



# PlateSpin® Forge 11.1

## Benutzerhandbuch

**März 2015**

## Rechtliche Hinweise

DIESES DOKUMENT UND DIE HIER BESCHRIEBENE SOFTWARE WERDEN GEMÄSS EINER LIZENZVEREINBARUNG ODER EINER VERSCHWIEGENHEITSVERPFLICHTUNG BEREITGESTELLT UND UNTERLIEGEN DEN JEWEILIGEN BESTIMMUNGEN DIESER VEREINBARUNGEN. SOFERN NICHT AUSDRÜCKLICH IN DER LIZENZVEREINBARUNG ODER VERSCHWIEGENHEITSVERPFLICHTUNG ERKLÄRT, STELLT DIE NETIQ CORPORATION DIESES DOKUMENT UND DIE IN DIESEM DOKUMENT BESCHRIEBENE SOFTWARE OHNE MÄNGELGEWÄHR UND OHNE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNGEN JEDLICHER ART BEREIT, BEISPIELSWEISE UNTER ANDEREM STILLSCHWEIGENDE GEWÄHRLEISTUNGEN HINSICHTLICH DER MARKTGÄNGIGKEIT ODER DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. IN EINIGEN LÄNDERN SIND HAFTUNGSAUSSCHLÜSSE FÜR AUSDRÜCKLICHE ODER STILLSCHWEIGENDE GEWÄHRLEISTUNGEN IN BESTIMMTEN TRANSAKTIONEN NICHT ZULÄSSIG. AUS DIESEM GRUND HAT DIESE BESTIMMUNG FÜR SIE UNTER UMSTÄNDEN KEINE GÜLTIGKEIT.

Der Klarheit halber werden alle Module, Adapter und anderes Material („Modul“) gemäß den Bestimmungen der Endbenutzer-Lizenzvereinbarung (EULA) für die jeweilige Version des NetIQ-Produkts oder der NetIQ-Software lizenziert, zu dem/der diese Module gehören oder mit dem/der sie zusammenarbeiten. Durch den Zugriff auf ein Modul bzw. durch das Kopieren oder Verwenden eines Moduls erklären Sie sich an diese Bestimmungen gebunden. Falls Sie den Bestimmungen der Endbenutzer-Lizenzvereinbarung nicht zustimmen, sind Sie nicht berechtigt, ein Modul zu verwenden oder zu kopieren bzw. auf ein Modul zuzugreifen, und Sie sind verpflichtet, jegliche Kopien des Moduls zu vernichten und weitere Anweisungen bei NetIQ zu erfragen.

Ohne vorherige schriftliche Genehmigung der NetIQ Corporation dürfen dieses Dokument und die in diesem Dokument beschriebene Software nicht vermietet, verkauft oder verschenkt werden, soweit dies nicht anderweitig gesetzlich gestattet ist. Ohne vorherige schriftliche Genehmigung der NetIQ Corporation darf dieses Dokument oder die in diesem Dokument beschriebene Software weder ganz noch teilweise reproduziert, in einem Abrufsystem gespeichert oder auf jegliche Art oder auf jeglichem Medium (elektronisch, mechanisch oder anderweitig) gespeichert werden, soweit dies nicht ausdrücklich in der Lizenzvereinbarung oder Verschwiegenheitsverpflichtung dargelegt ist. Ein Teil der Unternehmen, Namen und Daten in diesem Dokument dienen lediglich zur Veranschaulichung und stellen keine realen Unternehmen, Personen oder Daten dar.

Dieses Dokument enthält unter Umständen technische Ungenauigkeiten oder Rechtschreibfehler. Die hierin enthaltenen Informationen sind regelmäßigen Änderungen unterworfen. Diese Änderungen werden ggf. in neuen Ausgaben dieses Dokuments eingebunden. Die NetIQ Corporation ist berechtigt, jederzeit Verbesserungen oder Änderungen an der in diesem Dokument beschriebenen Software vorzunehmen.

Einschränkungen für US-amerikanische Regierungsstellen: Wenn die Software und Dokumentation von einer US-amerikanischen Regierungsstelle, im Namen einer solchen oder von einem Auftragnehmer einer US-amerikanischen Regierungsstelle erworben wird, unterliegen die Rechte der Regierung gemäß 48 C.F.R. 227.7202-4 (für Käufe durch das Verteidigungsministerium, Department of Defense (DOD)) bzw. 48 C.F.R. 2.101 und 12.212 (für Käufe einer anderen Regierungsstelle als das DOD) an der Software und Dokumentation in allen Punkten den kommerziellen Lizenzrechten und Einschränkungen der Lizenzvereinbarung. Dies umfasst auch die Rechte der Nutzung, Änderung, Vervielfältigung, Ausführung, Anzeige und Weitergabe der Software oder Dokumentation.

© 2015 NetIQ Corporation. Alle Rechte vorbehalten.

Weitere Informationen zu den Marken von NetIQ finden Sie im Internet unter <https://www.netiq.com/company/legal/>.

### 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* ([https://www.netiq.com/documentation/platespin\\_licensing/platespin\\_licensing\\_qs/data/platespin\\_licensing\\_qs.html](https://www.netiq.com/documentation/platespin_licensing/platespin_licensing_qs/data/platespin_licensing_qs.html)) für Drittanbieter-Lizenzen in PlateSpin Forge.

---

# Inhalt

<b>Info zu diesem Handbuch und zur Bibliothek</b>	<b>7</b>
<b>Info zu NetIQ Corporation</b>	<b>9</b>
<b>1 Produktübersicht</b>	<b>13</b>
1.1 Informationen zu PlateSpin Forge	13
1.2 Unterstützte Konfigurationen	13
1.2.1 Unterstützte Windows-Workloads	14
1.2.2 Unterstützte Linux-Workloads	16
1.2.3 Unterstützte VM-Container	18
1.2.4 Unterstützte System-Firmware	18
1.3 Sicherheit und Datenschutz	19
1.3.1 Sicherheit der Workload-Daten bei der Übertragung	19
1.3.2 Sicherheit der Client-Server-Kommunikation	19
1.3.3 Sicherheit von Berechtigungsnachweisen	19
1.3.4 Benutzerautorisierung und -authentifizierung	19
1.3.5 Einstellungen für Netzwerk-Ports	20
1.3.6 Zusätzliche Sicherheitsverbesserungen	21
1.4 Leistung	21
1.4.1 Allgemeines zu Produktleistungsmerkmalen	21
1.4.2 Datenkomprimierung	22
1.4.3 Bandbreitendrosselung	22
1.4.4 RPO-, RTO- und TTO-Spezifikationen	22
1.4.5 Skalierbarkeit	23
<b>2 PlateSpin Forge-Anwendungskonfiguration</b>	<b>25</b>
2.1 Produktlizenzierung	25
2.1.1 Abrufen eines Lizenzaktivierungscode	25
2.1.2 Online-Lizenzaktivierung	25
2.1.3 Offline-Lizenzaktivierung	26
2.2 Einrichten der Benutzerautorisierung und -authentifizierung	27
2.2.1 Info über die Benutzerautorisierung und -authentifizierung von PlateSpin Forge	27
2.2.2 Verwalten von PlateSpin Forge-Zugriff und -Berechtigungen	28
2.2.3 Verwalten von PlateSpin Forge-Sicherheitsgruppen und -Workload-Berechtigungen	30
2.3 Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk	31
2.3.1 Anforderungen für geöffnete Ports für die Forge-VM	31
2.3.2 Zugriffs- und Kommunikationsanforderungen für Workloads	31
2.3.3 Zugriffs- und Kommunikationsanforderungen für Container	33
2.3.4 Schutz über öffentliche und private Netzwerke durch NAT	33
2.3.5 Außerkraftsetzen der Standard-Bash-Shell zum Ausführen von Befehlen auf Linux-Workloads	34
2.3.6 Anforderungen für VMware DRS-Cluster als Container	34
2.4 Konfigurieren von PlateSpin Forge-Standardoptionen	35
2.4.1 Einrichten automatischer Email-Benachrichtigungen zu Ereignissen und Berichten	35
2.4.2 Einrichtung der Sprache bei internationalen Versionen von PlateSpin Forge	39
2.4.3 Konfigurieren des Verhaltens des PlateSpin-Servers mithilfe von XML-Konfigurationsparametern	40
2.4.4 Konfigurieren der Unterstützung für VMware vCenter Site Recovery Manager	43
2.4.5 Sortieren von Workloads mithilfe von Tags	45

<b>3</b>	<b>Appliance-Einrichtung und Wartung</b>	<b>47</b>
3.1	Einrichten des Appliance-Netzwerks . . . . .	47
3.1.1	Einrichten des Appliance-Host-Netzwerks. . . . .	47
3.2	Physische Standortänderung der Appliance . . . . .	48
3.2.1	Szenario 1 – Standortänderung der Forge-Appliance (neue IP-Adresse bekannt) . . . . .	48
3.2.2	Szenario 2 – Standortänderung der Forge-Appliance (neue IP-Adresse nicht bekannt). . . . .	49
3.3	Verwenden externer Speicherlösungen mit PlateSpin Forge. . . . .	51
3.3.1	Verwenden von Forge mit einem SAN-Speicher . . . . .	51
3.3.2	Hinzufügen einer SAN-LUN zu Forge . . . . .	52
3.4	Forge Management-VM im Appliance-Host – Zugriff und Verwendung . . . . .	53
3.4.1	Herunterladen des vSphere-Clientprogramms . . . . .	53
3.4.2	Starten des vSphere-Clients und Zugriff auf die Forge Management-VM . . . . .	53
3.4.3	Starten und Herunterfahren der Forge Management-VM . . . . .	54
3.4.4	Verwalten von Forge-Snapshots auf dem Appliance-Host . . . . .	54
3.4.5	Manuelles Importieren von VMs in die Datenablage des Appliance-Hosts . . . . .	55
3.4.6	Richtlinien zur Anwendung von Sicherheitsaktualisierungen auf die PlateSpin Forge Management-VM . . . . .	55
3.5	Zurücksetzen von Forge auf die Werkseinstellungen . . . . .	56
<b>4</b>	<b>Aufgestellt und in Betrieb</b>	<b>59</b>
4.1	Starten der PlateSpin Forge-Weboberfläche . . . . .	59
4.2	Elemente der PlateSpin Forge-Weboberfläche . . . . .	60
4.2.1	Navigationsleiste . . . . .	61
4.2.2	Teilfenster mit visueller Zusammenfassung. . . . .	61
4.2.3	Teilfenster mit Aufgaben und Ereignissen . . . . .	62
4.3	Workloads und Workload-Befehle . . . . .	62
4.3.1	Workload-Schutz- und Wiederherstellungsbefehle . . . . .	63
4.4	Verwalten mehrerer Instanzen von PlateSpin Protect und PlateSpin Forge . . . . .	64
4.4.1	Verwenden der PlateSpin Forge-Verwaltungskonsole . . . . .	64
4.4.2	Informationen zu PlateSpin Forge-Verwaltungskonsolenkarten . . . . .	65
4.4.3	Hinzufügen von Instanzen von PlateSpin Protect und PlateSpin Forge zur Verwaltungskonsole. . . . .	66
4.4.4	Verwalten von Karten auf der Verwaltungskonsole . . . . .	66
4.5	Generieren von Workload- und Workload-Schutz-Berichten . . . . .	67
<b>5</b>	<b>Workload-Schutz und Wiederherstellung</b>	<b>69</b>
5.1	Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung . . . . .	69
5.2	Hinzufügen von Containern (Schutzziel) . . . . .	71
5.3	Hinzufügen von Workloads . . . . .	72
5.4	Konfigurieren der Schutzdetails und Vorbereiten der Reproduktion . . . . .	73
5.4.1	Workload-Schutz-Details . . . . .	74
5.5	Starten des Workload-Schutzes . . . . .	77
5.6	Abbrechen von Befehlen . . . . .	77
5.7	Failover . . . . .	78
5.7.1	Erkennen von Offline-Workloads . . . . .	78
5.7.2	Durchführen eines Failovers . . . . .	79
5.7.3	Verwenden der Funktion „Failover testen“. . . . .	79
5.8	Failback . . . . .	80
5.8.1	Automatischer Failback auf eine VM-Plattform . . . . .	80
5.8.2	Halbautomatischer Failback auf einen physischen Computer. . . . .	83
5.8.3	Halbautomatischer Failback auf eine virtuelle Maschine. . . . .	84
5.9	Erneutes Schützen eines Workloads . . . . .	85

<b>6</b>	<b>Grundlagen des Workload-Schutzes</b>	<b>87</b>
6.1	Workload-Lizenzverbrauch	87
6.2	Richtlinien für Workload- und Container-Berechtigungs-nachweise	88
6.3	Datenübertragung	88
6.3.1	Übertragungsmethoden	89
6.3.2	Datenverschlüsselung	90
6.4	Schutzebenen	90
6.5	Wiederherstellungspunkte	92
6.6	Anfängliche Reproduktionsmethode (vollständig und inkrementell)	92
6.7	Steuerung von Diensten und Daemons	93
6.8	Verwenden von Freeze- und Thaw-Skripts für alle Reproduktionen (Linux)	94
6.9	Volumes	95
6.10	Netzwerke	96
6.11	Failback auf physische Computer	96
6.11.1	Herunterladen des PlateSpin-Boot-ISO-Image	97
6.11.2	Einfügen weiterer Gerätetreiber in das Boot-ISO-Image	97
6.11.3	Registrieren von physischen Computern als Failback-Ziele mit PlateSpin Forge	99
6.12	Themen zu erweitertem Workload-Schutz	99
6.12.1	Schützen von Windows-Clustern	99
6.12.2	Verwenden von Workload-Schutz-Funktionen über die PlateSpin Forge-Web-Services-API	102
<b>7</b>	<b>Hilfswerkzeuge für die Arbeit mit physischen Computern</b>	<b>105</b>
7.1	Verwalten der Gerätetreiber	105
7.1.1	Verpacken von Gerätetreibern für Windows-Systeme	105
7.1.2	Verpacken von Gerätetreibern für Linux-Systeme	106
7.1.3	Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin Forge	106
7.1.4	Verwenden der Funktion für die Plug-&-Play(PnP)-ID-Übersetzung	108
<b>8</b>	<b>ProtectAgent-Dienstprogramm</b>	<b>111</b>
<b>9</b>	<b>Fehlersuche</b>	<b>115</b>
9.1	Fehlerbehebung bei der Workload-Inventarisierung (Windows)	115
9.1.1	Durchführen von Verbindungstests	116
9.1.2	Deaktivieren der Virenschutz-Software	118
9.1.3	Aktivieren von Datei-/Freigabe-Berechtigungen und -Zugriff	118
9.2	Fehlerbehebung bei der Workload-Inventarisierung (Linux)	119
9.3	Beheben von Problemen während der Ausführung des Befehls „Reproduktion vorbereiten“ (Windows)	120
9.3.1	Gruppenrichtlinie und Benutzerrechte	120
9.4	Fehlerbehebung bei der Workload-Reproduktion	120
9.5	Fehlersuche bei Workloads, die Datenverkehr weiterleiten	122
9.6	Fehlersuche bei der Online-Hilfe	123
9.7	Generieren und Anzeigen von Diagnoseberichten	123
9.8	Entfernen von Workloads	123
9.9	Workload-Bereinigung nach dem Schutz	124
9.9.1	Bereinigen von Windows-Workloads	124
9.9.2	Bereinigen von Linux-Workloads	124
9.10	Verkleinern der PlateSpin Forge-Datenbanken	126
<b>A</b>	<b>Von Forge unterstützte Linux-Verteilungen</b>	<b>127</b>
A.1	Analisieren Ihres Linux-Workloads	127

A.1.1	Ermitteln der Versionszeichenkette . . . . .	127
A.1.2	Ermitteln der Architektur . . . . .	127
A.2	PlateSpin Forge Vorkompilierter „blkwatch“-Treiber (Linux) . . . . .	128
<b>B</b>	<b>Synchronisieren von Seriennummern im lokalen Clusterknoten-Speicher</b>	<b>129</b>
<b>C</b>	<b>Anpassen der PlateSpin Forge-Weboberfläche an das Markenbild</b>	<b>131</b>
C.1	Anpassen der Benutzeroberfläche an das Markenbild mithilfe von Konfigurationsparametern . . . .	131
C.2	Anpassen des Produktnamens an das Markenbild in der Windows-Registrierungsdatenbank . . . .	135
	<b>Glossar</b>	<b>137</b>

---

# Info zu diesem Handbuch und zur Bibliothek

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

## Zielgruppe

Dieses Handbuch ist für IT-Mitarbeiter wie beispielsweise 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 \(https://www.netiq.com/documentation/platespin-forge/\)](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 mit dem *PlateSpin Forge Field Rebuild Kit*.

### Aufrüstungshandbuch

Informationen zum Aufrüsten der Appliance-Software.

### Hilfe

Kontextabhängige Informationen und Schritt-für-Schritt-Anweisungen für häufig anfallende Aufgaben in der Benutzeroberfläche.

# Zusätzliche Ressourcen

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

- ♦ [PlateSpin Forge-Forum \(https://forums.netiq.com/forumdisplay.php?56-Platespin-Forge\)](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 \(https://www.netiq.com/products/forge/\)](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 \(https://www.netiq.com/communities/\)](https://www.netiq.com/communities/): Eine webbasierte Community mit verschiedenen Diskussionsthemen.
- ♦ [NetIQ Support-Knowledgebase \(https://www.netiq.com/support/kb/\)](https://www.netiq.com/support/kb/): Eine Sammlung ausführlicher technischer Artikel.
- ♦ [NetIQ Support-Foren \(https://forums.netiq.com/forum.php\)](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 \(https://www.netiq.com/f/mynetiq/\)](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 physikalischen, 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 den Vertriebssupport

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 Vertriebssupport-Team.

<b>Weltweit:</b>	<a href="http://www.netiq.com/about_netiq/officelocations.asp">www.netiq.com/about_netiq/officelocations.asp</a>
<b>Vereinigte Staaten und Kanada:</b>	1-888-323-6768
<b>Email:</b>	<a href="mailto:info@netiq.com">info@netiq.com</a>
<b>Website:</b>	<a href="http://www.netiq.com">www.netiq.com</a>

## Kontakt zum technischen Support

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

<b>Weltweit:</b>	<a href="http://www.netiq.com/support/contactinfo.asp">www.netiq.com/support/contactinfo.asp</a>
<b>Nord- und Südamerika:</b>	1-713-418-5555
<b>Europa, Naher Osten und Afrika:</b>	+353 (0) 91-782 677
<b>Email:</b>	<a href="mailto:support@netiq.com">support@netiq.com</a>
<b>Website:</b>	<a href="http://www.netiq.com/support">www.netiq.com/support</a>
<b>Produktspezifische Informationen:</b>	<a href="https://www.netiq.com/support/kb/product.php?id=PlateSpin_Forge">https://www.netiq.com/support/kb/product.php?id=PlateSpin_Forge</a>

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

## Kontakt zum Dokumentationsupport

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/) (<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](mailto: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 Produktübersicht

Dieser Abschnitt enthält folgende Informationen:

- ♦ [Abschnitt 1.1, „Informationen zu PlateSpin Forge“ auf Seite 13](#)
- ♦ [Abschnitt 1.2, „Unterstützte Konfigurationen“ auf Seite 13](#)
- ♦ [Abschnitt 1.3, „Sicherheit und Datenschutz“ auf Seite 19](#)
- ♦ [Abschnitt 1.4, „Leistung“ auf Seite 21](#)

## 1.1 Informationen zu PlateSpin Forge

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.

## 1.2 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 die unterstützten Plattformkonfigurationen beschrieben.

- ♦ [Abschnitt 1.2.1, „Unterstützte Windows-Workloads“ auf Seite 14](#)
- ♦ [Abschnitt 1.2.2, „Unterstützte Linux-Workloads“ auf Seite 16](#)
- ♦ [Abschnitt 1.2.3, „Unterstützte VM-Container“ auf Seite 18](#)
- ♦ [Abschnitt 1.2.4, „Unterstützte System-Firmware“ auf Seite 18](#)

## 1.2.1 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 mit bestimmten Einschränkungen unterstützt. Weitere Informationen hierzu finden Sie unter [Abschnitt 6.3](#), „Datenübertragung“ auf Seite 88.

*Tabelle 1-1 Unterstützte Windows-Workloads*

Betriebssystem	Notizen
<b>Serverklassen-Workloads</b>	
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 <a href="#">Wissensdatenbankartikel 7920501</a> .
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 <a href="#">Wissensdatenbankartikel 7920501</a> .
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.
<b>Serverbasierte Cluster-Workloads</b>	
Windows 2008 R2 Server-basiertes Microsoft-Failovercluster	Nur blockbasierte Übertragung.
Windows 2003 R2 Server-basiertes Microsoft-Failovercluster	Nur blockbasierte Übertragung.
<b>Hypervisor-Klassen-Workloads</b>	
Windows Server 2012 mit Hyper-V-Rolle	
<b>Arbeitsstationsklassen-Workloads</b>	

Betriebssystem	Notizen
Windows 8.1 Windows 8	<p><b>WARNUNG:</b> Sie müssen den Energiesparplan <b>Hohe Leistung</b> an der Windows 8-Quelle auswählen, damit die Workload-Failover- und -Failback-Funktion korrekt funktioniert.</p> <p>So konfigurieren Sie diesen Energiesparplan in der Windows-Systemsteuerung:</p> <ol style="list-style-type: none"> <li>1. Wählen Sie <b>Alle Systemsteuerungselemente &gt; Energieoptionen</b> aus.</li> <li>2. Wählen Sie im Dialogfeld <b>Energiesparplan wählen oder anpassen</b> die Optionen <b>Weitere Energiesparpläne einblenden &gt; Hohe Leistung</b>.</li> <li>3. Schließen Sie die Systemsteuerung.</li> </ol>
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 Cluster finden Sie unter „[Schützen von Windows-Clustern](#)“ auf Seite 99.

