies kann passieren, wenn Ihr PlateSpin-Server über ein WAN mit dem VM-Container verbunden ist und Ihr VM-Container eine große Anzahl an Datenablagen enthält.
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.

Probleme oder Meldungen	Lösungen
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 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 71.

`Die Dateiübertragung kann nicht beginnen – Port 3725 wird bereits verwendet`
 	
oder
 	
`3725 – Herstellen einer Verbindung nicht möglich`
	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-Verbindung nicht hergestellt` 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 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 Server-Host herstellen kann.
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 Knowledgebase-Artikel 7920339 (https://www.netiq.com/support/kb/doc.php?id=7920339). ◆ Wenn lokale Richtlinien oder Domänenrichtlinien die erforderlichen Berechtigungen einschränken, führen Sie die im Knowledgebase-Artikel 7920862 (https://www.netiq.com/support/kb/doc.php?id=7920862) beschriebenen Schritte aus. Dieses Problem tritt häufig auf, wenn der PlateSpin 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 181.

Probleme oder Meldungen	Lösungen
Nach einer Windows-Aktualisierung werden einige Dateien im Ordner `C:\Windows\SoftwareDistribution` während der schrittweisen dateibasierten Reproduktion nicht an den Zielcomputer übertragen.	Dies ist eine allgemeine Vorgehensweise von Microsoft Windows: Zum Zweck der Optimierung werden einige Dateien für die Löschung im Registrierungsschlüssel `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot` markiert, um zu verhindern, dass sie in VSS-Snapshots integriert werden. Weitere Informationen finden Sie im Microsoft Developer Network-Artikel *Ausschließen von Dateien von Schattenkopien* (http://msdn.microsoft.com/en-us/library/aa819132.aspx). Im Allgemeinen werden diese Dateien vor der Löschung zur Installation von Windows-Aktualisierungen verwendet und sind nach der Aktualisierung nicht mehr erforderlich. Falls Sie diese Dateien wiederherstellen möchten, führen Sie die Windows-Aktualisierung nach dem Failover auf dem Zielcomputer aus, um den Ordner `SoftwareDistribution` neu zu füllen.

18.6 Fehlerbehebung beim Workload-Failover oder -Failback

Probleme oder Meldungen	Lösungen
Nach einem Failback sind Active Directory-Domänendienste nicht verfügbar (Windows)	Nach einem Failover werden die Active Directory-Domänendienste möglicherweise nicht angezeigt, wenn `chkdsk`-Fehler auftreten. Die beiden folgenden Ursachen für `chkdsk`-Fehler lassen sich leicht vermeiden: ◆ Protokolldateien mit Bezug zu Microsoft-Updates, wenn der Quellcomputer beim Ausführen der ersten vollständigen Reproduktion nicht mit allen von Microsoft empfohlenen Patches oder Updates auf dem neuesten Stand ist. ◆ Systemdateien und Ordner, die aus der Virenschutz-Software ausgeschlossen werden sollten. Damit diese Probleme nicht auftreten, beachten Sie die bewährten Verfahren unter Abschnitt 15.1, „Voraussetzungen für den Workload-Schutz“, auf Seite 147, bevor Sie die erste vollständige Reproduktion ausführen.

Probleme oder Meldungen	Lösungen
Beim Failback werden die falschen NICs zugeordnet und das Failback bleibt hängen	Schließen Sie das Failback mit einer der folgenden Behelfslösungen ab: ◆ Stellen Sie die IP-Konfiguration auf die erwarteten Zuordnungen um, sodass das Ziel erfolgreich konfiguriert wird. ◆ Booten Sie die Hardware für die Kontrollübernahme in den LRD neu und wiederholen Sie die Schritte, sodass die Hardware als Failback-Ziel verwendet wird. Die Chancen stehen gut, dass Protect beim nächsten Mal die richtigen Ethernet-Schnittstellen zuordnet. ◆ Wenn das Failback in der Weboberfläche kurz vor Abschluss hängenzubleiben scheint, kann das Failback-Ziel dem PlateSpin-Server wahrscheinlich nicht mitteilen, dass das Failback abgeschlossen ist. Stecken Sie die Netzwerkkabel an der Rückseite des Failback-Ziels um, sodass die richtige NIC in die gewünschten Netzwerke platziert wird. So kann das Failback-Ziel mit dem PlateSpin-Server kommunizieren und das Failback wird abgeschlossen.
X2P-Failback von Linux-Workloads verursacht einen Fehler der grafischen X-Server-Benutzeroberfläche	Das Problem wird durch eine Neukonfiguration der VM nach dem Failover ausgelöst, wenn VMware-Tools installiert sind. Zur Behebung dieses Problems suchen Sie die Dateien, deren Dateiname die Zeichenfolge `BeforeVMwareToolsInstall` enthält, mit dem folgenden Befehl: `find / -iname '*BeforeVMwareToolsInstall'.` Verschieben Sie alle aufgefundenen Dateien zurück an den Originalspeicherort, und booten Sie den Workload neu. Damit ist die X-Server-Benutzeroberfläche des Workloads wiederhergestellt.

