PlateSpin Forge® 11.2

Benutzerhandbuch

Oktober 2015

www.netiq.com/documentation

Rechtliche Hinweise

Lizenzerteilung

Die für PlateSpin Forge 11 oder neuere Versionen erworbenen Lizenzen können nicht für PlateSpin Forge 3.3 oder Vorgängerversionen verwendet werden.

Software von Drittanbietern

Weitere Informationen zu Software von Drittanbietern, die in PlateSpin Forge verwendet wird, finden Sie auf der Seite zu *Nutzung und Copyright für Drittanbieter-Lizenzen in PlateSpin (https://www.netiq.com/documentation/platespin_licensing/platespin_licensing_qs/data/platespin_licensing_qs.html)*.

Inhalt

Info zu diesem Handbuch und zur Bibliothek

Dieses *Benutzerhandbuch* enthält Informationen zur Verwendung von PlateSpin Forge. Hier finden Sie allgemeine Informationen, einen Überblick der Benutzeroberflächen und Schritt-für-Schritt-Anweisungen für häufig anfallende Aufgaben. Ferner sind Terminologiedefinitionen und Informationen zur Fehlerbehebung enthalten.

Zielgruppe

Dieses Dokument ist für IT-Mitarbeiter wie Rechenzentrumsadministratoren und -operatoren vorgesehen, die PlateSpin Forge in Workload-Schutzprojekten verwenden.

Informationen in der Bibliothek

Die Bibliothek für dieses Produkt finden Sie im HTML- und PDF-Format auf der Dokumentations-Website zu PlateSpin Forge (https://www.netiq.com/documentation/platespin-forge/). Die Online-Dokumentation steht in den Sprachen Chinesisch (vereinfacht), Chinesisch (traditionell), Deutsch, Englisch, Französisch, Japanisch und Spanisch zur Verfügung.

Die PlateSpin Forge-Bibliothek enthält folgende Informationsressourcen:

Versionshinweise

Informationen zu neuen Funktionen und Verbesserungen in der Version sowie zu bekannten Problemen.

Handbuch „Erste Schritte“

Informationen zum Konfigurieren der Appliance für Ihre Umgebung.

Benutzerhandbuch

Allgemeine Informationen, Überblick der Benutzeroberflächen und Schritt-für-Schritt-Anweisungen für häufig anfallende Aufgaben.

Handbuch zum Neuaufbauen

Informationen zum Neuaufbauen und Neukonfigurieren der Appliance.

Aufrüstungshandbuch

Informationen zum Aufrüsten der Appliance-Software.

Zusätzliche Ressourcen

Wir empfehlen Ihnen, die folgenden zusätzlichen Online-Ressourcen zu nutzen:

- PlateSpin Forge-Forum (https://forums.netiq.com/forumdisplay.php?56-Platespin-Forge): Web-Community mit Produktbenutzern, in der Sie die Funktionen von NetIQ-Produkten diskutieren und Ratschläge von anderen Produktbenutzern erhalten können.
- PlateSpin Forge-Produktseite (https://www.netiq.com/products/forge/): Webgestützte Produktbroschüre mit Informationen zu den Funktionen, Angaben zum Bestellvorgang, technischen Daten, häufig gestellten Fragen und zahlreichen Ressourcen wie Videos und Whitepaper.
- NetIQ User Community (https://www.netiq.com/communities/): Eine webbasierte Community mit verschiedenen Diskussionsthemen.
- NetIQ Support-Knowledgebase (https://www.netiq.com/support/kb/): Eine Sammlung ausführlicher technischer Artikel.
- NetIQ Support-Foren (https://forums.netiq.com/forum.php): Website, auf der die Produktbenutzer die Funktionen von NetIQ-Produkten diskutieren und Ratschläge von anderen Produktbenutzern erhalten können.
- MyNetIQ (https://www.netiq.com/f/mynetiq/): Website mit Informationen und Services, beispielsweise Zugriff auf wichtige Whitepaper, Webcast-Registrierung und Testversionen zum Herunterladen.

Info zu NetIQ Corporation

NetIQ ist ein globaler Hersteller von Unternehmenssoftware. Unser Blickpunkt liegt auf drei besonderen Herausforderungen, die Sie in Ihrer Umgebung meistern müssen: Änderungen, Komplexität und Risiken. Unser Ziel ist es, Sie dabei zu unterstützen.

Unser Standpunkt

Sich an Änderungen anzupassen und Komplexität und Risiken zu beherrschen ist nichts Neues

Unter den verschiedenen Herausforderungen, denen Sie gegenüberstehen, beeinflussen diese drei Punkte sicherlich am meisten Ihre Möglichkeiten, Ihre physischen, virtuellen und Cloud-Umgebungen sicher zu messen, zu überwachen und zu verwalten.

Kritische Geschäftsservices schneller und besser bereitstellen

Wir sind davon überzeugt, dass IT-Organisationen über eine möglichst große Kontrolle verfügen müssen, um eine zeitgerechte und kostenwirksame Servicebereitstellung zu ermöglichen. Der von Änderungen und Komplexität ausgehende, kontinuierliche Druck steigt ständig, weil sich die Unternehmen ständig ändern und die erforderlichen Technologien zur Verwaltung der Änderungen immer komplexer werden.

Unsere Philosophie

Intelligente Lösungen entwickeln, nicht einfach Software

Um zuverlässige Lösungen für die Kontrolle anbieten zu können, stellen wir erst einmal sicher, dass wir das Szenario, in dem Unternehmen wie das Ihre täglich arbeiten, gründlich verstehen. Nur so können wir praxistaugliche, intelligente IT-Lösungen entwickeln, die nachweisbar messbare Ergebnisse liefern. Und das ist für uns wesentlich bereichernder, als einfach eine Software zu verkaufen.

Ihr Erfolg ist unsere Leidenschaft

Ihr Erfolg ist der Wegweiser für unser Geschäft. Wir wissen, dass Sie von der Produktkonzeption bis hin zur Bereitstellung IT-Lösungen benötigen, die richtig funktionieren und nahtlos mit Ihren vorhandenen Investitionen integriert werden können. Sie benötigen fortlaufenden Support, Schulungen nach der Bereitstellung und jemanden, mit dem Sie unkompliziert arbeiten können. Ihr Erfolg ist auch unser Erfolg.

Unsere Lösungen

- Identitäts- und Zugriffsregelung
- Zugriffsverwaltung
- Sicherheitsverwaltung
- System- und Anwendungsverwaltung

- Workload-Management
- Serviceverwaltung

Anfragen an die Verkaufsunterstützung

Bei Fragen zu Produkten, Preisen und Funktionen wenden Sie sich an Ihren Händler vor Ort. Wenn dies nicht möglich ist, wenden Sie sich an unser Verkaufsunterstützungsteam.

Weltweit:	www.netiq.com/about_netiq/officelocations.asp
Vereinigte Staaten und Kanada:	1-888-323-6768
Email:	info@netiq.com
Website:	www.netiq.com

Kontakt zum technischen Support

Bei spezifischen Produktproblemen wenden Sie sich bitte an unseren technischen Support.

Weltweit:	www.netiq.com/support/contactinfo.asp
Nord- und Südamerika:	1-713-418-5555
Europa, Naher Osten und Afrika:	+353 (0) 91-782 677
Email:	support@netiq.com
Website:	www.netiq.com/support

Im *Handbuch zum technischen Support* (https://www.netiq.com/Support/process.asp#_Maintenance_Programs_and) finden Sie weitere Informationen zu den Services und Verfahren des NetIQ-Supports.

Kontakt zum Dokumentationssupport

Wir möchten Ihnen stets eine nützliche, aussagekräftige Dokumentation an die Hand geben. Die Dokumentation für dieses Produkt steht auf der Website der PlateSpin Forge-Dokumentation (https://www.netiq.com/documentation/platespin-forge/) im HTML- und PDF-Format zur Verfügung.

Wenn Sie uns einen Verbesserungsvorschlag in Bezug auf die Dokumentation mitteilen möchten, nutzen Sie die Schaltfläche **comment on this topic** (Kommentar zum Thema abgeben), die unten auf jeder Seite der HTML-Version der Dokumentation verfügbar ist. Sie können Verbesserungsvorschläge auch per Email an Documentation-Feedback@netiq.com senden. Wir freuen uns auf Ihre Rückmeldung.

Kontakt zur Online-Benutzer-Community

NetIQ Communities, die NetIQ-Online-Community, ist ein Netzwerk zur Zusammenarbeit mit anderen NetIQ-Benutzern und -Experten. NetIQ Communities bietet Ihnen aktuelle Informationen, nützliche Links zu hilfreichen Ressourcen und Kontakt zu NetIQ-Experten, damit Sie über alle Voraussetzungen verfügen, um das meiste aus den IT-Investitionen zu holen, auf die Sie sich verlassen. Weitere Informationen hierzu finden Sie im Internet unter http://community.netiq.com.

1 Planen der PlateSpin-Umgebung

Bei PlateSpin Forge handelt es sich um eine konsolidierte Hardware-Appliance zur Wiederherstellung, die mithilfe integrierter Virtualisierungstechnologie sowohl physische als auch virtuelle Workloads (Betriebssysteme, Middleware und Daten) schützt. Kommt es zu einer Katastrophe oder zum Ausfall eines Produktionsservers, werden Workloads von der PlateSpin Forge-Recovery-Umgebung schnell aufgefangen und bis zur Wiederherstellung der Produktionsumgebung völlig normal ausgeführt.

PlateSpin Forge bietet folgende Vorteile:

- Schnelle Wiederherstellung von Workloads nach einem Fehler
- Schutz von mehreren Workloads gleichzeitig (10 bis 50, modellabhängig)
- 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

Mit seinem internen Speicher verfügt Forge über eine Gesamtspeicherkapazität von 20 Terabyte. Allerdings lässt sich die Kapazität durch Verwendung von externen Speicherkonfigurationen, wie iSCSI- oder Fibre-Channel-Karten, nahezu unbegrenzt erweitern.

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

- Abschnitt 1.1, „Unterstützte Konfigurationen“ auf Seite 13
- Abschnitt 1.2, „Sicherheit und Datenschutz“ auf Seite 20
- Abschnitt 1.3, „Leistung“ auf Seite 23

1.1 Unterstützte Konfigurationen

PlateSpin Forge unterstützt Server-Workloads zum Schutz der 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 Forge 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 Forge 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.

- Abschnitt 1.1.1, „Unterstützte Windows-Workloads“ auf Seite 14
- Abschnitt 1.1.2, „Unterstützte Linux-Workloads“ auf Seite 17
- Abschnitt 1.1.3, „Unterstützte VM-Container“ auf Seite 18
- Abschnitt 1.1.4, „Unterstützte System-Firmware“ auf Seite 19
- Abschnitt 1.1.5, „Unterstützter Speicher“ auf Seite 19
- Abschnitt 1.1.6, „Unterstützte Browser für die PlateSpin Forge-Weboberfläche“ auf Seite 19

1.1.1 Unterstützte Windows-Workloads

PlateSpin Forge unterstützt Workloads für die meisten Versionen von Microsoft Windows. Eine Liste der unterstützten Windows-Versionen finden Sie unter Tabelle 1-1.

Sowohl die Reproduktionen auf Dateiebene als auch die auf Blockebene werden unterstützt, mit bestimmten Einschränkungen. Weitere Informationen hierzu finden Sie unter Abschnitt 6.3, „Datenübertragung“ auf Seite 92.

Tabelle 1-1 *Unterstützte Windows-Workloads*

Betriebssystem	Notizen
Serverklassen-Workloads	
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.
Serverbasierte Cluster-Workloads	

Betriebssystem	Notizen
Auf Windows Server 2012 R2 basierender Microsoft-Failover-Cluster	Die folgenden Cluster-Technologien werden unterstützt: Modelle *Knoten- und Datenträgermehrheits-Quorum* und *Keine Mehrheit: Quorum nur für Datenträger*. Nur blockbasierte Übertragung.
Auf Windows Server 2008 R2 basierender Microsoft-Failover-Cluster	Die folgenden Cluster-Technologien werden unterstützt: Modelle *Knoten- und Datenträgermehrheits-Quorum* und *Keine Mehrheit: Quorum nur für Datenträger*. Nur blockbasierte Übertragung.
Auf Windows Server 2003 R2 basierender Windows-Cluster-Server	Die folgende Clustering-Technologie wird unterstützt: Modell *Single-Quorum Device Cluster*. Nur blockbasierte Übertragung.
Hypervisor-Klassen-Workloads	
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.
Arbeitsstationsklassen-Workloads	
Windows 8.1 Windows 8	**WARNUNG:** Sie müssen den Energiesparplan **Hohe Leistung** an der Windows 8-Quelle auswählen, damit die Workload-Failover- und -Failback-Funktion korrekt funktioniert. So konfigurieren Sie diesen Energiesparplan in der Windows-Systemsteuerung: 1. Wählen Sie **Alle Systemsteuerungselemente > Energieoptionen**. 2. Wählen Sie im Dialogfeld **Energiesparplan wählen oder anpassen** die Optionen **Weitere Energiesparpläne einblenden > Hohe Leistung**. 3. Schließen Sie die Systemsteuerung.
Windows 7	Nur Professional, Enterprise und Ultimate Editions.

Unterstützte Windows-Dateisysteme

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

Unterstützte Windows-Cluster

Weitere Informationen zum Schutz von Workloads in einem unterstützten Cluster finden Sie unter „Schützen von Windows-Clustern“ auf Seite 105. Falls lokaler Speicher auf Clusterknoten vorliegt, beachten Sie auch „Synchronisieren von Seriennummern im lokalen Clusterknoten-Speicher“ auf Seite 143.

Unterstützte internationale Versionen

PlateSpin Forge unterstützt Versionen von Microsoft Windows in den Sprachen Französisch, Deutsch, Japanisch, Chinesisch (traditionell) und Chinesisch (vereinfacht). Weitere Informationen hierzu finden Sie unter „Konfigurieren der Spracheinstellungen bei internationalen Versionen von PlateSpin Forge“ auf Seite 41.

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

Unterstützung für Workload-Firmware (UEFI und BIOS)

PlateSpin Forge spiegelt die Microsoft-Unterstützung für UEFI- oder BIOS-basierte Windows-Workloads wider. Es überträgt Workloads (sowohl Block- als auch Dateitransfers werden unterstützt) von der Quelle an das Ziel und erzwingt die unterstützte Firmware für die entsprechende Quelle bzw. das Ziel und die Zielbetriebssysteme. Dies gilt auch für das Failback auf einen physischen Computer. Sobald ein Übergang (Failover oder Failback) zwischen UEFI- und BIOS-Systemen eingeleitet wird, analysiert Forge diesen Übergang, und Sie erhalten eine Mitteilung über dessen Gültigkeit.

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

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

- Beim Übertragen eines UEFI-basierten Workloads auf einen Container mit VMware vSphere 4.*x* (der UEFI nicht unterstützt), führt Forge 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 Forge den Firmware-Übergang von BIOS zu UEFI wieder um.
- Wenn Sie versuchen, ein Failback eines geschützten Windows 2003-Workloads auf einen UEFI-gestützten physischen Computer vorzunehmen, analysiert Forge die Auswahl und informiert Sie, dass dieser Vorgang nicht gültig ist. (Der Firmware-Übergang von BIOS zu UEFI wird nicht unterstützt, da Windows 2003 den UEFI-Startmodus nicht unterstützt).
- Beim Schützen eines UEFI-basierten Ursprungs auf einem BIOS-basierten Ziel migriert Forge 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.

Unterstützung für komplexe Workload-Festplattenpartitionierung

Neben dem MBR-Partitionierungsschema unterstützt PlateSpin Forge die GPT-Partitionierung von Festplatten für Windows-Workloads. Die vollständige Reproduktion wird für bis zu 57 Partitionen oder Volumes auf einer einzigen Festplatte unterstützt.

Windows Update

Aktualisieren Sie in jedem Fall Windows (Windows-Update) auf Ihrem Quellsystem, bevor Sie die erste vollständige Reproduktion ausführen. 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 Forge unterstützt eine Anzahl von Linux-Distributionen. Eine Liste der unterstützten Linux-Betriebssysteme finden Sie in Tabelle 1-2.

Die Reproduktion von geschützten Linux-Workloads erfolgt ausschließlich auf Blockebene. Weitere Informationen hierzu finden Sie unter „Anforderung eines blkwatch-Treibers“ auf Seite 18.

Tabelle 1-2 *Unterstützte Linux-Workloads*

Betriebssystem	Notizen
Linux-Serverklassen-Workloads	
Red Hat Enterprise Linux (RHEL) 7 Red Hat Enterprise Linux 6 Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 4	Eine Liste der unterstützten Linux-Kernelversionen und Architekturen für RHEL-Distributionen finden Sie in „Von Forge unterstützte Linux-Verteilungen“ auf Seite 139.
SUSE Linux Enterprise Server (SLES) 11 SUSE Linux Enterprise Server 10 SUSE Linux Enterprise Server 9	Eine Liste der unterstützten Linux-Kernelversionen und Architekturen für SLES-Distributionen finden Sie in „Von Forge unterstützte Linux-Verteilungen“ auf Seite 139. **HINWEIS:** 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.
Novell Open Enterprise Server (OES) 11 Novell Open Enterprise Server 2	PlateSpin Forge unterstützt Workloads für eine OES-2- oder OES-11-Version, wenn diese auf einer unterstützten SLES-Distribution beruht (sofern nicht anderweitig angegeben). Eine Liste der unterstützten Linux-Kernelversionen und Architekturen für SLES-Distributionen finden Sie in „Von Forge unterstützte Linux-Verteilungen“ auf Seite 139. **HINWEIS:** 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 Enterprise Linux (OEL)	PlateSpin Forge unterstützt Workloads für eine OEL-Version, wenn diese auf einer unterstützten RHEL-Distribution beruht (sofern nicht anderweitig angegeben). Eine Liste der unterstützten Linux-Kernelversionen und Architekturen für RHEL-Distributionen finden Sie in „Von Forge unterstützte Linux-Verteilungen“ auf Seite 139. **HINWEIS:** Workloads, die den Unbreakable Enterprise Kernel verwenden, werden nicht unterstützt.
CentOS 7 CentOS 6 CentOS 5 CentOS 4	PlateSpin Forge unterstützt Workloads für eine CentOS-Version, wenn diese auf einer unterstützten RHEL-Distribution beruht. Eine Liste der unterstützten Linux-Kernelversionen und Architekturen für RHEL-Distributionen finden Sie in „Von Forge unterstützte Linux-Verteilungen“ auf Seite 139.

Unterstützte Linux-Dateisysteme

PlateSpin Forge unterstützt die Dateisysteme EXT3, EXT4, EXT2, REISERFS, XFS und NSS (OES-2- und OES-11-Workloads) jeweils nur mit blockbasierter Übertragung.

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

Unterstützung für Workload-Firmware (UEFI und BIOS)

PlateSpin Forge unterstützt Benutzeroberflächen mit UEFI- und BIOS-Firmware.

Unterstützung für komplexe Workload-Festplattenpartitionierung

Neben dem MBR-Partitionierungsschema unterstützt PlateSpin Forge die GPT-Partitionierung von Festplatten für Linux-Workloads. Die vollständige Reproduktion wird für bis zu 57 Partitionen oder Volumes auf einer einzigen Festplatte unterstützt.

Anforderung eines `blkwatch`-Treibers

Zur blockbasierten Datenübertragung für einen Linux-Workload in PlateSpin Forge ist ein `blkwatch`-Treiber erforderlich, der speziell für die zu schützende Linux-Distribution kompiliert ist. Die PlateSpin Forge-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 Forge unterstützte Linux-Verteilungen“ auf Seite 139.

1.1.3 Unterstützte VM-Container

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

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

Container	Anmerkungen
VMware ESXi 6.0	◆ Unterstützt als Schutz- und Failback-Container. ◆ Die DRS-Konfiguration muss entweder **Teilweise automatisiert** oder **vollautomatisch** sein (sie darf nicht auf **Manuell** gesetzt sein). ◆ Als VM-Container darf der DRS-Cluster nur aus ESXi 6.0-Servern bestehen und kann nur von vCenter 6.0 verwaltet werden.
VMware ESXi 5.5 (GA2, Update 2)	◆ Unterstützt als Schutz- und Failback-Container. ◆ Die DRS-Konfiguration muss entweder **Teilweise automatisiert** oder **vollautomatisch** sein (sie darf nicht auf **Manuell** gesetzt sein). ◆ Als VM-Container darf der DRS-Cluster nur aus ESXi 5.5-Servern bestehen und kann nur von vCenter 5.5 verwaltet werden.
VMware ESXi 5.1 (GA2, Update 2)	◆ Unterstützt als Schutz- und Failback-Container. ◆ Die DRS-Konfiguration muss entweder **Teilweise automatisiert** oder **vollautomatisch** sein (sie darf nicht auf **Manuell** gesetzt sein). ◆ Als VM-Container darf der DRS-Cluster nur aus ESXi 5.1-Servern bestehen und kann nur von vCenter 5.1 verwaltet werden.

Container	Anmerkungen
VMware ESXi 4.1 (GA2, Update 3)	◆ Unterstützt als Schutz- und Failback-Container. ◆ Die DRS-Konfiguration muss entweder **Teilweise automatisiert** oder **vollautomatisch** sein (sie darf nicht auf **Manuell** gesetzt sein). ◆ Als VM-Container darf der DRS-Cluster nur aus ESXi 4.1-Servern bestehen und kann nur von vCenter 4.1 verwaltet werden.

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

1.1.4 Unterstützte System-Firmware

PlateSpin Forge unterstützt Benutzeroberflächen mit UEFI- und BIOS-Firmware.

Auf Windows-Systemen spiegelt PlateSpin Forge die Microsoft-Unterstützung für UEFI wider. Weitere Informationen finden Sie unter Unterstützung für Workload-Firmware (UEFI und BIOS) in „Unterstützte Windows-Workloads“ auf Seite 14.

1.1.5 Unterstützter Speicher

Die Workloads und der Speicher für den Schutz müssen auf Festplatten konfiguriert werden, die mit dem MBR- (Master Boot Record) oder dem GPT-Partitionierungsschema (GUID Partition Table) partitioniert wurden. Bei GPT sind bis zu 128 Partitionen pro Festplatte zulässig; PlateSpin Forge unterstützt jedoch nur maximal 57 GPT-Partitionen pro Festplatte.

PlateSpin Forge unterstützt mehrere Speichertypen, darunter einfache Festplatten, dynamische Windows-Datenträger, LVM (nur Version 2), RAID und SAN.

Bei Linux-Workloads bietet PlateSpin Forge folgende zusätzlichen Funktionen:

- Nicht-Volume-Speicher wie eine Swap-Partition, die mit dem Ursprungs-Workload verknüpft ist, werden im Failover-Workload neu erstellt.
- Das Layout der Volume-Gruppen und logischen Volumes wird beibehalten, sodass Sie es während des Failbacks neu erstellen können.
- (OES-11-Workloads) NLVM-Layouts (Novell Linux Volume Management) von Ursprungs-Workloads werden beibehalten und im Appliance-Host neu erstellt. NSS-Pools werden vom Ursprung in die Wiederherstellungs-VM kopiert.
- (OES 2-Workloads) EVMS-Layouts von Ursprungs-Workloads werden beibehalten und im Appliance-Host neu erstellt. NSS-Pools werden vom Ursprung in die Wiederherstellungs-VM kopiert.

1.1.6 Unterstützte Browser für die PlateSpin Forge-Weboberfläche

Die meisten Aktionen mit dem Produkt führen Sie über die browserbasierte PlateSpin Forge-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.

So aktivieren Sie JavaScript:

- **Chrome:**
  1. Wählen Sie im Chrome-Menü den Befehl **Einstellungen**, blättern Sie zum Link **Erweiterte Einstellungen** und klicken Sie darauf.
  2. Klicken Sie unter **Datenschutz** auf **Inhaltseinstellungen**.
  3. Blättern Sie zum Eintrag **JavaScript** und wählen Sie **Ausführung von JavaScript für alle Websites zulassen**.
  4. Klicken Sie auf **Fertig**.
- **Firefox:**
  1. Geben Sie `about:config` in die Adressleiste ein und drücken Sie die Eingabetaste.
  2. Klicken Sie auf **Ich werde vorsichtig sein, versprochen!**.
  3. Geben Sie in das Feld **Suchen** die Zeichenfolge `javascript.enabled` ein und drücken Sie die Eingabetaste.
  4. Prüfen Sie in den Suchergebnissen den Wert für den Parameter `javascript.enabled`. Wenn der Wert `false` vorliegt, klicken Sie mit der rechten Maustaste auf `javascript.enabled` und wählen Sie **Umschalten**. Der Wert wechselt zu `true`.
- **Internet Explorer:**
  1. Wählen Sie im Menü „Extras“ den Befehl **Internetoptionen**.
  2. Wählen Sie das Register **Sicherheit** und klicken Sie auf **Stufe anpassen**.
  3. Blättern Sie zum Eintrag **Skripting > Active Scripting** und wählen Sie **Aktivieren**.
  4. Klicken Sie in der Warnmeldung auf **Ja** und klicken Sie dann auf **OK**.
  5. Klicken Sie auf **Anwenden** > **OK**.

Informationen zur Verwendung der PlateSpin Forge-Weboberfläche und der integrierten Hilfe in einer der unterstützten Sprachen finden Sie unter „Konfigurieren der Spracheinstellungen bei internationalen Versionen von PlateSpin Forge“ auf Seite 41.

1.2 Sicherheit und Datenschutz

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

1.2.1 Sicherheit der Workload-Daten bei 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 78.

1.2.2 Sicherheit der Client-Server-Kommunikation

Da der PlateSpin-Server SSL auf der Forge-VM aktiviert, ist die sichere Datenübertragung zwischen Ihrem Webbrowser und dem PlateSpin-Server bereits auf HTTPS (Hypertext Transfer Protocol Secure) konfiguriert.

1.2.3 Sicherheit von Berechtigungsnachweisen

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

1.2.4 Benutzerautorisierung und -authentifizierung

PlateSpin Forge 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 unter „Konfigurieren der Benutzerautorisierung und -authentifizierung“ auf Seite 29.

1.2.5 Einstellungen für Netzwerk-Ports

Tabelle 1-4 zeigt eine Liste der Standard-Ports in PlateSpin Forge. Wenn Sie benutzerdefinierte Ports konfigurieren, müssen Sie entsprechend diese individuellen Ports öffnen. Für die Kommunikation zwischen dem PlateSpin Forge-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). Weitere Informationen zum Konfigurieren des Netzwerkzugriffs für die PlateSpin-Server-Umgebung finden Sie in „Konfigurieren der Zugriffs- und Kommunikationseinstellungen im gesamten Schutznetzwerk“ auf Seite 34.

Tabelle 1-4 Standard-Ports in PlateSpin Forge

Portnummer	Protokoll	Funktionsweise	Details
80	TCP	HTTP	(Nicht sicher) Für die HTTP-Kommunikation zwischen der Forge-VM und den verwalteten Ursprungs- und Zielcomputern. Öffnen Sie diesen Port auf der Forge-VM, im Ursprungs- und Ziel-Workload sowie auf den VMware-ESXi-Hosts.
443	TCP	HTTPS	(Sicher) Für die HTTPS-Kommunikation zwischen der Forge-VM und den Ursprungs- und Zielcomputern, wenn SSL aktiviert ist. Öffnen Sie diesen Port auf der Forge-VM, 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 der Forge-VM 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 17.
25	TCP	SMTP	Für den SMTP-Datenverkehr, wenn die E-Mail-Benachrichtigung deaktiviert ist. Öffnen Sie diesen Port auf der Forge-VM 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 der Forge VM 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 Admin-Verbindung 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.

1.2.6 Zusätzliche Sicherheitsverbesserungen

Im Knowledgebase-Artikel 7015818 (https://www.netiq.com/support/kb/doc.php?id=7015818) finden Sie Informationen, wie Sie die Angreifbarkeit durch potenzielle POODLE-Angriffe (Padding Oracle On Downgraded Legacy Encryption) von Ihren PlateSpin-Servern beseitigen.

1.3 Leistung

1.3.1 Allgemeines zu Produktleistungsmerkmalen

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

- Hardware- und Softwareprofile Ihrer Ursprungs-Workloads
- Hardware- und Softwareprofile Ihrer Ziel-Container
- 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.

1.3.2 Datenkomprimierung

Falls erforderlich, kann PlateSpin Forge 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 95.

1.3.3 Bandbreitendrosselung

In PlateSpin Forge können Sie die Menge an Netzwerkbandbreite, die im Verlauf eines Workload-Schutzes durch die direkte Ursprung-zu-Ziel-Kommunikation verbraucht wird, steuern. Sie können für jeden Schutzvertrag 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 95.