### Unterstützte internationale Versionen

PlateSpin Forge unterstützt Versionen von Microsoft Windows in den Sprachen Französisch, Deutsch, Japanisch, Chinesisch (traditionell) und Chinesisch (vereinfacht).

**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 Protect 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 Protect 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 Protect-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 Protect zum Zeitpunkt des Failbacks einen Übergang der UEFI-Firmware des Workloads zur BIOS-Firmware durch. Wenn dann das Failback auf einem UEFI-basierten physischen Computer ausgewählt wird, kehrt Protect den Firmware-Übergang von BIOS zu UEFI wieder um.
- ♦ Wenn Sie versuchen, ein Failback eines geschützten Windows 2003-Workloads auf einen UEFI-gestützten physischen Computer vorzunehmen, analysiert Protect 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 Protect die Startlaufwerke des UEFI-Systems (bislang GPT) zu MBR-Laufwerken. Bei einem Failback dieses BIOS-Workloads auf einen UEFI-basierten physischen Computer werden die Startlaufwerke wieder zu GPT zurückkonvertiert.

### Unterstützung für komplexe Workload-Festplattenpartitionierung

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

## 1.2.2 Unterstützte Linux-Workloads

PlateSpin Forge unterstützt eine Anzahl von Linux-Distributionen. Eine Liste der unterstützten Linux-Versionen finden Sie in [Tabelle 1-2](#).

Die Reproduktion von geschützten Linux-Workloads erfolgt auf Blockebene. Die PlateSpin Forge-Software umfasst vorkonfigurierte Versionen des `blkwatch`-Moduls/-Treibers. Diese gelten nur für Nicht-Debugkernels der Linux-Verteilungen (sowohl 32 Bit als auch 64 Bit).

*Tabelle 1-2 Linux-Verteilungen mit einem entsprechenden vorkonfigurierten `blkwatch`-Modul/-Treiber*

Betriebssystem	Notizen
<b>Linux-Serverklassen-Workloads</b>	
Red Hat Enterprise Linux (RHEL) 7	Eine Liste der unterstützten Red Hat-Kernelversionen finden Sie in <a href="#">Anhang A, „Von Forge unterstützte Linux-Verteilungen“</a> , auf Seite 127.
Red Hat Enterprise Linux 6	Eine Liste der unterstützten Red Hat-Kernelversionen finden Sie in <a href="#">Anhang A, „Von Forge unterstützte Linux-Verteilungen“</a> , auf Seite 127.
Red Hat Enterprise Linux 5	Eine Liste der unterstützten Red Hat-Kernelversionen finden Sie in <a href="#">Anhang A, „Von Forge unterstützte Linux-Verteilungen“</a> , auf Seite 127.
Red Hat Enterprise Linux 4	Eine Liste der unterstützten Red Hat-Kernelversionen finden Sie in <a href="#">Anhang A, „Von Forge unterstützte Linux-Verteilungen“</a> , auf Seite 127.



Betriebssystem	Notizen
SUSE Linux Enterprise Server (SLES) 11	<p>Eine Liste der unterstützten SLES-Kernelversionen finden Sie in <a href="#">Anhang A, „Von Forge unterstützte Linux-Verteilungen“</a>, auf Seite 127.</p> <p><b>HINWEIS:</b> 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.</p>
SUSE Linux Enterprise Server 10	<p>Eine Liste der unterstützten SLES-Kernelversionen finden Sie in <a href="#">Anhang A, „Von Forge unterstützte Linux-Verteilungen“</a>, auf Seite 127.</p>
SUSE Linux Enterprise Server 9	<p>Eine Liste der unterstützten SLES-Kernelversionen finden Sie in <a href="#">Anhang A, „Von Forge unterstützte Linux-Verteilungen“</a>, auf Seite 127.</p>
Novell Open Enterprise Server (OES) 11, SP1 und SP2	<p>Eine Liste der unterstützten SLES-Kernelversionen finden Sie in <a href="#">Anhang A, „Von Forge unterstützte Linux-Verteilungen“</a>, auf Seite 127.</p> <p><b>HINWEIS:</b> 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. Nur blockbasierte Übertragung.</p>
Oracle Enterprise Linux (OEL)	<p>Eine Liste der unterstützten Red Hat-Kernelversionen finden Sie in <a href="#">Anhang A, „Von Forge unterstützte Linux-Verteilungen“</a>, auf Seite 127.</p> <p><b>HINWEIS:</b> Workloads, die den Unbreakable Enterprise Kernel verwenden, werden nicht unterstützt.</p>
CentOS 7	

### Unterstützte Linux-Dateisysteme

PlateSpin Forge unterstützt die Dateisysteme EXT2, EXT3, EXT4, REISERFS, XFS und NSS (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

PlateSpin Forge unterstützt 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

Die Reproduktion von geschützten Linux-Workloads erfolgt auf Blockebene. Für die PlateSpin Forge-Software ist ein blkwatch-Treiber erforderlich, der für die zu schützende Linux-Distribution kompiliert wurde. Eine Liste der Distributionen, die den blkwatch-Treiber enthalten, finden Sie unter [Anhang A, „Von Forge unterstützte Linux-Verteilungen“](#), auf Seite 127.

Wenn die Distribution den blkwatch-Treiber nicht enthält, können Sie einen benutzerdefinierten Treiber erstellen. Führen Sie dazu die im [Wissensdatenbankartikel 7005873](#) beschriebenen Schritte aus.

## 1.2.3 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.

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

Container	Haftnotizen
VMware ESXi 5.5 (GA2, Update 2)	<ul style="list-style-type: none"><li>◆ Unterstützt als Schutz- und Failback-Container.</li><li>◆ Die DRS-Konfiguration muss entweder <b>Teilweise automatisiert</b> oder <b>vollautomatisch</b> sein (sie darf nicht auf <b>Manuell</b> gesetzt sein.)</li><li>◆ Als VM-Container darf der DRS-Cluster nur aus ESXi 5.5-Servern bestehen und kann nur von vCenter 5.5 verwaltet werden.</li></ul>
VMware ESXi 5.1 (GA2, Update 2)	<ul style="list-style-type: none"><li>◆ Unterstützt als Schutz- und Failback-Container.</li><li>◆ Die DRS-Konfiguration muss entweder <b>Teilweise automatisiert</b> oder <b>vollautomatisch</b> sein (sie darf nicht auf <b>Manuell</b> gesetzt sein.)</li><li>◆ Als VM-Container darf der DRS-Cluster nur aus ESXi 5.1-Servern bestehen und kann nur von vCenter 5.1 verwaltet werden.</li></ul>
VMware ESXi 4.1 (GA2, Update 3)	<ul style="list-style-type: none"><li>◆ Unterstützt als Schutz- und Failback-Container.</li><li>◆ Die DRS-Konfiguration muss entweder <b>Teilweise automatisiert</b> oder <b>vollautomatisch</b> sein (sie darf nicht auf <b>Manuell</b> gesetzt sein.)</li><li>◆ Als VM-Container darf der DRS-Cluster nur aus ESXi 4.1-Servern bestehen und kann nur von vCenter 4.1 verwaltet werden.</li></ul>

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

## 1.2.4 Unterstützte System-Firmware

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

Auf Windows-Systemen spiegelt PlateSpin Protect die Microsoft-Unterstützung für UEFI wider. Weitere Informationen finden Sie unter [Unterstützung für Workload-Firmware \(UEFI und BIOS\)](#) in [Abschnitt 1.2.1, „Unterstützte Windows-Workloads“](#) auf Seite 14.

## 1.3 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.

- ♦ [Abschnitt 1.3.1, „Sicherheit der Workload-Daten bei der Übertragung“ auf Seite 19](#)
- ♦ [Abschnitt 1.3.2, „Sicherheit der Client-Server-Kommunikation“ auf Seite 19](#)
- ♦ [Abschnitt 1.3.3, „Sicherheit von Berechtigungsnachweisen“ auf Seite 19](#)
- ♦ [Abschnitt 1.3.4, „Benutzerautorisierung und -authentifizierung“ auf Seite 19](#)
- ♦ [Abschnitt 1.3.5, „Einstellungen für Netzwerk-Ports“ auf Seite 20](#)
- ♦ [Abschnitt 1.3.6, „Zusätzliche Sicherheitsverbesserungen“ auf Seite 21](#)

### 1.3.1 Sicherheit der Workload-Daten bei der Übertragung

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

Sie können die Verschlüsselung für jeden Workload einzeln aktivieren oder deaktivieren. Weitere Informationen hierzu finden Sie unter [Abschnitt 5.4.1, „Workload-Schutz-Details“ auf Seite 74](#).

### 1.3.2 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.

### 1.3.3 Sicherheit von Berechtigungsnachweisen

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

### 1.3.4 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 [Abschnitt 2.2, „Einrichten der Benutzerautorisierung und -authentifizierung“ auf Seite 27](#).

## 1.3.5 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. Weitere Informationen zum Konfigurieren des Netzwerkzugriffs für die PlateSpin-Server-Umgebung finden Sie in [Abschnitt 2.3, „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“](#) auf Seite 31.

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

Portnummer	Protokoll	Details
80	TCP	(Nicht sicher) Für die HTTP-Kommunikation zwischen der Forge-VM und den Ursprungs- und Zielcomputern.  Öffnen Sie diesen Port auf der Forge-VM, im Ursprungs- und Ziel-Workload sowie auf den VMware-ESXi-Hosts.
443	TCP	(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-Server.
3725	TCP	Für die Datenübertragung zwischen Ursprungs- und Zielcomputer (auch dateibasierte und blockbasierte Übertragung).  Öffnen Sie diesen Port auf dem Ursprungs- und Zielservers für alle Workloads. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 1.2, „Unterstützte Konfigurationen“</a> auf Seite 13.
135, 445	TCP	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 auf dem Ursprungs- und Zielservers für alle Windows-Workloads. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 1.2.1, „Unterstützte Windows-Workloads“</a> auf Seite 14.
137, 138, 139	TCP	Für die NetBIOS-Kommunikation (Namensdienst, Datagrammdienst und Sitzungsdienst).  Öffnen Sie diese Ports für die Kommunikation auf dem Ursprungs- und Zielservers für alle Windows-Workloads. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 1.2.1, „Unterstützte Windows-Workloads“</a> auf Seite 14.
137, 138	UDP	Für die SMB-Kommunikation zur Dateiübertragung des Take-Control-Orders und der zugehörigen Dateien vom PlateSpin-Server auf den Ursprungscomputer.
139, 445	TCP	
22	TCP	Für die SSH- und SCP-Kommunikation auf Linux-Computern während des Ermittlungsvorgangs.  Öffnen Sie diesen Port auf dem Ursprungs- und Zielservers für alle Linux-Workloads. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 1.2.2, „Unterstützte Linux-Workloads“</a> auf Seite 16.
25	TCP und UDP	Für den SMTP-Datenverkehr, wenn die E-Mail-Benachrichtigung deaktiviert ist.  Öffnen Sie diesen Port auf der Forge-VM.

Portnummer	Protokoll	Details
1443	TCP	Für die Microsoft SQL Server-Kommunikation zur Authentifizierung und Datenübertragung an einen Remote-SQL-Server.  Öffnen Sie diesen Port auf der Forge-VM und dem Remote-SQL-Server-Host.  Weitere Informationen zu den Port-Anforderungen für SQL Server finden Sie unter <a href="#">Konfigurieren der Firewall für den Server-Zugriff</a> im Microsoft Developers Network.
1434	TCP	Für die dedizierte Admin-Verbindung zu Microsoft SQL Server.
1434	UDP	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	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.

## 1.3.6 Zusätzliche Sicherheitsverbesserungen

Im [Wissensdatenbankartikel 7015818](#) finden Sie Informationen, wie Sie die Angreifbarkeit durch potenzielle POODLE-Angriffe (Padding Oracle On Downgraded Legacy Encryption) von Ihren PlateSpin-Servern beseitigen.

## 1.4 Leistung

- ♦ [Abschnitt 1.4.1, „Allgemeines zu Produktleistungsmerkmalen“ auf Seite 21](#)
- ♦ [Abschnitt 1.4.2, „Datenkomprimierung“ auf Seite 22](#)
- ♦ [Abschnitt 1.4.3, „Bandbreitendrosselung“ auf Seite 22](#)
- ♦ [Abschnitt 1.4.4, „RPO-, RTO- und TTO-Spezifikationen“ auf Seite 22](#)
- ♦ [Abschnitt 1.4.5, „Skalierbarkeit“ auf Seite 23](#)

### 1.4.1 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.

## 1.4.2 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 Volumens 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 [Abschnitt 6.4, „Schutzebenen“ auf Seite 90](#).

## 1.4.3 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 [Abschnitt 6.4, „Schutzebenen“ auf Seite 90](#).

## 1.4.4 RPO-, RTO- und TTO-Spezifikationen

- ♦ **Angestrebter Wiederherstellungszeitpunkt (RPO):** Beschreibt die akzeptable Menge an Datenverlust, gemessen in Zeit. Der RPO ermittelt sich aus der Zeit zwischen den inkrementellen Reproduktionen eines geschützten Workloads und wird vom aktuellen Nutzungsumfang von PlateSpin 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 [Abschnitt 5.7, „Failover“ auf Seite 78](#).

- ♦ **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 79](#).

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 [Abschnitt 4.5, „Generieren von Workload- und Workload-Schutz-Berichten“ auf Seite 67](#).

## 1.4.5 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 Kapazitätswerte stufenweise anpassen und sie zur Bestimmung der maximalen Skalierbarkeit verwenden.





---

# 2 PlateSpin Forge- Anwendungskonfiguration

Dieser Abschnitt enthält folgende Informationen:

- ♦ [Abschnitt 2.1, „Produktlizenzierung“ auf Seite 25](#)
- ♦ [Abschnitt 2.2, „Einrichten der Benutzerautorisierung und -authentifizierung“ auf Seite 27](#)
- ♦ [Abschnitt 2.3, „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“ auf Seite 31](#)
- ♦ [Abschnitt 2.4, „Konfigurieren von PlateSpin Forge-Standardoptionen“ auf Seite 35](#)

## 2.1 Produktlizenzierung

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

- ♦ [Abschnitt 2.1.1, „Abrufen eines Lizenzaktivierungscode“ auf Seite 25](#)
- ♦ [Abschnitt 2.1.2, „Online-Lizenzaktivierung“ auf Seite 25](#)
- ♦ [Abschnitt 2.1.3, „Offline-Lizenzaktivierung“ auf Seite 26](#)

### 2.1.1 Abrufen eines Lizenzaktivierungscode

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

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

### 2.1.2 Online-Lizenzaktivierung

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

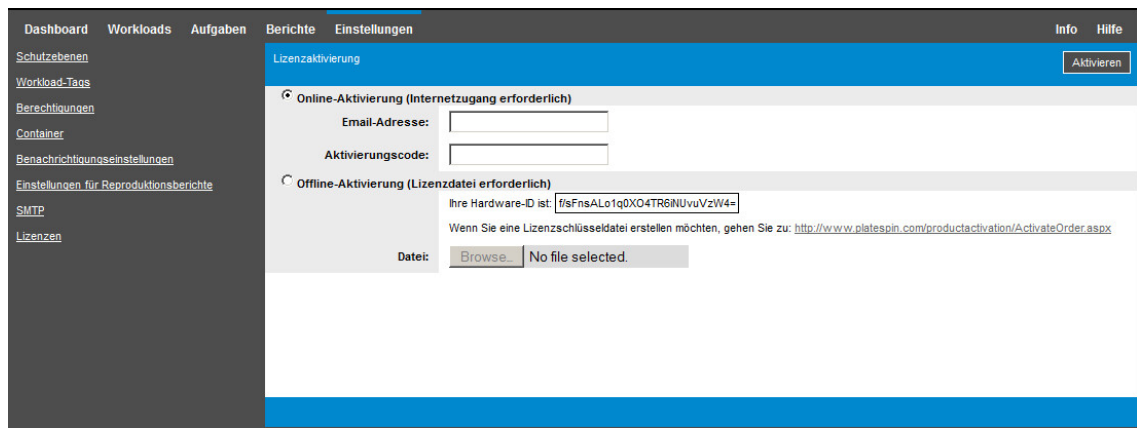
---

**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 **Einstellungen > Lizenzen > Lizenz hinzufügen**. Die Seite „Lizenzaktivierung“ wird angezeigt.



- 2 Wählen Sie **Online-Aktivierung**, geben Sie die E-Mail-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.

## 2.1.3 Offline-Lizenzaktivierung

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

---

**HINWEIS:** Sie müssen über ein Novell-Konto verfügen, um einen Lizenzschlüssel abrufen zu können. Wenn Sie bereits PlateSpin-Kunde sind und kein Customer Center-Konto besitzen, müssen Sie zunächst [ein Konto erstellen](#). Verwenden Sie Ihren bestehenden PlateSpin-Benutzernamen (eine gültige bei PlateSpin registrierte E-Mail-Adresse) als Benutzernamen für Ihr Customer Center-Konto.

---

### So aktivieren Sie eine Offline-Lizenz:

- 1 Klicken Sie auf **Einstellungen > Lizenz** und dann auf **Lizenz hinzufügen**. Die Seite „Lizenzaktivierung“ wird angezeigt.
- 2 Wählen Sie **Offline-Aktivierung** aus und kopieren Sie die angezeigte Hardware-ID.
- 3 Navigieren Sie in einem Webbrowser auf einem Computer mit Internetanschluss zur [PlateSpin-Produktaktivierungs-Website \(http://www.platespin.com/productactivation/ActivateOrder.aspx\)](http://www.platespin.com/productactivation/ActivateOrder.aspx). Melden Sie sich mit Ihrem Novell-Benutzernamen und Ihrem Passwort an.
- 4 Füllen Sie die entsprechenden Felder aus:
  - ♦ Den erhaltenen Aktivierungscode
  - ♦ Die bei der Auftragserteilung angegebene E-Mail-Adresse
  - ♦ Die in [Schritt 2](#) kopierte Hardware-ID
- 5 Klicken Sie auf **Aktivieren**.

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

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

## 2.2 Einrichten der Benutzerautorisierung und -authentifizierung

Der Abschnitt enthält folgende Informationen:

- ♦ [Abschnitt 2.2.1, „Info über die Benutzerautorisierung und -authentifizierung von PlateSpin Forge“ auf Seite 27](#)
- ♦ [Abschnitt 2.2.2, „Verwalten von PlateSpin Forge-Zugriff und -Berechtigungen“ auf Seite 28](#)
- ♦ [Abschnitt 2.2.3, „Verwalten von PlateSpin Forge-Sicherheitsgruppen und -Workload-Berechtigungen“ auf Seite 30](#)

### 2.2.1 Info über die Benutzerautorisierung und -authentifizierung von 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

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

Darüber hinaus bietet die PlateSpin 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 [Abschnitt 2.2.3, „Verwalten von PlateSpin Forge-Sicherheitsgruppen und -Workload-Berechtigungen“](#) auf Seite 30.

## 2.2.2 Verwalten von PlateSpin Forge-Zugriff und -Berechtigungen

Die folgenden Abschnitte enthalten weitere Informationen:

- ♦ [„Hinzufügen von PlateSpin Forge-Benutzern“](#) auf Seite 29
- ♦ [„Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Forge-Benutzer“](#) auf Seite 29

## 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 29](#) weiter.

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

Jetzt können Sie dem gerade erstellten Benutzer eine Workload-Schutz-Rolle zuweisen. Weitere Informationen hierzu finden Sie unter [„Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Forge-Benutzer“ auf Seite 29](#).

## 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 27](#).

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

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

### So starten Sie den Webserver neu:

- 1 Wechseln Sie in das Unterverzeichnis `bin\RestartPlateSpinServer` des PlateSpin-Servers.
- 2 Doppelklicken Sie auf die Programmdatei `RestartPlateSpinServer.exe`.  
Es wird ein Befehlszeilenfenster geöffnet, in dem Sie aufgefordert werden, den Vorgang zu bestätigen.
- 3 Geben Sie `y` ein und drücken Sie die `Eingabetaste`.

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 30](#).

## 2.2.3 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.

**So richten Sie eine Sicherheitsgruppe ein:**

- 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.
- 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**.