18.7 Verkleinern der PlateSpin Protect-Datenbanken

Sobald die PlateSpin Protect-Datenbanken (`0FX`, `PortabilitySuite` und `Protection`) eine vordefinierte Kapazität erreichen, werden diese Datenbanken in regelmäßigen Abständen bereinigt. Falls Sie die Größe oder den Inhalt dieser Datenbanken noch weitergehend steuern möchten, können Sie sie mit einem speziellen Protect-Dienstprogramm (`PlateSpin.DBCleanup.exe`) weiter bereinigen und verkleinern. Im Knowledgebase-Artikel 7006458 (https://www.netiq.com/support/kb/doc.php?id=7006458) finden Sie Angaben zum Speicherort und den verfügbaren Optionen für dieses Werkzeug, mit denen Sie Offline-Datenbankvorgänge ausführen können.

18.8 Workload-Bereinigung nach dem Schutz

Befolgen Sie diese 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.

- Abschnitt 18.8.1, „Bereinigen von Windows-Workloads“, auf Seite 186
- Abschnitt 18.8.2, „Bereinigen von Linux-Workloads“, auf Seite 186

18.8.1 Bereinigen von Windows-Workloads

Komponente	Entfernungsanweisung
Blockbasierte PlateSpin-Übertragungskomponente	Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7005616 (https://www.netiq.com/support/kb/doc.php?id=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.
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. Öffnen Sie eine Eingabeaufforderung auf dem Ursprungs-Workload und wechseln Sie das aktuelle Verzeichnis wie folgt: ◆ `\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..

18.8.2 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 in der 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`*

Komponente	Entfernungsanweisung

NSS-Snapshot	NSS-Snapshot, der in PlateSpin für laufende Reproduktionen erstellt und verwendet wird. Der Snapshot-Name endet mit dem Suffix `PSSNP`.
	
	So entfernen Sie diese NSS-Snapshots:
	
	1. Erstellen Sie anhand einer der folgenden Methoden eine Liste der Snapshots auf dem erforderlichen Workload:
	◆ Erstellen Sie in der Weboberfläche einen Job-Bericht für den fehlgeschlagenen Job. Der Bericht sollte Informationen über die NSS-Snapshots und deren Namen enthalten.
	- oder -
	◆ Geben Sie auf dem erforderlichen Open Enterprise Server-Workload den folgenden Befehl ein, sodass eine Liste aller NSS-Snapshots angezeigt wird:
	`# NLVM list snaps`
	- oder -
	◆ Starten Sie NSSMU auf dem erforderlichen Open Enterprise Server-Workload und rufen Sie mit **Snapshot** eine Liste der Snapshots ab.
	2. Notieren Sie sich die Namen und Standorte der Snapshots, die entfernt werden sollen.
	3. Entfernen Sie die entsprechenden Snapshots auf dem Open Enterprise Server-Workload mit einer der folgenden Methoden:
	◆ Geben Sie den folgenden Befehl ein:
	`NLVM delete snap <`*Snapshot_Name*`>`
	- oder -
	◆ Starten Sie NSSMU und wählen Sie **Snapshot**. Markieren Sie jeweils die zu löschenden Snapshots und klicken Sie auf „Löschen“.

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`

V PlateSpin-Werkzeuge

PlateSpin Protect bietet zusätzliche Werkzeuge, die die Produktionsumgebung erweitern.