1.3.4 RPO-, RTO- und TTO-Spezifikationen

- **Angestrebter Wiederherstellungszeitpunkt (RPO):** Beschreibt die akzeptable Menge an Datenverlust, gemessen in Zeit. Der RPO ermittelt sich aus der Zeit zwischen den inkrementellen Reproduktionen eines geschützten Workloads und wird vom aktuellen Nutzungsumfang von PlateSpin Forge, der Rate und dem Ausmaß von Änderungen im Workload sowie von der Netzwerkgeschwindigkeit und dem gewählten Reproduktionszeitplan beeinflusst.
- **Angestrebte Wiederherstellungszeit (RTO):** Beschreibt die Zeit, die für einen Failover-Vorgang (einen Failover-Workload in den Online-Modus versetzen, um einen geschützten Produktions-Workload vorübergehend zu ersetzen) benötigt wird.

  Die für einen Failover eines Workloads auf dessen virtuelle Reproduktion benötigte RTO wird von der Zeit beeinflusst, die für das Konfigurieren und Ausführen des Failover-Vorgangs benötigt wird (10 bis 45 Minuten). Weitere Informationen hierzu finden Sie unter „Failover“ auf Seite 82.
- **Angestrebte Testzeit (TTO):** Beschreibt die Zeit, die zum Testen des Wiederherstellungsplans benötigt wird, damit der Dienst erfolgreich wiederhergestellt werden kann.

  Verwenden Sie die Funktion **Failover testen**, um verschiedene Szenarien zu durchlaufen und Vergleichsdaten zu generieren. Weitere Informationen hierzu finden Sie unter „Verwenden der Funktion „Failover testen““ auf Seite 84.

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

Führen Sie zum Ermitteln der durchschnittlichen Failover-Zeiten für Workloads in Ihrer Umgebung Test-Failovers zu unterschiedlichen Zeiten durch und verwenden Sie sie als Vergleichsdaten in Ihren Gesamtwiederherstellungsplänen. Weitere Informationen hierzu finden Sie unter „Generieren von Workload- und Workload-Schutz-Berichten“ auf Seite 72.

1.3.5 Skalierbarkeit

Die Skalierbarkeit hängt von den folgenden Hauptmerkmalen Ihres PlateSpin Forge-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.

2 PlateSpin Forge-Anwendungskonfiguration

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

2.1 Starten der PlateSpin Forge-Weboberfläche

Informationen zur Verwendung der PlateSpin Forge-Weboberfläche und der integrierten Hilfe in einer der unterstützten Sprachen finden Sie unter „Konfigurieren der Spracheinstellungen bei internationalen Versionen von PlateSpin Forge“ auf Seite 41.

So starten Sie die PlateSpin Forge-Weboberfläche:

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

   `https://`*<Hostname | IP-Adresse>*`/Forge`

   Ersetzen Sie *<Hostname | IP-Adresse>* durch den DNS-Hostnamen bzw. die IP-Adresse Ihrer Forge-VM.

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

   Wenn Sie sich zum ersten Mal bei PlateSpin Forge anmelden, wird der Browser automatisch zur Seite für die Lizenzaktivierung umgeleitet.

2. Melden Sie sich mit den standardmäßigen Berechtigungsnachweisen für die Forge-VM an.

Die standardmäßigen Berechtigungsnachweise für die Forge-Management-VM umfassen den Benutzernamen `Administrator` und das Passwort `Password1`. Zum Ändern des Administratorbenutzer-Passworts können Sie sich im Remote-Verfahren am Windows-Desktop anmelden und das neue Passwort mit den Windows-Verwaltungstools festlegen.

Weitere Informationen zum Einrichten zusätzlicher Benutzer für PlateSpin finden Sie unter Abschnitt 2.3, „Konfigurieren der Benutzerautorisierung und -authentifizierung“ auf Seite 29.

2.2 Aktivieren Ihrer Produktlizenz

Die PlateSpin Forge-Produktlizenz berechtigt Sie zu einer bestimmten oder auch unbegrenzten Anzahl von Workloads zum Schutz durch die Workload-Lizenzierung. Weitere Informationen finden Sie unter Abschnitt 6.1, „Workload-Lizenzverbrauch“ auf Seite 91.

Für die Produktlizenzierung von PlateSpin Forge benötigen Sie einen Lizenzaktivierungscode. Falls Sie nicht über einen Lizenzaktivierungscode verfügen, können Sie diesen beim Customer Center (http://www.netiq.com/customercenter/) anfordern. Sie erhalten dann eine Email mit einem Lizenzaktivierungscode.

HINWEIS: Wenn Sie bereits PlateSpin-Kunde sind und kein Customer Center-Konto haben, müssen Sie zunächst eins mit derselben E-Mail-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.

- Abschnitt 2.2.1, „Online-Lizenzaktivierung“ auf Seite 28
- Abschnitt 2.2.2, „Offline-Lizenzaktivierung“ auf Seite 29

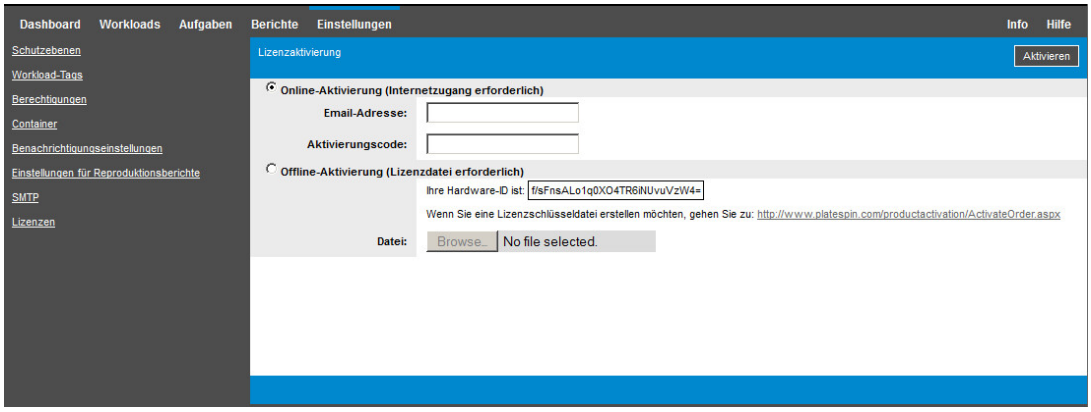
2.2.1 Online-Lizenzaktivierung

Für die Online-Aktivierung von PlateSpin Forge 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 PlateSpin Forge-Weboberfläche auf **PlateSpin Forge-Lizenz hinzufügen > 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.

2.2.2 Offline-Lizenzaktivierung

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

1 Klicken Sie in der PlateSpin Forge-Weboberfläche auf **PlateSpin Forge-Lizenz hinzufügen > 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 PlateSpin Forge-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.

2.3 Konfigurieren der Benutzerautorisierung und -authentifizierung

Der Abschnitt enthält folgende Informationen:

2.3.1 Informationen zum rollenbasierten Zugriff in PlateSpin Forge

Der Benutzerautorisierungs- und -authentifizierungsmechanismus von PlateSpin Forge 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 Forge-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 Forge herzustellen, wird der über den Browser angegebene Berechtigungsnachweis vom IIS geprüft. Wenn der Benutzer keiner der Workload-Schutz-Rollen angehört, wird die Verbindung verweigert.

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

Details zu Workload-Schutz-Rollen	Administratoren	Power-Benutzer	Operatoren
Workload hinzufügen	Zulässig	Zulässig	Verweigert
Workload entfernen	Zulässig	Zulässig	Verweigert
Schutz konfigurieren	Zulässig	Zulässig	Verweigert
Reproduktion vorbereiten	Zulässig	Zulässig	Verweigert
(Voll-)Reproduktion 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

Details zu Workload-Schutz-Rollen	Administratoren	Power-Benutzer	Operatoren
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 Forge-Software einen auf *Sicherheitsgruppen* basierenden Mechanismus, der definiert, welche Benutzer auf welche Workloads im Workload-Inventar von PlateSpin Forge zugreifen dürfen.

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

1. Fügen Sie Benutzer zu den erforderlichen, in Tabelle 2-1 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 Forge-Sicherheitsgruppen und -Workload-Berechtigungen“ auf Seite 32.

2.3.2 Verwalten von PlateSpin Forge-Zugriff und -Berechtigungen

Die folgenden Abschnitte enthalten weitere Informationen:

- „Ändern des Administratorbenutzer-Passworts für die Forge-Management-VM“ auf Seite 31
- „Hinzufügen von PlateSpin Forge-Benutzern“ auf Seite 32
- „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Forge-Benutzer“ auf Seite 32

Ändern des Administratorbenutzer-Passworts für die Forge-Management-VM

Die standardmäßigen Berechtigungsnachweise für die Forge-Management-VM umfassen den Benutzernamen `Administrator` und das Passwort `Password1`.

So bearbeiten Sie das Administratorbenutzer-Passwort:

1. Stellen Sie eine Remote-Desktop-Verbindung zur Forge-Management-VM über die IP-Adresse her, die Sie für die VM konfiguriert haben.
2. Melden Sie sich mit den aktuellen Berechtigungsnachweisen als Administrator an.
3. Legen Sie mit den Windows-Verwaltungstool ein neues Passwort für den Administratorbenutzer fest.
4. Melden Sie sich ab, und schließen Sie die Remote-Desktop-Verbindung.

Hinzufügen von PlateSpin Forge-Benutzern

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

Wenn Sie einem auf der Forge-VM vorhandenen Benutzer bestimmte Rollenberechtigungen gewähren möchten, lesen Sie bitte unter „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Forge-Benutzer“ auf Seite 32 weiter.

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 Forge-Benutzer“ auf Seite 32.

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

Bevor Sie einem Benutzer eine Rolle zuweisen, ermitteln Sie, welche Berechtigungen für diesen Benutzer am besten geeignet sind. Weitere Informationen hierzu finden Sie unter Tabelle 2-1, „Details zu Workload-Schutz-Rollen und -Berechtigungen“, auf Seite 30.

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. Wechseln Sie in das Unterverzeichnis `bin\RestartPlateSpinServer` des PlateSpin-Servers.
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 Forge-Sicherheitsgruppe hinzufügen und ihm eine angegebene Sammlung von Workloads zuweisen. Weitere Informationen hierzu finden Sie unter „Verwalten von PlateSpin Forge-Sicherheitsgruppen und -Workload-Berechtigungen“ auf Seite 32.

2.3.3 Verwalten von PlateSpin Forge-Sicherheitsgruppen und -Workload-Berechtigungen

PlateSpin Forge 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 Forge-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 Forge-Benutzer“ auf Seite 32.
2. Greifen Sie als Administrator über die PlateSpin Forge-Weboberfläche auf PlateSpin Forge zu, und klicken Sie anschließend auf **Einstellungen** > **Berechtigungen**.

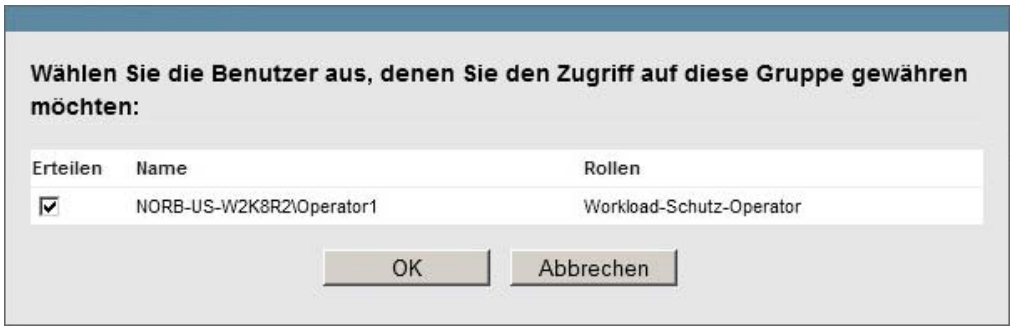
   Die Seite „Sicherheitsgruppen“ wird angezeigt.

3 Klicken Sie auf **Sicherheitsgruppe erstellen**.

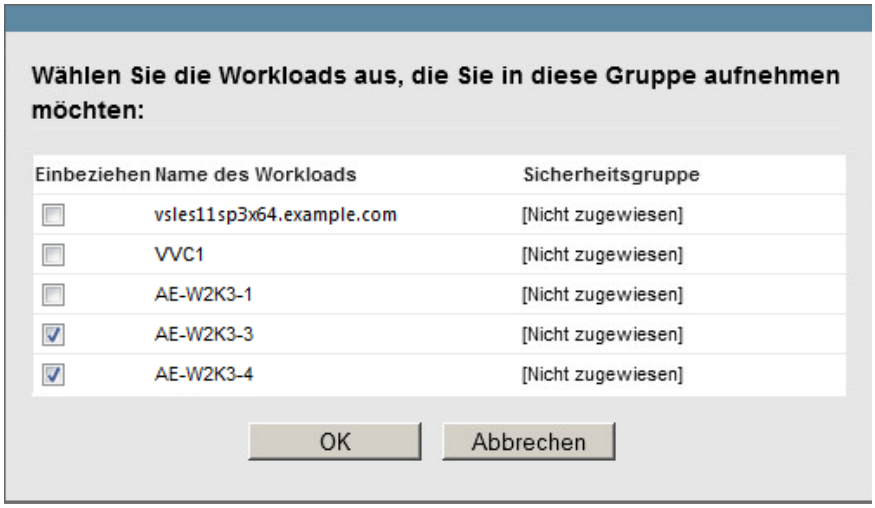
4 Geben Sie im Feld **Name der Sicherheitsgruppe** einen Namen für Ihre Sicherheitsgruppe ein.

5 Klicken Sie auf **Benutzer hinzufügen** und wählen Sie die erforderlichen Benutzer für diese Sicherheitsgruppe aus.

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



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



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

7 Klicken Sie auf **Erstellen**.

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

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

2.4 Konfigurieren der Zugriffs- und Kommunikationseinstellungen im gesamten Schutznetzwerk

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

2.4.1 Erforderliche geöffnete Ports für PlateSpin-Server-Host/ Forge-VM-Weboberfläche

Tabelle 2-2 zeigt die Ports, die auf der Forge-VM geöffnet sein müssen, damit der Zugriff auf die PlateSpin Forge-Weboberfläche zugelassen wird.

Tabelle 2-2 *Erforderliche geöffnete Ports für PlateSpin-Server-Host/Forge-VM*

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

2.4.2 Zugriffs- und Kommunikationsanforderungen für Workloads

Tabelle 2-3 zeigt die Software-, Netzwerk- und Firewall-Anforderungen für Workloads, die mithilfe von PlateSpin Forge geschützt werden sollen.

Tabelle 2-3 *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	

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** (`firewell.cpl`) und wählen Sie in der Liste der Ausnahmen die Option **Datei- und Druckerfreigabe** aus. - ODER - ◆ **Option 2 mit der Firewall mit erweiterter Sicherheit:** Verwenden Sie das Dienstprogramm Windows-Firewall mit erweiterter Sicherheit (`wf.msc`), bei dem die folgenden **Eingangsregeln** aktiviert und auf `Zulassen` festgelegt sind: ◆ **Datei- und Druckerfreigabe (Echoanforderung 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 17.	Secure Shell (SSH)-Server	TCP 22, 3725

2.4.3 Zugriffs- und Kommunikationsanforderungen für Container

Tabelle 2-4 zeigt die Software-, Netzwerk- und Firewall-Anforderungen für die unterstützten Workload-Container.

Tabelle 2-4 *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 18.	◆ VMware-Konto mit Administratorrolle ◆ VMware Web-Services-API und Dateiverwaltungs-API	HTTPS (TCP 443)
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)

2.4.4 Schutz über öffentliche und private Netzwerke durch NAT

In einigen Fällen kann sich ein Ursprung, ein Ziel oder PlateSpin Forge 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 Forge ermöglicht Ihnen, dieses Problem zu umgehen, je nachdem, welcher der folgenden Hosts sich hinter dem NAT-Gerät befindet:

- **PlateSpin-Server:** Fügen Sie die diesem Host zugewiesenen zusätzlichen IP-Adressen zum *PlateSpin Server Configuration*-Werkzeug Ihres Servers hinzu. Weitere Informationen hierzu finden Sie unter „Konfigurieren der Anwendung zum Funktionieren über NAT“ auf Seite 37.
- **Workload:** Geben Sie bei dem Versuch, einen Workload hinzuzufügen, die öffentliche (interne) IP-Adresse dieses Workloads in den Ermittlungsparametern an.
- **Failover-VM:** Bei einem Failback können Sie eine alternative IP-Adresse für den Failover-Workload in Failback-Details (Workload an VM) (Seite 86) 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 der Forge-VMangeben oder eine ihrer öffentlichen (externen) Adressen, die im *PlateSpin Server Configuration*-Werkzeug des Servers aufgezeichnet wurden (siehe oben unter *PlateSpin-Server*).

Konfigurieren der Anwendung zum Funktionieren über NAT

Damit der PlateSpin Forge-Server über alle NAT-aktivierten Umgebungen funktioniert, müssen Sie zusätzliche IP-Adressen Ihres PlateSpin Forge-Servers in der Datenbank im *PlateSpin Server Configuration*-Werkzeug aufzeichnen, die der Server beim Starten liest.

Weitere Informationen zum Aktualisierungsvorgang finden Sie unter „Konfigurieren des Verhaltens des PlateSpin-Servers mithilfe von XML-Konfigurationsparametern“ auf Seite 44.

2.4.5 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.

Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7010676 (https://www.netiq.com/support/kb/doc.php?id=7010676).

2.4.6 Anforderungen für VMware DRS-Cluster als Container

Um ein gültiges Schutzziel sein zu können, muss Ihr VMware DRS-Cluster dem Satz der (inventarisierten) Container als VMware-Cluster hinzugefügt werden. Sie sollten nicht versuchen, einen DRS-Cluster als einen Satz von individuellen ESX-Servern hinzuzufügen. Weitere Informationen hierzu finden Sie unter „Hinzufügen von Containern (Schutzziele)“ auf Seite 75.

Außerdem muss Ihr VMware-Cluster die folgenden Konfigurationsanforderungen erfüllen:

- DRS ist aktiviert und auf `Teilweise automatisiert` oder auf `vollautomatisch` gesetzt.
- Mindestens eine Datenablage muss für alle ESX-Server im VMware-Cluster freigegeben sein.
- Mindestens ein vSwitch und eine virtuelle Portgruppe bzw. ein dezentraler vNetwork-Schalter ist für alle ESX-Server im VMware-Cluster gleich.
- Die Failover-Workloads (VMs) für jeden Schutzvertrag werden ausschließlich in Datenablagen, vSwitches und virtuellen Portgruppen platziert, die über alle ESX-Server im VMware-Cluster gemeinsam genutzt werden.

2.5 Konfigurieren automatischer E-Mail-Benachrichtigungen zu Ereignissen und Berichten

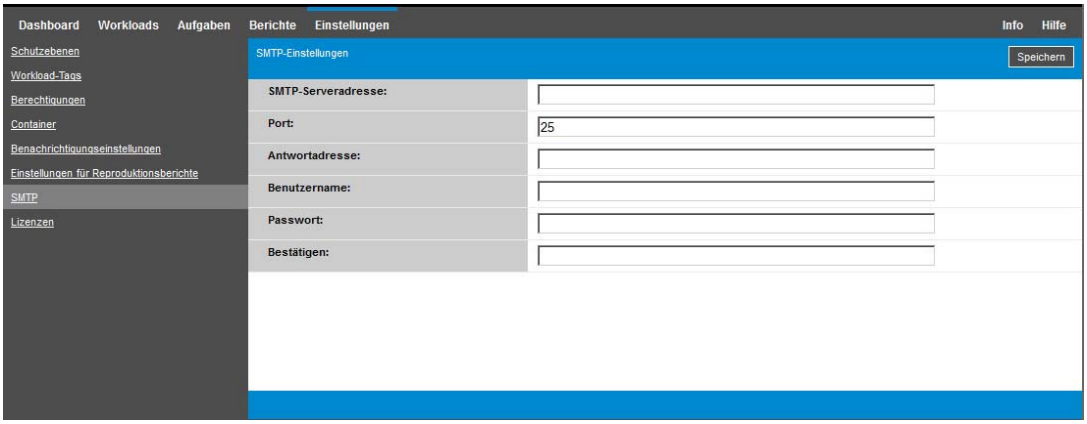
Sie können PlateSpin Forge so konfigurieren, dass es automatisch Benachrichtigungen zu Ereignissen und Reproduktionsberichte an angegebene Email-Adressen sendet. Für diese Funktion ist es erforderlich, dass Sie zuerst einen gültigen SMTP-Server für PlateSpin Forge angeben.

- Abschnitt 2.5.1, „SMTP-Konfiguration“ auf Seite 38
- Abschnitt 2.5.2, „Einrichten automatischer Ereignisbenachrichtigungen per Email“ auf Seite 38
- Abschnitt 2.5.3, „Einrichten automatischer Reproduktionsberichte per Email“ auf Seite 40

2.5.1 SMTP-Konfiguration

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

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



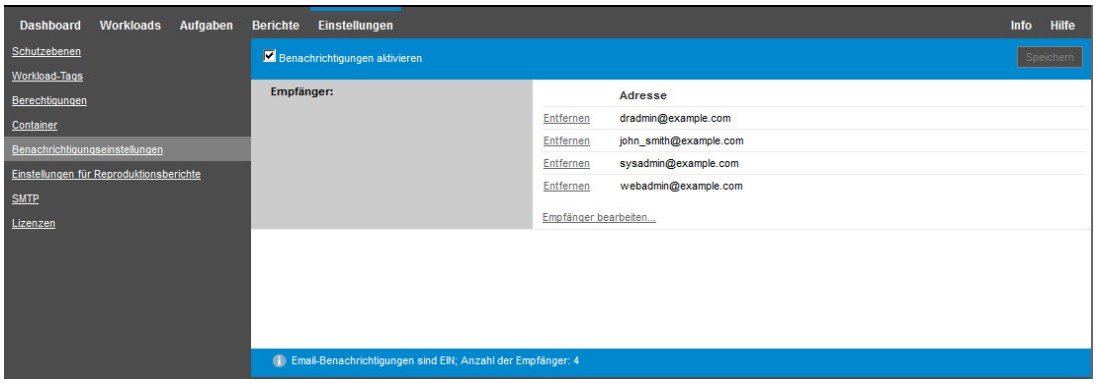
So konfigurieren Sie die SMTP-Einstellungen:

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

2.5.2 Einrichten automatischer Ereignisbenachrichtigungen per Email

So richten Sie automatische Ereignisbenachrichtigungen ein:

1. Richten Sie einen SMTP-Server für PlateSpin Forge ein. Weitere Informationen hierzu finden Sie unter „SMTP-Konfiguration“ auf Seite 38.
2. Klicken Sie auf der PlateSpin Forge-Weboberfläche auf **Einstellungen > Benachrichtigungen**.
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 2-5 genannten Ereignisarten können E-Mail-Benachrichtigungen auslösen, wenn die Benachrichtigungsfunktion konfiguriert ist. Die Ereignisse werden stets in das Systemanwendungs-Ereignisprotokoll mit den Protokolleintragsarten „Warnmeldung“, „Fehler“ und „Informationen“ eingetragen.

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

Tabelle 2-5 *Ereignistypen nach Protokolleintragsarten*

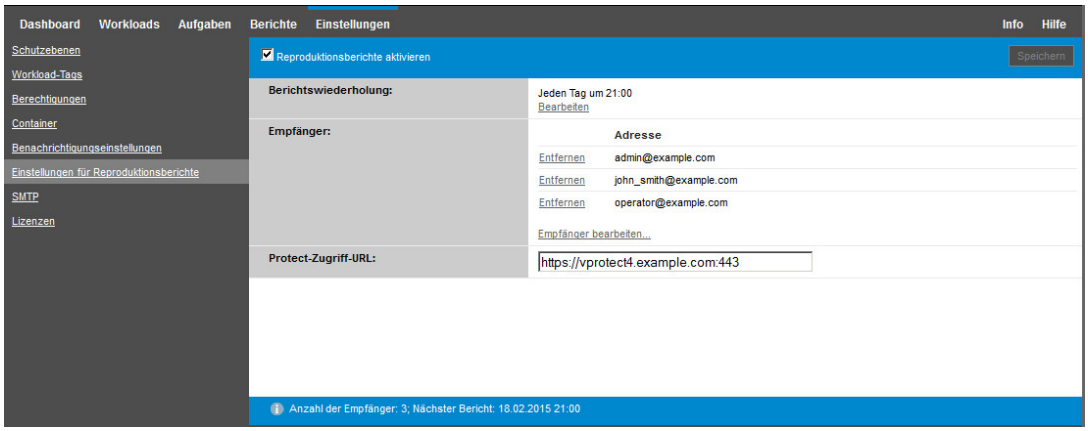
Ereignisarten	Anmerkungen
Protokolleintragsart: Warnmeldung	
`FullReplicationMissed`	Ähnlich dem Ereignis `Inkrementelle Reproduktion verpasst`.
`IncrementalReplicationMissed`	Wird generiert, wenn Folgendes zutrifft: ◆ Eine Reproduktion wird manuell angehalten, wenn eine geplante inkrementelle Reproduktion 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`	

Ereignisarten	Anmerkungen
`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.

2.5.3 Einrichten automatischer Reproduktionsberichte per Email

So richten Sie PlateSpin Forge für das automatische Senden von Reproduktionsberichten per E-Mail ein:

1. Richten Sie einen SMTP-Server für PlateSpin Forge ein. Weitere Informationen hierzu finden Sie unter SMTP-Konfiguration (Seite 38).
2. Klicken Sie auf der PlateSpin Forge-Weboberfläche auf **Einstellungen > 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 Forge**-Zugriff-URL** eine nicht standardmäßige URL für Ihren PlateSpin-Server ein (z. B. wenn Ihre Forge-VM 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 72.

2.6 Konfigurieren der Spracheinstellungen bei internationalen Versionen von PlateSpin Forge

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

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

1 Rufen Sie 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 Forge-Server herstellen. Weitere Informationen hierzu finden Sie unter „Starten der PlateSpin Forge-Weboberfläche“ auf Seite 27.

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

Die Sprache eines geringen Anteils der vom PlateSpin Forge-Server generierten Systemmeldungen hängt von der Sprache der Betriebssystemschnittstelle ab, die in Ihrer Forge-VM ausgewählt ist:

So ändern Sie die Sprache des Betriebssystems:

1 Rufen Sie Ihre Forge-VM auf.

Weitere Informationen hierzu finden Sie unter „Forge Management-VM im Appliance-Host – Zugriff und Verwendung“ auf Seite 57.

2 Starten Sie das Applet für die Regions- und Sprachoptionen (klicken Sie auf **Start > Ausführen**, geben Sie `intl.cpl` ein und drücken Sie die Eingabetaste) und klicken Sie anschließend auf die Registerkarte **Sprachen** (Windows Server 2003) bzw. **Tastaturen und Sprachen** (Windows Server 2008).

3 Installieren Sie das erforderliche Sprachpaket, sofern es noch nicht installiert ist. Möglicherweise benötigen Sie Zugriff auf die Installationsmedien Ihres Betriebssystems.

4 Wählen Sie die erforderliche Sprache als Oberflächensprache des Betriebssystems aus. Wenn eine entsprechende Aufforderung angezeigt wird, melden Sie sich ab oder starten Sie das System neu.

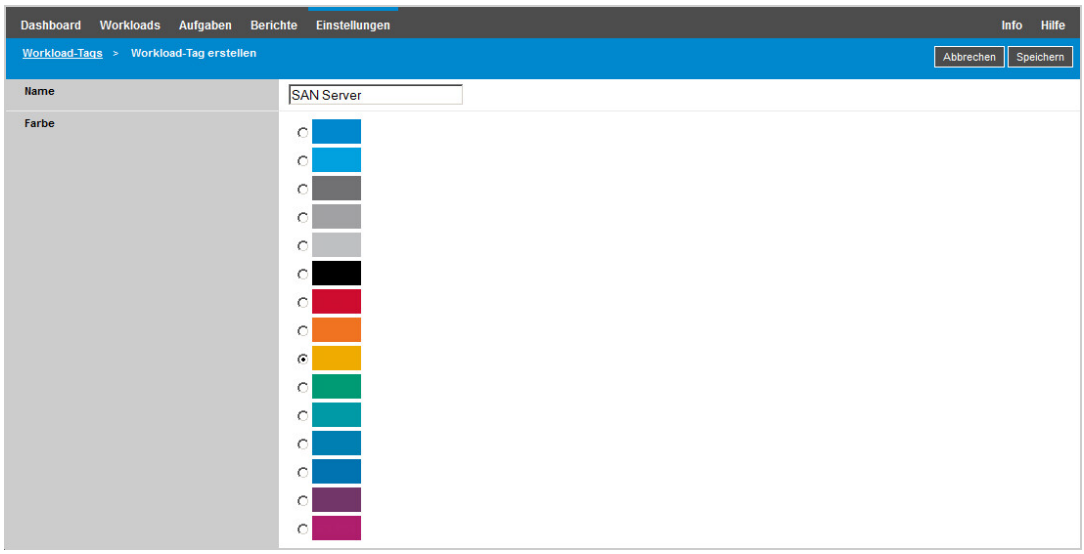
2.7 Sortieren von Workloads mithilfe von Tags

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.