Erteilen	Name	Rollen
<input checked="" type="checkbox"/>	NORB-US-W2K8R2\Operator1	Workload-Schutz-Operator

OK Abbrechen

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

Einbeziehen	Name des Workloads	Sicherheitsgruppe
<input type="checkbox"/>	vsles11sp3x64.example.com	[Nicht zugewiesen]
<input type="checkbox"/>	VVC1	[Nicht zugewiesen]
<input type="checkbox"/>	AE-W2K3-1	[Nicht zugewiesen]
<input checked="" type="checkbox"/>	AE-W2K3-3	[Nicht zugewiesen]
<input checked="" type="checkbox"/>	AE-W2K3-4	[Nicht zugewiesen]

OK Abbrechen

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

7 Klicken Sie auf **Erstellen**.

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

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

## 2.3 Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk

Dieser Abschnitt enthält folgende Informationen:

- [Abschnitt 2.3.1, „Anforderungen für geöffnete Ports für die Forge-VM“ auf Seite 31](#)
- [Abschnitt 2.3.2, „Zugriffs- und Kommunikationsanforderungen für Workloads“ auf Seite 31](#)
- [Abschnitt 2.3.3, „Zugriffs- und Kommunikationsanforderungen für Container“ auf Seite 33](#)
- [Abschnitt 2.3.4, „Schutz über öffentliche und private Netzwerke durch NAT“ auf Seite 33](#)
- [Abschnitt 2.3.5, „Außerkräftsetzen der Standard-Bash-Shell zum Ausführen von Befehlen auf Linux-Workloads“ auf Seite 34](#)
- [Abschnitt 2.3.6, „Anforderungen für VMware DRS-Cluster als Container“ auf Seite 34](#)

### 2.3.1 Anforderungen für geöffnete Ports für die Forge-VM

Die folgenden Anforderungen gelten für geöffnete Ports für die Forge-VM.

*Table 2-2 Anforderungen für geöffnete Ports für PlateSpin-Server-Hosts*

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

### 2.3.2 Zugriffs- und Kommunikationsanforderungen für Workloads

Nachfolgend werden die Software-, Netzwerk- und Firewall-Anforderungen für Workloads beschrieben, die mithilfe von PlateSpin Forge geschützt werden sollen.

*Table 2-3 Zugriffs- und Kommunikationsanforderungen für Workloads*

Workload-Typ	Voraussetzungen	Erforderliche Ports (Standards)
Alle Workloads	Ping-Unterstützung (ICMP-Echoanfrage und -antwort)	

Workload-Typ	Voraussetzungen	Erforderliche Ports (Standards)
Alle Windows-Workloads. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 1.2.1, „Unterstützte Windows-Workloads“</a> auf Seite 14.	<ul style="list-style-type: none"> <li>◆ Microsoft .NET Framework 3.5 Service Pack 1</li> <li>◆ Microsoft .NET Framework 4.0</li> </ul>	
Alle Windows-Workloads. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 1.2.1, „Unterstützte Windows-Workloads“</a> auf Seite 14.	<ul style="list-style-type: none"> <li>◆ Integrierter Administrator- oder Domänen-Administrator-Kontoberechtigungs-nachweis (die Mitgliedschaft in der lokalen Administratorgruppe reicht nicht aus).</li> <li>◆ Die Windows-Firewall, die so konfiguriert ist, dass sie die <b>Datei- und Druckerfreigabe</b> zulässt. Verwenden Sie eine der folgenden Optionen: <ul style="list-style-type: none"> <li>◆ <b>Option 1 mit der Windows-Firewall:</b> Verwenden Sie das grundlegende Systemsteuerungselement <b>Windows-Firewall</b> (<code>firewall.cpl</code>) und wählen Sie in der Liste der Ausnahmen die Option <b>Datei- und Druckerfreigabe</b> aus.</li> <li>- ODER -</li> <li>◆ <b>Option 2 mit der Firewall mit erweiterter Sicherheit:</b> Verwenden Sie das Dienstprogramm <b>Windows-Firewall mit erweiterter Sicherheit</b> (<code>wf.msc</code>), bei dem die folgenden <b>Eingangsregeln</b> aktiviert und auf <b>Zulassen</b> festgelegt sind: <ul style="list-style-type: none"> <li>◆ <b>Datei- und Druckerfreigabe (Echoanforderung Alt+0150 ICMPv4In)</b></li> <li>◆ <b>Datei- und Druckerfreigabe (Echoanforderung Alt+0150 ICMPv6In)</b></li> <li>◆ <b>Datei- und Druckerfreigabe (NB-Datagramm eingehend)</b></li> <li>◆ <b>Datei- und Druckerfreigabe (NB-Name eingehend)</b></li> <li>◆ <b>Datei- und Druckerfreigabe (NB-Sitzung eingehend)</b></li> <li>◆ <b>Datei- und Druckerfreigabe (SMB eingehend)</b></li> <li>◆ <b>Datei- und Druckerfreigabe (Spoolerdienst Alt+0150 RPC)</b></li> <li>◆ <b>Datei- und Druckerfreigabe (Spoolerdienst – RPC-EPMAP)</b></li> </ul> </li> </ul> </li> </ul>	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)	<p><b>HINWEIS:</b> Nach dem Aktivieren der erforderlichen Anschlüsse aktivieren Sie die PlateSpin-Remote-Verwaltung mit dem folgenden Befehl an der Server-Eingabeaufforderung:</p> <pre>netsh firewall set service RemoteAdmin enable</pre> <p>Weitere Informationen zum Befehl „netsh“ finden Sie im Microsoft TechNet-Artikel <a href="http://technet.microsoft.com/en-us/library/cc785383%28v=ws.10%29.aspx">Das Befehlszeilenprogramm „Netsh“</a> (<a href="http://technet.microsoft.com/en-us/library/cc785383%28v=ws.10%29.aspx">http://technet.microsoft.com/en-us/library/cc785383%28v=ws.10%29.aspx</a>).</p>	TCP 3725, 135, 139, 445 UDP 137, 138, 139



Workload-Typ	Voraussetzungen	Erforderliche Ports (Standards)
Alle Linux-Workloads. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 1.2.2</a> , „Unterstützte Linux-Workloads“ auf Seite 16	Secure Shell (SSH)-Server	TCP 22, 3725

## 2.3.3 Zugriffs- und Kommunikationsanforderungen für Container

Die folgenden Software-, Netzwerk- und Firewall-Anforderungen gelten 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 <a href="#">Abschnitt 1.2.3</a> , „Unterstützte VM-Container“ auf Seite 18.	<ul style="list-style-type: none"> <li>◆ VMware-Konto mit Administratorrolle</li> <li>◆ VMware Web-Services-API und Dateiverwaltungs-API</li> </ul>	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)

## 2.3.4 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 34.
- ◆ **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 \(Workload an VM\) \(Seite 82\)](#) angeben.
- ♦ **Failback-Ziel:** Wenn Sie bei dem Versuch ein Failback-Ziel zu registrieren dazu aufgefordert werden, die IP-Adresse des PlateSpin-Servers anzugeben, müssen Sie entweder die lokale Adresse des Protect-Server-Hosts angeben oder eine seiner öffentlichen (externen) Adressen, die im *PlateSpin Server Configuration*-Werkzeug des Servers aufgezeichnet wurden (weitere Informationen hierzu finden Sie 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 [Abschnitt 2.4.3, „Konfigurieren des Verhaltens des PlateSpin-Servers mithilfe von XML-Konfigurationsparametern“ auf Seite 40.](#)

### 2.3.5 Außerkräftsetzen 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](#).

### 2.3.6 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 \(Schutzziel\)“ auf Seite 71.](#)

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.

## 2.4 Konfigurieren von PlateSpin Forge-Standardoptionen

Dieser Abschnitt enthält folgende Informationen:

- ◆ [Abschnitt 2.4.1, „Einrichten automatischer Email-Benachrichtigungen zu Ereignissen und Berichten“ auf Seite 35](#)
- ◆ [Abschnitt 2.4.2, „Einrichtung der Sprache bei internationalen Versionen von PlateSpin Forge“ auf Seite 39](#)
- ◆ [Abschnitt 2.4.3, „Konfigurieren des Verhaltens des PlateSpin-Servers mithilfe von XML-Konfigurationsparametern“ auf Seite 40](#)
- ◆ [Abschnitt 2.4.4, „Konfigurieren der Unterstützung für VMware vCenter Site Recovery Manager“ auf Seite 43](#)
- ◆ [Abschnitt 2.4.5, „Sortieren von Workloads mithilfe von Tags“ auf Seite 45](#)

### 2.4.1 Einrichten automatischer Email-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.

- ◆ [„SMTP-Konfiguration“ auf Seite 35](#)
- ◆ [„Einrichten automatischer Ereignisbenachrichtigungen per Email“ auf Seite 36](#)
- ◆ [„Einrichten automatischer Reproduktionsberichte per Email“ auf Seite 38](#)

### 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)

SMTP-Einstellungen		Speichern
SMTP-Serveradresse:	<input type="text"/>	
Port:	<input type="text" value="25"/>	
Antwortadresse:	<input type="text"/>	
Benutzername:	<input type="text"/>	
Passwort:	<input type="password"/>	
Bestätigen:	<input type="text"/>	

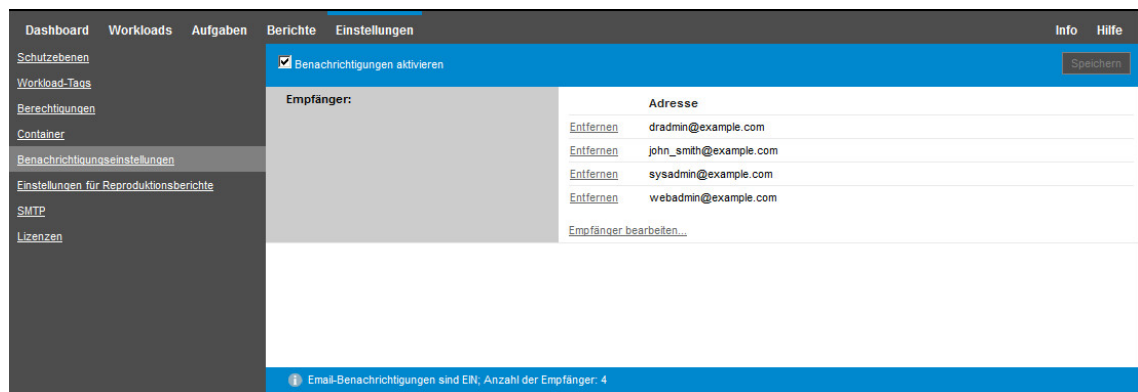
## So konfigurieren Sie die SMTP-Einstellungen:

- 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**.

## 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 35.
- 2 Klicken Sie auf der PlateSpin Forge-Weboberfläche auf **Einstellungen > E-Mail > 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**.  
Klicken Sie zum Löschen aufgelisteter Email-Adressen auf **Löschen** neben den zu entfernenden Adressen.

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*

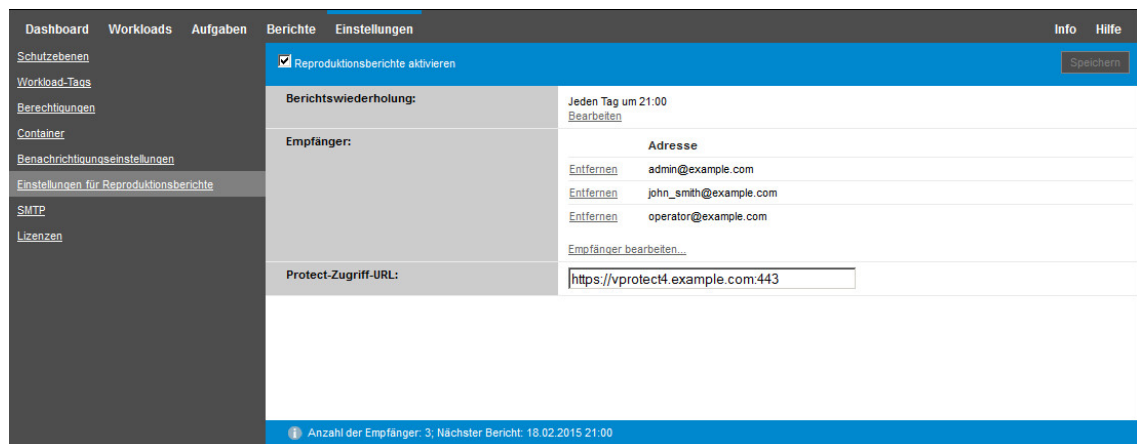
Ereignisarten	Anmerkungen
<b>Protokolleintragsart: Warnmeldung</b>	
FullReplicationMissed	Ähnlich dem Ereignis Inkrementelle Reproduktion verpasst.
IncrementalReplicationMissed	<p>Wird generiert, wenn Folgendes zutrifft:</p> <ul style="list-style-type: none"> <li>◆ Eine Reproduktion wird manuell angehalten, wenn eine geplante inkrementelle Reproduktion fällig ist.</li> <li>◆ Das System versucht, eine geplante inkrementelle Reproduktion auszuführen, während gerade eine manuell ausgelöste Reproduktion stattfindet.</li> <li>◆ Das System stellt fest, dass das Ziel nicht über genügend freien Speicherplatz verfügt.</li> </ul>
WorkloadOfflineDetected	<p>Wird generiert, wenn das System erkennt, dass ein Workload, der zuvor online war, nun offline ist.</p> <p>Betrifft Workloads, deren Schutzvertragsstatus nicht <b>Unterbrochen</b> lautet.</p>
<b>Protokolleintragsart: Fehler</b>	
FailoverFailed	
FullReplicationFailed	
IncrementalReplicationFailed	
PrepareFailoverFailed	
<b>Protokolleintragsart: Informationen</b>	
FailoverCompleted	
FullReplicationCompleted	
IncrementalReplicationCompleted	
PrepareFailoverCompleted	
TestFailoverCompleted	Wird generiert, wenn ein Failover-Test-Vorgang manuell als ordnungsgemäß durchgeführt oder als Fehler gekennzeichnet wird.

Ereignisarten	Anmerkungen
WorkloadOnlineDetected	Wird generiert, wenn das System erkennt, dass ein Workload, der zuvor offline war, nun online ist.  Betrifft Workloads, deren Schutzvertragsstatus nicht <b>Unterbrochen</b> lautet.

## Einrichten automatischer Reproduktionsberichte per Email

So richten Sie PlateSpin Forge zum Automatischen Senden von Reproduktionsberichten per Email ein:

- 1 Richten Sie einen SMTP-Server für PlateSpin Forge ein. Weitere Informationen hierzu finden Sie unter „SMTP-Konfiguration“ auf Seite 35.
- 2 Klicken Sie auf der PlateSpin Forge-Weboberfläche auf **Einstellungen > E-Mail > Reproduktionsberichte**.
- 3 Wählen Sie die Option **Reproduktionsberichte aktivieren**.
- 4 Klicken Sie im Abschnitt **Berichtswiederholung** auf **Konfigurieren** und geben Sie das erforderliche Wiederholungsmuster für die Berichte an.
- 5 Klicken Sie im Abschnitt **Empfänger** auf **Empfänger bearbeiten**, geben Sie die erforderlichen Email-Adressen getrennt durch Kommas ein und klicken Sie anschließend auf **OK**.



- 6 (Optional) Geben Sie im Abschnitt **Protect-Zugriff-URL** eine nicht standardmäßige URL für Ihren PlateSpin-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 [Abschnitt 4.5, „Generieren von Workload- und Workload-Schutz-Berichten“](#) auf Seite 67.

## 2.4.2 Einrichtung der Sprache 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.

### So fügen Sie Ihrem Webbrowser eine Sprache hinzu:

- 1 Rufen Sie im Webbrowser die Spracheinstellung auf:
  - ♦ **Internet Explorer:** Klicken Sie auf **Extras > Internetoptionen > Registerkarte „Allgemein“ > Sprachen.**
  - ♦ **Firefox:** Klicken Sie auf **Extras > Einstellungen > Registerkarte „Inhalt“ > Sprachen.**
  - ♦ **Chrome:** Klicken Sie im Chrome-Menü auf **Einstellungen**, blättern Sie zu **Erweiterte Einstellungen**, und klicken Sie auf diese Option. Wählen Sie dann unter **Sprachen** die Option **Sprach- und Eingabeeinstellungen.**
- 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 [Abschnitt 4.1, „Starten der PlateSpin Forge-Weboberfläche“ auf Seite 59.](#)

---

**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 [Abschnitt 3.4, „Forge Management-VM im Appliance-Host – Zugriff und Verwendung“ auf Seite 53.](#)
- 2 Starten Sie das Applet für die Regions- und Sprachoptionen (klicken Sie auf **Start > Ausführen**, geben Sie `intl.cpl` ein und drücken Sie die Eingabetaste) und klicken Sie anschließend auf die Registerkarte **Sprachen** (Windows Server 2003) bzw. **Tastaturen und Sprachen** (Windows Server 2008).
- 3 Installieren Sie das erforderliche Sprachpaket, sofern es noch nicht installiert ist. Möglicherweise benötigen Sie Zugriff auf die Installationsmedien Ihres Betriebssystems.
- 4 Wählen Sie die erforderliche Sprache als Oberflächensprache des Betriebssystems aus. Wenn eine entsprechende Aufforderung angezeigt wird, melden Sie sich ab oder starten Sie das System neu.

## 2.4.3 Konfigurieren des Verhaltens des PlateSpin-Servers mithilfe von XML-Konfigurationsparametern

Bestimmte Aspekte des Verhaltens des PlateSpin-Servers werden anhand von Konfigurationsparametern gesteuert, die Sie auf einer Konfigurationsseite auf der Forge-VM ([https://Thre\\_Forge-VM/platespinconfiguration/](https://Thre_Forge-VM/platespinconfiguration/)) festlegen.

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

### So ändern Sie Konfigurationsparameter und wenden sie an:

- 1 Navigieren Sie auf der Forge-VM zum angegebenen Verzeichnis.
- 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 40
- ♦ „[Einrichten der Unterstützung für SRM](#)“ auf Seite 42

## 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 [Abschnitt 2.4.3, „Konfigurieren des Verhaltens des PlateSpin-Servers mithilfe von XML-Konfigurationsparametern“](#) auf Seite 40.

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.



**Table 2-6** Standardmäßige und optimierte Konfigurationsparameter für die Dateiübertragung in [https://Ihre\\_PlateSpin-Forge-VM/platespinconfiguration/](https://Ihre_PlateSpin-Forge-VM/platespinconfiguration/)

Parameter	Standardwert	Höchstwert
AlwaysUseNonVSSFileTransferForWindows2003	Falsch	
FileTransferCompressionThreadsCount	2	nicht zutreffend
<p>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.</p>		
FileTransferBufferThresholdPercentage	10	
<p>Bestimmt die Mindestdatenmenge, die im Puffer gespeichert wird, bevor neue Netzwerkpakete erstellt und gesendet werden.</p>		
FileTransferKeepAliveTimeOutMilliSec	120000	
<p>Gibt an, wie lange mit dem Absenden von Keep-Alive-Meldungen gewartet werden soll, wenn eine TCP-Zeitüberschreitung eingetreten ist.</p>		
FileTransferLongerThan24HoursSupport	Wahr	
FileTransferLowMemoryThresholdInBytes	536870912	
<p>Bestimmt die Untergrenze für die Speichermenge auf dem Server. (Unterhalb dieser Mindestmenge treten bestimmte Netzwerkverhaltensweisen stärker auf.)</p>		
FileTransferMaxBufferSizeForLowMemoryInBytes	5242880	
<p>Bestimmt die Größe des internen Puffers bei mangelndem Speicherplatz.</p>		
FileTransferMaxBufferSizeInBytes	31457280	
<p>Bestimmt die Größe des internen Puffers für die Speicherung von Paketdaten.</p>		
FileTransferMaxPacketSizeInButes	1048576	
<p>Bestimmt die Größe der größten noch versendbaren Pakete.</p>		
FileTransferMinCompressionLimit	0 (deaktiviert)	Max. 65536 (64 KB)
<p>Gibt den Schwellwert für die Komprimierung auf Paketebene in Byte an.</p>		
FileTransferPort	3725	

Parameter	Standardwert	Höchstwert
FileTransferSendReceiveBufferSize	0 (8192 Byte)	Max. 5242880 (5 MB)
<p>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.</p> <p>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:</p> $((\text{Verbindungsgeschwindigkeit}(\text{MB/s})/8) * \text{Verzögerung}(\text{Sek.})) * 1000 * 1000$ <p>Beispielsweise wäre die geeignete Puffergröße bei einer 100-Mb/s-Verbindung mit 10 ms Latenz wie folgt:</p> $(100/8) * 0,01 * 1000 * 1000 = 125000 \text{ Byte}$		
FileTransferSendReceiveBufferSizeLinux	0 (253952 Byte)	
<p>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.</p> <p>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.</p> <p><b>HINWEIS:</b> In früheren Versionen vor PlateSpin Forge 11.1, PlateSpin Protect 11.1 und PlateSpin Migrate 12 mussten Sie diesen Parameter auf die Hälfte des gewünschten Werts einstellen; dies ist nicht mehr erforderlich.</p>		
FileTransferShutDownTimeOutInMinutes	1090	
FileTransferTCPTimeOutMilliSec	30.000	
<p>Legt den Zeitraum für die Zeitüberschreitung für TCP-Senden und TCP-Empfang fest.</p>		
PostFileTransferActionsRequiredTimeInMinutes	60	

## Einrichten der Unterstützung für SRM

Workloads, die von PlateSpin Forge reproduziert und vom VMware vCenter Site Recovery Manager (SRM) verwaltet werden, funktionieren nahtlos, wenn Sie die Unterstützung für SRM konfigurieren. Im Rahmen der Konfiguration müssen einige XML-Konfigurationsparameter des PlateSpin Servers geändert werden. Informationen über diese Konfigurationsänderungen finden Sie im Abschnitt [Abschnitt 2.4.4, „Konfigurieren der Unterstützung für VMware vCenter Site Recovery Manager“](#) auf Seite 43.