E Verwenden von Workload-Schutz-Funktionen über die PlateSpin Protect-Server-API

Mithilfe der PlateSpin Protect-Server-API (protectionservices) können Sie die Workload-Schutz-Funktionen von `PlateSpin Protect` programmatisch von Ihren Anwendungen aus verwenden. Alle Programmier- oder Skriptsprachen, die einen HTTP-Client und das JSON-Serialisierungs-Framework nutzen, sind verwendbar.

HINWEIS: Die Protect Server-API befindet sich noch im Versuchsstadium. Die Angaben in diesem Abschnitt gelten als Technologie-Vorschau.

E.1 API-Übersicht

PlateSpin Protect verfügt über eine REST-basierte API-Technologievorschau, die Entwickler bei der Erstellung eigener Anwendungen für das Produkt verwenden können. Die API enthält Informationen über die folgenden Vorgänge:

- Container ermitteln
- Workloads ermitteln
- Schutz konfigurieren
- Reproduktionen, Failover-Vorgänge und Failback ausführen
- Workload- und Container-Status abfragen
- Status laufender Vorgänge abfragen
- Sicherheitsgruppen und deren Schutzverbindungen

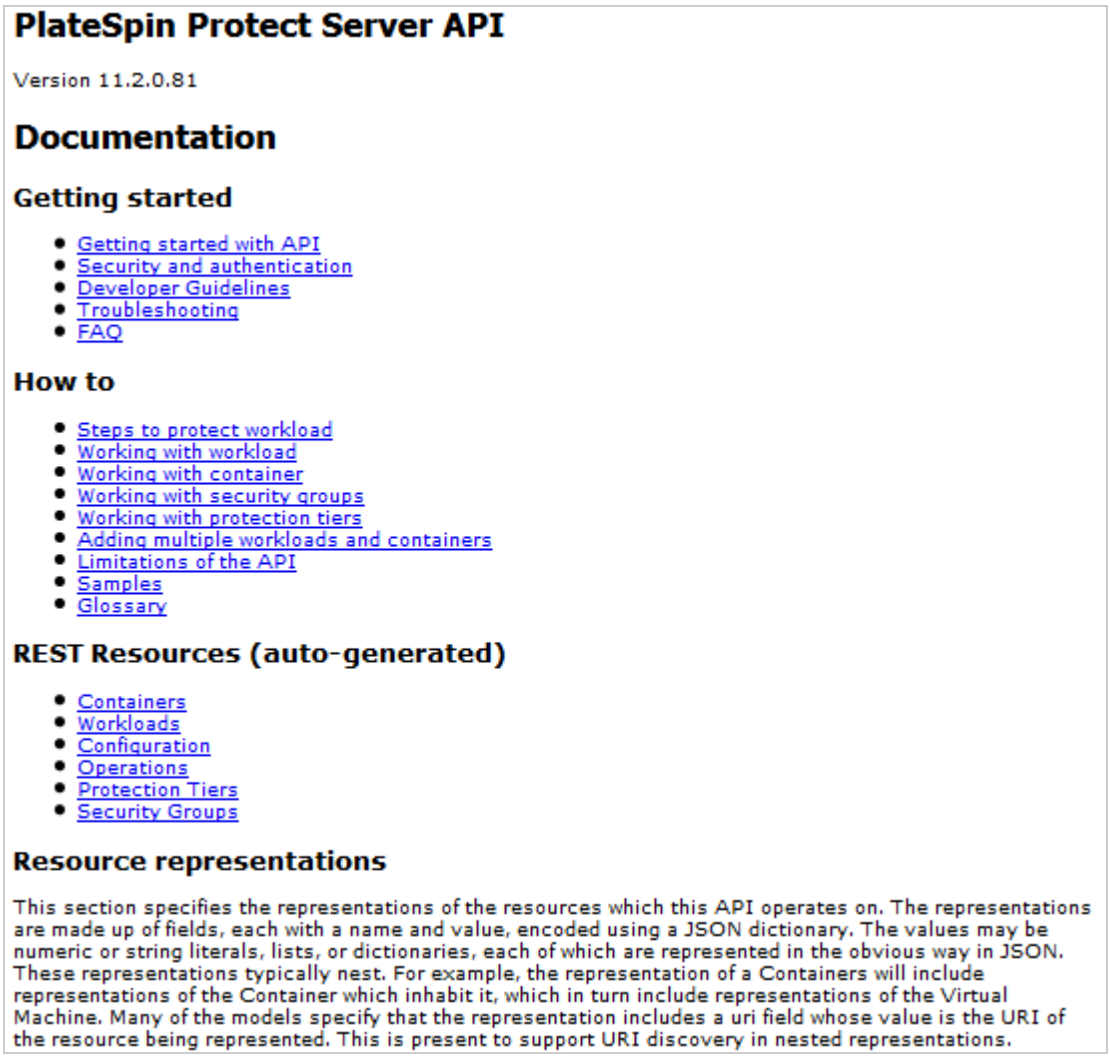
E.2 Dokumentation zur PlateSpin Protect-Server-API