So richten Sie ein Workload-Tag ein:

1 Klicken Sie auf der PlateSpin Forge-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.

So bearbeiten oder löschen Sie ein verfügbares Workload-Tag:

1 Klicken Sie auf der PlateSpin Forge-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**.

3 Löschen Sie die nicht mehr benötigten Tags. Klicken Sie neben dem Tag auf **Löschen**, und bestätigen Sie mit **OK**. Sie können ein Tag nicht löschen, wenn es noch mindestens einem Workload zugewiesen ist.

So können Sie ein einzelnes Tag zu einem Workload hinzufügen (*zuweisen*):

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**.

So können Sie ein einzelnes Tag aus einem Workload entfernen (die *Zuweisung aufheben*):

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**.

2.8 Konfigurieren des Verhaltens des PlateSpin-Servers mithilfe von XML-Konfigurationsparametern

Bestimmte Aspekte des Verhaltens des PlateSpin-Servers werden anhand von Konfigurationsparametern gesteuert, die Sie auf einer Konfigurations-Webseite auf der Forge-VM 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 `https://`*`Ihr_PlateSpin-Server`*`/platespinconfiguration/` in einem beliebigen Webbrowser.

2 Suchen Sie den gewünschten Serverparameter und ändern Sie dessen Wert.

3 Speichern Sie die Einstellungen und schließen Sie die Seite.

Nach Änderungen im Konfigurationswerkzeug ist kein Neustart des Computers oder der Dienste erforderlich.

In den nachfolgenden Themen finden Sie Informationen zu verschiedenen Situationen, in denen Sie das Produktverhalten mithilfe eines XML-Konfigurationswerts ändern müssen:

- „Optimieren des Datentransfers über WAN-Verbindungen“ auf Seite 44
- „Optimieren des Datentransfers über WAN-Verbindungen“ auf Seite 44
- „Anpassen der PlateSpin Forge-Weboberfläche an das Markenbild“ auf Seite 145

2.9 Optimieren des Datentransfers über WAN-Verbindungen

Sie können die Datentransferleistung optimieren und sie für WAN-Verbindungen fein abstimmen. Dazu können Sie die Konfigurationsparameter ändern, die das System von den Einstellungen im Konfigurationswerkzeug auf Ihrer Forge-VM liest. Weitere Informationen zu dem generischen Vorgang finden Sie unter „Konfigurieren des Verhaltens des PlateSpin-Servers mithilfe von XML-Konfigurationsparametern“ auf Seite 44.

Verwenden Sie diese Einstellungen zur Optimierung der Datentransfers 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 2-6 enthält eine Liste der Konfigurationsparameter, die die Dateiübertragungsgeschwindigkeit mit den Standard- bzw. Höchstwerten steuern. Zum Optimieren der Funktionsfähigkeit in einer WAN-Umgebung mit hoher Latenz können Sie diese Werte nach dem Versuch von Versuch und Irrtum bearbeiten.

Tabelle 2-6 *Standardmäßige und optimierte Konfigurationsparameter für die Dateiübertragung in* `https://Ihr_PlateSpin-Server/platespinconfiguration/`

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	
`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)

Parameter	Standardwert	Höchstwert
`FileTransferPort`	3725	

`FileTransferSendReceiveBufferSize`
 	
Gibt die Einstellung der TCP/IP-Fenstergröße für Dateiübertragungsverbindungen an. Sie steuert die Anzahl der Byte, die ohne TCP-Acknowledgement gesendet werden. Angabe in Byte.
 	
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(MB/s)/ 8)*Verzögerung(Sek.))*1000*1000
 	
Beispielsweise wäre die geeignete Puffergröße bei einer 100-Mb/s-Verbindung mit 10 ms Latenz wie folgt:
 	
`(100/8)*0,01 * 1000 * 1000 = 125000 Byte`
	0 (8192 Byte)	Max. 5242880 (5 MB)

`FileTransferSendReceiveBufferSizeLinux` Gibt die Einstellung der TCP/IP-Fenstergröße 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	

2.10 Konfigurieren der Unterstützung für VMware vCenter Site Recovery Manager

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

- Konfigurieren Sie eine Einstellung, damit die PlateSpin Forge-ISO und -Datenträger in derselben Datenablage gespeichert werden wie die VMware `.vmx`- und `.vmdk`-Dateien.
- Bereiten Sie die PlateSpin Forge-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 2.10.1, „Einrichten von Workload-Dateien in derselben Datenablage“ auf Seite 47
- Abschnitt 2.10.2, „Einrichten der VMware-Tools für Failover-Ziele“ auf Seite 47
- Abschnitt 2.10.3, „Beschleunigen des Konfigurationsprozesses“ auf Seite 48

2.10.1 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.

2.10.2 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 Forge 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*:** 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 aus den vom VMware Server extrahierten Setup-Paketen OFX-Pakete:

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 `%ProgramFiles(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.

In der folgenden Tabelle sind die Serverversionen, die VMware Tools-Architektur und der GUID-Bezeichner aufgeführt, die Sie zum Kopieren des Pakets in das richtige Verzeichnis benötigen:

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

2.10.3 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.

3 Appliance-Einrichtung und Wartung

Dieser Abschnitt enthält Informationen zu Einrichtungs- und Wartungsaufgaben für die Appliance, die Sie möglicherweise regelmäßig ausführen müssen.

3.1 Einrichten des Appliance-Netzwerks

Dieses Kapitel bietet Informationen zum Anpassen der Netzwerkeinstellungen des Appliance-Hosts.

3.1.1 Einrichten des Appliance-Host-Netzwerks

Die PlateSpin Forge-Appliance verfügt über sechs für den externen Zugriff konfigurierte physische Netzwerkschnittstellen:

- **Externes Testnetzwerk:** Dient der Isolierung des Netzwerkdatenverkehrs beim Testen eines Failover-Workloads mit der Funktion „Failover testen“.
- **Internes Testnetzwerk:** Zum Testen eines Failover-Workloads in völliger Isolation vom Produktionsnetzwerk.
- **Reproduktionsnetzwerk:** Bereitstellung eines Netzwerks für das System, das dem laufenden Datenverkehr zwischen dem Produktions-Workload und seiner Reproduktion in der Management-VM vorbehalten ist.
- **Produktionsnetzwerk:** Dient der Fortführung der realen Geschäftsprozesse, wenn ein Failover oder ein Failback durchgeführt wird.
- **Management-Netzwerk:** Das Forge Management-VM-Netzwerk.
- **Appliance-Host-Netzwerk:** Hypervisor-Management-Netzwerk. In der PlateSpin Forge-Weboberfläche steht dieses Netzwerk nicht zur Auswahl.

Zum Standardlieferumfang von PlateSpin Forge gehören alle sechs physischen Netzwerkschnittstellen, die einem einzelnen vSwitch im Hypervisor zugeordnet sind. Sie können die Zuordnung gemäß den Anforderungen Ihrer Umgebung entsprechend anpassen. Sie können beispielsweise einen Workload mit zwei Netzwerkkarten schützen, wobei eine Netzwerkarte für die Produktionskonnektivität und die andere ausschließlich für Reproduktionen verwendet werden. Weitere Informationen finden Sie im Knowledgebase-Artikel 7921062 (https://www.netiq.com/support/kb/doc.php?id=7921062).

Darüber hinaus können Sie jeder dieser einzelnen Portgruppen unterschiedliche VLAN-IDs zuweisen, um die Steuerung des Netzwerkdatenverkehrs ausgefeilter abzustimmen. Dadurch wird sichergestellt, dass das Produktionsnetzwerk nicht von dem Datenverkehr der Workload-Schutz- und Wiederherstellungsvorgänge gestört wird. Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 21057 (https://www.netiq.com/support/kb/doc.php?id=7921057).

3.2 Physische Standortänderung der Appliance

Eine Änderung des Standorts Ihrer PlateSpin Forge-Appliance erfordert eine Änderung der IP-Adressen ihrer Komponenten, um die neue Umgebung zu reflektieren. Dies sind die IP-Adressen, die Sie während der anfänglichen Einrichtung der Appliance angegeben haben (siehe *Handbuch „Erste Schritte“ zu PlateSpin Forge*).

Vor Beginn der Standortänderung:

1. Unterbrechen Sie alle Reproduktionszeitpläne. Stellen Sie dabei sicher, dass mindestens eine inkrementelle Reproduktion für jeden Workload ausgeführt wurde:
   - **1a** Wählen Sie im Web-Client der PlateSpin Forge-Weboberfläche alle Workloads aus, und klicken Sie auf **Unterbrechen** und anschließend auf **Ausführen**.
   - **1b** Stellen Sie sicher, dass der Status **Unterbrochen** für alle Workloads angezeigt wird.

Die Vorgehensweise für die Standortänderung hängt davon ab, ob die neue IP-Adresse der Appliance am Zielstandort bekannt (Szenario 1) oder nicht bekannt (Szenario 2) ist.

- Abschnitt 3.2.1, „Szenario 1 – Standortänderung der Forge-Appliance (neue IP-Adresse bekannt)“ auf Seite 52
- Abschnitt 3.2.2, „Szenario 2 – Standortänderung der Forge-Appliance (neue IP-Adresse nicht bekannt)“ auf Seite 53

3.2.1 Szenario 1 – Standortänderung der Forge-Appliance (neue IP-Adresse bekannt)

So ändern Sie den Standort der Forge Application-Hardware, wenn Ihnen die neue IP-Adresse bekannt ist:

1. Unterbrechen Sie alle Reproduktionen. Weitere Informationen hierzu finden Sie unter Schritt 1a und Schritt 1b oben.
2. Starten Sie die Forge Appliance Configuration Console (Forge ACC): Öffnen Sie einen Browser und navigieren Sie zu `http://<Forge_IP_Adresse>:10000`.
3. Melden Sie sich mit dem `forgeuser`-Konto an und klicken Sie auf **Configure Host** (Host konfigurieren).
4. Geben Sie die neuen Netzwerkeinstellungen ein und klicken Sie auf **Anwenden**.
5. Warten Sie, bis der Konfigurationsvorgang abgeschlossen ist und im Browser das Meldungsfenster „Configuration Successful“ (Konfiguration erfolgreich) geöffnet wird.

HINWEIS: Der Link für die neue Forge ACC-Adresse im Meldungsfenster funktioniert erst, nachdem Sie die Appliance physisch getrennt und an das neue Teilnetz angeschlossen haben.

---

6 Fahren Sie die Appliance herunter:

6a Fahren Sie die Forge Management-VM herunter. Weitere Informationen hierzu finden Sie unter „Starten und Herunterfahren der Forge Management-VM“ auf Seite 58.

6b Fahren Sie den Appliance-Host herunter:

6b1 Drücken Sie an der Forge-Konsole „Alt-F2“, um zur ESX-Serverkonsole zu wechseln.

6b2 Melden Sie sich als „superuser“ an (Benutzer `root` und das zugehörige Passwort).

6b3 Geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
shutdown -h now
```

6c Fahren Sie die Appliance herunter.

7 Trennen Sie die Appliance und stellen Sie sie am neuen Standort auf. Verbinden Sie die Appliance mit dem neuen Teilnetz und schalten Sie sie ein.

Die neue IP-Adresse sollte jetzt gültig sein.

8 Starten Sie die ACC und melden Sie sich mit dem `forgeuser`-Konto an. Klicken Sie auf **Configure Forge VM** (Forge-VM konfigurieren), geben Sie die erforderlichen Parameter an und klicken Sie auf **Apply** (Anwenden).

9 Vergewissern Sie sich, dass die Einstellungen korrekt sind, klicken Sie auf **Continue** (Fortfahren) und warten Sie, bis der Vorgang abgeschlossen ist.

HINWEIS: Wenn die Forge-VM für DHCP eingerichtet wurde, führen Sie nach der Standortänderung die folgenden Schritte aus:

1. Ermitteln Sie die neue IP-Adresse der Forge-VM (greifen Sie mithilfe des vSphere-Clientprogramms auf die Forge-VM zu und suchen Sie die Adresse in der Windows-Schnittstelle der VM. Weitere Informationen hierzu finden Sie unter „Starten des vSphere-Clients und Zugriff auf die Forge Management-VM“ auf Seite 57).

2. Verwenden Sie die neue IP-Adresse, um die PlateSpin Forge-Weboberfläche zu starten, und aktualisieren Sie den Container (klicken Sie auf **>** Einstellungen > Container und anschließend auf das Symbol).

---

10 Setzen Sie die angehaltenen Reproduktionen fort.

3.2.2 Szenario 2 – Standortänderung der Forge-Appliance (neue IP-Adresse nicht bekannt)

So ändern Sie den Standort der Forge Appliance-Hardware, wenn die neue IP-Adresse nicht bekannt ist:

1 Unterbrechen Sie alle Reproduktionen. Weitere Informationen hierzu finden Sie unter Schritt 1a und Schritt 1b auf Seite 52.

2 Fahren Sie die Appliance herunter:

2a Fahren Sie die Forge Management-VM herunter. Weitere Informationen hierzu finden Sie unter „Starten und Herunterfahren der Forge Management-VM“ auf Seite 58.

2b Fahren Sie den Appliance-Host herunter:

2b1 Drücken Sie an der Forge-Konsole „Alt-F2“, um zur ESX-Serverkonsole zu wechseln.

2b2 Melden Sie sich als „superuser“ an (Benutzer `root` und das zugehörige Passwort).

2b3 Geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
shutdown -h now
```

2c Schalten Sie die Appliance aus.

3 Trennen Sie die Appliance und stellen Sie sie am neuen Standort auf. Verbinden Sie die Appliance mit dem neuen Netzwerk und schalten Sie sie ein.

4 Richten Sie einen Computer (Notebook empfohlen) so ein, dass er mit Forge über die aktuelle IP-Adresse (die IP-Adresse am alten Standort) kommunizieren kann. Schließen Sie anschließend den Computer an der Appliance an.

Weitere Informationen finden Sie im *PlateSpin Forge-Handbuch „Erste Schritte“*.

5 Starten Sie die Forge-ACC: Öffnen Sie einen Browser und navigieren Sie zu `http://<Forge_IP_Adresse>:10000`.

6 Melden Sie sich mit dem `forgeuser`-Konto an und klicken Sie auf **Configure Host** (Host konfigurieren).

7 Geben Sie die neuen Netzwerkeinstellungen ein und klicken Sie auf **Anwenden**.

8 Warten Sie, bis der Konfigurationsvorgang abgeschlossen ist und im Browser das Meldungsfenster „Configuration Successful“ (Konfiguration erfolgreich) geöffnet wird.

HINWEIS: Der Link für die neue Forge ACC-Adresse im Meldungsfenster funktioniert erst, nachdem Sie die Appliance physisch getrennt und an das neue Teilnetz angeschlossen haben.

---

9 Trennen Sie den Computer von der Appliance und schließen Sie die Appliance an das neue Teilnetz an.

Die neue IP-Adresse sollte jetzt gültig sein.

10 Starten Sie die ACC und melden Sie sich mit dem `forgeuser`-Konto an. Klicken Sie auf **Configure Forge VM** (Forge-VM konfigurieren), geben Sie die erforderlichen Parameter an und klicken Sie auf **Apply** (Anwenden).

11 Vergewissern Sie sich, dass die Einstellungen korrekt sind, klicken Sie auf **Continue** (Fortfahren) und warten Sie, bis der Vorgang abgeschlossen ist.

HINWEIS: Wenn die Forge-VM für DHCP eingerichtet wurde, führen Sie nach der Standortänderung die folgenden Schritte aus:

1. Ermitteln Sie die neue IP-Adresse der Forge-VM (greifen Sie mithilfe des vSphere-Clientprogramms auf die Forge-VM zu und suchen Sie die Adresse in der Windows-Schnittstelle der VM. Weitere Informationen hierzu finden Sie unter „Starten des vSphere-Clients und Zugriff auf die Forge Management-VM“ auf Seite 57).

2. Verwenden Sie die neue IP-Adresse, um die PlateSpin Forge-Weboberfläche zu starten, und aktualisieren Sie den Container (klicken Sie auf **>** Einstellungen > Container und anschließend auf das Symbol).

---

12 Setzen Sie die angehaltenen Reproduktionen fort.

3.3 Verwenden externer Speicherlösungen mit PlateSpin Forge

Folgende Abschnitte enthalten Informationen, die Ihnen bei der Einrichtung und Konfiguration eines externen Speichers für die PlateSpin Forge-Appliance helfen.

- Abschnitt 3.3.1, „Verwenden von Forge mit einem SAN-Speicher“ auf Seite 55
- Abschnitt 3.3.2, „Hinzufügen einer SAN-LUN zu Forge“ auf Seite 56

3.3.1 Verwenden von Forge mit einem SAN-Speicher

Die PlateSpin Forge-Appliance unterstützt vorhandene externe Speicherlösungen wie z. B. SAN-Implementierungen (Storage Area Network). Sowohl Fibre-Channel-(FC-) als auch iSCSI-Lösungen werden unterstützt. Die SAN-Unterstützung für Fibre-Channel- und iSCSI-HBAs ermöglicht den Anschluss einer Forge-Appliance an einen SAN-Array. Somit können Sie SAN-Array-LUNs (Logical Units) zum Speichern von Workload-Daten verwenden. Die Verwendung der Forge-Appliance mit einem SAN verbessert die Flexibilität, Effizienz und Zuverlässigkeit.

Jedes SAN-Produkt weist individuelle Merkmale und Unterschiede auf, die von Hardwarehersteller zu Hardwarehersteller verschieden sind. Dies zeigt sich insbesondere dann, wenn es um die Art und Weise geht, wie diese Produkte mit der Forge Management-VM verbunden werden und mit dieser interagieren. Aus diesem Grund sprengen spezifische Konfigurationsschritte für jede mögliche Umgebung und jeden Kontext den Rahmen dieses Handbuchs.

Wenden Sie sich für diese Art von Informationen an Ihren Hardware-Anbieter oder Vertriebsbeauftragter für das SAN-Produkt. Viele Hardware-Anbieter verfügen über Dokumentation, in der diese Aufgaben detailliert beschrieben sind. Eine Vielzahl an Informationen finden Sie auf folgenden Websites:

Website für VMware-Dokumentation (http://www.vmware.com/support/pubs/).

- Im *Fibre Channel SAN Configuration Guide* wird die Verwendung des ESX-Servers mit Fibre-Channel-SANs erörtert.
- Im *iSCSI SAN Configuration Guide* wird die Verwendung des ESX-Servers mit iSCSI-SANs erörtert.
- Im *VMware I/O Compatibility Guide* werden die aktuell genehmigten HBAs, HBA-Treiber und Treiberversionen aufgeführt.
- Im *VMware Storage/SAN Compatibility Guide* werden die aktuell genehmigten Speicher-Arrays aufgeführt.
- Die *VMware-Versionshinweise* bieten Informationen zu bekannten Problemen und Ausweichlösungen.
- Die *VMware Knowledge Bases* enthalten Informationen zu bekannten Problemen und Ausweichlösungen.

Folgende Hersteller bieten Speicherprodukte, die von VMware getestet wurden:

- 3PAR (http://www.3par.com)
- Bull (http://www.bull.com) (nur FC)
- Dell (http://www.dell.com)
- Dell Compellent (http://www.dell.com/us/business/p/dell-compellent)
- EMC (http://www.emc.com)
- EqualLogic (http://www.equallogic.com) (nur iSCSI)

- Fujitsu (http://www.fujitsu.com) und Fujitsu Siemens (http://www.fujitsu-siemens.com)
- HP (http://www.hp.com)
- Hitachi (http://www.hitachi.com) und Hitachi Data Systems (http://www.hds.com) (nur FC)
- IBM (http://www.ibm.com)
- NEC (http://www.nec.com) (nur FC)
- Network Appliance (NetApp) (http://www.netapp.com)
- Nihon Unisys (http://www.unisys.com) (nur FC)
- Pillar Data (http://www.pillardata.com) (nur FC)
- Sun Microsystems (http://www.sun.com)
- Xiotech (http://www.xiotech.com) (nur FC)

Weitere Informationen zu iSCSI finden Sie auf der Website der Storage Networking Industry Association (http://www.snia.org/education/storage_networking_primer/ipstorage/).

3.3.2 Hinzufügen einer SAN-LUN zu Forge

PlateSpin Forge unterstützt die SAN-Speicherung (Storage Area Network). Damit Forge auf ein vorhandenes SAN zugreifen kann, muss jedoch zuerst eine SAN-LUN (Logical Unit) zum Forge-ESX-Server hinzugefügt werden.

1. Richten Sie Ihr SAN-System ein und konfigurieren Sie es.
2. Greifen Sie auf den Appliance-Host zu (siehe „Herunterladen des vSphere-Clientprogramms“ auf Seite 57).
3. Klicken Sie im VMware-Client im Inventarbereich auf den Stammknoten (den obersten Knoten) und wählen Sie die Registerkarte **Konfiguration**.
4. Klicken Sie auf den Hyperlink **Add Storage** (Speicher hinzufügen) oben rechts.
5. Klicken Sie im Assistenten zum Hinzufügen von Speicher auf **Next** (Weiter), bis Sie aufgefordert werden, Datenablageinformationen anzugeben.
6. Geben Sie einen Datenablagenamen ein und klicken Sie in den daraufhin angezeigten Assistentenseiten auf **Next** (Weiter). Klicken Sie auf **Fertig stellen**, wenn der Assistent abgeschlossen ist.
7. Klicken Sie unter **Hardware** auf *Storage* (Speicher), um die Forge-Datenablagen anzuzeigen. Die neu hinzugefügte SAN-LUN sollte im Fenster angezeigt werden.
8. Beenden Sie das VMware-Clientprogramm.

In der Weboberfläche der PlateSpin Forge-Appliance wird die neue Datenablage erst nach der nächsten Reproduktion und Aktualisierung des Anwendungshosts angezeigt. Sie können eine Aktualisierung erzwingen, indem Sie **Settings > Containers** (Einstellungen, Container) wählen und auf nahe dem Appliance-Hostnamen klicken.

3.4 Forge Management-VM im Appliance-Host – Zugriff und Verwendung

Gelegentlich müssen Sie auf die Forge Management-VM zugreifen und Wartungsaufgaben durchführen, wie in diesem Handbuch beschrieben, oder Sie erhalten vom PlateSpin-Support die Empfehlung zur Durchführung von Wartungsarbeiten.

Verwenden Sie die vSphere-Clientsoftware, um auf die Forge Management-VM, deren Betriebssystemschnittstelle und die VM-Einstellungen zuzugreifen.

3.4.1 Herunterladen des vSphere-Clientprogramms

Laden Sie die Clientsoftware vom Appliance-Host herunter und installieren Sie sie auf einer Windows-Arbeitsstation außerhalb von der PlateSpin Forge-Appliance.

So laden Sie den vSphere-Client herunter:

1. Laden Sie die Clientsoftware herunter:
   - Laden Sie für die Forge-Appliance Version 3 mit VMware ESXi 5.5 Update 1 das Programm VMware vSphere Client 5.5 Update 1 herunter.
2. Starten Sie das heruntergeladene Installationsprogramm und befolgen Sie die Anweisungen zum Installieren der Software.

3.4.2 Starten des vSphere-Clients und Zugriff auf die Forge Management-VM

So starten Sie den vSphere-Client:

1. Klicken Sie auf **Start > Programme > VMWare > VMware vSphere | Virtual Infrastructure Client**.

   Das Anmeldedialogfeld des vSphere-Clients wird angezeigt.
2. Geben Sie Ihren Berechtigungsnachweis der Administratorebene ein und melden Sie sich an. Ignorieren Sie eventuell angezeigte Zertifikatswarnungen.

   Das vSphere-Clientprogramm wird geöffnet.
3. Wählen Sie im Inventarbereich auf der linken Seite das Element **PlateSpin Forge VM** aus. Klicken Sie im rechten Bereich auf die Registerkarte **Console** (Konsole).

   Der Konsolenbereich des Clients zeigt die Windows-Schnittstelle der Forge Management-VM an.

Arbeiten Sie über die Konsole genauso mit der Management-VM, wie Sie auf einem physischen Computer mit Windows arbeiten würden.

Klicken Sie zum Entsperren der Management-VM in die Konsole und drücken Sie „Strg+Alt+Einfg“.

Um den Cursor für die Arbeit außerhalb des vSphere-Clientprogramms freizugeben, drücken Sie „Strg+Alt“.

3.4.3 Starten und Herunterfahren der Forge Management-VM

Gelegentlich kann es erforderlich sein, die Forge Management-VM herunterzufahren und neu zu starten, z. B. wenn sich der Standort der Appliance ändert.

So fahren Sie die VM herunter und starten sie neu:

1. Verwenden Sie den vSphere-Client für den Zugriff auf den Forge Management-VM-Host. Weitere Informationen hierzu finden Sie unter „Herunterladen des vSphere-Clientprogramms“ auf Seite 57.
2. Verwenden Sie das Windows-Standardverfahren zum Herunterfahren der VM (**Start > Herunterfahren**).

So starten Sie die Management-VM neu:

1. Klicken Sie im Inventarbereich auf der linken Seite mit der rechten Maustaste auf das Element **PlateSpin Forge Management VM** und wählen Sie **Power on** (Einschalten).

3.4.4 Verwalten von Snapshots der Forge-VM auf dem Appliance-Host

Gelegentlich kann es erforderlich sein, einen Snapshot der Management-VM zu erstellen, z. B. beim Aufrüsten der Forge-Software oder bei Aufgaben zur Fehlerbehebung. Möglicherweise müssen Sie auch Snapshots (Wiederherstellungspunkte) entfernen, um Speicherplatz frei zu machen.

So verwalten Sie Snapshots auf der Forge-Management-VM:

1. Verwenden Sie den vSphere-Client für den Zugriff auf den Appliance-Host. Weitere Informationen hierzu finden Sie unter „Herunterladen des vSphere-Clientprogramms“ auf Seite 57.
2. Klicken Sie im Inventarbereich auf der linken Seite mit der rechten Maustaste auf das Element **PlateSpin Forge Management VM** und wählen Sie **Snapshot > Take Snapshot** (Snapshot, Snapshot erstellen).
3. Geben Sie einen Namen und eine Beschreibung für den Snapshot ein und klicken Sie anschließend auf **OK**.

So versetzen Sie die Management-VM in einen früheren Zustand zurück:

1. Klicken Sie im Inventarbereich auf der linken Seite mit der rechten Maustaste auf das Element **PlateSpin Forge Management VM** und wählen Sie **Snapshot > Snapshot Manager**.
2. Wählen Sie in der Baumdarstellung der VM-Zustände einen Snapshot aus und klicken Sie anschließend auf **Go to** (Wechseln zu).

So entfernen Sie Snapshots, die Wiederherstellungspunkte darstellen:

1. Klicken Sie im Inventarbereich auf der linken Seite mit der rechten Maustaste auf das Element **PlateSpin Forge Management VM** und wählen Sie **Snapshot > Snapshot Manager**.
2. Wählen Sie in der Baumdarstellung der VM-Zustände einen Snapshot aus und klicken Sie anschließend auf **Remove** (Entfernen).

3.4.5 Manuelles Importieren von VMs in die Datenablage des Appliance-Hosts

So importieren Sie eine VM manuell in die Datenablage des Appliance-Hosts:

1. Erstellen Sie am Produktionsstandort eine VM aus Ihrem Produktions-Workload (z. B. mit PlateSpin Migrate), und kopieren Sie die VM-Dateien von der Datenablage des ESX-Host auf einen Wechseldatenträger, z. B. auf eine externe Festplatte oder einen USB-Stick. Verwenden Sie den „Datenspeicherbrowser“ der Clientsoftware zum Auffinden der Dateien.
2. Schließen Sie am Disaster-Recovery-Standort den Wechseldatenträger an einer Arbeitsstation an, die über Netzwerkzugriff auf Forge verfügt und auf der das vSphere-Clientprogramm installiert ist. Weitere Informationen hierzu finden Sie unter „Herunterladen des vSphere-Clientprogramms“ auf Seite 57.
3. Verwenden Sie den "Datenspeicherbrowser" des vSphere-Clients, um auf die Forge-Datenablage (**Storage1**) zuzugreifen, und laden Sie die VM-Dateien vom Wechseldatenträger hoch. Verwenden Sie die hochgeladene VM, um sie mit dem Appliance-Host zu registrieren (klicken Sie mit der rechten Maustaste auf **Zur Bestandsliste hinzufügen**).
4. Aktualisieren Sie das PlateSpin Forge-Inventar. (Klicken Sie in der PlateSpin Forge-Weboberfläche auf **Einstellungen > Container** und anschließend auf das Symbol neben dem Appliance-Host).