## 2.4.4 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 ein 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.

Die Konfiguration für die Unterstützung für Forge SRM umfasst die folgenden Anpassungen:

- ◆ Konfigurieren Sie eine Einstellung, damit die PlateSpin Forge-ISO und -Datenträger in derselben Datenablage gespeichert werden wie die VMware `.vmtx`- 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.

**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.

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 ESXi-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

---

## 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.

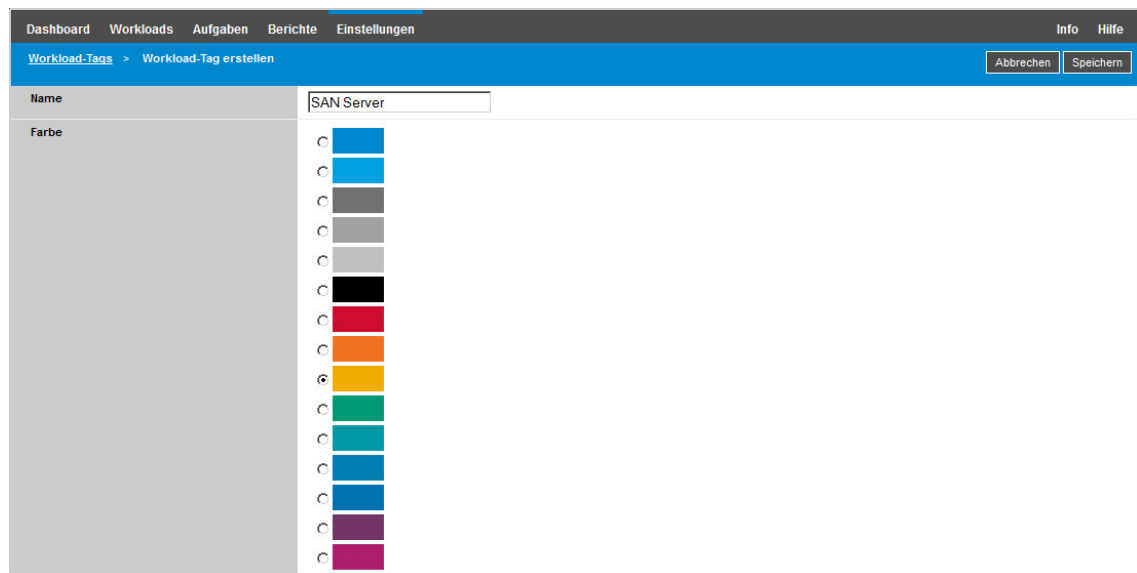
## 2.4.5 Sortieren von Workloads mithilfe von Tags

Die Workloads-Ansicht in der Weboberfläche enthält unter Umständen eine sehr lange Liste mit Workloads. Das Durchsuchen dieser Workloads zum Ausführen von Aktionen für ähnliche Workloads kann äußerst zeitaufwendig werden.

Zur einfachen Sortierung der Workload-Liste können Sie einem oder mehreren Workloads in der Workload-Liste optional ID-Tags zuweisen, so dass sie mit einer eindeutigen Farbe und Beschreibung gekennzeichnet werden. Wenn Tags zugeordnet sind, können Sie die Liste nach dem Tag-Attribut sortieren. Hierbei werden die Tags gruppiert, was die Massenauswahl für das Festlegen von Aktionen erleichtert.

**So richten Sie Workload-Tags ein:**

- 1 Klicken Sie auf der PlateSpin Forge-Weboberfläche auf **Einstellungen > Workload-Tags > Workload-Tag erstellen**. Die Seite „Workload-Tag erstellen“ wird geöffnet.



Auf dieser Seite können Sie einen Tag-Namen (max. 25 Zeichen) angeben und dieser Beschreibung eine Farbe zuweisen. Sie können beliebig viele eindeutige Tags anlegen; die Auswahl an Farben ist allerdings begrenzt.

Beim Speichern wird das neue Tag auf der Seite „Einstellungen“ in der Ansicht „Workload-Tags“ in die Liste der verfügbaren Workload-Tags aufgenommen. In dieser Ansicht können Sie die Tags in der Liste bearbeiten oder löschen.

Auf der Seite „Workloads“ in der Spalte „Tag“ wird jeweils das eindeutige Tag angezeigt, das Sie den einzelnen Workloads zugewiesen haben. Beim Sortieren nach dieser Spalte können Sie die Tags gruppieren und so verfügbare Aktionen gleichzeitig für diese getaggten Workloads ausführen.

**So weisen Sie ein einzelnes Tag einem Workload zu:**

- 1 Wählen Sie in der Liste der Workloads den zu taggenden Workload aus, und klicken Sie auf **Konfigurieren**. Die Konfigurationsseite für diesen Workload wird geöffnet.
- 2 Öffnen Sie auf der Konfigurationsseite unter „Tag“ die Dropdown-Liste, wählen Sie den Namen des Tags aus, das dem Workload zugewiesen werden soll, und klicken Sie auf **Speichern**.

## Weitere Informationen zu Tags

Beachten Sie auch die folgenden Informationen zu Workload-Tags:

- ♦ Wenn Sie einen Workload auf einen neuen Server exportieren, bleiben seine Tag-Einstellungen erhalten.
- ♦ Sie können ein Tag nicht löschen, wenn es noch mindestens einem Workload in der Liste zugewiesen ist.
- ♦ Soll ein Tag aus einem Workload entfernt werden (also seine Zuweisung aufgehoben werden), wählen Sie in der Dropdown-Liste der Tag-Namen den „leeren“ Eintrag aus.

---

# 3 Appliance-Einrichtung und Wartung

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

- ♦ [Abschnitt 3.1, „Einrichten des Appliance-Netzwerks“ auf Seite 47](#)
- ♦ [Abschnitt 3.2, „Physische Standortänderung der Appliance“ auf Seite 48](#)
- ♦ [Abschnitt 3.3, „Verwenden externer Speicherlösungen mit PlateSpin Forge“ auf Seite 51](#)
- ♦ [Abschnitt 3.4, „Forge Management-VM im Appliance-Host – Zugriff und Verwendung“ auf Seite 53](#)
- ♦ [Abschnitt 3.5, „Zurücksetzen von Forge auf die Werkseinstellungen“ auf Seite 56](#)

## 3.1 Einrichten des Appliance-Netzwerks

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

- ♦ [Abschnitt 3.1.1, „Einrichten des Appliance-Host-Netzwerks“ auf Seite 47](#)

### 3.1.1 Einrichten des Appliance-Host-Netzwerks

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

- ♦ **Externes Testnetzwerk:** 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:** Fortführung der realen Geschäftsprozesse, wenn ein Failover oder ein Failback durchgeführt wird.
- ♦ **Forge VM Management-Netzwerk:** Das Management-Netzwerk, das die Forge-Management-VM hostet.
- ♦ **Management-Netzwerk:** Hypervisor-Management-Netzwerk. Im PlateSpin Forge-Web-Client steht dieses Netzwerk nicht zur Auswahl.

Zum Standardlieferungsumfang 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 Netzwerkkarte für die Produktionskonnektivität und die andere ausschließlich für Reproduktionen verwendet werden. Weitere Informationen finden Sie im [Wissensdatenbankartikel 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](#).

## 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-Appliance alle Workloads aus, 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 48](#)
- [Abschnitt 3.2.2, „Szenario 2 – Standortänderung der Forge-Appliance \(neue IP-Adresse nicht bekannt\)“ auf Seite 49](#)

### 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 [Abschnitt 3.4.3, „Starten und Herunterfahren der Forge Management-VM“ auf Seite 54](#).
  - 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 [Abschnitt 3.4.2, „Starten des vSphere-Clients und Zugriff auf die Forge Management-VM“ auf Seite 53](#)).
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 48](#).
- 2 Fahren Sie die Appliance herunter:
  - 2a Fahren Sie die Forge Management-VM herunter. Weitere Informationen hierzu finden Sie unter [Abschnitt 3.4.3, „Starten und Herunterfahren der Forge Management-VM“ auf Seite 54](#).
  - 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 Abschnitt zum „[Appliance-Konfigurationsprozess](#)“ 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 53).
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 51](#)
- ♦ [Abschnitt 3.3.2, „Hinzufügen einer SAN-LUN zu Forge“ auf Seite 52](#)

### 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- 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 \(http://www.vmware.com/support/pubs/\)](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 Ausweidlösungen.
- ♦ Die *VMware Knowledge Bases* enthalten Informationen zu bekannten Problemen und Ausweidlösungen.

Folgende Hersteller bieten Speicherprodukte, die von VMware getestet wurden:

- ♦ [3PAR \(http://www.3par.com\)](http://www.3par.com)
- ♦ [Bull \(http://www.bull.com\)](http://www.bull.com) (nur FC)
- ♦ [Compellent \(http://www.compellent.com\)](http://www.compellent.com)
- ♦ [Dell \(http://www.dell.com\)](http://www.dell.com)
- ♦ [EMC \(http://www.emc.com\)](http://www.emc.com)
- ♦ [EqualLogic \(http://www.equallogic.com\)](http://www.equallogic.com) (nur iSCSI)

- ♦ Fujitsu (<http://www.fujitsu.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.xitech.com>) (nur FC)


Weitere Informationen zu iSCSI finden Sie auf der [Website der Storage Networking Industry Association](http://www.snia.org/tech_activities/ip_storage/iscsi/) ([http://www.snia.org/tech\\_activities/ip\\_storage/iscsi/](http://www.snia.org/tech_activities/ip_storage/iscsi/)).

### 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.

**So fügen Sie eine SAN-LUN zu Forge hinzu:**

- 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 53).
- 3 Klicken Sie auf der vSphere-Client-Oberfläche 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 vSphere-Clientprogramm.

Im Web-Client 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 **Einstellungen** > **Container** wählen und auf  neben 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.

- ♦ [Abschnitt 3.4.1, „Herunterladen des vSphere-Clientprogramms“ auf Seite 53](#)
- ♦ [Abschnitt 3.4.2, „Starten des vSphere-Clients und Zugriff auf die Forge Management-VM“ auf Seite 53](#)
- ♦ [Abschnitt 3.4.3, „Starten und Herunterfahren der Forge Management-VM“ auf Seite 54](#)
- ♦ [Abschnitt 3.4.4, „Verwalten von Forge-Snapshots auf dem Appliance-Host“ auf Seite 54](#)
- ♦ [Abschnitt 3.4.5, „Manuelles Importieren von VMs in die Datenablage des Appliance-Hosts“ auf Seite 55](#)
- ♦ [Abschnitt 3.4.6, „Richtlinien zur Anwendung von Sicherheitsaktualisierungen auf die PlateSpin Forge Management-VM“ auf Seite 55](#)

### 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+Einf“.

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 53](#).
- 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 Forge-Snapshots 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 53](#).
- 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 (ESX 3.5 und höher) aus Ihrem Produktions-Workload (z. B. mit PlateSpin Migrate) und kopieren Sie die VM-Dateien von der Datenablage des ESX-Host auf einen Wechseldatenträger, wie z. B. 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 53](#).
- 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 im PlateSpin Forge-Web-Client 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 92](#)).

---

### 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 53](#).
- 2 Suchen Sie von der Windows-Benutzeroberfläche der Forge Management-VM aus nach Sicherheitsaktualisierungen von Microsoft.
- 3 Versetzen Sie PlateSpin Forge mithilfe des PlateSpin Forge-Web-Clients in den Wartungsmodus, indem Sie alle Reproduktionszeitpläne anhalten und warten, bis alle laufenden Reproduktionen abgeschlossen sind.
- 4 Erstellen Sie einen Snapshot der Forge Management-VM. Weitere Informationen hierzu finden Sie unter [„Verwalten von Forge-Snapshots auf dem Appliance-Host“ auf Seite 54](#).

- 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 des PlateSpin Forge-Web-Clients 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 Forge-Snapshots auf dem Appliance-Host](#)“ auf Seite 54.

## 3.5 Zurücksetzen von Forge auf die Werkseinstellungen

---

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

---

### So setzen Sie die Forge 11.1 Appliance (Version 3) auf die Werkseinstellungen zurück:

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

---

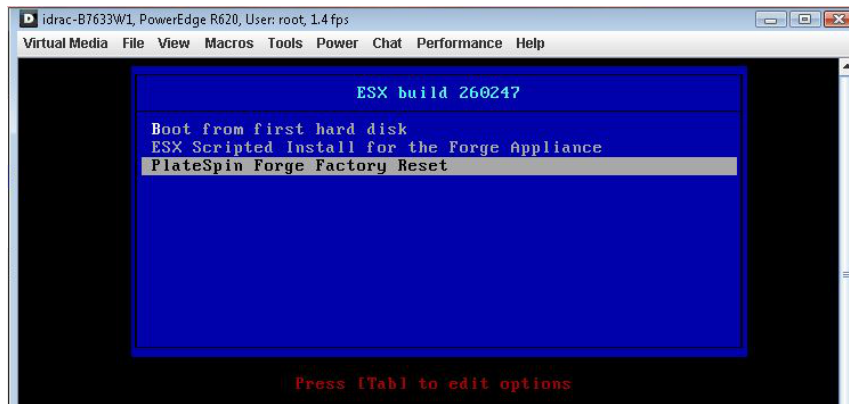
**WICHTIG:** Notieren Sie sich die auf dieser Seite angezeigte IP-Adresse der Appliance zum Zurücksetzen auf die Werkseinstellungen. Diese Adresse benötigen Sie zur Anmeldung am Forge ACC und zum Verschieben des Containers an eine bekannte, gültige IP-Adresse. Gehen Sie vor wie in [Abschnitt 3.2, „Physische Standortänderung der Appliance“](#) auf Seite 48 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.

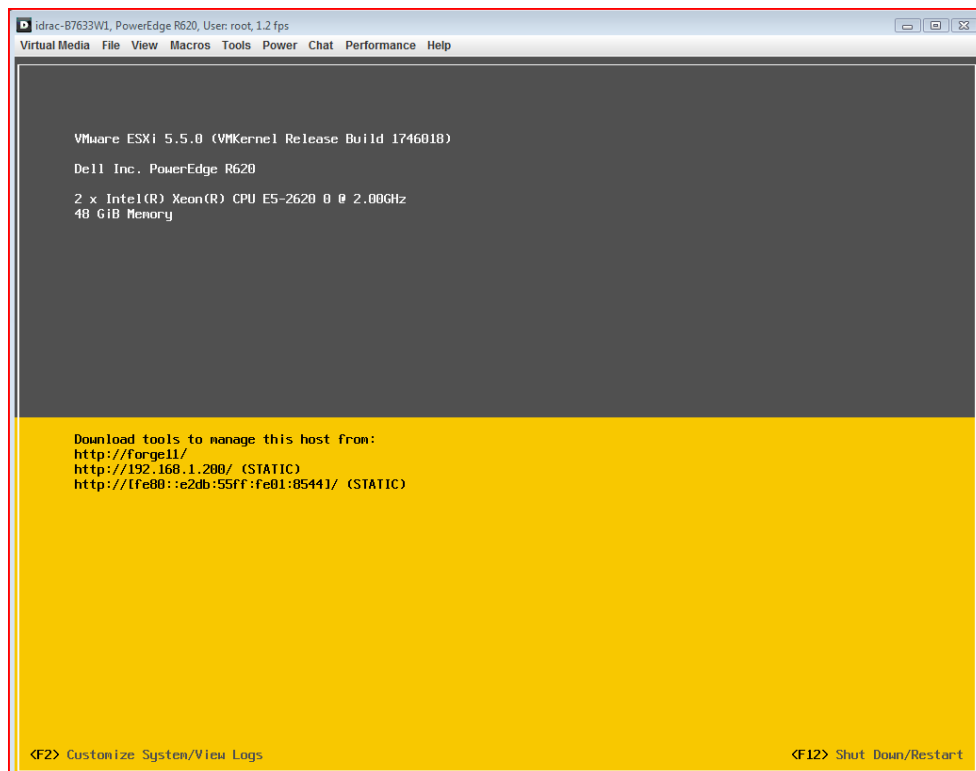


- 3f Booten Sie die Appliance über die Forge-CD (oder stellen Sie über iDRAC eine Verbindung zum ISO-Image her) und warten Sie, bis das SYSLINUX -Menü angezeigt wird.

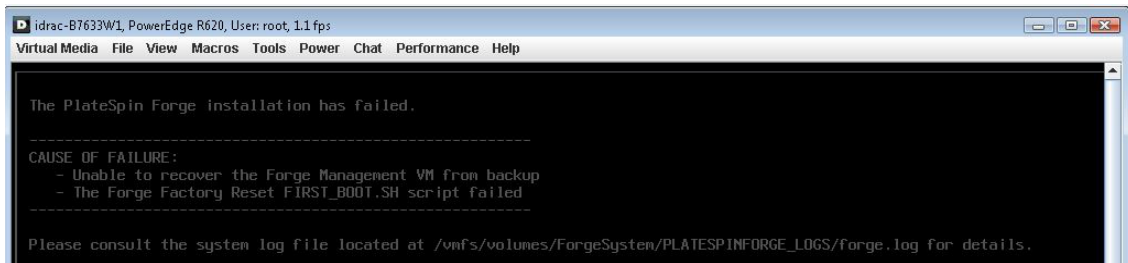


- 4 Wählen Sie die Option **PlateSpin Forge Factory Reset** (PlateSpin Forge-Reset) und drücken Sie die Eingabetaste. Dieser Schritt muss ausgeführt werden, bevor die Standardkonfiguration automatisch übernommen wird. (Etwa 10 Sekunden.)
- 5 Warten Sie, bis der Vorgang abgeschlossen ist.

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



Wird der Prozess zum Zurücksetzen nicht erfolgreich abgeschlossen, sieht der Bildschirm etwa so aus:



```
idrac-B7633W1, PowerEdge R620, User: root, 1.1 fps
Virtual Media File View Macros Tools Power Chat Performance Help

The PlateSpin Forge installation has failed.
-----
CAUSE OF FAILURE:
- Unable to recover the Forge Management VM from backup
- The Forge Factory Reset FIRST_BOOT.SH script failed
-----

Please consult the system log file located at /vmfs/volumes/ForgeSystem/PLATESPINFORGE_LOGS/forge.log for details.
```

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.

- ♦ [Abschnitt 4.1, „Starten der PlateSpin Forge-Weboberfläche“ auf Seite 59](#)
- ♦ [Abschnitt 4.2, „Elemente der PlateSpin Forge-Weboberfläche“ auf Seite 60](#)
- ♦ [Abschnitt 4.3, „Workloads und Workload-Befehle“ auf Seite 62](#)
- ♦ [Abschnitt 4.4, „Verwalten mehrerer Instanzen von PlateSpin Protect und PlateSpin Forge“ auf Seite 64](#)
- ♦ [Abschnitt 4.5, „Generieren von Workload- und Workload-Schutz-Berichten“ auf Seite 67](#)

## 4.1 Starten der 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:

- ♦ **Chrome:** Klicken Sie im Chrome-Menü auf **Einstellungen**, blättern Sie zu **Erweiterte Einstellungen anzeigen**, und klicken Sie auf diese Option. Wählen Sie dann **Inhaltseinstellungen > Ausführung von JavaScript für alle Websites zulassen**.
- ♦ **IE:** Wählen Sie im Menü „Extras“ den Eintrag **Internetoptionen > Sicherheit**. Klicken Sie auf **Stufe Anpassen**. Blättern Sie zu **Active Scripting**, und wählen Sie diesen Eintrag aus. Wählen Sie **Aktivieren**, klicken Sie im Warnfenster auf **Ja**, und klicken Sie auf **OK** und dann auf **Anwenden > OK**.
- ♦ **Firefox:** Klicken Sie auf **Extras > Einstellungen > Inhalt** und wählen Sie anschließend die Option **JavaScript aktivieren** aus.

---

Informationen zur Verwendung der PlateSpin Forge-Weboberfläche und der integrierten Hilfe in einer der unterstützten Sprachen finden Sie unter [Abschnitt 2.4.2, „Einrichtung der Sprache bei internationalen Versionen von PlateSpin Forge“ auf Seite 39](#).