Auf der Startseite der PlateSpin Protect-Server-API für `/protectionservices/` finden Sie Dokumentation und Beispiele, die für Entwickler und Administratoren nützlich sein können. Weitere Informationen finden Sie auf dem PlateSpin-Server-Host:

`https://`*Ihr_PlateSpin_Server*`/protectionservices`

Ersetzen Sie *Ihr_PlateSpin_Server* durch den Hostnamen oder die IP-Adresse Ihres PlateSpin-Server-Hosts. Wenn SSL nicht aktiviert ist, verwenden Sie `http` in der URL.

Abbildung E-1 *Die Startseite der Protect-Server-API*



E.3 Beispiele und weitere Referenzen

Protect-Administratoren können über ein JScript-Beispiel in der Befehlszeile aus über die API auf das Produkt zugreifen. Beachten Sie auf dem PlateSpin-Server-Host das Beispiel unter

https://localhost/protectionservices/Documentation/Samples/protect.js

Anhand des Beispiels können Sie Skripte schreiben, die Ihnen die Arbeit mit dem Produkt erleichtern. Mit dem Befehlszeilenprogramm können Sie die folgenden Vorgänge durchführen:

- Einzelnen Workload hinzufügen
- Einzelnen Container hinzufügen
- Reproduktions-, Failover- und Failback-Vorgänge ausführen
- Mehrere Workloads und Container gleichzeitig hinzufügen

HINWEIS: Weitere Informationen über diesen Vorgang finden Sie in der API-Dokumentation unter

https://localhost/protectionservices/Documentation/AddWorkloadsAndContainersFromCsvFile.htm

- Alle Workloads gleichzeitig entfernen
- Alle Container gleichzeitig entfernen

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.

F Verwenden des iPerf-Werkzeugs zum Testen des Netzwerks und Optimieren des Netzwerkdurchsatzes für PlateSpin-Produkte

Testen Sie die Verbindung vor dem Ausführen einer Reproduktion, um Verbindungs- und Bandbreitenprobleme zu erkennen und zu lösen. In diesem Abschnitt wird beschrieben, wie Sie mithilfe des Open Source-Werkzeugs iPerf zum Testen des Netzwerks den Durchsatz einer Verbindung optimieren.

F.1 Einführung

Damit PlateSpin-Administratoren den Netzwerkdurchsatz bei der Verwendung von PlateSpin-Produkten verbessern können, wird das iPerf-Werkzeug zum Testen des Netzwerks in der PlateSpin-LRD-Umgebung (LRD, Linux RAM-Datenträger) bereitgestellt, die die Kontrolle übernimmt. In der iPerf-Dokumentation wird Folgendes erläutert: „Das primäre Ziel von iPerf ist die Feinabstimmung der TCP-Verbindungen für einen bestimmten Pfad. Das Hauptproblem bei der TCP-Feinabstimmung ist die Größe des TCP-Fensters, die steuert, wie viele Daten sich zu einem bestimmten Zeitpunkt im Netzwerk befinden können.“

In diesem Abschnitt wird eine grundlegende Methode für die Feinabstimmung und das Testen des Netzwerks in Bezug auf die Verwendung von PlateSpin-Produkten beschrieben. Zunächst berechnen Sie die theoretisch optimale Größe des TCP-Fensters. Dann verwenden Sie das iPerf-Werkzeug zur Bestätigung und Feinabstimmung der berechneten Größe und messen den Durchsatz, der sich ergibt. Mit dieser Methode kann auch der tatsächlich erreichbare Durchsatz für ein gegebenes Netzwerk bestimmt werden.