TIPP: Sie können diese Option verwenden, wenn Sie Ihren Failover-Workload unterschiedlich erstellen möchten (siehe „Anfängliche Reproduktionsmethode (vollständig und inkrementell)“ auf Seite 97).

3.4.6 Richtlinien zur Anwendung von Sicherheitsaktualisierungen auf die PlateSpin Forge Management-VM

So wenden Sie Sicherheitspatches auf die Forge-Management-VM an:

1. Rufen Sie während eines Wartungsfensters die Forge Management-VM über das VMware vSphere-Clientprogramm auf. Weitere Informationen hierzu finden Sie unter „Herunterladen des vSphere-Clientprogramms“ auf Seite 57.
2. Suchen Sie von der Windows-Benutzeroberfläche der Forge Management-VM aus nach Sicherheitsaktualisierungen von Microsoft.
3. Versetzen Sie PlateSpin Forge mithilfe der PlateSpin Forge-Weboberfläche in den Wartungsmodus. Halten Sie hierzu alle Reproduktionszeitpläne an, und warten Sie ab, bis alle laufenden Reproduktionen abgeschlossen sind.
4. Erstellen Sie einen Snapshot der Forge Management-VM. Weitere Informationen hierzu finden Sie unter „Verwalten von Snapshots der Forge-VM auf dem Appliance-Host“ auf Seite 58.

5 Laden Sie die erforderlichen Sicherheitspatches herunter und installieren Sie sie. Wenn die Installation abgeschlossen ist, starten Sie die Forge Management-VM neu.

6 Nehmen Sie die in Schritt 3 angehaltenen Reproduktionen mithilfe der PlateSpin Forge-Weboberfläche wieder auf, und vergewissern Sie sich, dass die Reproduktionen ordnungsgemäß funktionieren.

7 Entfernen Sie den in Schritt 4 erstellten Snapshot der Forge Management-VM. Weitere Informationen hierzu finden Sie unter „Verwalten von Snapshots der Forge-VM auf dem Appliance-Host“ auf Seite 58.

3.5 Zurücksetzen von Forge auf die Werkseinstellungen

TIPP: Je nach dem jeweiligen Forge-Modell dauert dieser Vorgang bis zu 45 Minuten oder länger.

So setzen Sie die Forge-Appliance auf die Werkseinstellungen zurück:

1 Trennen Sie alle externen/Remote-/freigegebenen Speichersysteme von Forge (iSCSI, FiberChannel, NFS).

2 Ziehen Sie alle Netzwerkkabel von Forge ab.

WARNUNG: Wenn Sie mehrere Forge-Appliances, die mit demselben physischen Switch verbunden sind, auf die Werkseinstellungen zurücksetzen und diesen Schritt überspringen, kann dies zu IP-Adresskonflikten und Fehlern führen.

3 Booten Sie den Appliance-Host neu:

   3a Melden Sie sich entweder direkt oder über iDRAC beim Hypervisor (VMware ESXi) an.

   3b Drücken Sie F2, um die ESXi-Konsole zu öffnen.

   WICHTIG: Notieren Sie sich die auf dieser Seite angezeigte IP-Adresse der Appliance zum Zurücksetzen auf die Werkseinstellungen. Diese Adresse benötigen Sie zur Anmeldung am Forge ACC und zum Verschieben des Containers an eine bekannte, gültige IP-Adresse. Gehen Sie vor wie in „Physische Standortänderung der Appliance“ auf Seite 52 beschrieben, um die IP ordnungsgemäß zurückzusetzen.

   3c Drücken Sie F12, um die ESXi-Konsole herunterzufahren.

   3d Melden Sie sich mit dem Berechtigungsnachweis eines Administrators an.

   3e Drücken Sie F2, um ESXi herunterzufahren und die Appliance neu zu booten.

   3f Booten Sie die Appliance über die Forge-CD (oder stellen Sie über iDRAC eine Verbindung zum ISO-Image her) und warten Sie, bis das SYSLINUX -Menü angezeigt wird.

4 Wählen Sie die Option **PlateSpin Forge Factory Reset** (PlateSpin Forge-Reset) und drücken Sie die Eingabetaste. Dieser Schritt muss ausgeführt werden, bevor die Standardkonfiguration automatisch übernommen wird. (Etwa 10 Sekunden.)

5 Warten Sie, bis der Vorgang abgeschlossen ist.

   Wenn der Prozess zum Zurücksetzen erfolgreich abgeschlossen wird, erscheint ein ähnliches Befehlszeilenfenster wie in der Abbildung dargestellt:

Bei Fehler:

- Wenden Sie sich an den PlateSpin-Support und halten Sie die Protokolldateien bereit. Folgende Protokolldateien werden zur Fehlerbehebung des Prozesses zum Zurücksetzen benötigt:
  - `/var/log/forge/forge-recovery.log`
  - `/var/log/forge/INSTALL_LOG.log`
  - `/var/log/weasel.log`
  - `/vmfs/volumes/forgeSystem/PLATESPINFORGE_LOGS/forge.log`

  Der Inhalt dieser Protokolldateien sollte auch über die Forge ACC-Schnittstelle verfügbar sein.

- Bauen Sie Forge ggf. mit einem *Field Rebuild Kit* neu auf. Dieses Kit erhalten Sie vom PlateSpin-Support.

4 Aufgestellt und in Betrieb

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

4.1 Zugreifen auf die PlateSpin Forge-Weboberfläche

So starten Sie die PlateSpin Forge-Weboberfläche:

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

   `https://`*<Hostname | IP-Adresse>*`/Forge`

   Ersetzen Sie *<Hostname | IP-Adresse>* durch den DNS-Hostnamen bzw. die IP-Adresse Ihrer Forge-VM.

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

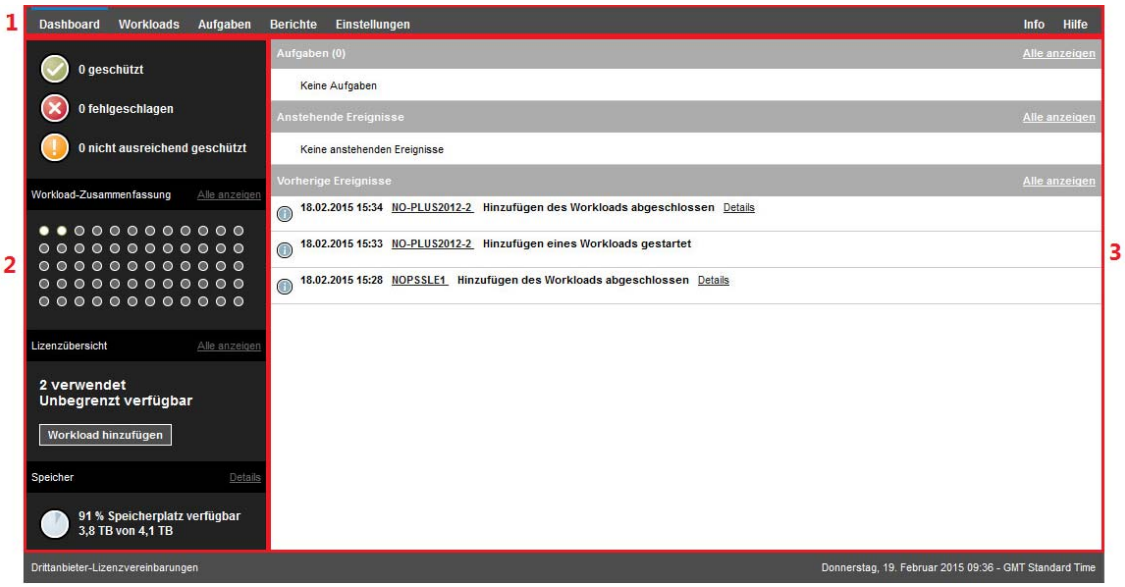
2. Melden Sie sich mit dem Berechtigungsnachweis des lokalen Administratorbenutzers für die Forge-VM oder als autorisierter Benutzer an.

   Weitere Informationen zum Einrichten zusätzlicher Benutzer für PlateSpin finden Sie unter „Konfigurieren der Benutzerautorisierung und -authentifizierung“ auf Seite 29.

4.2 Elemente der PlateSpin Forge-Weboberfläche

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

Abbildung 4-1 *Die Standard-Dashboard-Seite der PlateSpin Forge-Weboberfläche*



Die Dashboard-Seite besteht aus den folgenden Elementen:

1. **Navigationsleiste:** Auf den meisten Seiten der PlateSpin Forge-Weboberfläche enthalten.
2. **Teilfenster mit visueller Zusammenfassung:** Bietet einen umfassenden Überblick über den Gesamtstatus des Workload-Inventars von PlateSpin Forge.
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 4.2.1, „Navigationsleiste“ auf Seite 65
- Abschnitt 4.2.2, „Teilfenster mit visueller Zusammenfassung“ auf Seite 65
- Abschnitt 4.2.3, „Teilfenster mit Aufgaben und Ereignissen“ auf Seite 66

HINWEIS: Sie können bestimmte Elemente der Weboberfläche an das Markenbild Ihres Unternehmens anpassen. Weitere Informationen finden Sie unter „Anpassen der PlateSpin Forge-Weboberfläche an das Markenbild“ auf Seite 145.

4.2.1 Navigationsleiste

Die Navigationsleiste enthält folgende Links:

- **Dashboard:** Zeigt die Standardseite „Dashboard“ an.
- **Workloads:** Zeigt die Seite „Workloads“ an. Weitere Informationen hierzu finden Sie unter „Workloads und Workload-Befehle“ auf Seite 67.
- **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 72.
- **Einstellungen:** Zeigt die Seite „Einstellungen“ an, die Zugriff auf die folgenden Konfigurationsoptionen bietet:
  - **Schutzebenen:** Weitere Informationen hierzu finden Sie unter „Schutzebenen“ auf Seite 95.
  - **Workload-Tags:** Weitere Informationen hierzu finden Sie unter „Sortieren von Workloads mithilfe von Tags“ auf Seite 42.
  - **Berechtigungen:** Weitere Informationen hierzu finden Sie unter „Konfigurieren der Benutzerautorisierung und -authentifizierung“ auf Seite 29.
  - **Benachrichtigungseinstellungen:** „Einrichten automatischer Ereignisbenachrichtigungen per Email“ auf Seite 38.
  - **Einstellungen für Reproduktionsberichte:** „Einrichten automatischer Reproduktionsberichte per Email“ auf Seite 40
  - **SMTP:** Weitere Informationen hierzu finden Sie unter „SMTP-Konfiguration“ auf Seite 38.
  - **Lizenzen:** Weitere Informationen hierzu finden Sie unter „Aktivieren Ihrer Produktlizenz“ auf Seite 28.

4.2.2 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 4-1 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 4-1 *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 Forge verfügbaren Container-Speicherplatz sowie den derzeit belegten Speicherplatz.

4.2.3 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 automatischer E-Mail-Benachrichtigungen zu Ereignissen und Berichten“ auf Seite 37.

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

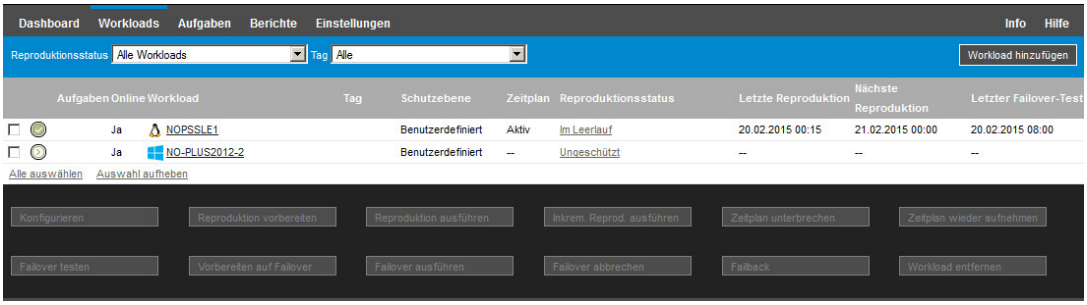
Sie auf eine der Aufgaben klicken, wird der Failover-Test abgebrochen und es wird ein entsprechendes Ereignis in das Protokoll geschrieben. Ein weiteres Beispiel ist das Ereignis `FullReplicationFailed`, das zusammen mit einer `StartFull`-Aufgabe gezeigt wird. Sie finden eine vollständige Liste der aktuellen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

4.3 Workloads und Workload-Befehle

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

Abbildung 4-2 *Die Seite „Workloads“*

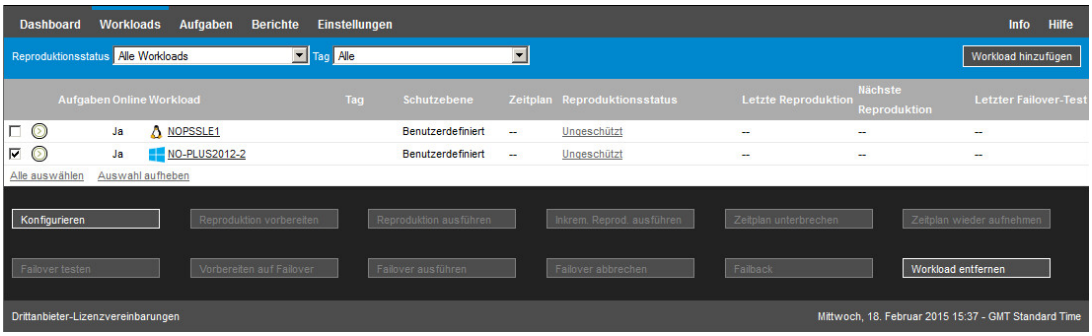


HINWEIS: Alle Zeitstempel entsprechen der Zeitzone der Forge-VM. Diese kann sich von der Zeitzone des geschützten Workloads oder der Zeitzone des Hosts, auf dem Sie die PlateSpin Forge-Weboberfläche ausführen, unterscheiden. Unten rechts im Client-Fenster werden das Serverdatum und die Serveruhrzeit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

4.3.1 Workload-Schutz- und Wiederherstellungsbefehle

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

Abbildung 4-3 *Workload-Befehle*



In Tabelle 4-2 finden Sie eine Übersicht über die Workload-Befehle sowie deren Beschreibung.

Tabelle 4-2 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).
Workload entfernen	Entfernt einen Workload aus dem Inventar.

4.4 Verwalten mehrerer Instanzen von PlateSpin Protect und PlateSpin Forge

PlateSpin Forge enthält eine webbasierte Client-Anwendung, die PlateSpin Forge-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.

- Abschnitt 4.4.1, „Verwenden der PlateSpin Forge-Verwaltungskonsole“ auf Seite 69
- Abschnitt 4.4.2, „Informationen zu PlateSpin Forge-Verwaltungskonsolenkarten“ auf Seite 69
- Abschnitt 4.4.3, „Hinzufügen von Instanzen von PlateSpin Protect und PlateSpin Forge zur Verwaltungskonsole“ auf Seite 70
- Abschnitt 4.4.4, „Verwalten von Karten auf der Verwaltungskonsole“ auf Seite 71

4.4.1 Verwenden der PlateSpin Forge-Verwaltungskonsole

So verwenden Sie die Verwaltungskonsole:

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

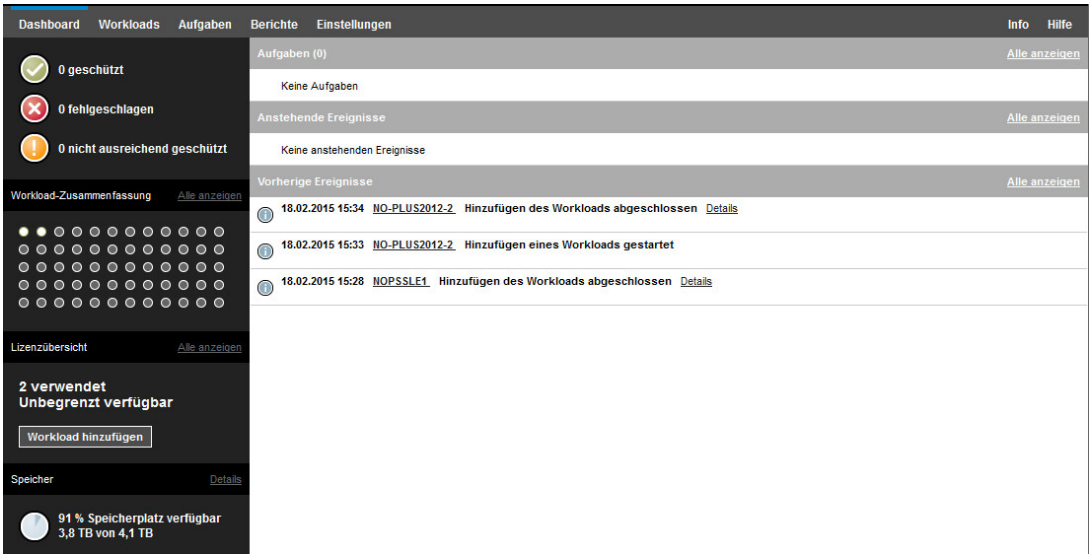
   `https://`*<IP-Adresse | Hostname>*`/console`.

   Ersetzen Sie *<IP-Adresse | Hostname>* durch die IP-Adresse oder den DNS-Hostnamen der Forge-VM, die als Manager festgelegt wurde.

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

   Die Standardseite „Dashboard“ der Konsole wird angezeigt.

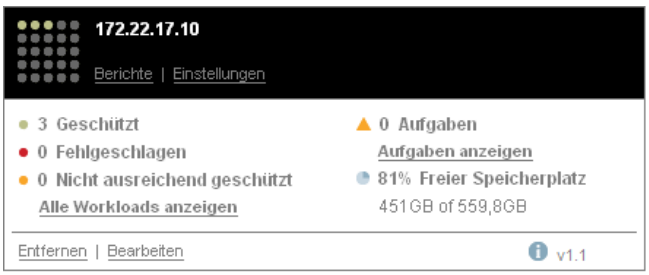
Abbildung 4-4 *Die Standardseite „Dashboard“ der Verwaltungskonsole*



4.4.2 Informationen zu PlateSpin Forge-Verwaltungskonsolenkarten

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

Abbildung 4-5 *PlateSpin Forge-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.

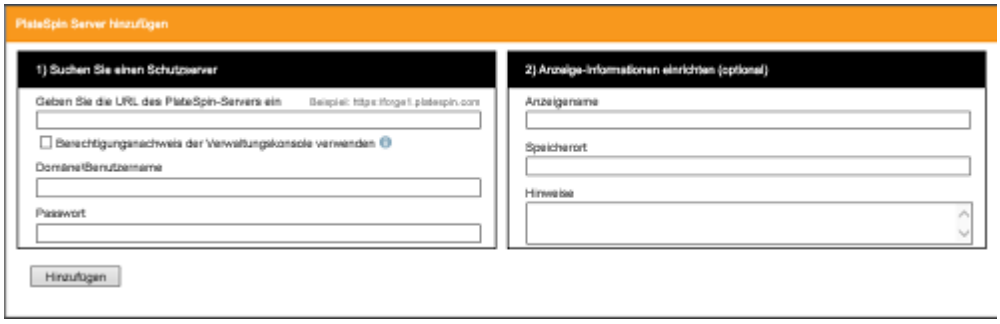
4.4.3 Hinzufügen von Instanzen von PlateSpin Protect und PlateSpin Forge zur Verwaltungskonsole

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.

4.4.4 Verwalten von Karten auf der Verwaltungskonsole

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

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

   Die Seite **Hinzufügen/Bearbeiten** der Konsole wird angezeigt.

2 Nehmen Sie alle gewünschten Änderungen vor und klicken Sie anschließend auf **Hinzufügen/ Speichern**.

   Das aktualisierte Konsolen-Dashboard wird angezeigt.

So entfernen Sie eine Karte von der Verwaltungskonsole:

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

   Es wird eine Bestätigungsaufforderung angezeigt.

2 Klicken Sie auf **OK**.

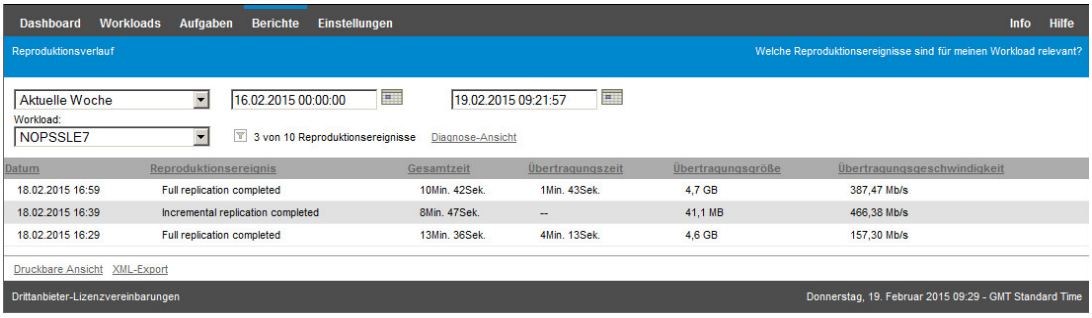
   Die individuelle Karte wird vom Dashboard entfernt.

4.5 Generieren von Workload- und Workload-Schutz-Berichten

Mit PlateSpin Forge 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 4-6 *Optionen für einen Reproduktionsverlaufsbericht*



So erzeugen Sie einen Bericht:

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

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

5 Workload-Schutz und Wiederherstellung

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

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

5.1 Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung

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

1 **Vorbereitung:** Für diesen Schritt fallen Vorbereitungsschritte an, mit denen sichergestellt werden soll, dass Ihre Workloads, die Container und die Umgebung die erforderlichen Kriterien erfüllen.

   1a Stellen Sie sicher, dass PlateSpin Forge Ihren Workload unterstützt.

   Weitere Informationen hierzu finden Sie unter „Unterstützte Konfigurationen“ auf Seite 13.

   1b Stellen Sie sicher, dass Ihre Workloads und VM-Container die Zugriffs- und Netzwerkvoraussetzungen erfüllen.

   Weitere Informationen hierzu finden Sie unter „Konfigurieren der Zugriffs- und Kommunikationseinstellungen im gesamten Schutznetzwerk“ auf Seite 34.

   1c (nur Linux)

   - (Bedingt) Wenn Sie planen, einen unterstützten Linux-Workload zu schützen, der einen nicht-standardmäßigen, benutzerdefinierten oder neueren Kernel hat, bauen Sie das PlateSpin `blkwatch`-Modul neu auf, das für eine Datenreproduktion auf Blockebene erforderlich ist.

     Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7005873 (https://www.netiq.com/support/kb/doc.php?id=7005873).

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

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

- (Optional) Bereiten Sie die Skripte `freeze` und `thaw` vor, so dass sie bei jeder Reproduktion auf dem Ursprungs-Workload ausgeführt werden.

  Weitere Informationen hierzu finden Sie unter „Verwenden von Freeze- und Thaw-Skripts für alle Reproduktionen (Linux)“ auf Seite 99.

2 **Inventar:** In diesem Schritt fügen Sie Workloads in die PlateSpin-Server-Datenbank ein.

  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. Weitere Informationen hierzu finden Sie unter „Hinzufügen von Containern (Schutzziele)“ auf Seite 75 und „Hinzufügen von Workloads“ auf Seite 76.

3 **Definition des Schutzvertrags:** In diesem Schritt definieren Sie die Details und die Spezifikationen des Schutzvertrags, und Sie bereiten die Reproduktion vor.

  Weitere Informationen hierzu finden Sie unter „Konfigurieren der Schutzdetails und Vorbereiten der Reproduktion“ auf Seite 77.

4 **Initiieren des Schutzes:** Mit diesem Schritt beginnt der Schutzvertrag gemäß Ihren Anforderungen.

  Weitere Informationen hierzu finden Sie unter „Starten des Workload-Schutzes“ auf Seite 81.

5 **Optionale Schritte im Schutz-Lebenszyklus:** 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.

  - *Manuell/inkrementell*. Mit **Inkrementelle Reproduktion ausführen** starten Sie manuell eine inkrementelle Reproduktion außerhalb des Workload-Schutzvertrags.
  - *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“.

6 **Failover:** Mit diesem Schritt wird ein Failover des geschützten Workloads auf die Reproduktion vorgenommen, die auf Ihrem Appliance-Host ausgeführt wird. Weitere Informationen hierzu finden Sie unter „Failover“ auf Seite 82.

7 **Failback:** Dieser Schritt entspricht der Phase der Wiederaufnahme des Betriebs, nachdem Sie die Probleme mit dem Produktions-Workload behoben haben. Weitere Informationen hierzu finden Sie unter „Failback“ auf Seite 85.

8 **Erneuter Schutz:** In diesem Schritt definieren Sie den ursprünglichen Schutzvertrag für den Workload neu. Weitere Informationen hierzu finden Sie unter „Erneutes Schützen eines Workloads“ auf Seite 89

Der Großteil dieser Schritte kann über Workload-Befehle auf der Seite „Workloads“ durchgeführt werden. Weitere Informationen hierzu finden Sie unter „Workloads und Workload-Befehle“ auf Seite 67.

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

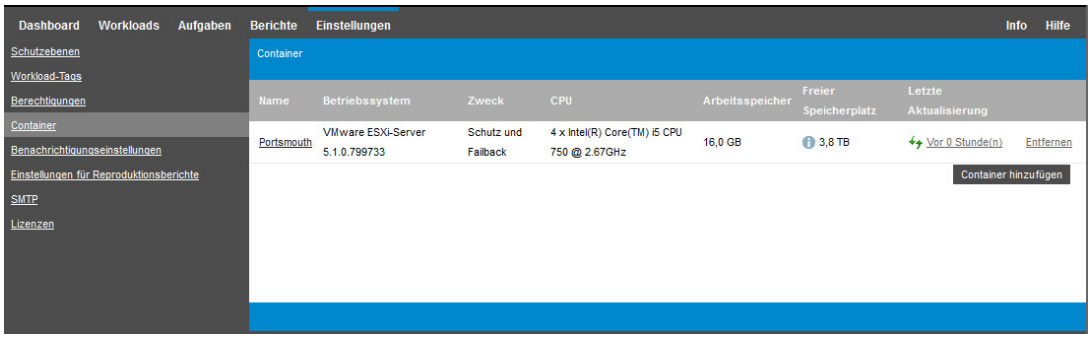
5.2 Hinzufügen von Containern (Schutzziele)

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. PlateSpin Forge befindet sich in einem Schutzcontainer auf der Appliance. Sie können nur Failback-Container definieren, die sich in der Infrastruktur einer Ziel-VM befinden.

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



2 Geben Sie die folgenden Parameter an:

- **Typ:** Wählen Sie den Typ des Containers aus:
  - **VMware ESX-Server**
  - **VMware DRS-Cluster**

  Stellen Sie sicher, dass der VM-Container unterstützt wird. Weitere Informationen hierzu finden Sie unter „Unterstützte VM-Container“ auf Seite 18.
- **Hostname oder IP-Adresse:** Geben Sie den Hostnamen oder die IP-Adresse des Containers ein.
- **vCenter-Hostname oder -IP-Adresse:** (Nur DRS-Cluster) Geben Sie den Hostnamen oder die IP-Adresse des vCenter-Servers ein.
- **Clustername:** (Nur DRS-Cluster) Geben Sie den Namen des erforderlichen DRS-Clusters ein.

  Wenn Sie versuchen, einen DRS-Cluster hinzuzufügen oder zu aktualisieren, kann der zugrunde liegende Ermittlungsvorgang in folgenden Fällen fehlschlagen:
  - Ein Cluster enthält keine ESX-Hosts.
  - Ein Clustername im vCenter-Server ist nicht eindeutig (auch wenn er einen eindeutigen Inventarpfad hat).
  - Keines der Cluster-Mitglieder ist zugänglich (z. B. weil der vCenter-Server im Wartungsmodus ist).
- **Benutzername/Passwort:** Geben Sie den Administrator-Berechtigungsnachweis für den Zugriff auf den Ziel-Host ein. Weitere Informationen hierzu finden Sie unter „Richtlinien für Workload- und Container-Berechtigungsnachweise“ auf Seite 92.

- **Beschreibung:** (Nur VM-Container) Wählen Sie den gewünschten Zweck für den VM-Container aus:
  - **Failback**

  In PlateSpin Forge können Sie Container lediglich für Failback-Vorgänge hinzufügen.

3 Klicken Sie auf **Hinzufügen**.

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

So aktualisieren Sie einen Container:

1 Klicken Sie auf das Symbol **Aktualisieren** neben dem zu aktualisierenden Container.

Dadurch wird der Container neu inventarisiert.

So entfernen Sie einen Container:

1 Klicken Sie auf **Entfernen** neben dem zu entfernenden Container.

5.3 Hinzufügen von Workloads

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.