**So starten Sie die PlateSpin Forge-Weboberfläche:**

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

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

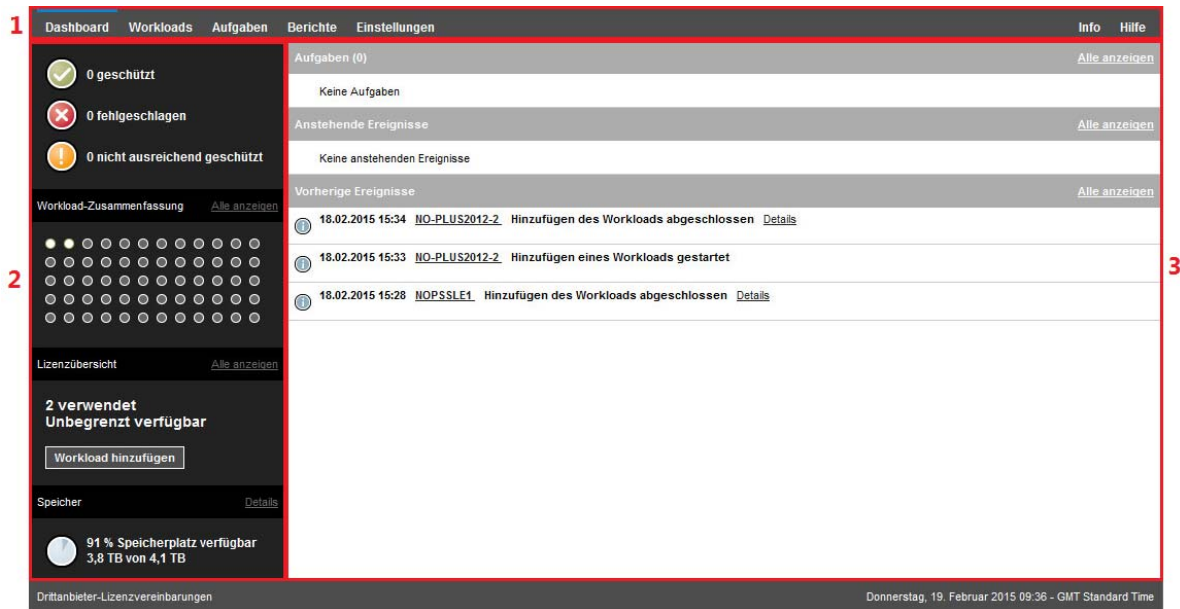
Ersetzen Sie `<Hostname | IP-Adresse>` durch den Hostnamen bzw. die IP-Adresse Ihrer Forge-VM.

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

## 4.2 Elemente der PlateSpin Forge-Weboberfläche

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

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 61](#)
- ♦ [Abschnitt 4.2.2, „Teilfenster mit visueller Zusammenfassung“ auf Seite 61](#)
- ♦ [Abschnitt 4.2.3, „Teilfenster mit Aufgaben und Ereignissen“ auf Seite 62](#)

---

**HINWEIS:** Sie können bestimmte Elemente der Weboberfläche an das Markenbild Ihres Unternehmens anpassen. Weitere Informationen finden Sie in [Anhang C, „Anpassen der PlateSpin Forge-Weboberfläche an das Markenbild“](#), auf Seite 131.

---

## 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 62](#).
- ♦ **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 67](#).
- ♦ **Einstellungen:** Zeigt die Seite „Einstellungen“ an, die Zugriff auf die folgenden Konfigurationsoptionen bietet:
  - ♦ **Schutzebenen:** Weitere Informationen hierzu finden Sie unter [„Schutzebenen“ auf Seite 90](#).
  - ♦ **Workload Tags:** Weitere Informationen hierzu finden Sie unter [„Sortieren von Workloads mithilfe von Tags“ auf Seite 45](#).
  - ♦ **Berechtigungen:** Weitere Informationen hierzu finden Sie unter [„Einrichten der Benutzerautorisierung und -authentifizierung“ auf Seite 27](#).
  - ♦ **Benachrichtigungseinstellungen:** [„Einrichten automatischer Ereignisbenachrichtigungen per Email“ auf Seite 36](#).
  - ♦ **Einstellungen für Reproduktionsberichte:** [„Einrichten automatischer Reproduktionsberichte per Email“ auf Seite 38](#)
  - ♦ **SMTP:** Weitere Informationen hierzu finden Sie unter [„Einrichten automatischer Email-Benachrichtigungen zu Ereignissen und Berichten“ auf Seite 35](#).
  - ♦ **Lizenzen:** Weitere Informationen hierzu finden Sie unter [„Produktlizenzierung“ auf Seite 25](#).

## 4.2.2 Teilfenster mit visueller Zusammenfassung

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

Inventarisierte Workloads werden in drei Kategorien dargestellt:

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

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

*Tabelle 4-1 Punktsymbol-Darstellung des Workload-Status*

---

● Ungeschützt	● Nicht ausreichend geschützt
○ Ungeschützt – Fehler	● Fehlgeschlagen

---

- Geschützt
- Abgelaufen
- Nicht verwendet

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

**Speicher** bietet Informationen über den für PlateSpin Forge verfügbaren Container-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 „[Einrichten automatischer Email-Benachrichtigungen zu Ereignissen und Berichten](#)“ auf Seite 35.

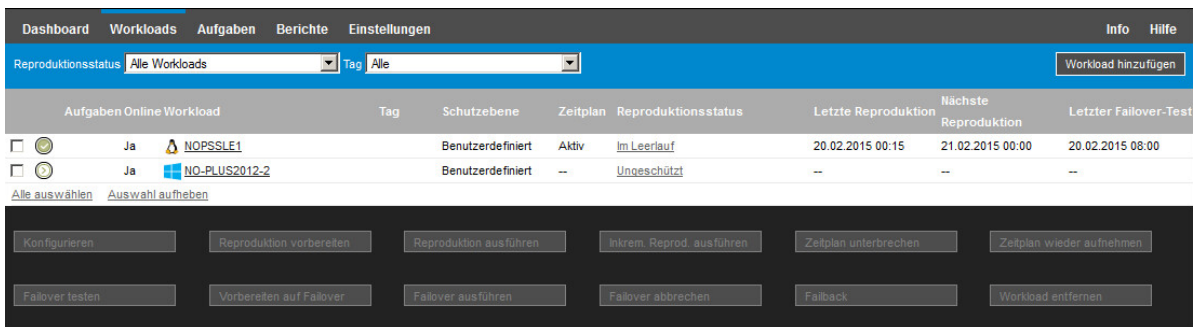
Aufgaben sind spezielle Befehle, die mit Ereignissen verbunden sind, die den Eingriff des Benutzers erfordern. Beispiel: Nach Abschluss des Befehls „Failover testen“ generiert das System ein Ereignis, das mit zwei Aufgaben verbunden ist: Mark. 'Test erfolgr.' und Mark. 'Test n. best.'. Wenn Sie auf eine 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“

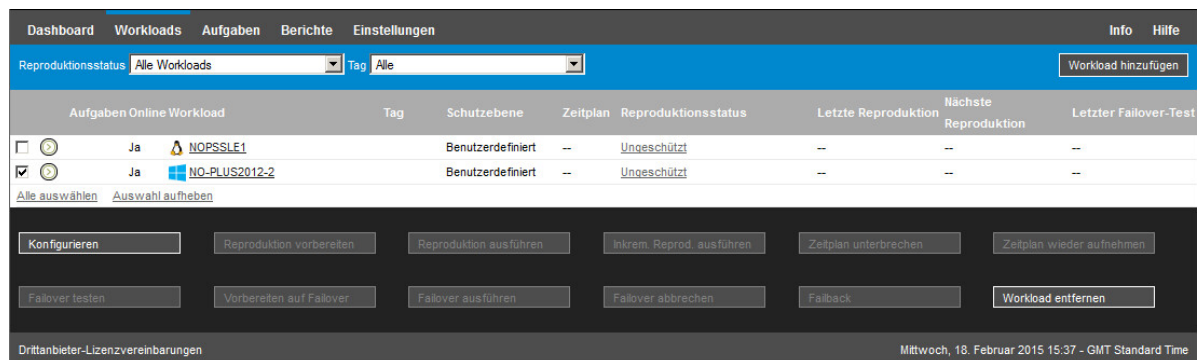


**HINWEIS:** Alle Zeitstempel entsprechen der Zeitzone der Forge-VM. Diese kann sich von der Zeitzone des geschützten Workloads oder der Zeitzone des Hosts, auf dem Sie die PlateSpin Forge-Weboberfläche ausführen, unterscheiden. Unten rechts im Client-Fenster werden das Serverdatum und die Serveruhrzeit 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
<b>Konfigurieren</b>	Startet die Konfiguration des Workload-Schutzes mit Parametern, die auf einen inventarisierten Workload anwendbar sind.
<b>Reproduktion vorbereiten</b>	Installiert die erforderliche Datentransfersoftware im Quell-Container und erstellt einen Failover-Workload (einen virtuellen Computer) im Ziel-Container zur Vorbereitung der Workload-Reproduktion.
<b>Reproduktion ausführen</b>	Startet die Reproduktion des Workloads entsprechend der angegebenen Parameter (vollständige Reproduktion).
<b>Inkrementell ausführen</b>	Führt eine inkrementelle Übertragung von geänderten Daten vom Ursprung zum Ziel außerhalb der im Vertrag für den Workload-Schutz festgelegten Zeiten durch.
<b>Zeitplan unterbrechen</b>	Setzt den Schutz aus; alle geplanten Reproduktionen werden übersprungen bis der Zeitplan wieder aufgenommen wird.
<b>Zeitplan wieder aufnehmen</b>	Nimmt den Schutz gemäß den gespeicherten Schutzeinstellungen wieder auf.
<b>Failover testen</b>	Bootet und konfiguriert den Failover-Workload für Testzwecke in einer isolierten Umgebung innerhalb des Containers.
<b>Vorbereiten auf Failover</b>	Bootet den Failover-Workload in Vorbereitung eines Failover-Vorgangs.

Workload-Befehl	Beschreibung
<b>Failover ausführen</b>	Bootet und konfiguriert den Failover-Workload, der die Geschäftsdienste eines fehlgeschlagenen Workloads übernimmt.
<b>Failover abbrechen</b>	Bricht den Failover-Vorgang ab.
<b>Failback</b>	Überführt den Failover-Workload nach einem Failover-Vorgang per Failback wieder in die ursprüngliche oder in eine neue Infrastruktur (virtuell oder physisch).
<b>Workload entfernen</b>	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 64](#)
- ♦ [Abschnitt 4.4.2, „Informationen zu PlateSpin Forge-Verwaltungskonsolenkarten“ auf Seite 65](#)
- ♦ [Abschnitt 4.4.3, „Hinzufügen von Instanzen von PlateSpin Protect und PlateSpin Forge zur Verwaltungskonsole“ auf Seite 66](#)
- ♦ [Abschnitt 4.4.4, „Verwalten von Karten auf der Verwaltungskonsole“ auf Seite 66](#)

### 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:

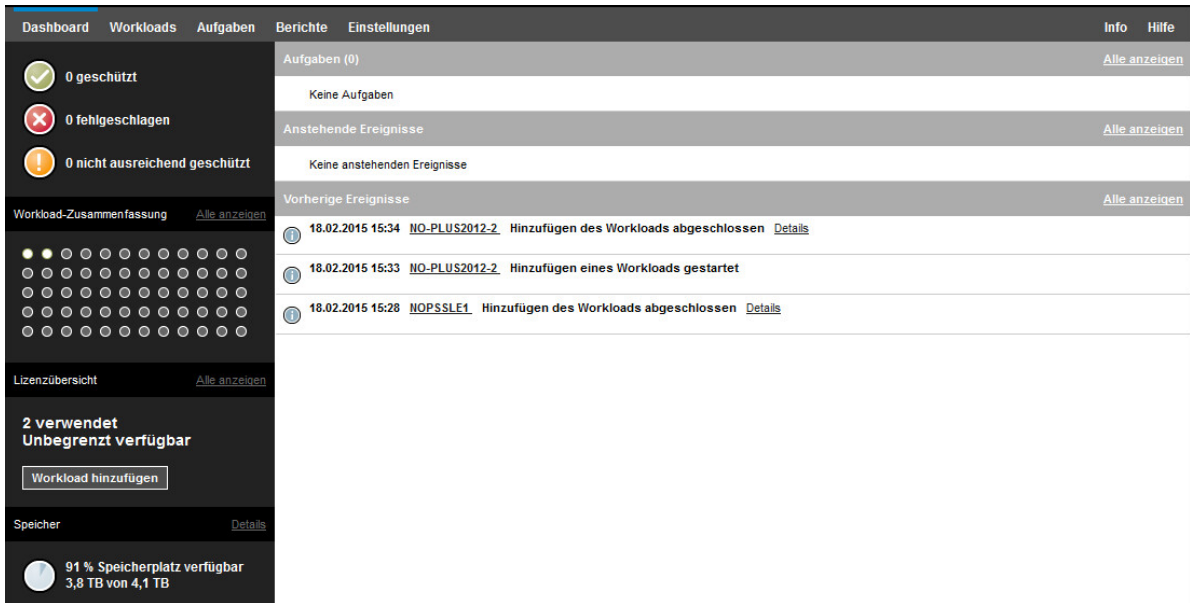
`https://<IP-Adresse | Hostname>/console.`

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

- 2 Melden Sie sich mit Ihrem Benutzernamen und Passwort an.  
Die Standardseite „Dashboard“ der Konsole wird angezeigt.



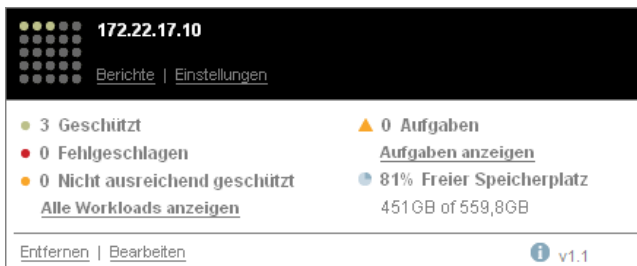
Abbildung 4-4 Die Standardseite „Dashboard“ der Verwaltungskonsole



## 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 oder PlateSpin Forge an, z. B.:

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

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

### 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**.  
Die Seite **Hinzufügen/Bearbeiten** wird angezeigt.
- 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 **Berechtigungs-nachweis der Verwaltungskonsole verwenden**, um denselben Berechtigungs-nachweis zu verwenden, der von der Konsole verwendet wird. Wenn diese Option ausgewählt ist, füllt die Konsole automatisch das Feld **Domäne\Benutzername** aus.
- 4 Geben Sie im Feld **Domäne\Benutzername** einen Domänennamen und einen Benutzernamen ein, die für die von Ihnen hinzugefügte PlateSpin Protect- oder Plate Spin Forge-Instanz gültig sind. Geben Sie im Feld **Passwort** das entsprechende Passwort ein.
- 5 (Optional) Geben Sie einen beschreibenden oder identifizierenden **Anzeigenamen** (max. 15 Zeichen), einen **Speicherort** (max. 20 Zeichen) und ggf. erforderliche **Hinweise** ein (max. 400 Zeichen).
- 6 Klicken Sie auf **Hinzufügen/Speichern**.  
Es wird eine neue Karte zum Dashboard hinzugefügt.

### 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

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

Die folgenden Berichtstypen werden unterstützt:

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

Abbildung 4-6 Optionen für einen Reproduktionsverlaufsbericht

Datum	Reproduktionsereignis	Gesamtzeit	Übertragszeit	Übertragsgröße	Übertragungsgeschwindigkeit
18.02.2015 16:59	Full replication completed	10Min. 42Sek.	1Min. 43Sek.	4,7 GB	387,47 Mb/s
18.02.2015 16:39	Incremental replication completed	8Min. 47Sek.	--	41,1 MB	466,38 Mb/s
18.02.2015 16:29	Full replication completed	13Min. 36Sek.	4Min. 13Sek.	4,6 GB	157,30 Mb/s

## 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.

- ♦ [Abschnitt 5.1, „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“ auf Seite 69](#)
- ♦ [Abschnitt 5.2, „Hinzufügen von Containern \(Schutzziel\)“ auf Seite 71](#)
- ♦ [Abschnitt 5.3, „Hinzufügen von Workloads“ auf Seite 72](#)
- ♦ [Abschnitt 5.4, „Konfigurieren der Schutzdetails und Vorbereiten der Reproduktion“ auf Seite 73](#)
- ♦ [Abschnitt 5.5, „Starten des Workload-Schutzes“ auf Seite 77](#)
- ♦ [Abschnitt 5.6, „Abbrechen von Befehlen“ auf Seite 77](#)
- ♦ [Abschnitt 5.7, „Failover“ auf Seite 78](#)
- ♦ [Abschnitt 5.8, „Failback“ auf Seite 80](#)
- ♦ [Abschnitt 5.9, „Erneutes Schützen eines Workloads“ auf Seite 85](#)

## 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 [Abschnitt 1.2, „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 [Abschnitt 2.3, „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“ auf Seite 31](#).
  - 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](#).

- ♦ (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](#).
- ♦ (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 [Abschnitt 6.8, „Verwenden von Freeze- und Thaw-Skripts für alle Reproduktionen \(Linux\)“](#) auf Seite 94.

**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 \(Schutzziel\)“](#) auf Seite 71 und [„Hinzufügen von Workloads“](#) auf Seite 72.

**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 [Abschnitt 5.4, „Konfigurieren der Schutzdetails und Vorbereiten der Reproduktion“](#) auf Seite 73.

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

Weitere Informationen hierzu finden Sie unter [Abschnitt 5.5, „Starten des Workload-Schutzes“](#) auf Seite 77.

**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 [Abschnitt 5.7.3, „Verwenden der Funktion „Failover testen““](#) auf Seite 79.

**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 [Abschnitt 5.7, „Failover“](#) auf Seite 78.

**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 [Abschnitt 5.8, „Failback“](#) auf Seite 80.

**8 Erneuter Schutz:** In diesem Schritt definieren Sie den ursprünglichen Schutzvertrag für den Workload neu. Weitere Informationen hierzu finden Sie unter [Abschnitt 5.9, „Erneutes Schützen eines Workloads“](#) auf Seite 85

Der Großteil dieser Schritte kann über Workload-Befehle auf der Seite „Workloads“ durchgeführt werden. Weitere Informationen hierzu finden Sie unter [Abschnitt 4.3, „Workloads und Workload-Befehle“](#) auf Seite 62.

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

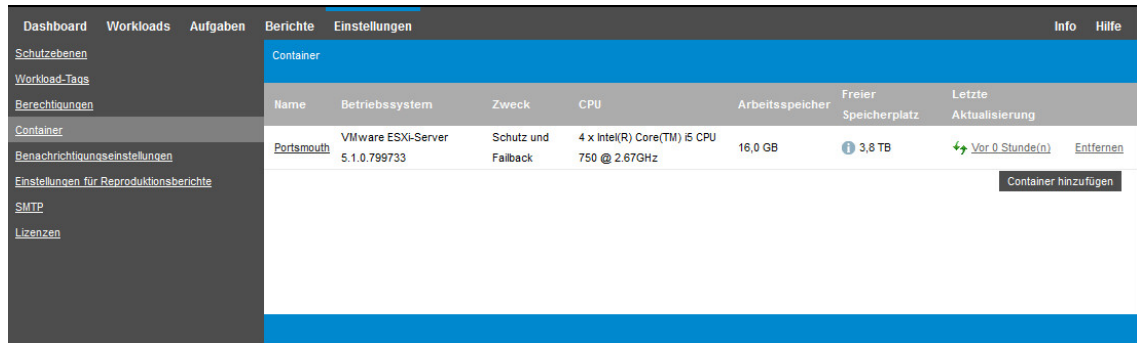
## 5.2 Hinzufügen von Containern (Schutzziel)

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 Ziel-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 [Abschnitt 1.2.3, „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-Berechtigungs-nachweis für den Zugriff auf den Ziel-Host ein. Weitere Informationen hierzu finden Sie unter [„Richtlinien für Workload- und Container-Berechtigungs-nachweise“](#) auf Seite 88.

- ♦ **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.

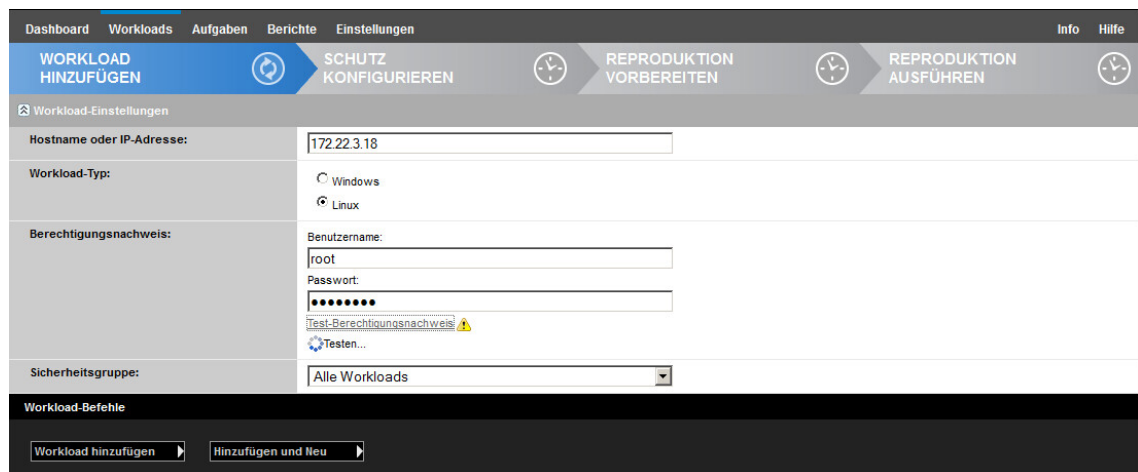
## 5.3 Hinzufügen von Workloads

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 69.
- 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-Berechtigungs-nachweis an.