Sowohl beim iPerf-Werkzeug als auch bei PlateSpin-Produkten beeinflusst die *TCP-Puffergröße zum Senden/Empfangen* die intern ausgewählte *TCP-Fenstergröße*. Diese Begriffe werden im Folgenden synonym verwendet.

HINWEIS: Es gibt zahlreiche Faktoren, die sich auf den Netzwerkdurchsatz auswirken. Die umfangreichen Informationen im Internet können hilfreich sein, um das Verständnis zu verbessern. Eine dieser Ressourcen ist der *Rechner für den Netzwerkdurchsatz* (http://wintelguy.com/wanperf.pl),

mit dem der erwartete maximale TCP-Durchsatz anhand der Netzwerkeigenschaften des Kunden berechnet werden kann. Wir empfehlen, diesen Online-Rechner zu verwenden, um realistische Erwartungen hinsichtlich des Durchsatzes zu stellen.

F.2 Berechnungen

Die Feinabstimmung der TCP-Fenstergröße basiert auf mehreren Faktoren einschließlich der Netzwerkverbindungsgeschwindigkeit und Netzwerklatenz. Für unsere Zwecke in Bezug auf PlateSpin-Produkte basiert die anfänglich für die Feinabstimmung verwendete TCP-Fenstergröße auf folgenden Standardberechnungen (vielerorts im Internet und an anderen Stellen verfügbar):

```
WinSizeInBytes=((LINK_SPEED(Mbps)/8)*DELAY(sec))*1000*1024
```

Beispielsweise wäre die geeignete anfängliche Fenstergröße bei einer 54-Mb/s-Verbindung mit 150 ms Latenz wie folgt:

```
(54/8)*0,15*1000*1024 = 1.036.800 Byte
```

Die geeignete anfängliche Fenstergröße bei einer 1000-Mb/s-Verbindung mit 10 ms Latenz wäre wie folgt:

```
(1000/8)*0,01*1000*1024 = 1.280.000 Byte
```

Um einen Latenzwert für das Netzwerk zu erhalten, geben Sie an der Eingabeaufforderung (Windows) oder dem Terminal (Linux) den Befehl `ping` ein. Obwohl die `ping`-Durchlaufzeit (RTT, Round-Trip Time) eigentlich nicht ganz das Gleiche ist wie die Latenz, ist der erhaltene Wert zur Verwendung bei dieser Methode ausreichend genau.

Der folgende Abschnitt enthält eine Beispielausgabe für einen `ping`-Befehl unter Windows, bei dem die Latenz im Durchschnitt 164 ms beträgt:

```
ping 10.10.10.232 -n 5

Pinging 10.10.10.232 with 32 bytes of data:
Reply from 10.10.10.232: bytes=32 time=154ms TTL=61
Reply from 10.10.10.232: bytes=32 time=157ms TTL=61
Reply from 10.10.10.232: bytes=32 time=204ms TTL=61
Reply from 10.10.10.232: bytes=32 time=153ms TTL=61
Reply from 10.10.10.232: bytes=32 time=153ms TTL=61

Ping statistics for 10.10.10.232:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 153ms, Maximum = 204ms, Average = 164ms
```

Der folgende Abschnitt enthält eine Beispielausgabe für einen `ping`-Befehl unter Linux, bei dem Latenz im Durchschnitt 319 ms beträgt:

```
ping 10.10.10.232 -c 5

PING 10.10.10.232 (10.10.10.232) 56(84) bytes of data.
64 bytes from 10.10.10.232: icmp_seq=1 ttl=62 time=0.328 ms
64 bytes from 10.10.10.232: icmp_seq=2 ttl=62 time=0.280 ms
64 bytes from 10.10.10.232: icmp_seq=3 ttl=62 time=0.322 ms
64 bytes from 10.10.10.232: icmp_seq=4 ttl=62 time=0.349 ms
64 bytes from 10.10.10.232: icmp_seq=5 ttl=62 time=0.316 ms

--- 10.10.10.232 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.280/0.319/0.349/0.022 ms
```

In der Praxis sollten Sie mithilfe der Option `-n` oder `-c` eine größere Anzahl von ping-Paketen angeben, um den Latenzwert genauer zu messen.