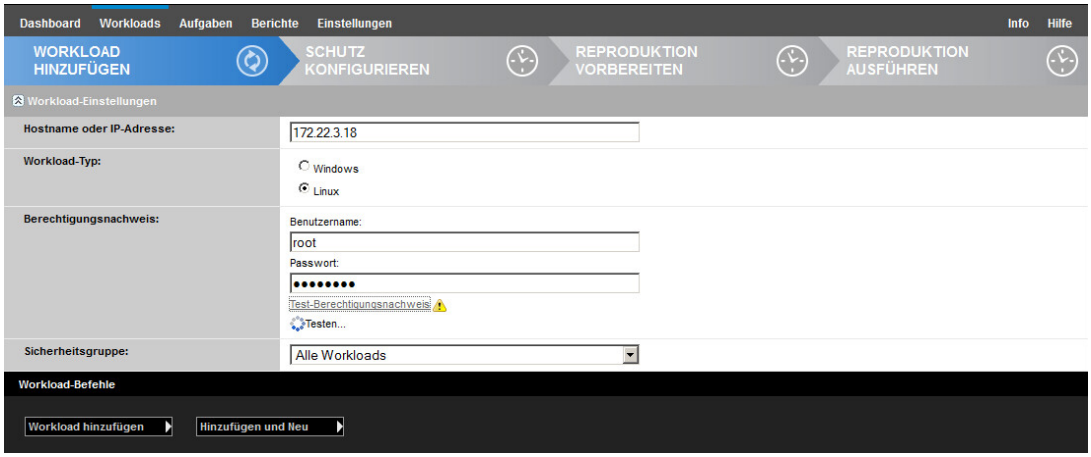
So fügen Sie einen Workload hinzu:

1 Führen Sie die erforderlichen Vorbereitungsschritte durch.

Siehe Schritt 1 unter „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“ auf Seite 73.

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

Auf der PlateSpin Forge-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 92).

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

4 Klicken Sie auf **Workload hinzufügen**.

PlateSpin Forge 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 „Hinzufügen von Containern (Schutzziele)“ auf Seite 75.

6 Fahren Sie mit „Konfigurieren der Schutzdetails und Vorbereiten der Reproduktion“ auf Seite 77 fort.

5.4 Konfigurieren der Schutzdetails und Vorbereiten der Reproduktion

Schutzdetails steuern die Workload-Schutz- und Wiederherstellungseinstellungen sowie das Verhalten im gesamten Lebenszyklus eines geschützten Workloads. In jeder Phase des Schutz- und Wiederherstellungs-Workflows (siehe „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“ auf Seite 73) werden relevante Einstellungen aus den Schutzdetails gelesen.

So konfigurieren Sie die Schutzdetails Ihres Workloads:

1 Fügen Sie einen Workload hinzu. Weitere Informationen hierzu finden Sie unter „Hinzufügen von Workloads“ auf Seite 76.

2 Fügen Sie einen Container hinzu. Weitere Informationen hierzu finden Sie unter „Hinzufügen von Containern (Schutzziele)“ auf Seite 75.

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 Forge-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 97.

5 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 78.

6 Korrigieren Sie alle Validierungsfehler, die eventuell auf der PlateSpin Forge-Weboberfläche angezeigt werden.

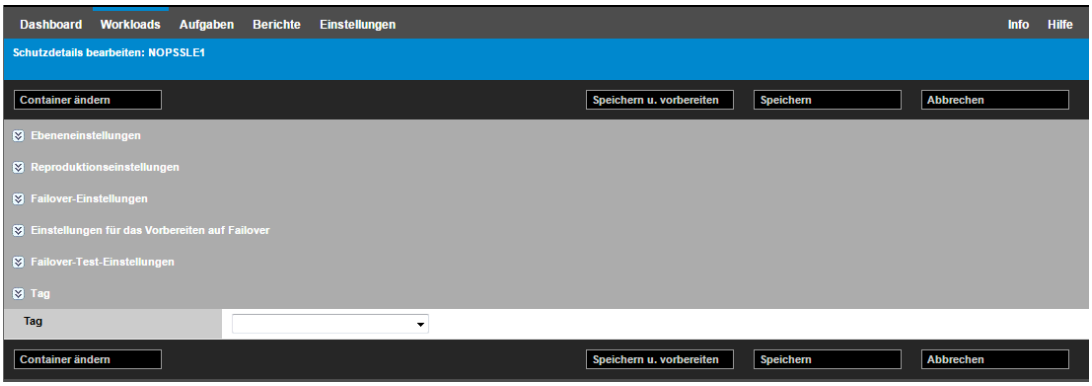
7 Klicken Sie auf **Speichern**.

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.

5.4.1 Workload-Schutz-Details

Workload-Schutz-Details werden in fünf Parametergruppen angegeben (siehe Tabelle 5-1):



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

Tabelle 5-1 *Workload-Schutz-Details*

Parametereinstellungen	Details
Ebeneneinstellungen	
Schutzebene	Gibt die Schutzebene des aktuellen Schutzes an. Weitere Informationen hierzu finden Sie unter „Schutzebenen“ auf Seite 95.
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 „Datenübertragung“ auf Seite 92. Wählen Sie zum Aktivieren der Verschlüsselung die Option **Datenübertragung verschlüsseln**. Weitere Informationen hierzu finden Sie in „Datenverschlüsselung“ auf Seite 94.
Übertragungsverschlüsselung	(Linux) Wählen Sie zum Aktivieren der Verschlüsselung die Option **Datenübertragung verschlüsseln**. Weitere Informationen hierzu finden Sie unter „Datenverschlüsselung“ auf Seite 94.

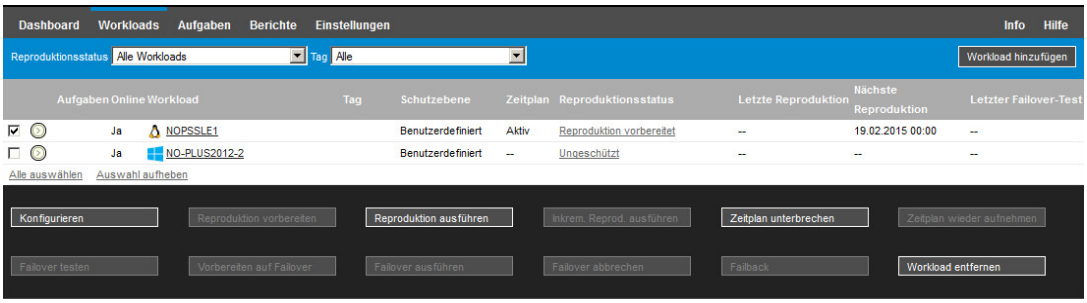
Parametereinstellungen	Details
Ursprungsberechtigungsnachweis	Geben Sie den erforderlichen Berechtigungsnachweis für den Zugriff auf den Workload an. Weitere Informationen hierzu finden Sie unter „Richtlinien für Workload- und Container-Berechtigungsnachweise“ auf Seite 92.
Prozessor	(VM-Container mit 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 wird der Reproduktionsdatenverkehr auf der Basis virtueller Netzwerke getrennt, die auf Ihrem Appliance-Host definiert sind. Weitere Informationen hierzu finden Sie unter „Netzwerke“ auf Seite 102. Für diese Einstellung können Sie außerdem einen MTU-Wert festlegen, der vom LRD-Reproduktionsnetzwerk (Linux RAM Disk) in PlateSpin Forge 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 Forge 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.

Parametereinstellungen	Details
Konfigurationsdatei-Datenablage	Wählen Sie eine mit dem Appliance-Host verbundene Datenablage zum Speichern von VM-Konfigurationsdateien aus. Weitere Informationen hierzu finden Sie unter „Wiederherstellungspunkte“ auf Seite 97.
Geschützte Volumes	Wählen Sie Volumes für den Schutz aus, und weisen Sie deren Reproduktionen bestimmten Datenablagen auf dem Appliance-Host zu.
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 98.
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 102.
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 98
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 102.
Testen der Failover-Einstellungen	
VM-Arbeitsspeicher	Weisen Sie dem temporären Workload den erforderlichen RAM zu.
Hostname	Weisen Sie dem temporären Workload einen Hostnamen zu.

Parametereinstellungen	Details
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 102.
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 98.
Kennungen	
Tag	(Optional) Weisen Sie diesem Workload ein Tag zu. Weitere Informationen hierzu finden Sie unter „Sortieren von Workloads mithilfe von Tags“ auf Seite 42.

5.5 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 Forge 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.

5.6 Abbrechen von Befehlen

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

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

1. Wechseln Sie zur Seite „Workloads“.
2. Suchen Sie den erforderlichen Workload, und klicken Sie auf den Link für den Befehl, der gerade auf diesem Workload ausgeführt wird, beispielsweise **Inkrementelle Reproduktion wird durchgeführt**.

   Auf der PlateSpin Forge-Weboberfläche wird die entsprechende Seite „Befehlsdetails“ angezeigt:

3. Klicken Sie auf **Abbrechen**.

5.7 Failover

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

- Abschnitt 5.7.1, „Erkennen von Offline-Workloads“ auf Seite 83
- Abschnitt 5.7.2, „Durchführen eines Failovers“ auf Seite 83
- Abschnitt 5.7.3, „Verwenden der Funktion „Failover testen““ auf Seite 84

5.7.1 Erkennen von Offline-Workloads

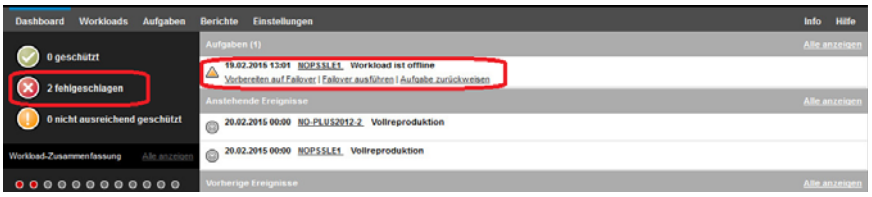
PlateSpin Forge überwacht ständig Ihre geschützten Workloads. Wenn die festgelegte Anzahl an Versuchen, einen Workload zu überwachen, fehlschlägt, generiert PlateSpin Forge das Ereignis **Workload ist offline**. Kriterien, anhand deren ein Workload-Fehler definiert und protokolliert wird, sind Teil der Ebeneneinstellungen eines Workload-Schutzes. Weitere Informationen finden Sie in der Zeile „Ebeneneinstellungen“ unter „Workload-Schutz-Details“ auf Seite 78.

Wenn zusammen mit den SMTP-Einstellungen Benachrichtigungen konfiguriert wurden, sendet PlateSpin Forge gleichzeitig eine Benachrichtigungs-Email an die angegebenen Empfänger. Weitere Informationen hierzu finden Sie unter „Konfigurieren automatischer E-Mail-Benachrichtigungen zu Ereignissen und Berichten“ auf Seite 37.

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 82) und fahren Sie dann mit dem Befehl **Failover ausführen** fort. Weitere Informationen hierzu finden Sie unter „Durchführen eines Failovers“ auf Seite 83.

Abbildung 5-1 zeigt die Dashboard-Seite der PlateSpin Forge-Weboberfläche beim Erkennen eines Workload-Fehlers. Beachten Sie die anwendbaren Aufgaben im Teilfenster mit den Aufgaben und Ereignissen:

Abbildung 5-1 *Die Dashboard-Seite bei Erkennen eines Workload-Fehlers („Workload offline“)*



5.7.2 Durchführen eines Failovers

Failover-Einstellungen, einschließlich der Netzwerkidentitäts- und LAN-Einstellungen des Failover-Workloads, werden zum Zeitpunkt der Konfiguration zusammen mit den Schutzdetails gespeichert. Siehe „Failover-Einstellungen“ in „Workload-Schutz-Details“ auf Seite 78.

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 5-1.
- 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 97). 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 84.

5.7.3 Verwenden der Funktion „Failover testen“

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

Wenn Sie diesen Befehl ausführen, wendet PlateSpin Forge die Failover-Test-Einstellungen, die in den Workload-Schutz-Details gespeichert sind, auf den Failover-Workload an. Siehe „Testen der Failover-Einstellungen“ in „Workload-Schutz-Details“ auf Seite 78.

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 97) und klicken Sie anschließend auf **Ausführen**.

   Anschließend generiert PlateSpin Forge 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 Appliance-Host zuzugreifen

   Weitere Informationen hierzu finden Sie unter „Herunterladen des vSphere-Clientprogramms“ auf Seite 57.
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 Aufgabe **Test als nicht bestanden markieren** oder **Test als erfolgreich markieren** verwirft PlateSpin Forge die temporären Einstellungen, die auf den Failover-Workload angewendet wurden. Der Schutz wird in den Zustand versetzt, den er vor dem Test hatte.

5.8 Failback

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

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 5.8.1, „Automatischer Failback auf eine VM-Plattform“ auf Seite 85
- Abschnitt 5.8.2, „Halbautomatischer Failback auf einen physischen Computer“ auf Seite 88
- Abschnitt 5.8.3, „Halbautomatischer Failback auf eine virtuelle Maschine“ auf Seite 89

5.8.1 Automatischer Failback auf eine VM-Plattform

PlateSpin Forge 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 18.

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 92).
   - **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 97.
     - **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“.

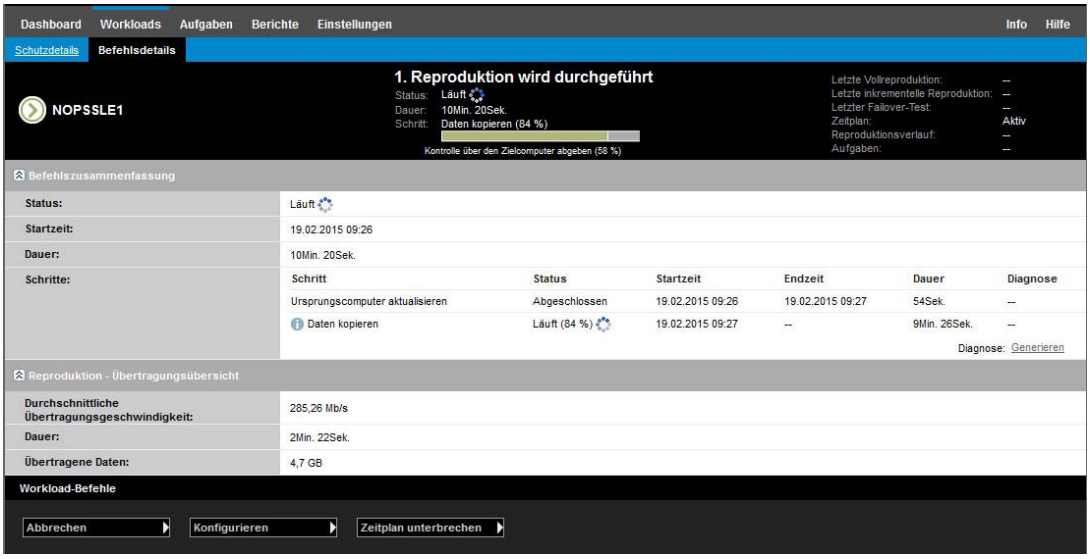
   Nach erfolgreichem Abschluss lädt PlateSpin Forge den Bildschirm „Bereit für Failback“ und fordert Sie auf, die Details des Failback-Vorgangs anzugeben.

4 Konfigurieren Sie die Failback-Details. Weitere Informationen hierzu finden Sie unter „Failback-Details (Workload an VM)“ auf Seite 86.

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

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

Abbildung 5-2 *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 5-2.

Tabelle 5-2 *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 „Datenübertragung“ auf Seite 92.
Failback-Netzwerk	Geben Sie das Netzwerk für den Failback-Datenverkehr an. Dies ist ein dediziertes Netzwerk, das auf den im Appliance-Host definierten virtuellen Netzwerken beruht. Weitere Informationen hierzu finden Sie unter „Netzwerke“ auf Seite 102.
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.

Parametereinstellungen	Details
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 98.
Alternative Adresse für Ursprung	Geben Sie ggf. eine zusätzliche IP-Adresse für den virtuellen Failover-Computer ein. Weitere Informationen hierzu finden Sie unter „Schutz über öffentliche und private Netzwerke durch NAT“ auf Seite 36.
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 98.
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.

Parametereinstellungen	Details
Erneut schützen nach Failback	Wählen Sie diese Option, wenn Sie planen, den Schutzvertrag für den Ziel-Workload neu zu erstellen. Wenn der Failback abgeschlossen ist, steht für den Failback-Workload der Befehl **Erneut schützen** auf der PlateSpin Forge-Weboberfläche zur Verfügung.
Kein erneutes Schützen	Wählen Sie diese Option, wenn Sie den Schutzvertrag für den Ziel-Workload nicht neu erstellen möchten. Zum Schützen des Failback-Workload nach dessen Abschluss müssen Sie diesen Workload neu inventarisieren und dessen Schutzdetails neu konfigurieren.

5.8.2 Halbautomatischer Failback auf einen physischen Computer

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

1. Registrieren Sie den erforderlichen physischen Computer bei Ihrem PlateSpin-Server. Weitere Informationen hierzu finden Sie unter „Failback auf physische Computer“ auf Seite 102.
2. Falls Treiber fehlen oder nicht kompatibel sind, laden Sie die erforderlichen Treiber in die Gerätetreiberdatenbank von PlateSpin Forge hoch. Weitere Informationen hierzu finden Sie unter „Verwalten der Gerätetreiber“ auf Seite 111.
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 92).
   - **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 97.
     - **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 Forge 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“.

5.8.3 Halbautomatischer Failback auf eine virtuelle Maschine

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

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
     ```

5.9 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** auf der PlateSpin Forge-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 85.

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.

6 Grundlagen des Workload-Schutzes

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

6.1 Workload-Lizenzverbrauch

Die PlateSpin Forge-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. Auf der Seite „Dashboard“ in der PlateSpin Forge-Weboberfläche zeigt die Lizenzübersicht die Anzahl der installierten Lizenzen sowie die aktuelle Anzahl der verbrauchten Lizenzen. Sie können eine verbrauchte Lizenz durch Entfernen eines Workloads bis zu maximal fünf Mal wiederherstellen.

Informationen über die Produktlizenzierung und die Lizenzaktivierung finden Sie unter „Aktivieren Ihrer Produktlizenz“ auf Seite 28.

6.2 Richtlinien für Workload- und Container-Berechtigungsnachweise

PlateSpin Forge 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 Forge aufgefordert, Berechtigungsnachweise in einem bestimmten Format einzugeben.

Tabelle 6-1 *Workload-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.	
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/ESXi 4.1; ESXi 5.0, ESXi 5.1, ESXi 5.5	VMware-Konto mit einer entsprechenden Rollenkonfiguration.	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.	

6.3 Datenübertragung

In den nachfolgenden Themen finden Sie Informationen zu den Mechanismen und Optionen für die Datenübertragung aus Ihren Workloads in die entsprechenden Reproduktionen.

6.3.1 Übertragungsmethoden

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

- „Unterstützte Übertragungsmethoden für Windows-Workloads“ auf Seite 93
- „Unterstützte Übertragungsmethoden für Linux-Workloads“ auf Seite 93

Unterstützte Übertragungsmethoden für Windows-Workloads

Für Windows-Workloads bietet PlateSpin Forge 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 Forge 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.

Unterstützte Übertragungsmethoden für Linux-Workloads

Für Linux-Workloads bietet PlateSpin Forge einen Mechanismus, mit dem Sie die Volume-Daten des Workloads ausschließlich auf Blockebene übertragen. Die Datenübertragung wird mithilfe einer Datenübertragungskomponente auf Blockebene durchgeführt, die LVM-Snapshots nutzt, sofern vorhanden (die standardmäßige und empfohlene Option). Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7005872 (https://www.netiq.com/support/kb/doc.php?id=7005872).

Die im Lieferumfang von PlateSpin Forge enthaltene blockbasierte Linux-Komponente ist für Standard- und Nicht-Debug-Kernels der unterstützen Linux-Distributionen vorkompiliert. Wenn Sie einen nicht-standardmäßigen, benutzerdefinierten oder neueren Kernel haben, können Sie die

blockbasierte Komponente gemäß den Spezifikationen Ihres Kernels neu aufbauen. Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7005873 (https://www.netiq.com/support/kb/doc.php?id=7005873).

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

6.3.2 Datenverschlüsselung

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 78.

6.3.3 Ändern des Speicherorts des Volume-Snapshotverzeichnisses für Windows-Workloads

Der PlateSpin-Server speichert die Volume-Snapshots standardmäßig in das folgende Verzeichnis:

```
\ProgramData\PlateSpin\Volume Snapshots
```

Unter Umständen muss der Pfad geändert werden:

- Wenn das aktuelle Laufwerk für den Pfad nicht genügend Speicherplatz für die Snapshots der Windows-Workloads enthält
- Wenn der Pfad an eine andere Position verschoben werden soll, damit Sie ihn leichter aus der Sicherungsliste ausschließen können

Mit dem globalen Parameter `VssSnapshotMountPath` auf der Konfigurationsseite für den PlateSpin-Server können Sie einen benutzerdefinierten Pfad zum Server angeben, auf dem die Snapshots gespeichert werden sollen. Wenn der Wert dieses Parameters leer ist, wird weiterhin der standardmäßige Pfad verwendet.

So geben Sie einen benutzerdefinierten Pfad für das Volume-Snapshotverzeichnis unter Windows an:

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

   https://*<IP-Adresse_des_PlateSpin-Servers>*/PlatespinConfiguration.
2. Suchen Sie den Eintrag `VssSnapshotMountPath`, und klicken Sie auf **Bearbeiten**.
3. Geben Sie in das Feld **Wert** den vollständigen Pfad des Verzeichnisses auf dem PlateSpin-Server an, auf dem die Volume-Snapshots für Windows-Workloads gespeichert werden sollen. Beispiel:

   ```
   G:\PlateSpin\Volume Snapshots
   ```
4. Klicken Sie auf **Speichern**.

6.3.4 Aus- oder Einschließen von Dateien bei Blockübertragungen für inkrementelle Reproduktionen

PlateSpin Forge schließt bestimmte Dateien bei der Datenübertragung für eine blockbasierte Reproduktion standardmäßig aus bzw. ein. Die Ausschluss- und Einschlusslisten für die blockbasierten Volume-Server können neben den standardmäßigen Dateien nun auch neue Dateien aufnehmen. Mit den folgenden globalen Parametern auf der Konfigurationsseite für den PlateSpin-Server fügen Sie eine neue Liste hinzu:

`BlockBasedTransferExcludeFileList`

`BlockBasedTransferIncludeFileList`

So geben Sie eine Datei an, die bei inkrementellen, blockbasierten Reproduktionen stets übertragen werden muss:

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

   https://<*IP-Adresse_des_PlateSpin-Servers*>/PlatespinConfiguration.
2. Suchen Sie den Eintrag `BlockBasedTransferIncludeFileList`, und klicken Sie auf **Bearbeiten**.
3. Tragen Sie im Feld **Wert** den Namen in die Liste ein.
4. Klicken Sie auf **Speichern**.

So geben Sie eine Datei an, die bei inkrementellen, blockbasierten Reproduktionen stets ausgeschlossen werden muss:

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

   https://<*IP-Adresse_des_PlateSpin-Servers*>/PlatespinConfiguration.
2. Suchen Sie den Eintrag `BlockBasedTransferExcludeFileList`, und klicken Sie auf **Bearbeiten**.
3. Tragen Sie im Feld **Wert** den Namen in die Liste ein.
4. Klicken Sie auf **Speichern**.

6.4 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 auf Ihrer PlateSpin Forge-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 24. 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 24. 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 97.
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.

6.5 Wiederherstellungspunkte

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

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 Forge nicht mehr ausreicht.

Informationen zum Entfernen von Wiederherstellungspunkten aus Ihrer Appliance finden Sie unter „Verwalten von Snapshots der Forge-VM auf dem Appliance-Host“ auf Seite 58.

6.6 Anfängliche Reproduktionsmethode (vollständig und inkrementell)

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

- **Vollständig:** Eine vollständige Volume-Übertragung erfolgt von einem Produktions-Workload auf dessen Reproduktion (der Failover-Workload) oder von einem Failover-Workload auf seine ursprüngliche virtuelle oder physische Infrastruktur.
- **Inkrementell:** Es werden nur Unterschiede vom Ursprung auf dessen Ziel übertragen, vorausgesetzt, sie verfügen über ähnliche Betriebssysteme und Volume-Profile.
  - **Beim Schutz:** Der Produktions-Workload wird mit einer vorhandenen VM im Appliance-Host 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 Appliance-Host importiert wurde, z. B. eine Workload-VM, die auf einem Wechseldatenträger physisch vom Produktionsstandort auf einen Remote-Wiederherstellungsstandort verschoben wird.

      Weitere Informationen hierzu finden Sie unter „Manuelles Importieren von VMs in die Datenablage des Appliance-Hosts“ auf Seite 59.
  - **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 Forge registriert ist (siehe „Halbautomatischer Failback auf einen physischen Computer“ auf Seite 88).

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.

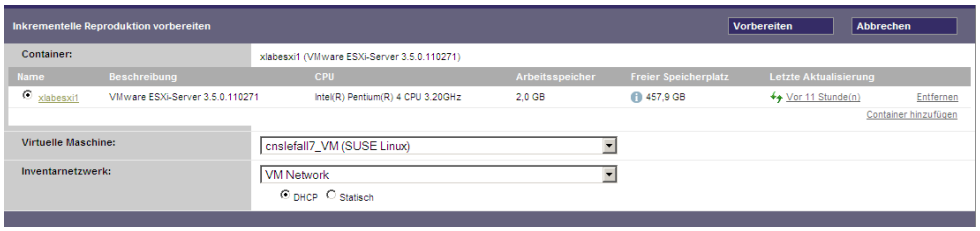
So richten Sie eine anfängliche Reproduktionsmethode ein:

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**.

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



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

5 Klicken Sie auf **Vorbereiten**.

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

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

6.7 Steuerung von Diensten und Daemons

PlateSpin Forge 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 99.

- **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.

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

Bei Linux-Systemen bietet PlateSpin Forge 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 98). 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`

6.9 Volumes Speicher

Beim Hinzufügen eines Workloads für den Schutz inventarisiert PlateSpin Forge die Speichermedien Ihres Ursprungs-Workloads und richtet automatisch Optionen auf der PlateSpin Forge-Weboberfläche ein, mit denen Sie die erforderlichen Volumes für den Schutz angeben können. Weitere Informationen finden Sie unter Abschnitt 1.1.5, „Unterstützter Speicher“ auf Seite 19.

Abbildung 6-1 zeigt die unter „Reproduktionseinstellungen“ festgelegten Parameter für einen Linux-Workload mit mehreren Volumes und zwei logischen Volumes in einer Volume-Gruppe.