Verwenden Sie das erforderliche Berechtigungs-nachweisformat (weitere Informationen hierzu finden Sie unter [Abschnitt 6.2, „Richtlinien für Workload- und Container-Berechtigungs-nachweise“](#) auf Seite 88).

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

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 [Abschnitt 5.2, „Hinzufügen von Containern \(Schutzziel\)“](#) auf Seite 71.

6 Fahren Sie mit [Abschnitt 5.4, „Konfigurieren der Schutzdetails und Vorbereiten der Reproduktion“](#) auf Seite 73 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 [Abschnitt 5.1, „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“](#) auf Seite 69) 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 [Abschnitt 5.3, „Hinzufügen von Workloads“](#) auf Seite 72.
- 2 Fügen Sie einen Container hinzu. Weitere Informationen hierzu finden Sie unter [„Hinzufügen von Containern \(Schutzziel\)“](#) auf Seite 71.
- 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 [Abschnitt 6.6, „Anfängliche Reproduktionsmethode \(vollständig und inkrementell\)“](#) auf Seite 92.

- 5 Weisen Sie ein Schutzziel zu. Dies kann entweder ein Container oder ein **vorbereiteter** Workload sein, falls Sie *Inkrementelle Reproduktion* als anfängliche Reproduktionsmethode ausgewählt haben. Weitere Informationen hierzu finden Sie unter „Anfängliche Reproduktionsmethode (vollständig und inkrementell)“ auf Seite 92.

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

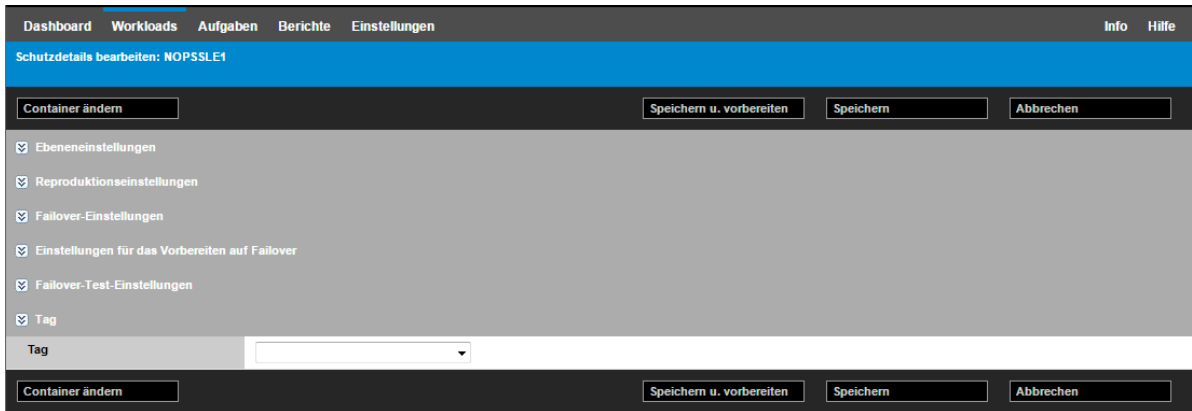
- 6 Konfigurieren Sie die Schutzdetails in jeder Einstellungsgruppe so, wie sie für die Aufrechterhaltung Ihres ununterbrochenen Geschäftsbetriebs erforderlich sind. Weitere Informationen hierzu finden Sie unter „Workload-Schutz-Details“ auf Seite 74.
- 7 Korrigieren Sie alle Validierungsfehler, die eventuell auf der PlateSpin Forge-Weboberfläche angezeigt werden.
- 8 Klicken Sie auf **Speichern**.

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

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

## 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

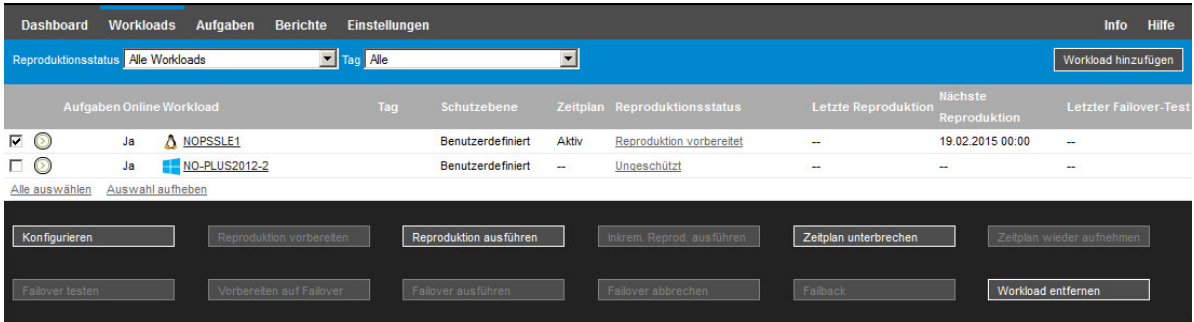
Parametereinstellungen	Details
<b>Ebeneinstellungen</b>	
Schutzebene	Gibt die Schutzebene des aktuellen Schutzes an. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 6.4</a> , „Schutzebenen“ auf Seite 90.
<b>Reproduktionseinstellungen</b>	

Parametereinstellungen	Details
Übertragungsmethode	(Windows) Wählen Sie eine Datenübertragungsmethode und Sicherheit durch Verschlüsselung aus. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 6.3, „Datenübertragung“</a> auf Seite 88.
Übertragungsverschlüsselung	(Windows) Wählen Sie zum Aktivieren der Verschlüsselung die Option <b>Datenübertragung verschlüsseln</b> . Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 1.3, „Sicherheit und Datenschutz“</a> auf Seite 19.
Ursprungsberechtigungs nachweis	Geben Sie den erforderlichen Berechtigungs nachweis für den Zugriff auf den Workload an. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 6.2, „Richtlinien für Workload- und Container-Berechtigungs nachweise“</a> auf Seite 88.
Anzahl der CPUs	Geben Sie die erforderliche Anzahl der vCPUs an, die dem Failover-Workload zugewiesen wurden (gilt nur dann, wenn Sie <b>Vollständig</b> als Methode der ursprünglichen Reproduktion ausgewählt haben).
Reproduktionsnetzwerk	<p>Hiermit wird der Reproduktionsdatenverkehr auf der Basis virtueller Netzwerke getrennt, die auf Ihrem Appliance-Host definiert sind. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 6.10, „Netzwerke“</a> auf Seite 96.</p> <p>Für diese Einstellung können Sie außerdem einen MTU-Wert festlegen, der vom LRD-Reproduktionsnetzwerk (Linux RAM Disk) in PlateSpin Protect verwendet werden soll. Dieser Wert kann dazu beitragen, übermäßigen Datenverkehr über Netzwerke (z. B. VPNs) mit kleinerem MTU-Wert zu vermeiden. Der Standardwert ist eine leere Zeichenkette (kein Eintrag im Textfeld). Wenn Networking im LRD konfiguriert ist, kann das Netzwerkgerät einen eigenen Standardwert festlegen (in der Regel 1500). Wenn Sie einen Wert eingeben, passt PlateSpin Forge den MTU-Wert beim Konfigurieren der Netzwerkschnittstelle entsprechend an.</p>
Zulässige Netzwerke	Geben Sie mindestens eine Netzwerkschnittstelle (NIC oder IP-Adresse) am Ursprung für den Reproduktionsdatenverkehr an.
Ressourcenpool für Ziel-VM	(VM-Container gehört zu einem DRS-Cluster) Geben Sie den Speicherort des Ressourcenpools an, in dem die Failover-VM erstellt werden soll.
VM-Ordner für Ziel-VM	(VM-Container gehört zu einem DRS-Cluster) Geben Sie den Speicherort des VM-Ordners an, in dem die Failover-VM erstellt werden soll.
Konfigurationsdatei-Datenbank	Wählen Sie eine mit dem Appliance-Host verbundene Datenablage zum Speichern von VM-Konfigurationsdateien aus. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 6.5, „Wiederherstellungspunkte“</a> auf Seite 92.
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.

<b>Parametereinstellungen</b>	<b>Details</b>
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 <a href="#">Geschützte logische Volumes</a> 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 <a href="#">Abschnitt 6.7, „Steuerung von Diensten und Daemons“</a> auf Seite 93.
<b>Failover-Einstellungen</b>	
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 <a href="#">Abschnitt 6.10, „Netzwerke“</a> auf Seite 96.
Zu ändernde Dienst-/Daemon-Status	Legen Sie den Anfangsstatus für bestimmte Anwendungsdienste (Windows) oder Daemons (Linux) fest. <a href="#">Abschnitt 6.7, „Steuerung von Diensten und Daemons“</a> auf Seite 93
<b>Einstellungen für das Vorbereiten auf Failover</b>	
Netzwerkverbindungen	Legen Sie die temporären LAN-Einstellungen für den Failover-Workload während der optionalen Vorbereitung auf den Failover fest. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 6.10, „Netzwerke“</a> auf Seite 96.
<b>Testen der Failover-Einstellungen</b>	
VM-Arbeitsspeicher	Weisen Sie dem temporären Workload den erforderlichen RAM zu.
Hostname	Weisen Sie dem temporären Workload einen Hostnamen zu.
Domäne/Arbeitsgruppe	Ordnen Sie den temporären Workload einer Domäne oder Arbeitsgruppe zu. Für die Domänenzugehörigkeit ist der Berechtigungsnachweis eines Domänenadministrators erforderlich.
Netzwerkverbindungen	Legen Sie die LAN-Einstellungen für den temporären Workload fest. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 6.10, „Netzwerke“</a> auf Seite 96.
Zu ändernde Dienst-/Daemon-Status	Legen Sie den Anfangsstatus für bestimmte Anwendungsdienste (Windows) oder Daemons (Linux) fest. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 6.7, „Steuerung von Diensten und Daemons“</a> auf Seite 93.

## 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, der den Befehl bezeichnet, der gerade auf diesem Workload ausgeführt wird.

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 78](#)
- ♦ [Abschnitt 5.7.2, „Durchführen eines Failovers“ auf Seite 79](#)
- ♦ [Abschnitt 5.7.3, „Verwenden der Funktion „Failover testen““ auf Seite 79](#)

### 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 derer ein Workload-Fehler definiert und protokolliert wird, sind Teil der Ebeneneinstellungen eines Workload-Schutzes. Siehe „[Ebeneneinstellungen](#)“ in [Abschnitt 5.4.1, „Workload-Schutz-Details“ auf Seite 74](#).

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 [Abschnitt 2.4.1, „Einrichten automatischer Email-Benachrichtigungen zu Ereignissen und Berichten“ auf Seite 35](#).

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 [Abschnitt 5.6, „Abbrechen von Befehlen“ auf Seite 77](#)) und fahren Sie dann mit dem Befehl **Failover ausführen** fort. Weitere Informationen hierzu finden Sie unter [Abschnitt 5.7.2, „Durchführen eines Failovers“ auf Seite 79](#).

[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 [Abschnitt 5.4.1](#), „Workload-Schutz-Details“ auf Seite 74.

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 [Abschnitt 6.5](#), „Wiederherstellungspunkte“ auf Seite 92). 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 [Abschnitt 5.7.3](#), „Verwenden der Funktion „Failover testen““ auf Seite 79.

## 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.

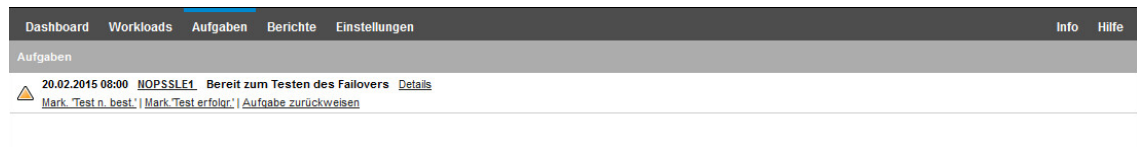
Wenn Sie diesen Befehl ausführen, wendet PlateSpin Forge die Failover-Test-Einstellungen, die in den Workload-Schutz-Details gespeichert sind, auf den Failover-Workload an. Siehe „Failover-Einstellungen“ in [Abschnitt 5.4.1](#), „Workload-Schutz-Details“ auf Seite 74.

**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 [Abschnitt 6.5](#), „Wiederherstellungspunkte“ auf Seite 92) 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 [Abschnitt 3.4.1](#), „Herunterladen des vSphere-Clientprogramms“ auf Seite 53.
- 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.

Unterstützte Failback-Methoden hängen vom Typ der Zielinfrastruktur und dem Grad der Automatisierung des Failback-Vorgangs ab:

- ♦ **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 80
- ♦ [Abschnitt 5.8.2](#), „Halbautomatischer Failback auf einen physischen Computer“ auf Seite 83
- ♦ [Abschnitt 5.8.3](#), „Halbautomatischer Failback auf eine virtuelle Maschine“ auf Seite 84

### 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 [Abschnitt 1.2.3](#), „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 [Abschnitt 6.2, „Richtlinien für Workload- und Container-Berechtigungsnachweise“](#) auf Seite 88).
- ♦ **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 [Abschnitt 6.6, „Anfängliche Reproduktionsmethode \(vollständig und inkrementell\)“](#) auf Seite 92.
  - ♦ **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 82.

- 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

**1. Reproduktion wird durchgeführt**

Status: Läuft

Dauer: 10Min. 20Sek

Schritt: Daten kopieren (84 %)

Kontrolle über den Ziellocomputer abgeben (58 %)

Letzte Vollreproduktion: --

Letzte inkrementelle Reproduktion: --

Letzter Failover-Test: --

Zeitplan: Aktiv

Reproduktionsverlauf: --

Aufgaben: --

**Befehlszusammenfassung**

Status: Läuft

Startzeit: 19.02.2015 09:26

Dauer: 10Min. 20Sek.

Schritt	Status	Startzeit	Endzeit	Dauer	Diagnose
Ursprungscomputer aktualisieren	Abgeschlossen	19.02.2015 09:26	19.02.2015 09:27	54Sek.	--
Daten kopieren	Läuft (84 %)	19.02.2015 09:27	--	9Min. 26Sek.	--

Diagnose: [Generieren](#)

**Reproduktion - Übertragungsübersicht**

Durchschnittliche Übertragungsgeschwindigkeit: 285,26 Mb/s

Dauer: 2Min. 22Sek.

Übertragene Daten: 4,7 GB

**Workload-Befehle**

## 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
<b>Failback Einstellungen</b>	
Übertragungsmethode	Wählen Sie eine Datenübertragungsmethode und Sicherheit durch Verschlüsselung aus. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 6.3, „Datenübertragung“</a> auf Seite 88.
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 <a href="#">Abschnitt 6.10, „Netzwerke“</a> auf Seite 96.
VM-Datenablage	Wählen Sie eine Datenablage aus, die dem Failback-Container für den Ziel-Workload zugeordnet ist.
Volume-Zuordnung	Wenn Sie als anfängliche Reproduktionsmethode die Option „Inkrementell“ ausgewählt haben, wählen Sie hier die Ursprungs-Volumes aus, und ordnen Sie sie dem Failback-Ziel zur Synchronisierung zu.
Anzuhaltende Dienste/Daemons	Geben Sie die Anwendungsdienste (Windows) oder Daemons (Linux) an, die beim Failback automatisch angehalten werden sollen. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 6.7, „Steuerung von Diensten und Daemons“</a> auf Seite 93.

Parametereinstellungen	Details
Alternative Adresse für Ursprung	Geben Sie ggf. eine zusätzliche IP-Adresse für den virtuellen Failover-Computer ein. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 2.3.4, „Schutz über öffentliche und private Netzwerke durch NAT“</a> auf Seite 33.
<b>Workload-Einstellungen</b>	
Anzahl der CPUs	Geben Sie die erforderliche Anzahl der dem Ziel-Workload zugewiesenen vCPUs an.
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 <a href="#">Abschnitt 6.7, „Steuerung von Diensten und Daemons“</a> auf Seite 93.
<b>Post-Failback-Zieleinstellungen</b>	
Workload erneut schützen	Wählen Sie diese Option, wenn Sie planen, den Schutzvertrag für den Ziel-Workload nach der Bereitstellung neu zu erstellen. Mit dieser Option kann der Ereignisverlauf für den Workload kontinuierlich geführt und eine Workload-Lizenz automatisch zugewiesen/festgelegt werden.
Erneut schützen nach Failback	Wählen Sie diese Option, wenn Sie planen, den Schutzvertrag für den Ziel-Workload neu zu erstellen. Wenn der Failback abgeschlossen ist, steht für den Failback-Workload der Befehl <b>Erneut schützen</b> 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.

**So führen Sie einen Failback für einen Workload auf einem physischen Computer aus:**

- 1 Registrieren Sie den erforderlichen physischen Computer bei Ihrem PlateSpin-Server. Weitere Informationen hierzu finden Sie unter [Abschnitt 6.11, „Failback auf physische Computer“](#) auf Seite 96.
- 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 [Abschnitt 7.1, „Verwalten der Gerätetreiber“](#) auf Seite 105.

- 3 Wählen Sie im Anschluss an einen Failover den Workload auf der Seite „Workloads“ aus und klicken Sie auf **Failback durchführen**.
- 4 Legen Sie die folgenden Parametergruppen fest:
  - ♦ **Workload-Einstellungen:** Geben Sie den Hostnamen oder die IP-Adresse Ihres Failover-Workloads und den Berechtigungsnachweis eines Administrators an. Verwenden Sie das erforderliche Berechtigungsnachweisformat (weitere Informationen hierzu finden Sie unter [Abschnitt 6.2, „Richtlinien für Workload- und Container-Berechtigungsnachweise“](#) auf Seite 88).
  - ♦ **Failback-Zieleinstellungen:** Geben Sie die folgenden Parameter an:
    - ♦ **Reproduktionsmethode:** Wählen Sie den Umfang der Datenreproduktion aus. Weitere Informationen hierzu finden Sie unter [Abschnitt 6.6, „Anfängliche Reproduktionsmethode \(vollständig und inkrementell\)“](#) auf Seite 92.
    - ♦ **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**, dem logischen nächsten Schritt nach einem **Failback** wird der Workload-Schutz-Lebenszyklus abgeschlossen und neu gestartet. Nach einem erfolgreichen Failback-Vorgang wird ein Befehl **Erneut schützen** auf der PlateSpin 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 [Abschnitt 5.8, „Failback“](#) auf Seite 80.

---

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.

- ♦ [Abschnitt 6.1, „Workload-Lizenzverbrauch“ auf Seite 87](#)
- ♦ [Abschnitt 6.2, „Richtlinien für Workload- und Container-Berechtigungs-nachweise“ auf Seite 88](#)
- ♦ [Abschnitt 6.3, „Datenübertragung“ auf Seite 88](#)
- ♦ [Abschnitt 6.4, „Schutzebenen“ auf Seite 90](#)
- ♦ [Abschnitt 6.5, „Wiederherstellungspunkte“ auf Seite 92](#)
- ♦ [Abschnitt 6.6, „Anfängliche Reproduktionsmethode \(vollständig und inkrementell\)“ auf Seite 92](#)
- ♦ [Abschnitt 6.7, „Steuerung von Diensten und Daemons“ auf Seite 93](#)
- ♦ [Abschnitt 6.8, „Verwenden von Freeze- und Thaw-Skripts für alle Reproduktionen \(Linux\)“ auf Seite 94](#)
- ♦ [Abschnitt 6.9, „Volumes“ auf Seite 95](#)
- ♦ [Abschnitt 6.10, „Netzwerke“ auf Seite 96](#)
- ♦ [Abschnitt 6.11, „Failback auf physische Computer“ auf Seite 96](#)
- ♦ [Abschnitt 6.12, „Themen zu erweitertem Workload-Schutz“ auf Seite 99](#)

## 6.1 Workload-Lizenzverbrauch

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

Informationen über die Produktlizenzierung und die Lizenzaktivierung finden Sie unter [Abschnitt 2.1, „Produktlizenzierung“ auf Seite 25](#).

## 6.2 Richtlinien für Workload- und Container-Berechtigungsachweise

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, Berechtigungsachweise in einem bestimmten Format einzugeben.