F.3 Einrichtung

Das iPerf-Werkzeug kann im Server- oder Client-Modus ausgeführt werden.

Die grundlegende Syntax zur Verwendung von `iperf` im Servermodus ist:

```
iperf -s -w <win_size>
```

Die grundlegende Syntax zur Verwendung von `iperf` im Clientmodus ist:

```
iperf -c <server_ip> -w <win_size>
```

Unser Ziel ist die Messung und Feinabstimmung des Netzwerks zwischen einem Ursprungs- und einem Ziel-Workload. In vielen Fällen kann es sich dabei um den tatsächlich verwendeten Ursprung und das Ziel handeln. Es ist möglich, Tests anhand eines anderen Workloads für Ursprung oder Ziel durchzuführen, sofern der verwendete Ersatz die gleichen Netzwerkmerkmale (NIC, Netzwerkverbindung usw.) wie das Original aufweist.

HINWEIS: Stellen Sie sicher, dass Sie nicht den Durchsatz des PlateSpin-Servers an den Ursprung oder das Ziel testen, da dieser Verkehr minimal ist und nicht dem Verkehr während einer Migration oder Reproduktion entspricht.

Während es möglich ist, einen Live-Workload (entweder Windows oder Linux) als Ziel/iperf-Server zu verwenden, kann mit der folgenden sehr empfehlenswerten Vorgehensweise eine Umgebung bereitgestellt werden, die derjenigen während einer Migration oder Reproduktion sehr ähnlich ist.

So richten Sie `iperf` auf dem Ziel ein und führen das Werkzeug aus:

1. Booten Sie das Ziel mithilfe des LRD.
2. Verwenden Sie das Helper-Terminal in der LRD-Konsole (kann über Alt-F2 aufgerufen werden), um folgende Schritte auszuführen:
   - **2a** Richten Sie Networking mit Option 5 ein.
   - **2b** Mounten Sie die CD-Medien mit Option 6.
3. Wechseln Sie in der LRD-Konsole zum Terminal für die Fehlersuche (kann über Alt-F7 aufgerufen werden), um in das Verzeichnis mit dem iPerf-Werkzeug zu gelangen:

   ```
   cd /mnt/cdrom/LRDTools/iperf_2.0.X/linux
   ```

4 Führen Sie das iPerf-Werkzeug im Servermodus aus. Eingabe

```
./iperf -s -w <win_size>
```

So richten Sie `iperf` auf dem Ursprung ein und führen das Werkzeug aus:

1 Mounten Sie das LRD-ISO mithilfe von Software oder physischen Medien.

2 Öffnen Sie die Eingabeaufforderung (Windows) oder das Terminal (Linux) und wechseln Sie in das Verzeichnis des iPerf-Werkzeugs:

```
cd <media>/LRDTools/iperf_2.0.X/
```

3 Wechseln Sie je nach Ihrem Ursprungs-Betriebssystem entweder in das Unterverzeichnis `windows` oder `linux`:

```
cd windows
```

```
-OR-
```

```
cd linux
```

4 Führen Sie das iPerf-Werkzeug im Clientmodus aus. Eingabe

```
iperf -c <target_ip> -w <win_size>
```

HINWEIS: Sie können `iperf3` herunterladen und für Berechnungen verwenden. Dies ist in bestimmten Szenarien hilfreich, in denen `iperf2` keine nützlichen Durchsatzzahlen generieren kann. Trotz der etwas anderen Befehlssyntax und Ausgabe von `iperf3` sollten die Anpassung und die Auslegung der neueren Ausgabe, falls nötig, keine Schwierigkeiten bereiten.

F.4 Methode

Führen Sie beginnend mit der im Abschnitt Berechnungen ermittelten `win_size` mehrere Iterationen des iPerf-Werkzeugs aus, wobei Sie sowohl den berechneten Wert als auch etwas größere und etwas kleinere Werte verwenden, und zeichnen Sie die Ausgaben auf. Es wird empfohlen, `win_size` in Inkrementen von etwa 10 % des Originalwerts zu erhöhen und zu verringern.

Im obigen Beispiel mit 1.280.000 Byte verringern oder erhöhen Sie `win_size` in Inkrementen von 100.000 Byte.