Abbildung 6-1 *Volumes, logische Volumes und Volume-Gruppen eines geschützten Linux-Workloads*

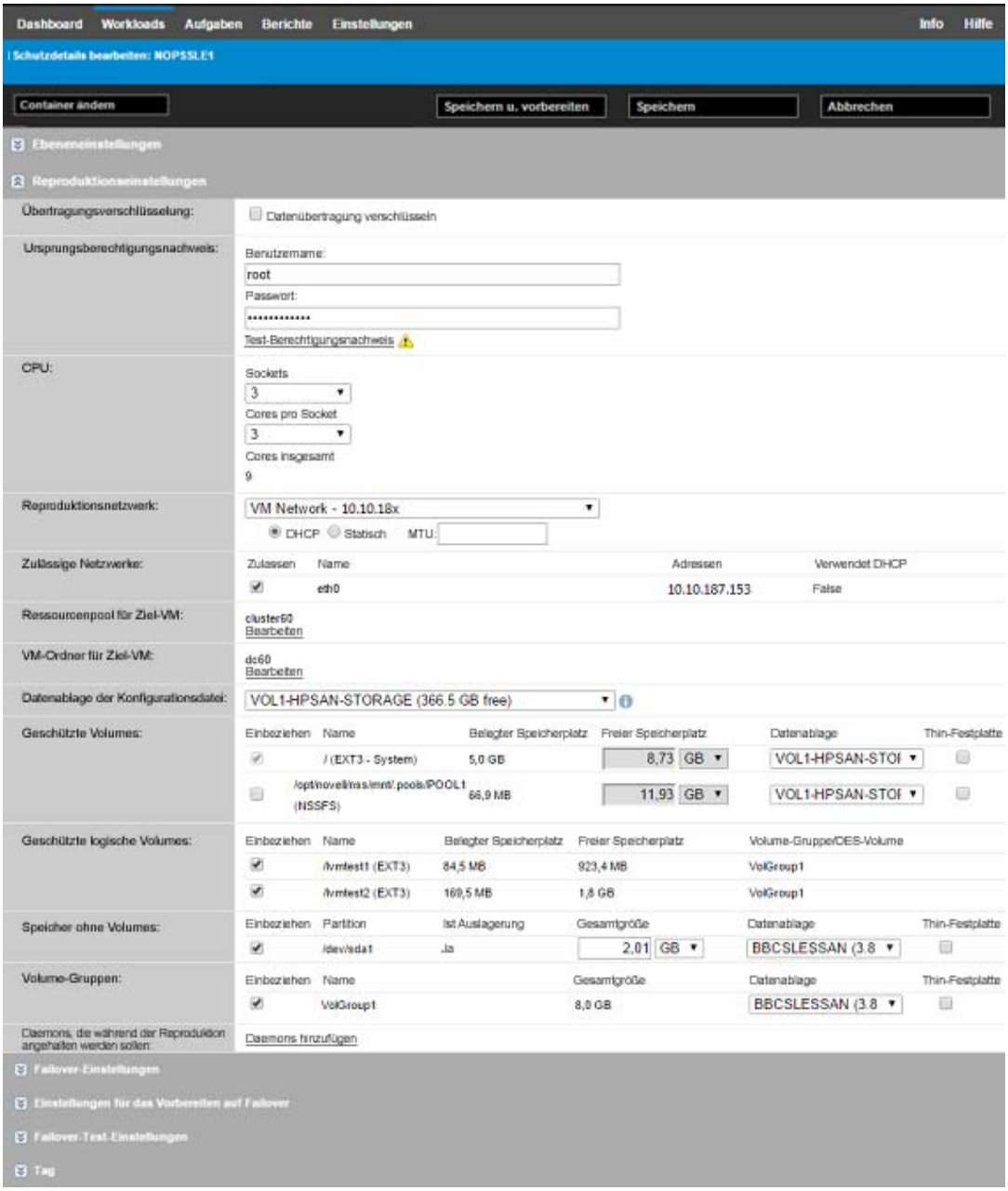


Abbildung 6-2 zeigt die Volume-Schutz-Optionen eines OES-11-Workloads, mit denen angegeben wird, dass das LVM2- und das NSS-Pool-Layout beibehalten und für den Failover-Workload neu erstellt werden soll:

Abbildung 6-2 *Reproduktionseinstellungen, Volume-bezogene Optionen (OES 11-Workload)*

Geschützte Volumes:	Einbeziehen	Name		Gesamtgröße	Datenablage	Thin-Festplatte
	☑	/ (EXT3 - System)		13,8 GB	BBCSLESSAN	☐
Geschützte logische Volumes:	Einbeziehen	Name		Gesamtgröße	Volume Group	
	☑	/lvmtest1 (EXT3)		1007,9 MB	VolGroup1	
	☑	/lvmtest2 (EXT3)		2,0 GB	VolGroup1	
	☑	/opt/novell/nss/mnt/.pools /POOL1 (NSSFS)		12,0 GB	POOL1	
Speicher ohne Volumes:	Einbeziehen	Partition	Ist Auslagerung	Gesamtgröße	Datenablage	Thin-Festplatte
	☑	/dev/sda1	Ja	2,0 GB	BBCSLESSAN	☐
Volume-Gruppen:	Einbeziehen	Name		Gesamtgröße	Datenablage	Thin-Festplatte
	☑	VolGroup1		8,0 GB	BBCSLESSAN	☐
OES-Volumes:	Einbeziehen	Name		Gesamtgröße	Datenablage	Thin-Festplatte
	☑	POOL1		12,0 GB	BBCSLESSAN	☐
Daemons, die während der Reproduktion angehalten werden sollen:	--					

Abbildung 6-3 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 6-3 *Reproduktionseinstellungen, Volume-bezogene Optionen (OES 2-Workload)*

Geschützte logische Volumes:	Einbeziehen	Name	Verwendeter Speicherplatz	Freier Speicherplatz	Volume-Gruppe / EVMS-Volumes	
	☑	/ (REISERFS)	2,2 GB	2,2 GB	system	
	☑	/boot (EXT2)	13,0 MB	55,3 MB	/dev/evms/sda1	
	☑	/opt/novell/nss/mnt/.pools/NEWPOOL (NSSFS)	23,3 MB	999,6 MB	NEWPOOL	
Speicher ohne Volumes:	Einbeziehen	Partition	Ist Auslagerung	Gesamtgröße	Datenablage-/Volume-Gruppe	
	☑	/dev/system/swap	Ja	1,48 GB	system	
Volume-Gruppen:	Einbeziehen	Name		Gesamtgröße	Datenablage	Thin-Festplatte
	☑	system		5,9 GB	dev-comp124:storage	☐
EVMS-Volumes	Einbeziehen	Name	Ist Auslagerung	Gesamtgröße	Datenablage	Thin-Festplatte
	☑	/dev/evms/sda1		70,6 MB	dev-comp124:storage	☐
	☑	NEWPOOL		1023,0 MB	dev-comp124:storage	☐
Daemons, die während der Reproduktion angehalten werden sollen:	Daemons hinzufügen					

6.10 Netzwerke

PlateSpin Forge 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.

6.11 Failback auf physische Computer

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

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

- Abschnitt 6.11.1, „Herunterladen des PlateSpin-Boot-ISO-Image“ auf Seite 102
- Abschnitt 6.11.2, „Einfügen weiterer Gerätetreiber in das Boot-ISO-Image“ auf Seite 102
- Abschnitt 6.11.3, „Registrieren von physischen Computern als Failback-Ziele mit PlateSpin Forge“ auf Seite 104

6.11.1 Herunterladen des PlateSpin-Boot-ISO-Image

Sie können die PlateSpin-Boot-ISO-Images (`p.iso` für BIOS-Firmware-basierte Ziele und bootofx.x2 für UEFI-Firmware-basierte Ziele) im Bereich PlateSpin Forge von NetIQ Downloads (http://dl.netiq.com) herunterladen. Führen Sie dazu eine Suche mit folgenden Parametern aus:

- **Produkt oder Technologie:** PlateSpin Forge
- **Version auswählen:** PlateSpin Forge 11.2
- **Datumsbereich:** Alle Datumsangaben

6.11.2 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
  ```

6.11.3 Registrieren von physischen Computern als Failback-Ziele mit PlateSpin Forge

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 Ihrer Forge-VM ein.

7 Geben Sie den Administrator-Berechtigungsnachweis für die Forge-VM 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 Forge-Weboberfläche verfügbar sein.

6.12 Schützen von Windows-Clustern

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

- **Windows Server 2012 R2:** Auf Server basierendes Microsoft-Failover-Cluster (Modelle *Knoten- und Datenträgermehrheit* und *Keine Mehrheit: Quorum nur für Datenträger*)
- **Windows Server 2008 R2:** Auf Server basierendes Microsoft-Failover-Cluster (Modelle *Knoten- und Datenträgermehrheit* und *Keine Mehrheit: Quorum nur für Datenträger*)
- **Windows Server 2003 R2:** Auf Server basierender Windows-Cluster-Server (*Single-Quorum Device Cluster*-Modell)

Sie können die Windows-Clusterermittlung in Ihrer PlateSpin-Umgebung je nach Bedarf aktivieren oder deaktivieren. Weitere Informationen hierzu finden Sie unter Abschnitt 6.12.2, „Aktivieren oder Deaktivieren der Windows-Clusterermittlung“ auf Seite 108.

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.

6.12.1 Schutz für Cluster-Workloads

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

- „Voraussetzungen“ auf Seite 106
- „Blockbasierte Übertragung“ auf Seite 107
- „Clusterknoten-Failover während der ersten vollständigen Reproduktion“ auf Seite 107
- „Clusterknoten-Failover während der Reproduktion“ auf Seite 107
- „Clusterknoten-Failover zwischen Reproduktionen“ auf Seite 107
- „Einrichtung des Schutzes“ auf Seite 108

Voraussetzungen

Der Umfang der Unterstützung des Cluster-Schutzes ist von folgenden Bedingungen abhängig:

- **Hostname oder IP-Adresse des aktiven Knotens:** Beim Hinzufügen eines Workloads 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.
- **Aktive Knotenermittlung:** Die globale PlateSpin-Konfigurationseinstellung `DiscoverActiveNodeAsWindowsCluster` muss auf `True` festgelegt sein. auf der Konfigurationsseite für den PlateSpin-Server. Das ist die Standardeinstellung. Weitere Informationen hierzu finden Sie unter Abschnitt 6.12.2, „Aktivieren oder Deaktivieren der Windows-Clusterermittlung“ auf Seite 108.
- **Suchwerte für den Ressourcennamen:** Geben Sie Suchwerte an, mit denen PlateSpin Forge den Namen der gemeinsam genutzten Cluster-IP-Adressressource vom Namen anderer IP-Adressressourcen im Cluster unterscheiden kann. Weitere Informationen hierzu finden Sie unter Abschnitt 6.12.3, „Suchwerte für den Ressourcennamen“ auf Seite 108.
- **Auflösbarer Hostname:** Der PlateSpin-Server muss den Hostnamen aller Knoten im Cluster auflösen können.

  HINWEIS: Der Hostname muss sich über die IP-Adresse auflösen lassen. Dies bedeutet, dass sowohl das Nachschlagen des Hostnamens als auch das rekursive Nachschlagen erforderlich ist.

- **Quorum-Ressource:** Die Quorum-Ressource eines Clusters muss in der Ressourcengruppe (Dienst) des zu schützenden Clusters koexistieren.
- **PowerShell 2.0:** Die Windows PowerShell 2.0-Engine muss auf allen Knoten im Cluster installiert sein.

Blockbasierte Übertragung

Bei einer blockbasierten Übertragung der Cluster-Workloads werden die blockbasierten Treiberkomponenten nicht auf dem Clusterknoten installiert. Die blockbasierte Übertragung erfolgt anhand einer treiberlosen Synchronisierung mit einer MD5-basierten Reproduktion. Da der blockbasierte Treiber nicht installiert ist, ist kein Neustart auf den Clusterknoten der Quelle erforderlich.

HINWEIS: Die dateibasierte Übertragung wird nicht unterstützt, um die Microsoft Windows-Cluster zu schützen.

Clusterknoten-Failover während der ersten vollständigen Reproduktion

Bei einem Cluster-Workload muss die erste vollständige Reproduktion fehlerfrei und ohne Clusterknoten-Failover abgeschlossen werden. Falls vor Abschluss der ersten vollständigen Reproduktion ein Clusterknoten-Failover erfolgt, müssen Sie den vorhandenen Workload entfernen, den Cluster über den aktiven Knoten erneut hinzufügen und dann den Vorgang wiederholen.

Clusterknoten-Failover während der Reproduktion

Wenn während einer vollständigen oder inkrementellen Reproduktion ein Clusterknoten-Failover vor Abschluss des Kopiervorgangs auftritt, dann wird der Befehl abgebrochen, und eine Meldung wird angezeigt, die besagt, dass die Reproduktion erneut ausgeführt werden muss.

Clusterknoten-Failover zwischen Reproduktionen

Die Knoten müssen ähnliche Profile aufweisen, damit der Reproduktionsvorgang nicht unterbrochen wird. Wenn ein Clusterknoten-Failover zwischen inkrementellen Reproduktionen eines geschützten Clusters auftritt und das neue Profil des aktiven Knotens in etwa dem fehlerhaften aktiven Knoten entspricht, wird der Schutzvertrag wie geplant für die nächste inkrementelle Reproduktion fortgesetzt. Andernfalls wird der Befehl für die nächste inkrementelle Reproduktion nicht ausgeführt.

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 143.

  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.

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 unter „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“ auf Seite 73.

6.12.2 Aktivieren oder Deaktivieren der Windows-Clusterermittlung

Der PlateSpin Forge-Server kann Windows Server-Failover-Cluster in der PlateSpin-Umgebung anhand des jeweils aktiven Knotens in den einzelnen Clustern ermitteln und inventarisieren. Alternativ werden alle aktiven und nicht aktiven Clusterknoten als eigenständige Computer behandelt.

Zum Aktivieren der Clusterermittlung für alle Windows-Cluster stellen Sie den Parameter `DiscoverActiveNodeAsWindowsCluster` auf `True` 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 „Voraussetzungen“ auf Seite 106.

Zum Deaktivieren der Clusterermittlung für alle Windows-Cluster stellen Sie den Parameter `DiscoverActiveNodeAsWindowsCluster` auf `False` 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**.

6.12.3 Suchwerte für den Ressourcennamen

Damit der aktive Knoten in einem Windows-Failovercluster erkannt werden kann, muss PlateSpin Forge 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 Forge 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**.

6.12.4 Zeitüberschreitung bei Quorumvermittlung

Mit dem globalen Parameter `FailoverQuorumArbitrationTimeout` auf der Konfigurationsseite für den PlateSpin-Server legen Sie den Regstrierungsschlüssel „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**.

6.12.5 Festlegen der Seriennummern des lokalen Volumes

Mit dem angepassten Dienstprogramm *Volume Manager* können Sie die Seriennummern des lokalen Volumes ändern, so dass sie in den einzelnen Knoten des Clusters übereinstimmen. Weitere Informationen hierzu finden Sie unter „Synchronisieren von Seriennummern im lokalen Clusterknoten-Speicher“ auf Seite 143.

6.12.6 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).

6.12.7 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 Failovers auf `Festplatte 1` und die zusätzlichen Festplatten des Failovers (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).

---

7 Hilfswerkzeuge für die Arbeit mit physischen Computern

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

7.1 Verwalten der Gerätetreiber

PlateSpin Forge wird mit einer Bibliothek an Gerätetreibern ausgeliefert. Die passenden Treiber werden automatisch auf den Ziel-Workloads installiert. Falls Treiber fehlen oder nicht kompatibel sind oder falls Sie für Ihre Zielinfrastruktur bestimmte Treiber benötigen, müssen Sie möglicherweise Treiber zur PlateSpin Forge-Treiberdatenbank hinzufügen (hochladen).

In den folgenden Abschnitten finden Sie weitere Details:

7.1.1 Verpacken von Gerätetreibern für Windows-Systeme

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

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

Die Treiber können nun hochgeladen werden. Weitere Informationen hierzu finden Sie unter „Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin“ auf Seite 112.

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

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

---

7.1.2 Verpacken von Gerätetreibern für Linux-Systeme

Wenn Sie ein Paket Ihrer Linux-Gerätetreiber erstellen möchten, um sie in die PlateSpin Forge-Treiberdatenbank hochzuladen, können Sie hierfür ein benutzerdefiniertes Dienstprogramm verwenden, das in Ihrem PlateSpin-ISO-Boot-Image enthalten ist.

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 Treibern in die Gerätetreiberdatenbank von PlateSpin“ auf Seite 112.

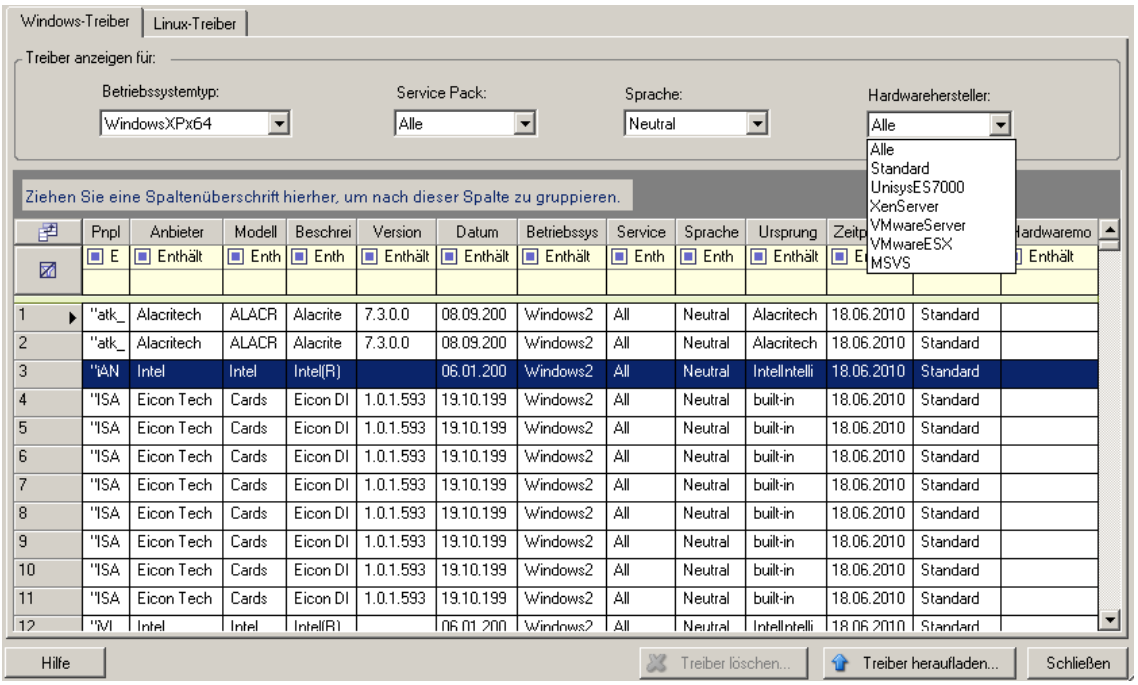
7.1.3 Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin

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

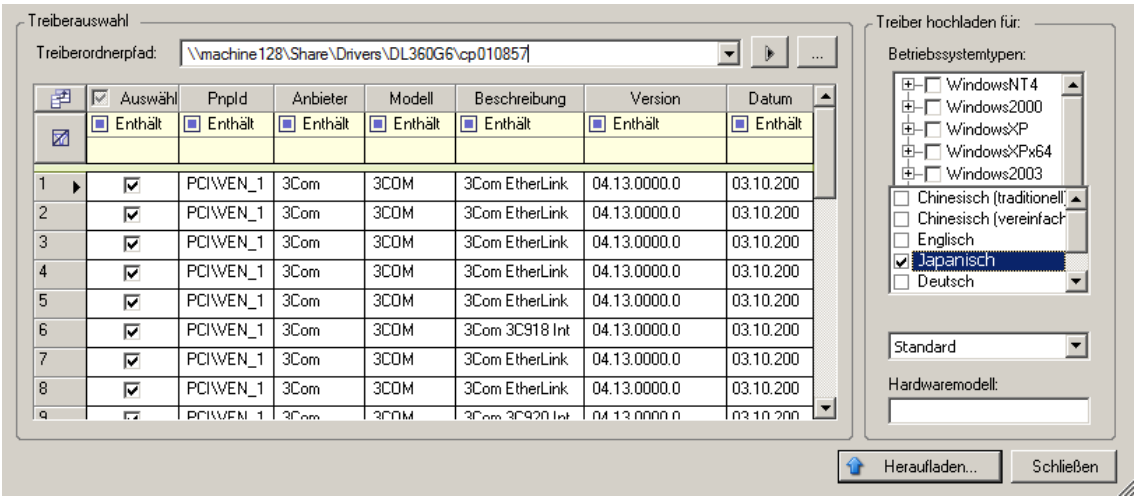
HINWEIS: Beim Heraufladen von Treibern überprüft PlateSpin Forge nicht, ob der Treiber zum ausgewählten Betriebssystem bzw. den Bit-Spezifikationen passt. Laden Sie daher nur solche Treiber herauf, die für die Zielinfrastruktur geeignet sind.

Upload-Prozedur für Gerätetreiber (Windows)

1. Beziehen Sie die erforderlichen Gerätetreiber und bereiten Sie diese vor. Weitere Informationen hierzu finden Sie unter Verpacken von Gerätetreibern für Windows-Systeme.
2. Starten Sie auf Ihrer Forge-VM unter `Programme\PlateSpin Forge Server\DriverManager` das Programm `DriverManager.exe` und wählen Sie die Registerkarte **Windows-Treiber** aus.



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



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

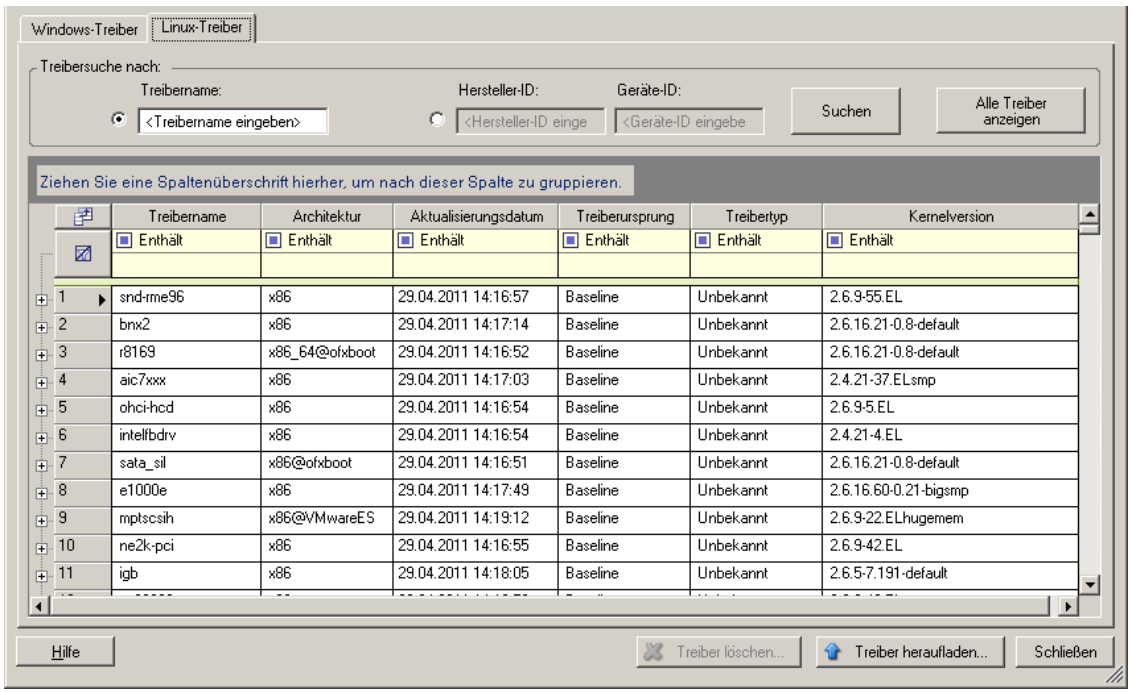
4 Klicken Sie auf **Heraufladen...** und bestätigen Sie Ihre Auswahl.

Das System lädt die ausgewählten Treiber in die Treiberdatenbank.

Upload-Prozedur für Gerätetreiber (Linux)

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

2 Klicken Sie auf **Werkzeuge** > **Gerätetreiber verwalten** und wählen Sie die Registerkarte **Linux-Treiber** aus:



3 Klicken Sie auf **Treiber heraufladen...**, 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.

7.1.4 Verwenden der Funktion für die Plug-&-Play-(PNP-)ID-Übersetzung

„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

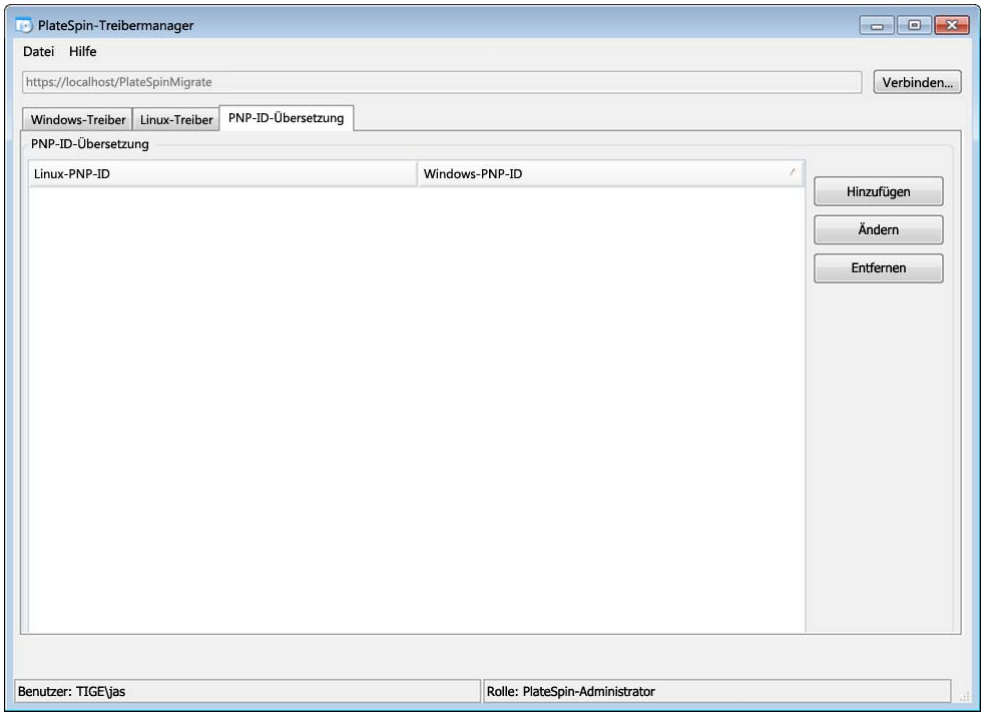
Betriebssysteme geführt. Da unter Windows und Linux unterschiedliche Formate für die PnP-IDs verwendet werden, enthält ein Windows-Workload, der vom Forge-Linux-RAM-Datenträger erkannt wird, PnP-IDs im Linux-Format.

Diese IDs sind einheitlich formatiert, so dass PlateSpin die zugehörige Windows-PnP-ID anhand der Standardumwandlung feststellen kann. Die Übersetzung erfolgt automatisch im PlateSpin-Produkt. Mit dieser Funktion sind Sie oder ein Kundendiensttechniker in der Lage, benutzerdefinierte PnP-Zuordnungen hinzuzufügen, zu bearbeiten oder zu entfernen.

So verwenden Sie die Übersetzungsfunktion für PnP-IDs:

1 Starten Sie den PlateSpin-Treibermanager, und stellen Sie eine Verbindung zum PlateSpin-Server her.

2 Wechseln Sie im Treibermanager zur Registerkarte „PNP-ID-Übersetzung“. Die Liste **PNP-ID-Übersetzung** mit den derzeit bekannten benutzerdefinierten PnP-ID-Zuordnungen wird geöffnet.



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

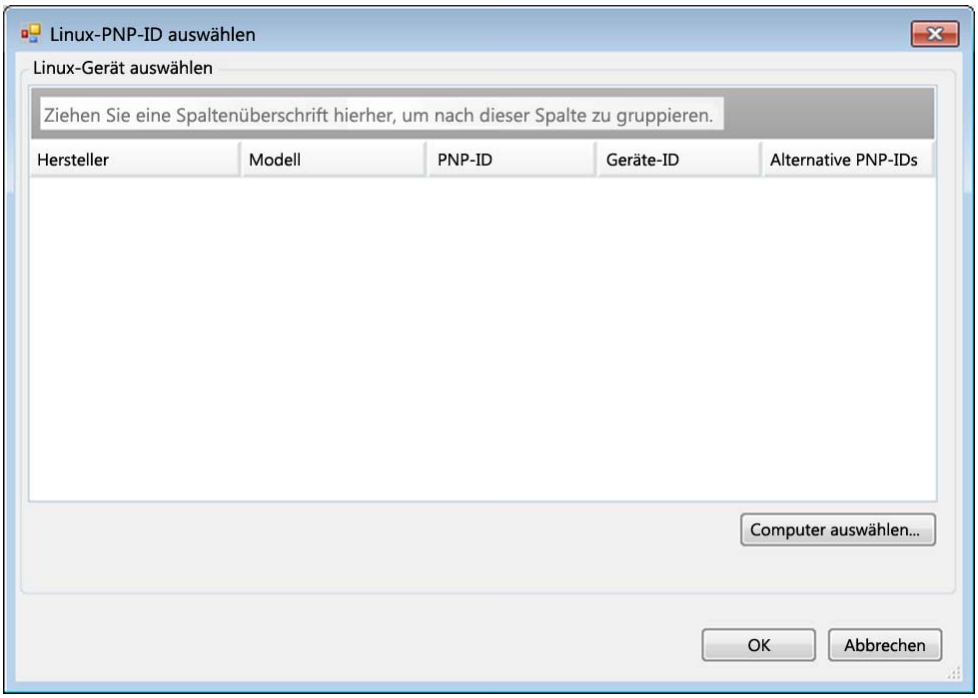
4 Fügen Sie dem Feld **Linux-PNP-ID** eine Linux-PnP-ID hinzu.

4a (Bedingt) Wenn Ihnen die Linux-PnP-ID bekannt ist, geben Sie diese ID ein.

Alternativ:

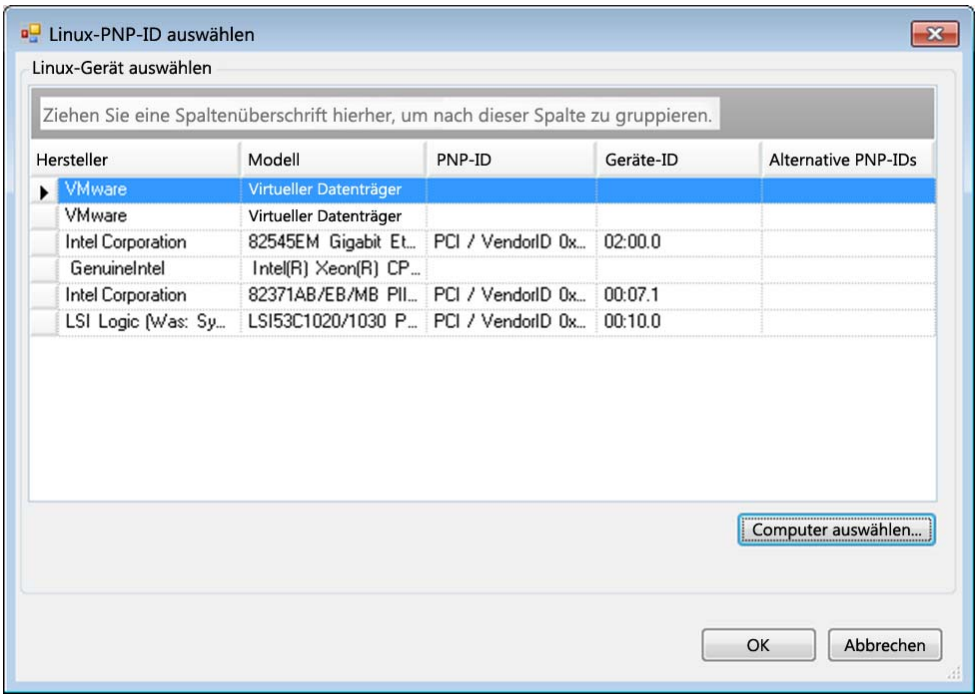
4b (Bedingt) Wählen Sie eine ID aus einem zuvor erkannten Workload aus:

4b1 Klicken Sie neben dem Feld **Linux-PNP-ID** auf **Auswählen**. Das Dialogfeld „Linux-PNP-ID auswählen“ wird geöffnet.



4b2 Klicken Sie im Dialogfeld auf **Computer auswählen**. Eine Liste der Computer, die zuvor durch den PlateSpin-Linux-RAM-Datenträger erkannt wurden, wird angezeigt.

4b3 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.



4b4 Wählen Sie ein Gerät aus 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.

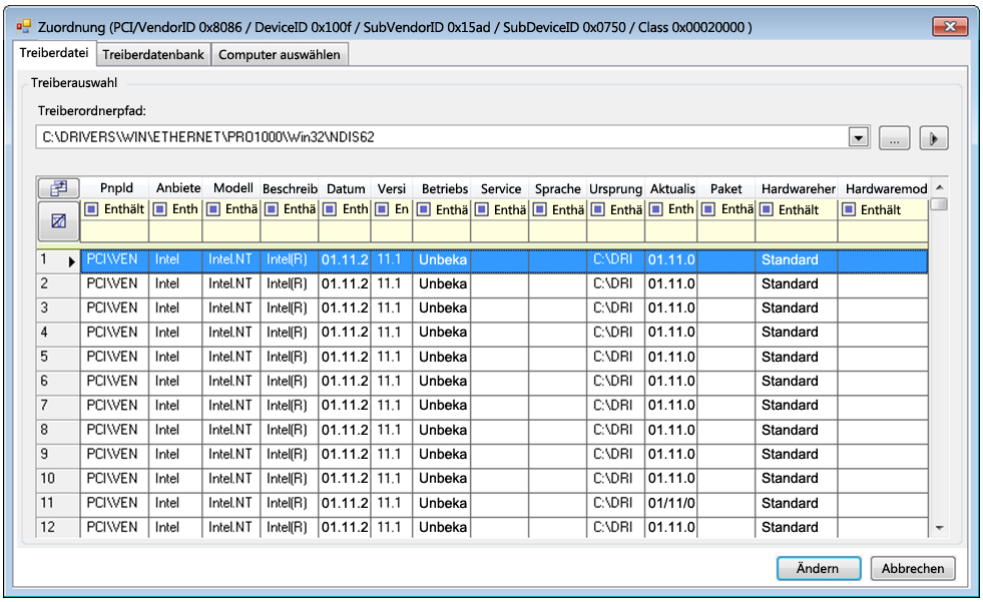
5 Fügen Sie dem Feld **Windows-PNP-ID** eine Windows-PnP-ID hinzu.

5a (Bedingt) Wenn Ihnen die Windows-PnP-ID bekannt ist, geben Sie diese ID ein.

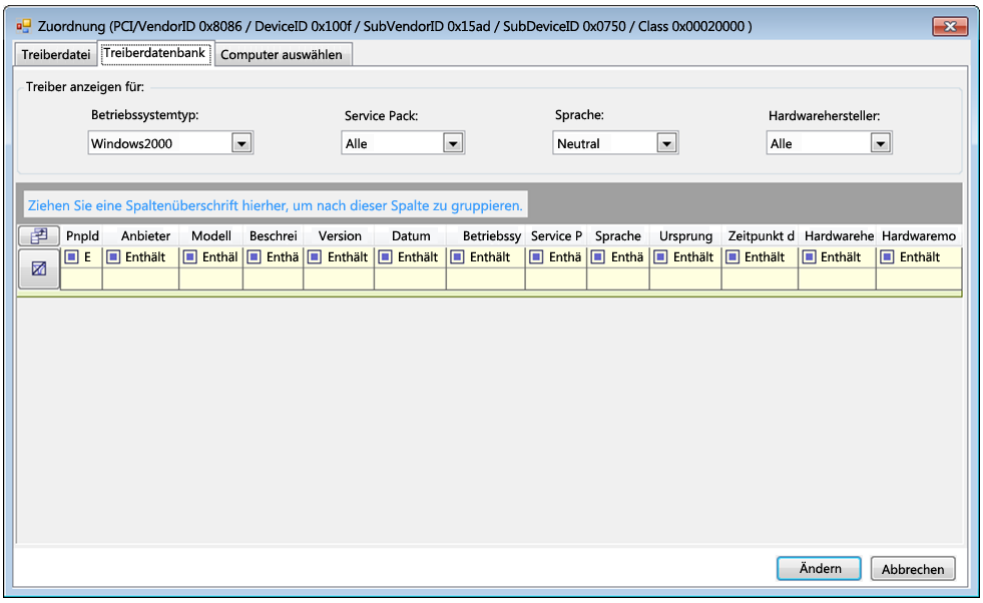
Alternativ:

5b (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:

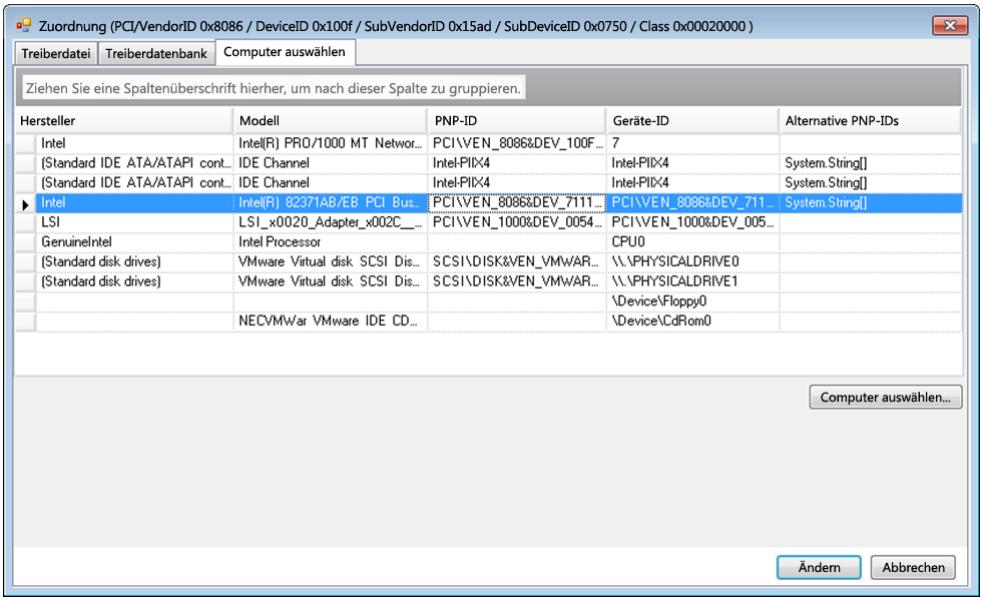
- Markieren Sie auf der Registerkarte **Treiberdatei** eine Windows-Treiberdatei (also eine Datei mit der Dateinamenerweiterung `*.inf`), wählen Sie die gewünschte PnP-ID aus, und klicken Sie auf **Ändern**.



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

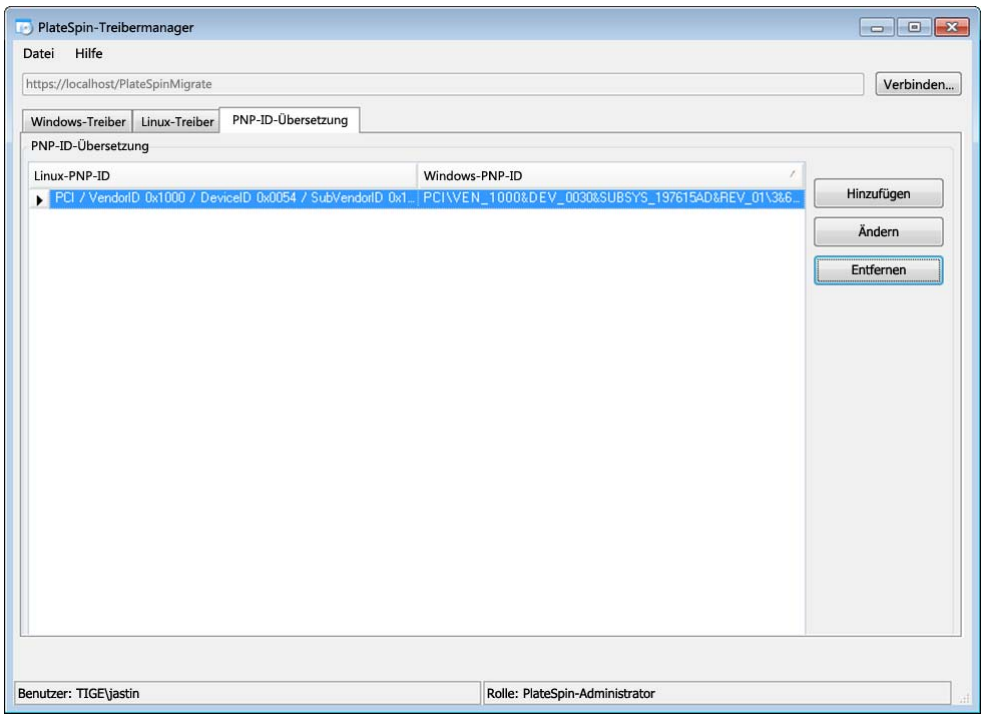


- Klicken Sie auf der Registerkarte **Computer auswählen** auf **Computer auswählen**. Wählen Sie dann in der Liste der Windows-Computer, die während der Live-Ermittlung erkannt wurden, einen Computer aus, und klicken Sie auf **OK**. Die Geräte dieses Computers werden angezeigt. Wählen Sie die gewünschte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

6 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.



7 (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:

7a Klicken Sie auf **Ändern**. Das Dialogfeld „PNP-ID-Zuordnung erstellen“ wird geöffnet.

7b Wiederholen Sie Schritt 5 auf Seite 117, und bearbeiten Sie die Windows-PnP-ID.

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

---

8 ProtectAgent-Dienstprogramm

Mit dem Befehlszeilenprogramm ProtectAgent (`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 ein Neustart erfolgen; mit ProtectAgent können Sie präzise steuern, wann diese Aktionen ausgeführt werden und somit wann der Server neu gestartet wird. Mit ProtectAgent ist es beispielsweise möglich, die Treiber während einer geplanten Ausfallzeit statt während der ersten Reproduktion zu installieren.

Die Syntax für das ProtectAgent-Dienstprogramm lautet:

```
ProtectAgent.cli.exe [Option] [/psserver=%IP%]
```

Tabelle 8-1 zeigt die verfügbaren Optionen und den verfügbaren Switch für den Befehl `ProtectAgent.cli.exe`.

Tabelle 8-1 *Befehlsoptionen und Switch für ProtectAgent*

Verwendung	Beschreibung
Optionen	
`h |? | help`	Zeigt die Nutzung und die Optionen für den Befehl.
`logs|view-logs`	Öffnet das Anwendungsprotokollverzeichnis.
`status`	Zeigt den Installationsstatus für den Controller und die Treiber in PlateSpin.
`din|driver-install`	Installiert die PlateSpin-Treiber.
`dup|driver-upgrade`	Rüstet die PlateSpin-Treiber auf.
`dun|driver-uninstall`	Deinstalliert die PlateSpin-Treiber.
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.

Eine Kopie der Treiber für die blockbasierte Übertragung ist im Bundle mit dem ProtectAgent-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 ProtectAgent-Befehlszeilenprogramm jedoch nicht.

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

Sie sollten das System 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 8-1). Während der Reproduktion wird die Benachrichtigung auf der Seite „Befehlsdetails“ angezeigt (Abbildung 8-2).

Abbildung 8-1 *Aufgabe für Neustart-Benachrichtigung*

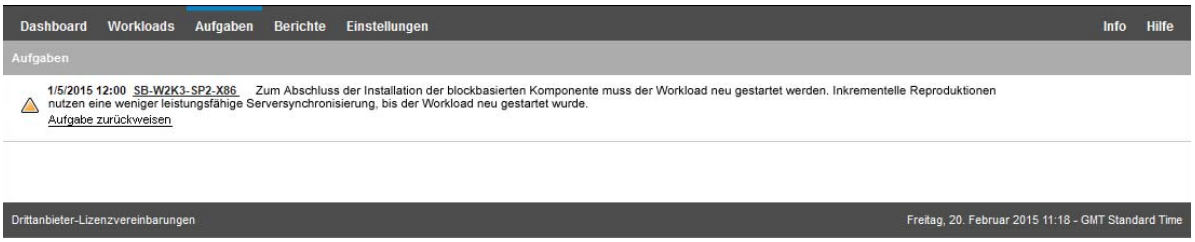
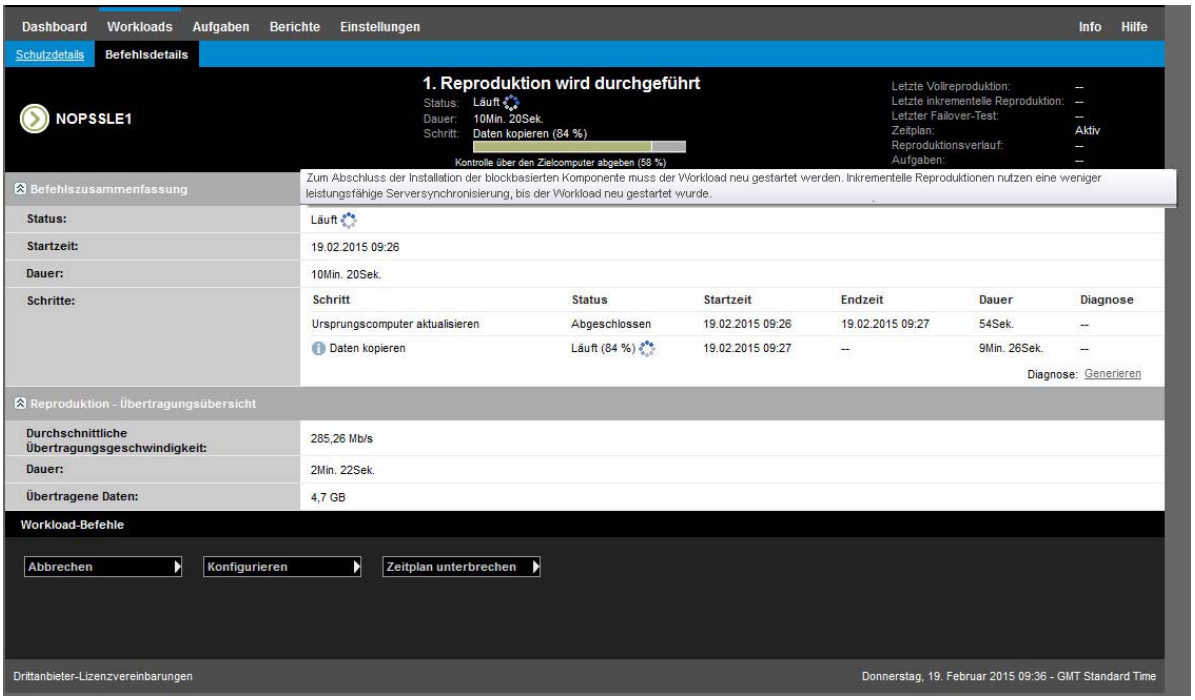
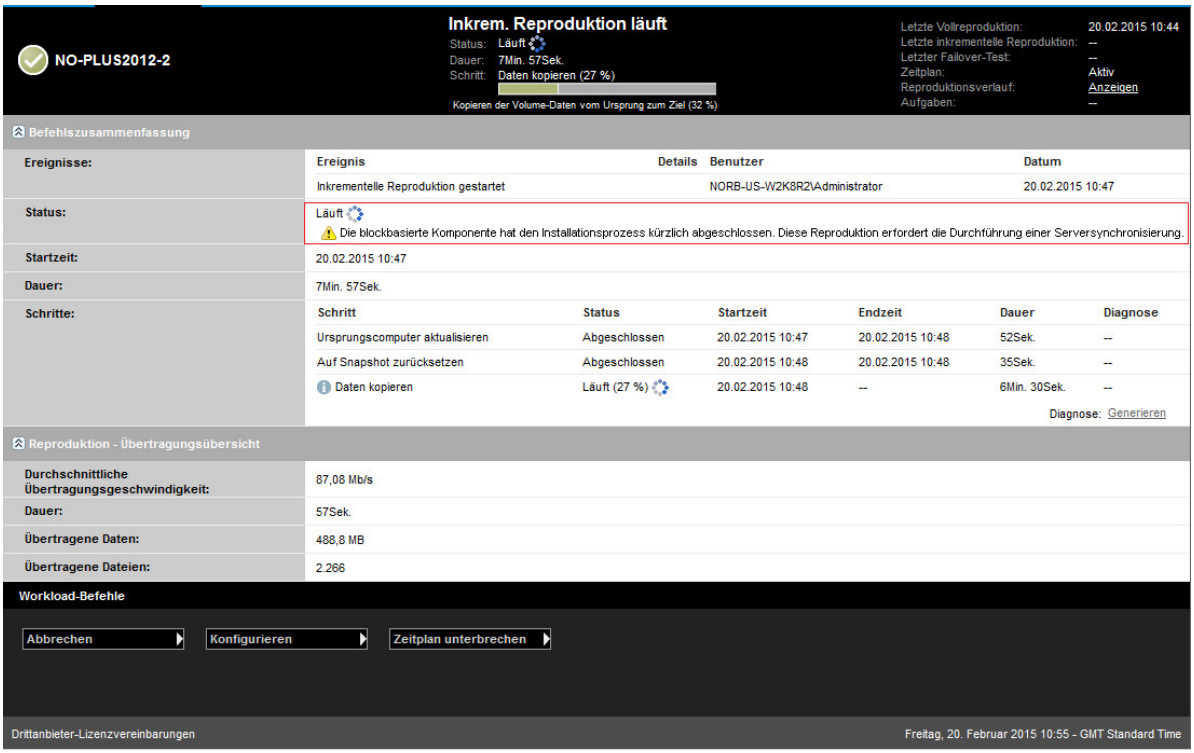


Abbildung 8-2 *Neustart-Benachrichtigung während der Reproduktion*



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 Serversynchronisierungs-Reproduktion wird dem Benutzer im Feld „Status“ als Warnmeldung angezeigt (Abbildung 8-3). Nachfolgende inkrementelle Reproduktionen werden ohne Warnmeldung ausgeführt.

Abbildung 8-3 *Benachrichtigung über erforderliche Serversynchronisierung*



9 Fehlersuche

Dieser Abschnitt enthält folgende Informationen:

9.1 Fehlerbehebung bei der Workload-Inventarisierung (Windows)

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

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.`	Bei dem Versuch, einen Workload hinzuzufügen, wurde ein Nicht-Administratorkonto verwendet. Verwenden Sie ein Administratorkonto oder fügen Sie den Benutzer zur Administratorgruppe hinzu und versuchen Sie es erneut. Diese Meldung kann auch auf einen WMI-Verbindungsfehler hinweisen. Probieren Sie die nachfolgend aufgeführten Lösungsmöglichkeiten aus und führen Sie dann den „WMI-Verbindungstest“ auf Seite 127 erneut durch. Wenn der Test erfolgreich ist, versuchen Sie erneut, den Workload hinzuzufügen. ◆ „Fehlerbehebung bei DCOM-Verbindungen“ auf Seite 127 ◆ „Fehlerbehebung bei der RPC-Dienst-Verbindung“ auf Seite 128
`Es konnte keine Verbindung zum Windows-Server hergestellt werden. Netzwerkpfad nicht gefunden.`	Netzwerk-Verbindungsfehler. Führen Sie die Tests in „Durchführen von Verbindungstests“ auf Seite 127 durch. Falls ein Test fehlschlägt, stellen Sie sicher, dass sich PlateSpin Forge 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 128.
	◆ Die Datei- und Drucker-Freigabe für Microsoft-Netzwerke ist möglicherweise nicht aktiviert. Aktivieren Sie die Freigabe in den Eigenschaften der Netzwerkschnittstellenkarte.
	◆ Die Admin$-Freigaben auf dem Ursprung sind möglicherweise nicht zugänglich. Stellen Sie sicher, dass PlateSpin Forge auf diese Freigaben zugreifen kann. Weitere Informationen hierzu finden Sie unter „Aktivieren von Datei-/Freigabe-Berechtigungen und -Zugriff“ auf Seite 128.
	◆ 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.

In den folgenden Abschnitten finden Sie weitere Informationen zur Fehlersuche bei Windows-Workloads:

- Abschnitt 9.1.1, „Durchführen von Verbindungstests“ auf Seite 127
- Abschnitt 9.1.2, „Deaktivieren der Virenschutz-Software“ auf Seite 128
- Abschnitt 9.1.3, „Aktivieren von Datei-/Freigabe-Berechtigungen und -Zugriff“ auf Seite 128

9.1.1 Durchführen von Verbindungstests

- „Netzwerk-Verbindungstest“ auf Seite 127
- „WMI-Verbindungstest“ auf Seite 127
- „Fehlerbehebung bei DCOM-Verbindungen“ auf Seite 127
- „Fehlerbehebung bei der RPC-Dienst-Verbindung“ auf Seite 128

Netzwerk-Verbindungstest

Führen Sie diesen Basistest der Netzwerkverbindung durch, um festzustellen, ob PlateSpin Forge mit dem Workload kommunizieren kann, den Sie zu schützen versuchen.

1. Wechseln Sie zu Ihrer Forge-VM.

   Weitere Informationen hierzu finden Sie unter „Herunterladen des vSphere-Clientprogramms“ auf Seite 57.

2. Öffnen Sie ein Befehlszeilenfenster und senden Sie einen Ping-Befehl an Ihren Workload:

   `ping` *Workload-IP-Adresse*

WMI-Verbindungstest

1. Wechseln Sie zu Ihrer Forge-VM.

   Weitere Informationen hierzu finden Sie unter „Herunterladen des vSphere-Clientprogramms“ auf Seite 57„Herunterladen des vSphere-Clientprogramms“ auf Seite 57.

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

   `\\win2k\root\cimv2`

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

   Wenn eine Fehlermeldung zurückgegeben wird, kann keine WMI-Verbindung zwischen PlateSpin Forge 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:

- PlateSpin Forge und der Workload müssen sich auf derselben Seite der Firewall befinden
- Öffnen spezifischer Ports zwischen PlateSpin Forge und dem Workload (siehe „Konfigurieren der Zugriffs- und Kommunikationseinstellungen im gesamten Schutznetzwerk“ auf Seite 34)

9.1.2 Deaktivieren der Virenschutz-Software

Virenschutz-Software kann gelegentlich einige der PlateSpin Forge-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. Dies kann mitunter die dateibasierte Datenreproduktion verhindern. Wenn Sie den Workload-Schutz konfigurieren, können Sie in diesem Fall die zu deaktivierenden Dienste auswählen, z. B. Dienste, die von Virenschutz-Software installiert und verwendet werden. Diese Dienste werden nur für die Dauer der Dateiübertragung deaktiviert. Sobald der Prozess abgeschlossen ist, werden sie wieder gestartet. Bei einer Datenreproduktion auf Blockebene ist dies nicht erforderlich.

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

Für den zuverlässigen Schutz eines Workloads muss PlateSpin Forge erfolgreich Software innerhalb des Workloads bereitstellen und installieren. Bei der Bereitstellung dieser Komponenten auf einem Workload sowie während des Hinzufügens eines Workloads verwendet PlateSpin Forge die

administrativen Freigaben des Workloads. PlateSpin Forge 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 von der Forge-VM aus zugänglich sind:

1. Wechseln Sie zu Ihrer Forge-VM.

   Weitere Informationen hierzu finden Sie unter „Herunterladen des vSphere-Clientprogramms“ auf Seite 57.
2. Klicken Sie auf **Start > Ausführen**, geben Sie `\\<Server-Host>\Admin$` ein und klicken Sie anschließend auf **OK**.
3. Verwenden Sie bei Aufforderung denselben Berechtigungsnachweis wie für das Hinzufügen des Workloads zum PlateSpin Forge-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 Forge ändert den vorhandenen Inhalt des Volumes nicht. Es erstellt jedoch ein eigenes Verzeichnis, für das es Zugriff und Berechtigungen benötigt.

9.2 Fehlerbehebung bei der Workload-Inventarisierung (Linux)

Probleme oder Meldungen	Lösungen
`Es konnte weder eine Verbindung zum SSH-Server, der auf <IP-Adresse> läuft, noch zu den VMware Virtual Infrastructure-Webdiensten unter <IP-Adresse>/sdk hergestellt werden.`	Diese Meldung wird aufgrund mehrerer möglicher Ursachen ausgegeben: ◆ Der Workload ist nicht erreichbar. ◆ Auf dem Workload wird SSH nicht ausgeführt. ◆ Die Firewall ist aktiv und die erforderlichen Ports wurden nicht geöffnet. ◆ Das spezifische Betriebssystem des Workloads wird nicht unterstützt. Informationen zu Netzwerk- und Zugriffsanforderungen für einen Workload finden Sie unter „Konfigurieren der Zugriffs- und Kommunikationseinstellungen im gesamten Schutznetzwerk“ auf Seite 34.
`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 92.

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

Probleme oder Meldungen	Lösungen
Authentifizierungsfehler beim Überprüfen der Controller-Verbindung während der Einrichtung des Controllers auf dem Ursprung.	Das für das Hinzufügen eines Workloads verwendete Konto muss von dieser Richtlinie zugelassen sein. Weitere Informationen hierzu finden Sie unter „Gruppenrichtlinie und Benutzerrechte“ auf Seite 131.
Es konnte nicht festgestellt werden, ob .NET Framework installiert ist (mit Ausnahme `Die vertrauenswürdige Beziehung zwischen dieser Arbeitsstation und der primären Domäne ist fehlgeschlagen`).	Überprüfen Sie, ob der Remoteregistrierungsdienst auf dem Ursprung aktiviert ist und ausgeführt wird. Siehe auch „Fehlerbehebung bei der Workload-Inventarisierung (Windows)“ auf Seite 125.

9.3.1 Gruppenrichtlinie und Benutzerrechte

Aufgrund der Art und Weise, wie PlateSpin Forge 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.

9.4 Fehlerbehebung bei der Workload-Reproduktion

Probleme oder Meldungen	Lösungen
Behebbarer Fehler bei der Reproduktion während des Vorgangs **Erstellen eines Snapshots der virtuellen Maschine planen** oder **Planen des Zurücksetzens der virtuellen Maschine auf Snapshot vor dem Start**.	Dieses Problem tritt auf, wenn der Server ausgelastet ist und der Vorgang länger als erwartet dauert. Warten Sie, bis die Reproduktion abgeschlossen ist.
Workload-Problem erfordert Benutzereingriff.	Diese Meldung kann von verschiedenen Problemen verursacht worden sein. In den meisten Fällen sollte die Meldung weitere Angaben zur Art des Problems und dem Problembereich (wie Konnektivität, Berechtigungsnachweis etc.) enthalten. Warten Sie nach der Fehlersuche einige Minuten. Wenden Sie sich an den PlateSpin-Support, falls die Meldung weiterhin angezeigt wird.
Bei allen Workloads treten behebbare Fehler auf, da kein Speicherplatz mehr vorhanden ist.	Überprüfen Sie den freien Speicherplatz. Wenn mehr Platz erforderlich ist, entfernen Sie einen Workload.
Langsame Netzwerkgeschwindigkeiten unter 1 MB.	Stellen Sie sicher, dass die Duplex-Einstellung der Netzwerkschnittstellenkarte des Ursprungscomputers aktiviert ist und dass der Switch, mit dem sie verbunden ist, eine entsprechende Einstellung hat. Wenn der Switch auf automatisch gesetzt ist, kann der Ursprung nicht auf 100 MB eingestellt werden.

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 Ihrer Forge-VM). 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 44.

`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 zur Forge-VM 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 zur Forge-VM 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 die Forge-VM mit einer Domäne verbunden ist und die Domänenrichtlinien mit Einschränkungen angewendet werden. Weitere Informationen hierzu finden Sie unter „Gruppenrichtlinie und Benutzerrechte“ auf Seite 131.

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.

9.5 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).

9.6 Fehlersuche bei der Online-Hilfe

Auf einigen Systemen mit erweiterten Browser-Sicherheitseinstellungen (z. B. Internet Explorer 8 auf Windows Server 2008) funktionieren die Symbole zum Erweitern und Komprimieren (+ und -) im Inhaltsverzeichnis möglicherweise nicht. Aktivieren Sie zur Behebung des Problems in Ihrem Browser JavaScript.

So aktivieren Sie JavaScript:

- **Chrome:**
  1. Wählen Sie im Chrome-Menü den Befehl **Einstellungen**, blättern Sie zum Link **Erweiterte Einstellungen** und klicken Sie darauf.
  2. Klicken Sie unter **Datenschutz** auf **Inhaltseinstellungen**.
  3. Blättern Sie zum Eintrag **JavaScript** und wählen Sie **Ausführung von JavaScript für alle Websites zulassen**.
  4. Klicken Sie auf **Fertig**.

- **Firefox:**
  1. Geben Sie `about:config` in die Adressleiste ein und drücken Sie die Eingabetaste.
  2. Klicken Sie auf **Ich werde vorsichtig sein, versprochen!**.
  3. Geben Sie in das Feld **Suchen** die Zeichenfolge `javascript.enabled` ein und drücken Sie die Eingabetaste.
  4. Prüfen Sie in den Suchergebnissen den Wert für den Parameter `javascript.enabled`. Wenn der Wert `false` vorliegt, klicken Sie mit der rechten Maustaste auf `javascript.enabled` und wählen Sie **Umschalten**. Der Wert wechselt zu `true`.
- **Internet Explorer:**
  1. Wählen Sie im Menü „Extras“ den Befehl **Internetoptionen**.
  2. Wählen Sie das Register **Sicherheit** und klicken Sie auf **Stufe anpassen**.
  3. Blättern Sie zum Eintrag **Skripting > Active Scripting** und wählen Sie **Aktivieren**.
  4. Klicken Sie in der Warnmeldung auf **Ja** und klicken Sie dann auf **OK**.
  5. Klicken Sie auf **Anwenden** > **OK**.

9.7 Generieren und Anzeigen von Diagnoseberichten

Nachdem Sie auf der PlateSpin Forge 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.

9.8 Entfernen von Workloads

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

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

   (Bedingt) Bei Windows-Workloads, die zuvor durch eine Reproduktion auf Blockebene geschützt wurden, fordert die PlateSpin Forge-Weboberfläche Sie auf, 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.

2 Klicken Sie auf der Seite „Befehlsbestätigung“ auf **Bestätigen**, um den Befehl auszuführen. Warten Sie, bis der Vorgang abgeschlossen ist.

9.9 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.

Die entsprechenden Informationen finden Sie in den folgenden Abschnitten:

- Abschnitt 9.9.1, „Bereinigen von Windows-Workloads“ auf Seite 135
- Abschnitt 9.9.2, „Bereinigen von Linux-Workloads“ auf Seite 136

9.9.1 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. Eine Eingabeaufforderung öffnen und das aktuelle Verzeichnis ändern in: ◆ `\Programme\platespin*` (32-Bit-Systeme) ◆ `\Programme (x86)\platespin*` (64-Bit-Systeme) 2. Führen Sie den folgenden Befehl aus: `ofxcontroller.exe /uninstall` 3. Verzeichnis `platespin*` entfernen.

9.9.2 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.

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`

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

9.10 Verkleinern der PlateSpin Forge-Datenbanken

Sobald die PlateSpin Forge-Datenbanken (OFX, 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 Forge-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.

9.11 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 Quellcmputer 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 Anti-Viren-Software ausgeschlossen werden sollten.

Zur Vermeidung dieser Probleme empfiehlt NetIQ die folgenden bewährten Vorgehensweisen vor der Ausführung der ersten vollständigen Reproduktion:

- Aktualisieren Sie in jedem Fall Windows (Windows-Update) auf Ihrem Quellsystem, bevor Sie die erste vollständige Reproduktion ausführen. 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.
- Richten Sie die Anti-Viren-Software so ein, dass empfohlene Dateien und Ordner gemäß den Angaben in folgendem Dokument ausgeschlossen werden: *Microsoft Knowledge-Artikel: Empfehlungen zum Virenscan auf Unternehmenscomputern, auf denen unterstützte Windows-Versionen ausgeführt werden (KB: 822158)* (https://support.microsoft.com/en-us/kb/822158).

A Von Forge unterstützte Linux-Verteilungen

Die PlateSpin Forge-Software umfasst vorkompilierte Versionen des `blkwatch`-Treibers für viele fehlerfreie Linux-Verteilungen (32-Bit und 64-Bit). Dieser Abschnitt enthält folgende Informationen:

- Abschnitt A.1, „Analysieren Ihres Linux-Workloads“ auf Seite 139
- Abschnitt A.2, „PlateSpin Forge: Vorkompilierter „blkwatch“-Treiber (Linux)“ auf Seite 140

A.1 Analysieren Ihres Linux-Workloads

Bevor Sie feststellen können, ob PlateSpin Forge 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. Dieser Abschnitt enthält folgende Informationen:

- Abschnitt A.1.1, „Ermitteln der Versionszeichenkette“ auf Seite 139
- Abschnitt A.1.2, „Ermitteln der Architektur“ auf Seite 139

A.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.

A.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.

A.2 PlateSpin Forge: Vorkompilierter „blkwatch“-Treiber (Linux)

Die folgende Liste enthält fehlerfreie Linux-Verteilungen, für die PlateSpin Forge einen `blkwatch`-Treiber umfasst. Sie können die Liste durchsuchen und so ermitteln, ob die Version und Architektur des Kernels Ihres Linux-Workloads mit einer unterstützten Verteilung in der „Liste der Distributionen“ übereinstimmen. Wird Ihre Version und Architektur gefunden, bietet PlateSpin Forge 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 A.2.1, „Liste mit Elementsyntax“ auf Seite 140
- Abschnitt A.2.2, „Liste der Verteilungen“ auf Seite 140
- Abschnitt A.2.3, „Weitere Linux-Distributionen mit Unterstützung für „blkwatch“-Treiber“ auf Seite 140

A.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
```