**Tabelle 6-1** Workload-Berechtigungsachweise

Ermitteln	Berechtigungsachweis	Anmerkungen
Alle Windows-Workloads	Berechtigungsachweise eines lokalen oder Domänen-Administrators.	Verwenden Sie für den Benutzernamen das folgende Format: <ul style="list-style-type: none"><li>◆ Bei Domänenmitgliedscomputern: <i>Autorität\Prinzipal</i></li><li>◆ Bei Arbeitsgruppenmitgliedscomputern: <i>Hostname\Prinzipal</i></li></ul>
Windows-Cluster	Berechtigungsachweis eines Domänen-Administrators.	
Alle Linux-Workloads	Root-äquivalenter Benutzername und Passwort	Andere Konten als das Root-Konto müssen für die Verwendung von <code>sudo</code> konfiguriert werden. Weitere Informationen hierzu finden Sie im <a href="#">Knowledgebase-Artikel 7920711</a> .
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 Berechtigungsachweis 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.

- ◆ [Abschnitt 6.3.1, „Übertragungsmethoden“ auf Seite 89](#)
- ◆ [Abschnitt 6.3.2, „Datenverschlüsselung“ auf Seite 90](#)



## 6.3.1 Übertragungsmethoden

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

- ♦ „Unterstützte Übertragungsmethoden für Windows-Workloads“ auf Seite 89
- ♦ „Unterstützte Übertragungsmethoden für Linux-Workloads“ auf Seite 90

### 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 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.

Wenn Windows-Cluster mit einer Datenübertragung auf Blockebene geschützt werden sollen, ist kein Neustart erforderlich.

- ♦ **Reproduktion mit der blockbasierten Komponente:** Diese Option verwendet eine blockbasierte Komponente und nutzt den Microsoft Volume Snapshot Service (VSS) mit Anwendungen und Diensten, die VSS unterstützen. 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.

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

- Windows-Reproduktion auf Dateiebene:** Die Daten werden dateiweise reproduziert (nur Windows).

## 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](#).

Die im Lieferumfang von PlateSpin Forge enthaltene blockbasierte Linux-Komponente ist für Standard- und Nicht-Debug-Kernels der unterstützten 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](#).

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

### 6.3.2 Datenverschlüsselung

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

---

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

---

## 6.4 Schutzebenen

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

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

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

**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 <b>Beginn der Wiederholung</b> eingeben oder auf das Kalendersymbol klicken, um ein Datum auszuwählen. Wählen Sie <b>Keine</b> 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	<p>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).</p> <p>Klicken Sie zum Festlegen einer Sperrzeit auf <b>Bearbeiten</b> und wählen Sie ein Wiederholungsmuster (Täglich, Wöchentlich etc.) sowie die Anfangs- und Endzeit der Sperrzeit.</p> <p><b>HINWEIS:</b> Die Anfangs- und Endzeiten für die Sperrzeit hängen von der Systemuhr an Ihrem PlateSpin-Server ab.</p>
Komprimierungsgrad	<p>Diese Einstellungen legen fest, ob und wie Workload-Daten vor der Übertragung komprimiert werden. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 1.4.2, „Datenkomprimierung“</a> auf Seite 22.</p> <p>Wählen Sie eine der verfügbaren Optionen aus. <b>Schnell</b> verbraucht die wenigsten CPU-Ressourcen auf dem Ursprung, geht jedoch mit einer geringeren Komprimierung einher. <b>Maximal</b> verbraucht die meisten Ressourcen, erzielt aber auch eine höhere Komprimierung. <b>Optimal</b> liegt dazwischen und ist die empfohlene Option.</p>
Bandbreitendrosselung	<p>Diese Einstellungen steuern die Bandbreitendrosselung. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 1.4.3, „Bandbreitendrosselung“</a> auf Seite 22.</p> <p>Um die Bandbreite bei Reproduktionen auf eine bestimmte Rate zu drosseln, geben Sie den erforderlichen Durchsatzwert in Mb/s sowie das Zeitmuster ein.</p>
Beizubehaltende Wiederherstellungspunkte	Geben Sie die Anzahl der beizubehaltenden Wiederherstellungspunkte für Workloads an, die diese Schutzebene verwenden. Weitere Informationen hierzu finden Sie unter <a href="#">Abschnitt 6.5, „Wiederherstellungspunkte“</a> auf Seite 92.
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 [Abschnitt 3.4.4, „Verwalten von Forge-Snapshots auf dem Appliance-Host“](#) auf Seite 54.

## 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 [Abschnitt 3.4.5, „Manuelles Importieren von VMs in die Datenablage des Appliance-Hosts“](#) auf Seite 55.
  - ♦ **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 [Abschnitt 5.8.2, „Halbautomatischer Failback auf einen physischen Computer“](#) auf Seite 83).

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.

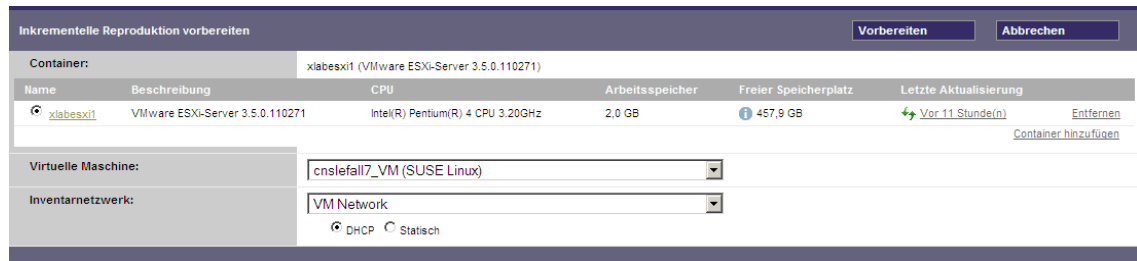
**So richten Sie eine anfängliche Reproduktionsmethode ein:**

- 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 [Abschnitt 6.8, „Verwenden von Freeze- und Thaw-Skripts für alle Reproduktionen \(Linux\)“](#) auf Seite 94.

- ♦ **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 93). 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

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, über die Sie die für den Schutz benötigten Volumes angeben können.

PlateSpin Forge unterstützt mehrere Speichertypen, darunter 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 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.

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

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

Dashboard Workloads Aufgaben Berichte Einstellungen Info Hilfe

Schutzdetails bearbeiten: NOPSSLE1

Container ändern Speichern u. vorbereiten Speichern Abbrechen

☑ Ebeneinstellungen

☑ Reproduktionseinstellungen

Übertragungsverschlüsselung:  Datenübertragung verschlüsseln

Ursprungsberechtigungsachweis: Benutzername: root  
Passwort: .....  
Test-Berechtigungsachweis ⚠

Anzahl der CPUs: 1

Reproduktionsnetzwerk:   DHCP  Statisch MTU:

Zulässige Netzwerke:

Zulassen	Name	Adresse	Verwendet DHCP
<input checked="" type="checkbox"/>	eth0	172.22.3.8	True

Datenablage der Konfigurationsdatei: datastore5 (1,5 TB frei)

Geschützte Volumes:

Einbeziehen Name	Belegter Speicherplatz	Freier Speicherplatz	Datenablage	Thin-Festplatte
<input checked="" type="checkbox"/> / (EXT3 - System)	5,3 GB	22,28 GB	datastore5 (1,5 TB fi	<input type="checkbox"/>

Speicher ohne Volumes:

Einbeziehen Partition	Ist Auslagerung	Gesamtgröße	Datenablage	Thin-Festplatte
<input checked="" type="checkbox"/> /dev/sda1	Ja	2,01 GB	datastore5 (1,5 TB fi	<input type="checkbox"/>

Daemons, die während der Reproduktion angehalten werden sollen: [Daemons hinzufügen](#)

☑ Failover-Einstellungen

☑ Einstellungen für das Vorbereiten auf Failover

☑ Failover-Test-Einstellungen

☑ Tag

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

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

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

## 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 97](#)
- [Abschnitt 6.11.2, „Einfügen weiterer Gerätetreiber in das Boot-ISO-Image“ auf Seite 97](#)
- [Abschnitt 6.11.3, „Registrieren von physischen Computern als Failback-Ziele mit PlateSpin Forge“ auf Seite 99](#)



## 6.11.1 Herunterladen des PlateSpin-Boot-ISO-Image

Sie können das PlateSpin-Boot-ISO-Image (`p.iso` für Ziele auf BIOS- bzw. UEFI-Firmware-Basis) im Bereich PlateSpin Forge von [NetIQ Downloads \(https://dl.netiq.com\)](https://dl.netiq.com) herunterladen. Führen Sie dazu eine Suche mit folgenden Parametern aus:

- ♦ **Produkt oder Technologie:** PlateSpin Forge
- ♦ **Version auswählen:** PlateSpin Forge 11.1
- ♦ **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 [Wissensdatenbankartikel 7005990](#).

---

- 2 Mounten Sie das Image in einem Linux-Computer (`root`-Berechtigungsnaechweis 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 `umount <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
<code>-i &lt;ISO-Datei&gt;</code>	<code>&lt;ISO-Datei&gt;</code> ist die ISO zum Bearbeiten, Auflisten etc.
<code>-v</code>	Falls dieser Befehl zusammen mit dem Argument <code>-l</code> verwendet wird, wird mit dieser Option der Befehl „modinfo“ zum Abrufen umfassender Treiberinformationen ausgelöst.
<code>-o</code>	Falls dieser Befehl zusammen mit dem Argument <code>-c</code> oder dem Argument <code>-d</code> verwendet wird, dann wird die alte Kopie der ISO-Datei nicht überschrieben.
<code>-m32</code>	Gibt an, dass die 32-Bit-initrd einbezogen wird.
<code>-m64</code>	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>	<p>&lt;Pfad&gt; gibt das Verzeichnis mit den Treibern an (d. h. *.ko-Dateien), die Sie einbeziehen möchten.</p> <p>Bei Anwendung dieses Befehls wird die ISO-Datei mit den hinzugefügten Treibern aktualisiert.</p>
-c <Pfad>	<p>&lt;Pfad&gt; gibt an, wo sich eine <code>ConfigureTakeControl.xml</code>-Datei befindet.</p>
-l [<Typ>]	<p>&lt;Typ&gt; gibt eine Teilmenge von Treibern an, die Sie auflisten möchten. Standardmäßig ist „alle“ Typen festgelegt.</p> <p>Aufgeführte Treibertypen, die mit einem Schrägstrich (/) beginnen, befinden sich vermutlich unter <code>&lt;Kernel-Modul-Verzeichnis&gt;/Kernel/</code></p> <p>Aufgeführte Treibertypen, die nicht mit einem Schrägstrich (/) beginnen, befinden sich vermutlich unter <code>&lt;Kernel-Modul-Verzeichnis&gt;/Kernel/Treiber/</code></p> <p><b>Beispiele für Treiber-Teilmenge:</b></p> <pre>-l scsi -l 'net video' -l '/net net'</pre> <p><b>Besondere Verwendung dieses Arguments:</b></p> <p>Wenn Sie die verfügbaren Unterverzeichnisse der einzelnen Teilmengen auflisten möchten, verwenden Sie das Argument wie folgt: <code>-l INDEX</code></p>

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

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

## 6.12 Themen zu erweitertem Workload-Schutz

- ♦ [Abschnitt 6.12.1, „Schützen von Windows-Clustern“ auf Seite 99](#)
- ♦ [Abschnitt 6.12.2, „Verwenden von Workload-Schutz-Funktionen über die PlateSpin Forge-Web-Services-API“ auf Seite 102](#)

### 6.12.1 Schützen von Windows-Clustern

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

- ♦ Auf Windows 2009 R2 Server basierender Microsoft-Failover-Cluster (Modelle *Node and Disk Majority Quorum* und *No Majority: Disk Only Quorum*)
- ♦ Auf Windows 2003 R2 Server basierender Windows-Cluster-Server (Modell *Single-Quorum Device Cluster*)

---

**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 -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 -Failback bezeichnet.

---

Dieser Abschnitt enthält folgende Informationen:

- ♦ „Workload-Schutz“ auf Seite 100
  - ♦ „PlateSpin-Failover“ auf Seite 101
  - ♦ „PlateSpin-Failback“ auf Seite 102
- 

**HINWEIS:** Weitere Informationen zum Neuaufbauen der Windows 2008R2-Failover-Cluster-Umgebung nach einem PlateSpin-Failover/-Failback finden Sie im [Wissensdatenbankartikel 7015576](#).

---

## Workload-Schutz

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.

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

- ♦ Geben Sie beim Vorgang **Workload hinzufügen** die virtuelle IP-Adresse des Clusters an, nicht die IP-Adresse eines Knotens im Cluster. Die virtuelle IP-Adresse eines Clusters steht stellvertretend für den Knoten, der jeweils als Eigentümer der Quorum-Ressource des Clusters fungiert. Wenn Sie die IP-Adresse eines einzelnen Knotens angeben, wird dieser Knoten als regulärer Windows-Workload inventarisiert (der Cluster bleibt unerkannt).
- ♦ Eine Quorum-Ressource eines Clusters muss zu der Ressourcengruppe (Dienst) des Clusters gehören, die geschützt wird.

Bei einer blockbasierten Übertragung 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.

---

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 der Clusterknoten werden als ähnlich erachtet, wenn:

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

- ♦ Seriennummern für lokale Volumes (System-Volume und Reserviertes System-Volume) müssen auf allen Clusterknoten gleich sein.

Wenn die lokalen Treiber auf allen Knoten des Clusters verschiedene Seriennummern aufweisen, können Sie nach einem Clusterknoten-Failover keine inkrementelle 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 inkrementelle Reproduktion des Workloads nicht ausgeführt.

In diesem Szenario stehen zwei unterstützte Optionen für Windows-Clustern zur Auswahl:

- ♦ (Empfohlen) Verwenden Sie das angepasste Dienstprogramm *Volume Manager*, um die Seriennummern des lokalen Volumes zu ändern, damit sie mit den einzelnen Knoten des Clusters übereinstimmen. Weitere Informationen finden Sie unter [Anhang B](#), „Synchronisieren von Seriennummern im lokalen Clusterknoten-Speicher“, auf Seite 129.
- ♦ (Bedingt und optional) Wenn Sie den folgenden Fehler sehen:

```
Volume mappings does not contain source serial number: xxxx-xxxx,
```

Er wurde möglicherweise durch eine Änderung im aktiven Knoten vor Ausführung der inkrementellen Reproduktion verursacht. In diesem Fall können Sie eine vollständige Reproduktion ausführen, um sicherzustellen, dass der Cluster wieder geschützt ist. Inkrementelle Reproduktionen sollten nach der vollständigen Reproduktion wieder funktionieren.

---

**HINWEIS:** Wenn die Volume-Seriennummern nicht mit den einzelnen Knoten im Cluster übereinstimmen sollen, ist nach einem Clusterknoten-Failover eine vollständige Reproduktion erforderlich.

---

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.

Um ein Windows-Cluster zu schützen, gehen Sie nach dem gleichen Ablaufplan wie für den normalen Workload-Schutz vor (siehe „[Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung](#)“ auf Seite 69).

## 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).

## 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-Volumen 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.

---

**HINWEIS:** Weitere Informationen zum Neuaufbauen der Windows 2008R2-Failover-Cluster-Umgebung nach einem PlateSpin-Failover/-Failback finden Sie im [Wissensdatenbankartikel 7015576](#).

---

Nach Abschluss des PlateSpin-Failbacks können Sie andere Knoten mit dem erneut reproduzierten Cluster zusammenführen.

### 6.12.2 Verwenden von Workload-Schutz-Funktionen über die PlateSpin Forge-Web-Services-API

Mithilfe der `protectionsservices`-API können Sie Workload-Schutz-Funktionen programmatisch von Ihren Anwendungen aus verwenden. Alle Programmier- oder Skriptsprachen, die einen HTTP-Client und das JSON-Serialisierungs-Framework nutzen, sind verwendbar.

```
https://<hostname | IP-Adresse>/protectionsservices
```

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.

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.

#### API-Übersicht

PlateSpin Protect verfügt über eine REST-basierte API-Technologievorschau, die Entwickler bei der Erstellung eigener Anwendungen für das Produkt verwenden können. Die API enthält Informationen über die folgenden Vorgänge:

- ♦ Container ermitteln
- ♦ Workloads ermitteln
- ♦ Schutz konfigurieren
- ♦ Reproduktionen, Failover-Vorgänge und Failback ausführen
- ♦ Workload- und Container-Status abfragen

- ◆ Status laufender Vorgänge abfragen
- ◆ Sicherheitsgruppen und deren Schutzverbindungen

Protect-Administratoren können ein Jscript-Beispiel (<https://localhost/protectionservices/Documentation/Samples/protect.js>) von der Befehlszeile aus verwenden, um über die API auf das Produkt zuzugreifen. 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

Auf der Startseite der PlateSpin Protect REST-API (<https://localhost/protectionservices/> oder <https://<server page>/protectionservices/>) finden Sie Links zu Inhalten, die für Entwickler und Administratoren nützlich sein können.

Diese Technologievorschau wird in späteren Versionen vollständig entwickelt sein und über weitere Funktionen verfügen.





---

# 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.

- ♦ [Abschnitt 7.1, „Verwalten der Gerätetreiber“ auf Seite 105](#)

## 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 (heraufladen).

- ♦ [Abschnitt 7.1.1, „Verpacken von Gerätetreibern für Windows-Systeme“ auf Seite 105](#)
- ♦ [Abschnitt 7.1.2, „Verpacken von Gerätetreibern für Linux-Systeme“ auf Seite 106](#)
- ♦ [Abschnitt 7.1.3, „Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin Forge“ auf Seite 106](#)
- ♦ [Abschnitt 7.1.4, „Verwenden der Funktion für die Plug-&-Play\(PnP\)-ID-Übersetzung“ auf Seite 108](#)

### 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 [Abschnitt 7.1.3, „Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin Forge“ auf Seite 106](#).

---

**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 einem Ihrer PlateSpin-ISO-Boot-Images 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 entsprechende 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 [Abschnitt 7.1.3, „Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin Forge“](#) auf Seite 106.

## 7.1.3 Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin Forge

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.

---

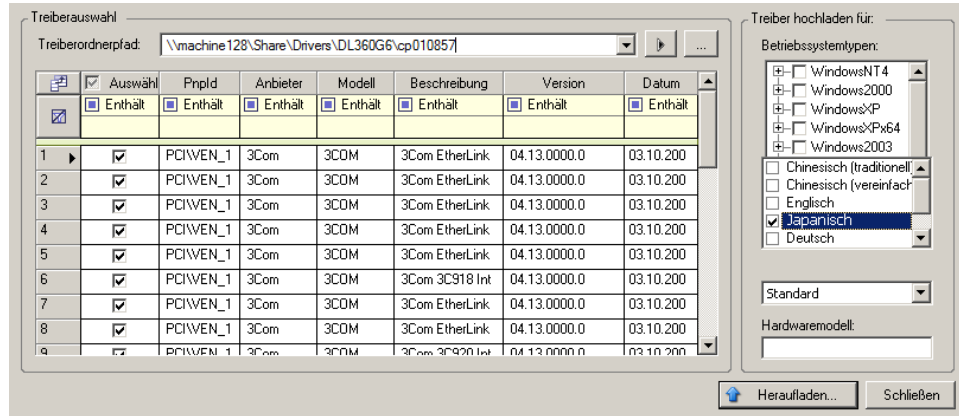
- ♦ „Upload-Prozedur für Gerätetreiber (Windows)“ auf Seite 106
- ♦ „Upload-Prozedur für Gerätetreiber (Linux)“ auf Seite 107

### Upload-Prozedur für Gerätetreiber (Windows)

So laden Sie einen Windows-Gerätetreiber herauf:

- 1 Beziehen Sie die erforderlichen Gerätetreiber und bereiten Sie diese vor. Weitere Informationen hierzu finden Sie unter [Abschnitt 7.1.1, „Verpacken von Gerätetreibern für Windows-Systeme“](#) auf Seite 105.

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



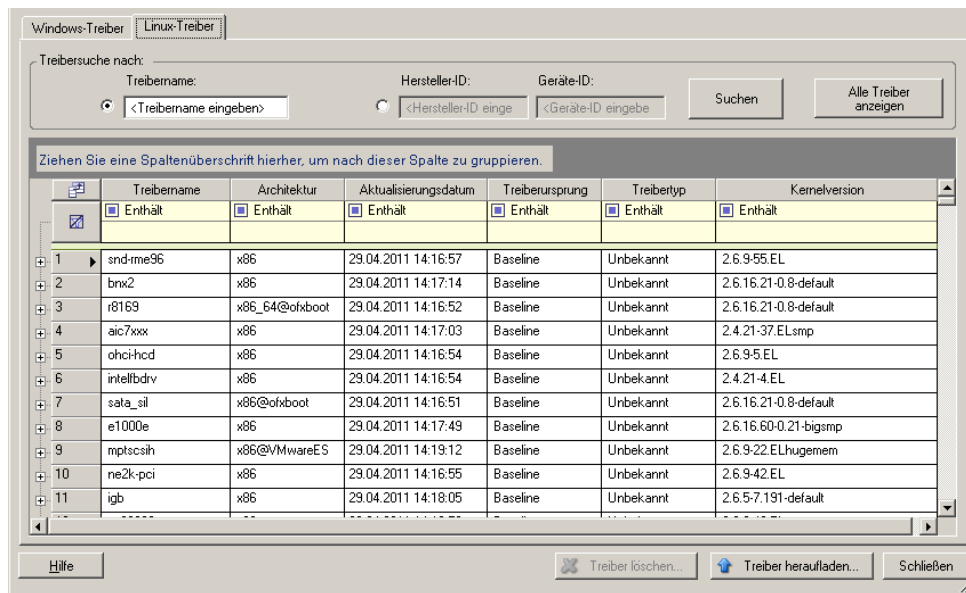
Wählen Sie **Standard** als Option für **Hardwarehersteller** aus, es sei denn, Ihre Treiber sind speziell für eine der aufgeführten Zielumgebungen vorgesehen.