HINWEIS: Die Option `-w` von `iperf` ermöglicht die Angabe von Einheiten wie K (Kilobyte) oder M (Megabyte).

Ausgehend vom gleichen Beispiel können Sie mit `-w` in Schritt 4 für `win_size` die Werte `1,28M`, `1,38M`, `1,18M` verwenden. Natürlich wird angenommen, dass bei jeder Iteration des iPerf-Werkzeugs nur der Schritt der Ausführung wiederholt wird.

Die Ausgabe einer iperf-Client-Iteration kann beispielsweise wie folgt aussehen:

```
iperf.exe -c 10.10.10.232 -w 1.1M

------------------------------------------------------------
Client connecting to 10.10.10.232, TCP port 5001
TCP window size: 1.10 MByte
------------------------------------------------------------
[296] local 10.10.10.224 port 64667 connected with 10.10.10.232 port 5001
[ ID] Interval       Transfer     Bandwidth
[296]  0.0-10.2 sec  11.3 MBytes  9.29 Mbits/sec
```

Die Ausgabe vom referenzierten Zielserver kann beispielsweise wie folgt aussehen:

```
./iperf -s -w .6M

------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 1.20 MByte (WARNING: requested 614 Kbyte)
------------------------------------------------------------
[  4] local 10.10.10.232 port 5001 connected with 10.10.10.224 port 64667
[  4] 0.0-10.2 sec  11.3 MBytes  9.29 Mbits/sec
```

HINWEIS:

- Der Client wird nach einer einzigen Iteration vom Server getrennt, während der Server die Überwachung fortsetzt, bis Sie zum Anhalten Strg-C drücken.
- Die für einen Linux-Server angegebene Fenstergröße entspricht der Hälfte des gewünschten Werts, da Linux die angeforderte TCP-Puffergröße automatisch verdoppelt.

Verwenden Sie mehrere Iterationen, um den optimalen Wert der TCP-Fenstergröße zu bestimmen. Denken Sie daran, nur die Hälfte des gewünschten Werts anzugeben, wenn Sie die Option `-w` zusammen mit `iperf` für Linux verwenden.

Ein höherer Durchsatz ist ein Hinweis darauf, dass Sie sich der optimalen TCP-Fenstergröße nähern. Während Sie dem optimalen Wert näherkommen, verwenden Sie längere Iterationen, um die realen Bedingungen genauer zu simulieren. Um längere Iterationen zu erzielen, geben Sie die Option `-t` <*`Zeit_in_Sekunden`*> für `iperf` an. Diese Option muss nur auf der Client-Seite angegeben werden.

Beispiel:

```
iperf.exe -c 10.10.10.232 -w 1.25M -t 60
```

Sobald Sie einen optimalen Wert ermittelt haben, konfigurieren Sie ihn im Parameter `FileTransferSendReceiveBufferSize` für den entsprechenden PlateSpin-Server unter:

https://<*mein_ps_server*>/PlatespinConfiguration/

Dieser globale Wert wird für alle Workloads auf dem PlateSpin-Server verwendet, sodass die Gruppierung der Workloads und ihrer jeweiligen Netzwerke auf den verfügbaren PlateSpin-Servern sorgfältig überlegt werden muss.

F.5 Erwartungen

Das indirekte Ändern der TCP-Fenstergröße mithilfe der TCP-Puffergröße zum Senden/Empfangen kann in einigen Szenarien eine sehr wirkungsvolle Methode zur Erhöhung des Netzwerkdurchsatzes sein. In manchen Fällen kann das Zwei- bis Dreifache des Originaldurchsatzes oder sogar noch mehr

erreicht werden. Es muss jedoch berücksichtigt werden, dass sich die Netzwerkmerkmale im Laufe der Zeit ändern (können), da sich die Netzwerkauslastungsmuster, Hardware, Software oder andere Infrastruktur ändert.

Es wird dringend empfohlen, dass Sie diese Methode zur gleichen Tageszeit und unter den gleichen Netzwerkauslastungsbedingungen wie bei der geplanten Live-Migration oder -Reproduktion verwenden, um den optimalen Wert zu berechnen. Es ist außerdem ratsam, die Einstellung regelmäßig neu zu berechnen, da sich die Netzwerkbedingungen ändern.