A.2.2 Liste der Verteilungen

Eine Liste der unterstützten Kernel-Distributionen finden Sie unter „Liste der Distributionen“ im *PlateSpin Forge-Benutzerhandbuch*.

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

CentOS: PlateSpin Forge unterstützt Workloads für eine CentOS-Version, wenn diese auf einer unterstützten Red Hat Enterprise-Distribution beruht. Beachten Sie die RHEL-Einträge in der „Liste der Distributionen“ im *PlateSpin Forge-Benutzerhandbuch*.

Open Enterprise Server: PlateSpin Forge unterstützt Workloads für eine OES-2- oder OES-11-Version für Kernel-Version 3.0.27 (oder höher), wenn die OES-Version auf einer unterstützten SLES-Distribution (SUSE Linux Enterprise Server) beruht. Beachten Sie die SLES-Einträge in der „Liste der Distributionen“ im *PlateSpin Forge-Benutzerhandbuch*.

Oracle Enterprise Linux: PlateSpin Forge unterstützt Workloads für eine Oracle Enterprise Linux-Version, wenn diese auf einer unterstützten Red Hat Enterprise-Distribution beruht, jedoch keine Workloads mit dem Unbreakable-Enterprise-Kernel. Beachten Sie die RHEL-Einträge in der „Liste der Distributionen“ im *PlateSpin Forge-Benutzerhandbuch*.

B 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. Suchen Sie auf der NetIQ Downloads-Website nach dem Produkt PlateSpin Forge, und klicken Sie auf **Anfrage absenden**.
2. Wählen Sie auf der Registerkarte „Produkte“ die Option PlateSpin Forge 11.2. Die produktspezifische Download-Seite wird geöffnet. Klicken Sie dann auf **Mit dem Download fortfahren**.
3. Klicken Sie auf der Download-Seite in der Zeile **VolumeManager.exe** auf `Herunterladen` oder wählen Sie den entsprechenden Download-Manager-Link aus.
4. Laden Sie das Dienstprogramm herunter und kopieren Sie es anschließend für jeden Clusterknoten an einen Speicherort, auf den zugegriffen werden kann.
5. 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.
6. Überprüfen Sie, ob alle Seriennummern im lokalen Speicher des aktiven Knotens mit den Seriennummern im lokalen Speicher der jeweils anderen Knoten im Cluster übereinstimmen.

   6a Führen Sie in jedem Clusterknoten den Befehl `VolumeManager.exe -l` aus, um dessen Volume-Seriennummern abzurufen.

   6b Vergleichen Sie die Seriennummern im lokalen Speicher des aktiven Knotens (Schritt 5) mit den Seriennummern im lokalen Speicher des Knotens (Schritt 6a).

6c (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`

6d Wenn Sie alle Volume-Seriennummern im Knoten eines Clusters geändert haben, müssen Sie diesen Knoten neu starten.

6e Wiederholen Sie Schritt 6a bis Schritt 6d für jeden Knoten im Cluster.

7 (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.

C Anpassen der PlateSpin Forge-Weboberfläche an das Markenbild

Sie können das Erscheinungsbild der PlateSpin Forge-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:

- Abschnitt C.1, „Anpassen der Benutzeroberfläche an das Markenbild mithilfe von Konfigurationsparametern“ auf Seite 145
- Abschnitt C.2, „Anpassen des Produktnamens an das Markenbild in der Windows-Registrierungsdatenbank“ auf Seite 149

C.1 Anpassen der Benutzeroberfläche an das Markenbild mithilfe von Konfigurationsparametern

Wie andere Aspekte des Verhaltens des PlateSpin-Servers können Sie auch das Erscheinungsbild der Weboberfläche anhand von Konfigurationsparametern steuern, die Sie auf einer Konfigurationswebseite mit Ihrer Forge-VM (`https://`*`Ihr_PlateSpin-Server`*`/platespinconfiguration/`) festlegen. Mit diesen Parametern verleihen Sie der Weboberfläche das unverkennbare „Erscheinungsbild“ Ihres eigenen Unternehmens. In diesem Abschnitt finden Sie Informationen zur Anpassung an das Marktbild.

Gehen Sie wie folgt vor, um Konfigurationsparameter zu ändern oder anzuwenden:

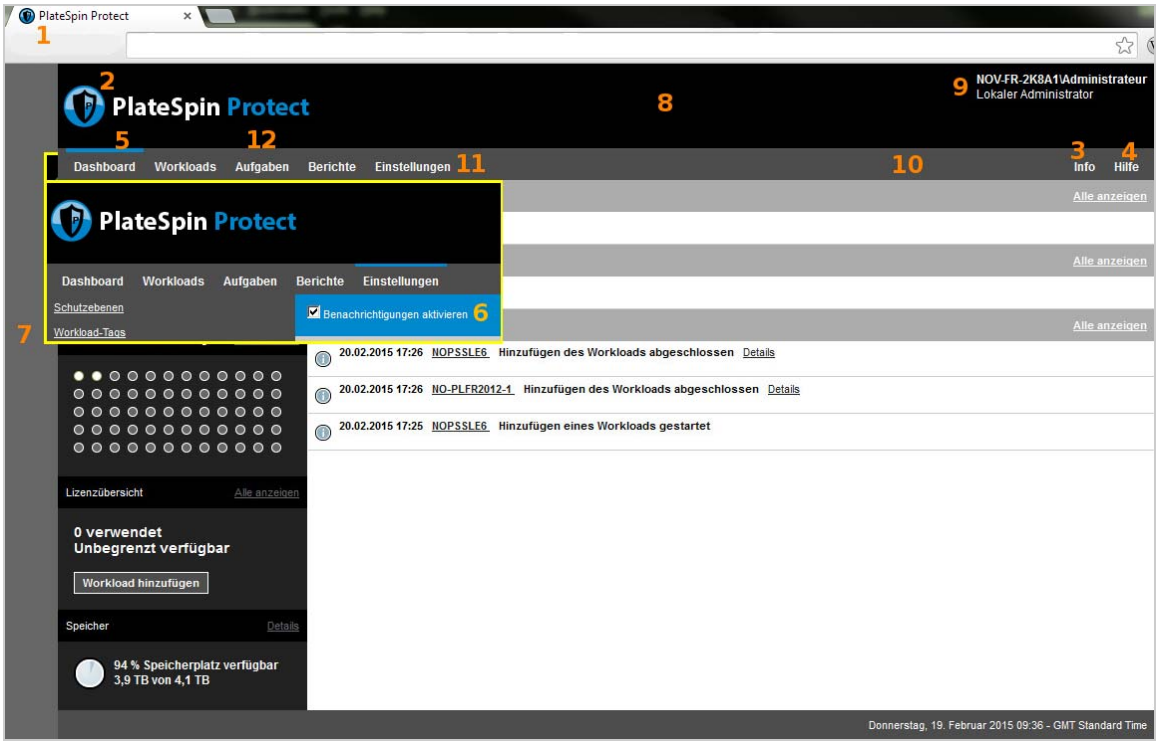
1. Öffnen Sie `https://`*`Ihr_PlateSpin-Server`*`/platespinconfiguration/` in einem beliebigen Webbrowser, und melden Sie sich als Administrator an.
2. Suchen Sie den gewünschten Serverparameter, klicken Sie auf **Bearbeiten**, und ändern Sie den Wert dieses Parameters.

   Weitere Informationen finden Sie in Abbildung C-1 sowie unter dem Namen, der Beschreibung und dem Standardwert für die Einstellungen der verschiedenen bearbeitbaren 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.

Die verschiedenen Seiten der Weboberfläche weisen einige gemeinsame Erscheinungsbildelemente auf. In der Darstellung des PlateSpin Forge-Dashboards in Abbildung C-1 sind die bearbeitbaren Elemente mit Zahlen gekennzeichnet.

Abbildung C-1 *PlateSpin Forge-Weboberfläche mit Kennzeichnung der konfigurierbaren Elemente (kleinere Zusatzabbildung eingefügt)*



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**.)

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`.

C.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\ForgeServer\Produktname`

   HINWEIS: Unter Umständen finden Sie diesen Registrierungsschlüssel hier:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PlateSpin\Forge`

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.

D 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 Forge 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.

D.1 API-Übersicht

PlateSpin Forge 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

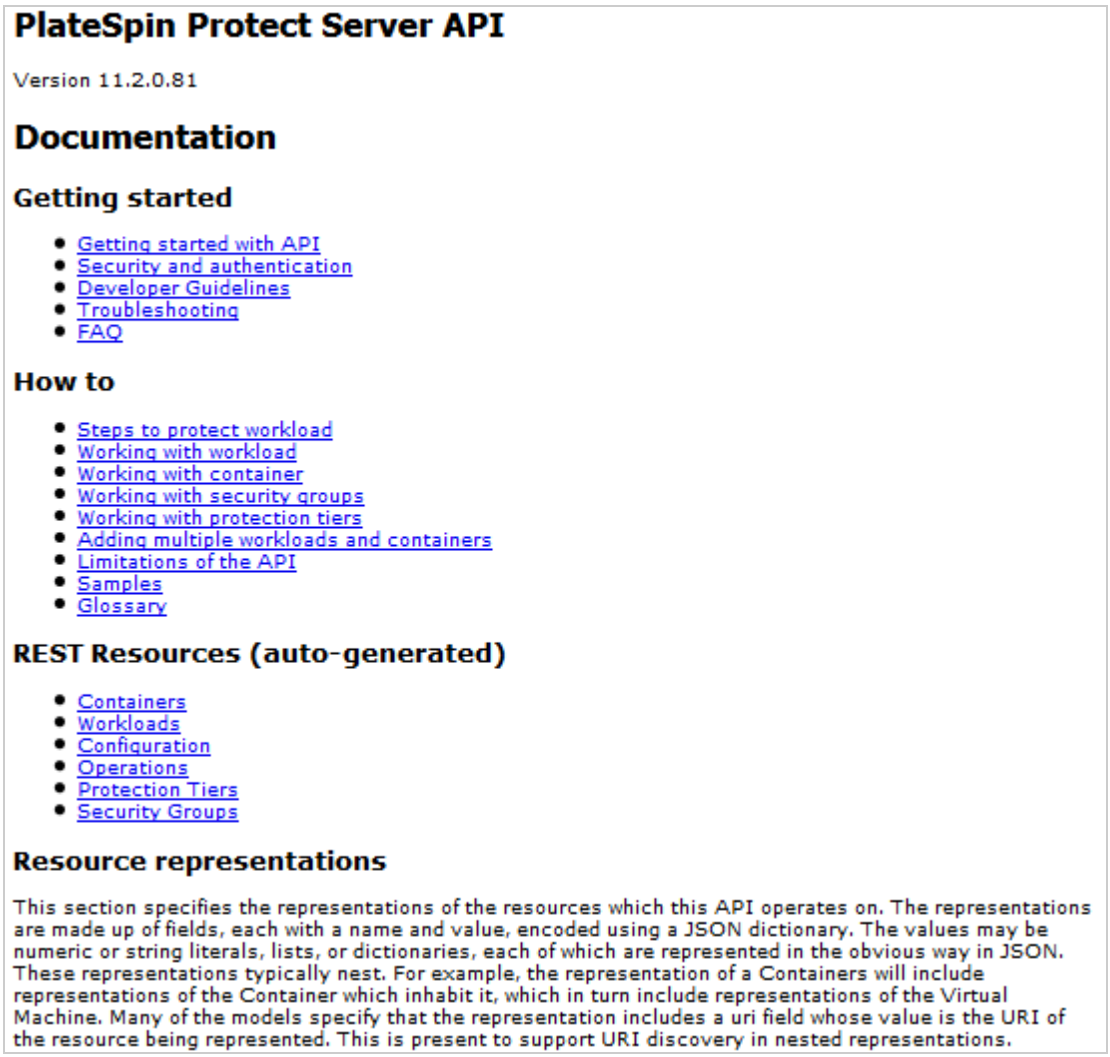
D.2 Dokumentation zur PlateSpin Protect-Server-API

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 der Forge-VM:

`https://`*<hostname | IP-Adresse>*`/protectionservices`

Ersetzen Sie *<Hostname | IP-Adresse>* durch den Hostnamen bzw. die IP-Adresse Ihrer Forge-VM. Wenn SSL nicht aktiviert ist, verwenden Sie `http` in der URL.

Abbildung D-1 *Die Startseite der Protect-Server-API*



PlateSpin Protect Server API

Version 11.2.0.81

Documentation

Getting started

- Getting started with API
- Security and authentication
- Developer Guidelines
- Troubleshooting
- FAQ

How to

- Steps to protect workload
- Working with workload
- Working with container
- Working with security groups
- Working with protection tiers
- Adding multiple workloads and containers
- Limitations of the API
- Samples
- Glossary

REST Resources (auto-generated)

- Containers
- Workloads
- Configuration
- Operations
- Protection Tiers
- Security Groups

Resource representations

This section specifies the representations of the resources which this API operates on. The representations are made up of fields, each with a name and value, encoded using a JSON dictionary. The values may be numeric or string literals, lists, or dictionaries, each of which are represented in the obvious way in JSON. These representations typically nest. For example, the representation of a Containers will include representations of the Container which inhabit it, which in turn include representations of the Virtual Machine. Many of the models specify that the representation includes a uri field whose value is the URI of the resource being represented. This is present to support URI discovery in nested representations.

D.3 Beispiele und weitere Referenzen

Forge-Administratoren können über ein JScript-Beispiel in der Befehlszeile aus über die API auf das Produkt zugreifen. Beachten Sie auf der Forge-VM 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.

Glossar

Angestrebte Testzeit (TTO). Ein Maß dafür, wie einfach sich ein Wiederherstellungsplan für den Katastrophenfall testen lässt. Es entspricht weitgehend der RTO, umfasst jedoch auch die Zeit, die ein Benutzer zum Testen des Failover-Workloads benötigt. Mit der Funktion **Failover testen** können Sie verschiedene Szenarien durchlaufen und Vergleichsdaten generieren.

Angestrebte Wiederherstellungszeit (RTO). Ein Wert für die tolerierbare Ausfallzeit eines Workloads, definiert durch die Zeit, die für einen Failover-Vorgang erforderlich ist. Die benötigte RTO wird von der Zeit beeinflusst, die für das Konfigurieren und Ausführen des Failover-Vorgangs benötigt wird (10 bis 45 Minuten).

Angestrebter Wiederherstellungszeitpunkt (RPO). In Zeit gemessener tolerierbarer Datenverlust, der durch ein konfigurierbares Intervall zwischen inkrementellen Reproduktionen eines geschützten Workloads definiert wird. Anders ausgedrückt: Welchen Datenverlust können Sie bei einem weitreichenden IT-Ausfall verkraften? Der RPO wird vom aktuellen Nutzungsumfang von PlateSpin Forge, der Rate und dem Ausmaß von Änderungen im Workload sowie von der Netzwerkgeschwindigkeit und dem gewählten Reproduktionszeitplan beeinflusst.

Appliance-Host. *Weitere Informationen hierzu finden Sie unter* Container.

Appliance-Management-Software. Software, die entweder eine Terminal-Konsole (Getty) oder eine proprietäre, browserbasierte Schnittstelle (Forge Appliance Configuration Console, *Forge ACC*) verwendet, um zu Installations- und Konfigurationszwecken (beispielsweise zum Einrichten der Host/VM-IP-Adressen, Hostnamen und für die Benutzerpasswortkonfiguration) eine direkte Verbindung zu einer Appliance herstellt.

Appliance-Version. Die Version der Appliance-Management-Software, mit der die Netzwerkeinstellungen für den Forge-ESX-Host und die Forge-Appliance-VM verwaltet werden. Die Appliance (Version) 1 nutzt eine Getty-Oberfläche, die Appliance (Version) 2 dagegen das Django Web-Framework und die ACC-Schnittstelle. Eine Aktualisierung der Appliance-Version ergibt sich vorwiegend aus Änderungen an der zugrunde liegenden VMware-ESX-Version.

Ermitteln Sie die Appliance-Version Ihrer Forge-Einheit anhand einer der folgenden Methoden:

- **Forge-Weboberfläche:** Auf der Seite *Help* > *About* (Hilfe > Info) der ACC finden Sie die Appliance-Versionsnummer. Diese Methode ist nur bei der Neukonfiguration von Forge möglich.
- **Lokale Konfigurationsschnittstelle:** Schließen Sie einen Bildschirm an die Appliance an, und schalten Sie ihn ein. Wenn der blaue Bildschirm der Forge-Konsole angezeigt wird, verwenden Sie die Appliance-Version 1. Wird der ESX-Konfigurationsbildschirm geöffnet, wird Appliance-Version 2 verwendet.
- **Remote-Konfigurationsschnittstelle:** Starten Sie die Forge Appliance Configuration Console (ACC) in einem Webbrowser, und geben Sie dabei die IP-Adresse Ihrer Forge-Einheit an (`http://<forge_esx_server>:1000`). Wenn die Verbindung mit der ACC möglich ist, wird Appliance-Version 2 verwendet.

Arbeitsverzeichnis. Speicherort im Netzwerk, an den das Forge-Aufrüstungskit kopiert wird. Beispiel: `D:\forge_backup\11.0_kit`.

Ausführbare Forge-Installations-/Aufrüstungsdatei. Die ausführbare Datei, die die Forge-Appliance-Software aufrüstet. Die ausführbare Datei (auch als „Aufrüstungsprogramm“ bezeichnet) ist im *Forge-Aufrüstungskit* enthalten.

Ausgabeverzeichnis. (auch **Ausgabeordner**). Speicherort im Netzwerk, an dem wichtige Sicherungsdaten auf dem Verwaltungscomputer gespeichert werden. Beispiel: `D:\forge_backup\out`.

Container. Der VM-Host, der den Failover-Workload (die bootfähige virtuelle Reproduktion eines geschützten Workloads) enthält.

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

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

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

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

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

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

Forge-Appliance. Ein Forge-Appliance-Host mit einer virtuellen Maschine, auf der ein Microsoft Windows-Betriebssystem ausgeführt wird und die Forge-Software installiert ist.

Forge-Software. PlateSpin-Software für den Schutz eines bestimmten virtuellen Workloads (also Betriebssystem, Middleware und Daten einer ESX-VM) unter Verwendung einer Virtualisierungstechnologie. Im Fall eines Ausfalls oder einer Katastrophe am Produktionsserver kann eine virtualisierte Reproduktion eines Workloads im Zielcontainer (einem VM-Host) aktiviert werden und weiterhin normal ausgeführt werden, bis die Produktionsumgebung wiederhergestellt ist.

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

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

Management-VM. Die virtuelle Management-Maschine, die die PlateSpin Forge-Software enthält.

Neuaufbau. Die Konfiguration der Forge-Dell-Hardware, des Forge-ESX-Hosts und der Forge-Appliance, die auf einem Windows Server-Betriebssystem ausgeführt wird.

Reproduktion.

1. *Ursprüngliche Reproduktion*, die Erstellung einer ursprünglichen Basiskopie eines Workloads. Kann als *vollständige Reproduktion* ausgeführt werden (siehe Vollständig) oder als *inkrementelle Reproduktion* (siehe Inkrementell (2)).
2. Jegliche Übertragung geänderter Daten von einem geschützten Workload auf seine Reproduktion im Container.

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

RPA (Recovery Point Actual). In Zeit gemessener tatsächlicher Datenverlust, der durch das tatsächlich gemessene Intervall zwischen inkrementellen Reproduktionen eines geschützten Workloads während eines Failover-Tests definiert wird.

RTA (Recovery Time Actual). Ein Wert für die tatsächliche Ausfallzeit eines Workloads, definiert durch die Zeit, die für einen Failover-Vorgang erforderlich ist.

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

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

Sicherung. Vorgang, bei dem die vorhandenen Datenbankdaten (vorhandene Workloads und Vereinbarungen) exportiert werden. Hierbei werden auch die VMs gesichert, die sich in der lokalen Datenablage auf dem Forge-Appliance-Host befinden.

Tatsächliche angestrebte Testzeit (tatsächliche TTO). Siehe Tatsächliche Testzeit (TTA).

Tatsächliche angestrebte Wiederherstellungszeit (tatsächliche RTO). Siehe Tatsächliche Wiederherstellungszeit (RTA).

Tatsächliche Testzeit (TTA). 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.

Tatsächlicher angestrebter Wiederherstellungszeitpunkt (tatsächlicher RPO). Siehe Tatsächlicher Wiederherstellungspunkt (RPA).

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

Siehe auch Ziel.

Vereinbarungsdaten. Exportierte Daten für die Schutzvereinbarungen. Das Aufrüstungsprogramm speichert diese in einer `.zip`-Datei.

Siehe auch Schutzvertrag.

Verwaltungscomputer. Ein Windows-Computer, der extern vom Appliance-Host zur Durchführung der Aufrüstung verwendet wird. Wir empfehlen Ihnen, für diesen Vorgang ein Notebook zu verwenden, da für den Aufbau der Forge-Hardware-Appliance und den Konfigurationsvorgang eine direkte Verbindung zur Dell-Hardware erforderlich ist, die als Forge-Appliance-Host verwendet wird.

Vollständig. 1. (Substantiv) Eine einzelne geplante oder manuelle Übertragung eines geschützten Workloads auf dessen „leere“ Reproduktion (die Failover-VM) oder von einem Failover-Workload auf seine ursprüngliche virtuelle oder physische Infrastruktur.

2. (Adjektiv) Beschreibt den Umfang der *Reproduktion (1)* , in dem die anfängliche Reproduktion eines geschützten Workloads auf der Basis aller Daten in diesem Workload erstellt wird.

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

Wiederherstellen. Der Vorgang, bei dem vorhandene Datenbankdaten (Workloads und Vereinbarungen) in dem Zustand importiert werden, in dem sie vor der Sicherung vorlagen. Hierbei werden auch alle lokalen VMs wiederhergestellt, die sich zuvor auf dem Forge-Appliance-Host befunden haben.

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

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

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

Siehe auch Ursprung.