- 4 Klicken Sie auf **Heraufladen...** und bestätigen Sie Ihre Auswahl.  
Das System lädt die ausgewählten Treiber in die Treiberdatenbank.

## Upload-Prozedur für Gerätetreiber (Linux)

So laden Sie einen Linux-Gerätetreiber herauf:

- 1 Beziehen Sie die erforderlichen Gerätetreiber und bereiten Sie diese vor. Weitere Informationen hierzu finden Sie unter [Abschnitt 7.1.2, „Verpacken von Gerätetreibern für Linux-Systeme“](#) auf [Seite 106](#).
- 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 Protect-Linux-RAM-Datenträger erkannt wird, PnP-IDs im Linux-Format.

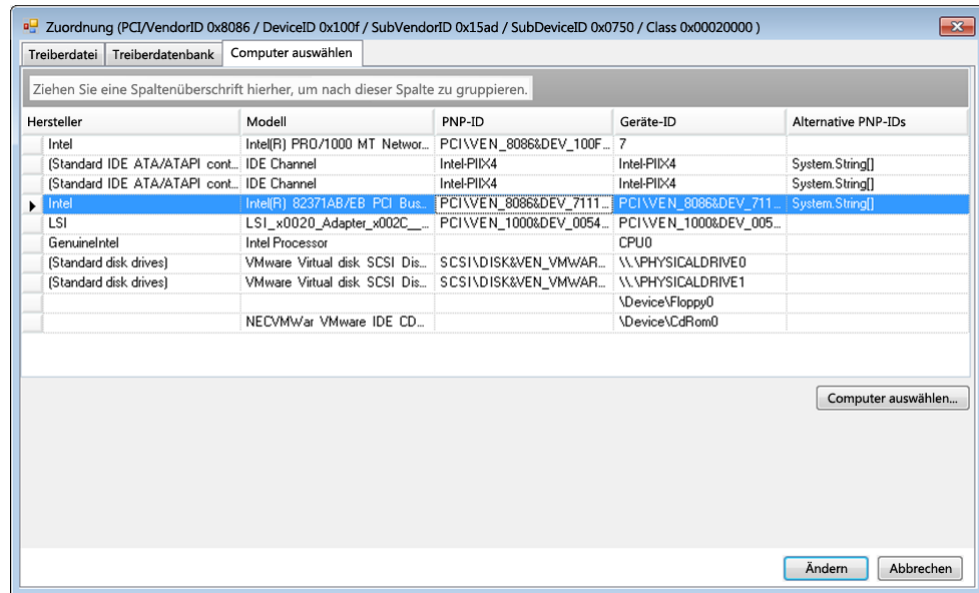
Diese IDs sind einheitlich formatiert, so dass PlateSpin die zugehörige Windows-PnP-ID anhand der Standardumwandlung feststellen kann. Die Übersetzung erfolgt automatisch im PlateSpin-Produkt. Mit dieser Funktion sind Sie oder ein Kundendiensttechniker in der Lage, benutzerdefinierte PnP-Zuordnungen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

### So verwenden Sie die Funktion „PnP-ID-Übersetzung“:

- 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 109](#), 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
<b>Optionen</b>	
<code>h   ?   help</code>	Zeigt die Nutzung und die Optionen für den Befehl.
<code>logs   view-logs</code>	Öffnet das Anwendungsprotokollverzeichnis.
<code>status</code>	Zeigt den Installationsstatus für den Controller und die Treiber in PlateSpin.
<code>din   driver-install</code>	Installiert die PlateSpin-Treiber.
<code>dup   driver-upgrade</code>	Rüstet die PlateSpin-Treiber auf.
<code>dun   driver-uninstall</code>	Deinstalliert die PlateSpin-Treiber.
<b>Switch</b>	
<code>/psserver=%IP%</code>	Lädt die Treiber für die blockbasierte Übertragung vom angegebenen Server herunter, sobald Sie die Option <code>status</code> , <code>driver-install</code> oder <code>driver-upgrade</code> 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

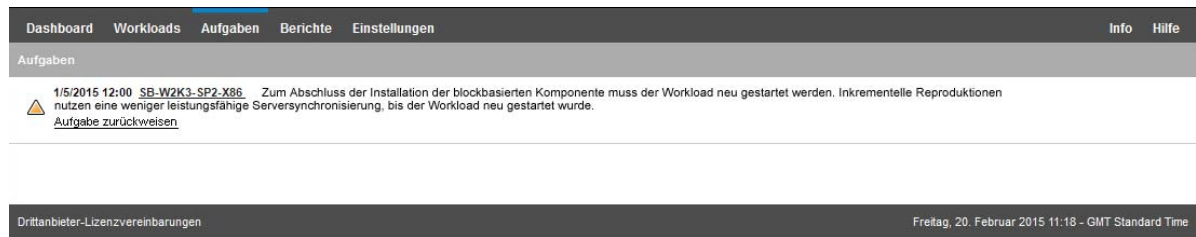




Abbildung 8-2 Neustart-Benachrichtigung während der Reproduktion

The screenshot shows the 'Befehlsdetails' (Command Details) page for a workload named 'NOPSSLE1'. The main heading is '1. Reproduktion wird durchgeführt' (1. Reproduction is being performed). The status is 'Läuft' (Running) with a refresh icon. The duration is '10Min. 20Sek.' and the current step is 'Daten kopieren (84%)' (Copying data (84%)). A progress bar is shown at 84%. Below this, there is a sub-section 'Kontrolle über den Ziellocomputer abgeben (58%)' (Handing over control to the target computer (58%)).

The 'Befehlszusammenfassung' (Command Summary) section provides a description: 'Zum Abschluss der Installation der blockbasierten Komponente muss der VWorkload neu gestartet werden. Inkrementelle Reproduktionen nutzen eine weniger leistungsfähige Serversynchronisierung, bis der Workload neu gestartet wurde.' (To complete the installation of the block-based component, the VWorkload must be restarted. Incremental reproductions use a less powerful server synchronization until the workload is restarted.)

The 'Reproduktion - Übertragungsübersicht' (Reproduction - Transfer Overview) section shows:
 

- Durchschnittliche Übertragungsgeschwindigkeit: 285,26 Mb/s
- Dauer: 2Min. 22Sek.
- Übertragene Daten: 4,7 GB

The 'Workload-Befehle' (Workload Commands) section contains three buttons: 'Abbrechen' (Cancel), 'Konfigurieren' (Configure), and 'Zeitplan unterbrechen' (Interrupt schedule).

At the bottom, there is a footer with 'Drittanbieter-Lizenzvereinbarungen' (Third-party license agreements) on the left and 'Donnerstag, 19. Februar 2015 09:36 - GMT Standard Time' on the right.

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

NO-PLUS2012-2

### Inkrem. Reproduktion läuft

Status: Läuft  
 Dauer: 7Min. 57Sek.  
 Schritt: Daten kopieren (27 %)  
Kopieren der Volume-Daten vom Ursprung zum Ziel (32 %)

Letzte Vollreproduktion: 20.02.2015 10:44  
 Letzte inkrementelle Reproduktion: --  
 Letzter Failover-Test: --  
 Zeitplan: --  
 Reproduktionsverlauf: [Aktiv](#)  
 Aufgaben: [Anzeigen](#)

**Befehlszusammenfassung**

Ereignisse:	Ereignis	Details	Benutzer	Datum
	Inkrementelle Reproduktion gestartet		NORB-US-W2K8RZ\Administrator	20.02.2015 10:47

Status:	Läuft <span style="color: #00aaff;">↻</span>
	<span style="color: #ff0000;">⚠</span> Die blockbasierte Komponente hat den Installationsprozess kürzlich abgeschlossen. Diese Reproduktion erfordert die Durchführung einer Serversynchronisierung.

Startzeit:	20.02.2015 10:47
Dauer:	7Min. 57Sek.

Schritte:	Schritt	Status	Startzeit	Endzeit	Dauer	Diagnose
	Ursprungscomputer aktualisieren	Abgeschlossen	20.02.2015 10:47	20.02.2015 10:48	52Sek.	--
	Auf Snapshot zurücksetzen	Abgeschlossen	20.02.2015 10:48	20.02.2015 10:48	35Sek.	--
	<span style="color: #00aaff;">i</span> Daten kopieren	Läuft (27 %) <span style="color: #00aaff;">↻</span>	20.02.2015 10:48	--	6Min. 30Sek.	--

Diagnose: [Generieren](#)

**Reproduktion - Übertragungsübersicht**

Durchschnittliche Übertragungsgeschwindigkeit:	87,08 Mb/s
Dauer:	57Sek.
Übertragene Daten:	488,8 MB
Übertragene Dateien:	2.266

**Workload-Befehle**

Abbrechen
Konfigurieren
Zeitplan unterbrechen

Drittanbieter-Lizenzvereinbarungen

Freitag, 20. Februar 2015 10:55 - GMT Standard Time

---

# 9 Fehlersuche

Dieser Abschnitt enthält folgende Informationen:

- ♦ [Abschnitt 9.1, „Fehlerbehebung bei der Workload-Inventarisierung \(Windows\)“ auf Seite 115](#)
- ♦ [Abschnitt 9.2, „Fehlerbehebung bei der Workload-Inventarisierung \(Linux\)“ auf Seite 119](#)
- ♦ [Abschnitt 9.3, „Beheben von Problemen während der Ausführung des Befehls „Reproduktion vorbereiten“ \(Windows\)“ auf Seite 120](#)
- ♦ [Abschnitt 9.4, „Fehlerbehebung bei der Workload-Reproduktion“ auf Seite 120](#)
- ♦ [Abschnitt 9.5, „Fehlersuche bei Workloads, die Datenverkehr weiterleiten“ auf Seite 122](#)
- ♦ [Abschnitt 9.6, „Fehlersuche bei der Online-Hilfe“ auf Seite 123](#)
- ♦ [Abschnitt 9.7, „Generieren und Anzeigen von Diagnoseberichten“ auf Seite 123](#)
- ♦ [Abschnitt 9.8, „Entfernen von Workloads“ auf Seite 123](#)
- ♦ [Abschnitt 9.9, „Workload-Bereinigung nach dem Schutz“ auf Seite 124](#)
- ♦ [Abschnitt 9.10, „Verkleinern der PlateSpin Forge-Datenbanken“ auf Seite 126](#)

## 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.	<p>Dieser Fehler tritt auf, wenn das Format des Berechtigungsnachweises falsch ist.</p> <p>Versuchen Sie, die Ermittlung unter Verwendung eines lokalen Administratorkontos mit dem Berechtigungsnachweisformat <code>Hostname\LocalAdmin</code> durchzuführen.</p> <p>Sie können auch versuchen, die Ermittlung unter Verwendung eines Domänen-Administratorkontos mit dem Berechtigungsnachweisformat <code>Domäne\DomainAdmin</code> durchzuführen.</p>
Es konnte keine Verbindung zum Windows-Server hergestellt werden. Zugriff verweigert.	<p>Beim Versuch, einen Workload hinzuzufügen, wurde ein Nicht-Administratorkonto verwendet. Verwenden Sie ein Administratorkonto oder fügen Sie den Benutzer zur Administratorgruppe hinzu und versuchen Sie es erneut.</p> <p>Diese Meldung kann auch auf einen WMI-Verbindungsfehler hinweisen. Probieren Sie die nachfolgend aufgeführten Lösungsmöglichkeiten aus und führen Sie dann den <a href="#">„WMI-Verbindungstest“ auf Seite 117</a> erneut durch. Wenn der Test erfolgreich ist, versuchen Sie erneut, den Workload hinzuzufügen.</p> <ul style="list-style-type: none"><li>♦ <a href="#">„Fehlerbehebung bei DCOM-Verbindungen“ auf Seite 117</a></li><li>♦ <a href="#">„Fehlerbehebung bei der RPC-Dienst-Verbindung“ auf Seite 118</a></li></ul>

---

Probleme oder Meldungen	Lösungen
Es konnte keine Verbindung zum Windows-Server hergestellt werden. Netzwerkpfad nicht gefunden.	Netzwerk-Verbindungsfehler. Führen Sie die Tests in „ <a href="#">Durchführen von Verbindungstests</a> “ auf Seite 116 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: <ul style="list-style-type: none"> <li>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 <a href="#">Wissensdatenbankartikel 7920339</a>.</li> <li>Wenn lokale Richtlinien oder Domänenrichtlinien die erforderlichen Berechtigungen einschränken, führen Sie die im <a href="#">Wissensdatenbankartikel 7920862</a> beschriebenen Schritte aus.</li> </ul>
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: <ul style="list-style-type: none"> <li>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 „<a href="#">Deaktivieren der Virenschutz-Software</a>“ auf Seite 118.</li> <li>Die Datei- und Drucker-Freigabe für Microsoft-Netzwerke ist möglicherweise nicht aktiviert. Aktivieren Sie die Freigabe in den Eigenschaften der Netzwerkschnittstellenkarte.</li> <li>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 „<a href="#">Aktivieren von Datei-/Freigabe-Berechtigungen und -Zugriff</a>“ auf Seite 118.</li> <li>Der Server- oder der Arbeitsstationsdienst läuft möglicherweise nicht. Wenn dies der Fall ist, aktivieren Sie den Dienst und stellen Sie den Startmodus auf <i>Automatisch</i> ein.</li> <li>Der Remoteregistrierungsdienst von Windows ist deaktiviert. Starten Sie den Dienst und stellen Sie den Starttyp auf „Automatisch“ ein.</li> </ul>

Dieser Abschnitt enthält außerdem die folgenden Informationen:

- ♦ [Abschnitt 9.1.1, „Durchführen von Verbindungstests“ auf Seite 116](#)
- ♦ [Abschnitt 9.1.2, „Deaktivieren der Virenschutz-Software“ auf Seite 118](#)
- ♦ [Abschnitt 9.1.3, „Aktivieren von Datei-/Freigabe-Berechtigungen und -Zugriff“ auf Seite 118](#)

## 9.1.1 Durchführen von Verbindungstests

- ♦ „[Netzwerk-Verbindungstest](#)“ auf Seite 117
- ♦ „[WMI-Verbindungstest](#)“ auf Seite 117
- ♦ „[Fehlerbehebung bei DCOM-Verbindungen](#)“ auf Seite 117
- ♦ „[Fehlerbehebung bei der RPC-Dienst-Verbindung](#)“ auf Seite 118

## 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 53.

- 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 [Abschnitt 3.4.1, „Herunterladen des vSphere-Clientprogramms“](#) auf Seite 53.

- 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 [Abschnitt 2.3](#), „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“ auf Seite 31)

### 9.1.2 Deaktivieren der Virenschutz-Software

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

### 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 [Abschnitt 3.4.1](#), „Herunterladen des vSphere-Clientprogramms“ auf Seite 53.

- 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 Volumens 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.	<p>Diese Meldung wird aufgrund mehrerer möglicher Ursachen ausgegeben:</p> <ul style="list-style-type: none"> <li>◆ Der Workload ist nicht erreichbar.</li> <li>◆ Auf dem Workload wird SSH nicht ausgeführt.</li> <li>◆ Die Firewall ist aktiv und die erforderlichen Ports wurden nicht geöffnet.</li> <li>◆ Das spezifische Betriebssystem des Workloads wird nicht unterstützt</li> </ul> <p>Informationen zu Netzwerk- und Zugriffsanforderungen für einen Workload finden Sie unter <a href="#">Abschnitt 2.3, „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“</a> auf Seite 31.</p>
Zugriff verweigert.	<p>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 <a href="#">Abschnitt 6.2, „Richtlinien für Workload- und Container-Berechtigungsnachweise“</a> auf Seite 88.</p>

## 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 <a href="#">Abschnitt 9.3.1, „Gruppenrichtlinie und Benutzerrechte“</a> auf Seite 120.
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 <a href="#">Abschnitt 9.1, „Fehlerbehebung bei der Workload-Inventarisierung (Windows)“</a> auf Seite 115.

### 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
Beherrbarer Fehler bei der Reproduktion während des Vorgangs <b>Erstellen eines Snapshots der virtuellen Maschine planen</b> oder <b>Planen des Zurücksetzens der virtuellen Maschine auf Snapshot vor dem Start</b> .	Dieses Problem tritt auf, wenn der Server ausgelastet ist und der Vorgang länger als erwartet dauert. Warten Sie, bis die Reproduktion abgeschlossen ist.



Probleme oder Meldungen	Lösungen
Workload-Problem erfordert Benutzereingriff.	<p>Diese Meldung kann von verschiedenen Problemen verursacht worden sein. In den meisten Fällen enthält die Meldung weitere Angaben zur Art des Problems und zum Problembereich (z. B. Konnektivität oder Berechtigungsnachweis). Warten Sie nach der Fehlersuche einige Minuten.</p> <p>Wenden Sie sich an den PlateSpin-Support, falls die Meldung weiterhin angezeigt wird.</p>
Bei allen Workloads treten behebbare Fehler auf, da kein Speicherplatz mehr vorhanden ist.	Überprüfen Sie den freien Speicherplatz. Wenn mehr Platz erforderlich ist, entfernen Sie einen Workload.
Langsame Netzwerkgeschwindigkeiten unter 1 MB.	Stellen Sie sicher, dass die Duplex-Einstellung der Netzwerkschnittstellenkarte des Ursprungscomputers aktiviert ist und dass der Switch, mit dem sie verbunden ist, eine entsprechende Einstellung hat. Wenn der Switch auf automatisch gesetzt ist, kann der Ursprung nicht auf 100 MB eingestellt werden.
Langsame Netzwerkgeschwindigkeiten über 1 MB.	<p>Messen Sie die Latenz, indem Sie folgenden Befehl vom Ursprungs-Workload aus ausführen:</p> <pre>ping ip -t</pre> <p>(ersetzen Sie <i>ip</i> durch die IP-Adresse Ihrer Forge-VM).</p> <p>Lassen Sie den Befehl für 50 Iterationen ausführen. Der Durchschnitt gibt dann die Latenz an.</p> <p>Siehe auch <a href="#">„Optimieren des Datentransfers über WAN-Verbindungen“</a> auf Seite 40.</p>
<p>Die Dateiübertragung kann nicht beginnen</p> <p>- Port 3725 wird bereits verwendet</p> <p>oder</p> <p>3725 - Herstellen einer Verbindung nicht möglich</p>	<p>Stellen Sie sicher, dass der Port offen ist und überwacht:</p> <p>Führen Sie <code>netstat -ano</code> auf dem Workload aus.</p> <p>Überprüfen Sie die Firewall.</p> <p>Wiederholen Sie die Reproduktion.</p>
<p>Controller-Verbindung nicht hergestellt</p> <p>Die Reproduktion schlägt beim Schritt <b>Kontrolle über die virtuelle Maschine übernehmen</b> fehl.</p>	<p>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.</p> <p>Ändern Sie die Reproduktions-IP in eine statische IP oder aktivieren Sie den DHCP-Server.</p> <p>Stellen Sie sicher, dass das für die Reproduktion ausgewählte virtuelle Netzwerk eine Verbindung zur Forge-VM herstellen kann.</p>

Probleme oder Meldungen	Lösungen
Der Reproduktionsauftrag startet nicht (hängt bei 0 %)	<p>Dieser Fehler kann aus unterschiedlichen Gründen auftreten. Es gibt für jede Ursache eine eigene Lösung:</p> <ul style="list-style-type: none"> <li>◆ 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 finden Sie im <a href="#">Wissensdatenbankartikel 20339</a>.</li> <li>◆ Wenn lokale Richtlinien oder Domänenrichtlinien die erforderlichen Berechtigungen einschränken, führen Sie die im <a href="#">Wissensdatenbankartikel 7920862</a> beschriebenen Schritte aus.</li> </ul> <p>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 <a href="#">Abschnitt 9.3.1, „Gruppenrichtlinie und Benutzerrechte“</a> auf Seite 120.</p>
<p>Nach einer Windows-Aktualisierung werden einige Dateien im Ordner  <code>C:\Windows\SoftwareDistribution</code> während der schrittweisen dateibasierten Reproduktion nicht an den Zielcomputer übertragen.</p>	<p>Dies ist eine allgemeine Vorgehensweise von Microsoft Windows: Zum Zweck der Optimierung werden einige Dateien für die Löschung im Registrierungsschlüssel  <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot</code> markiert, um zu verhindern, dass sie in VSS-Snapshots integriert werden. Weitere Informationen finden Sie im Microsoft Developer Network-Artikel <a href="#">Ausschließen von Dateien von Schattenkopien</a>.</p> <p>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 <code>SoftwareDistribution</code> neu zu füllen.</p>

## 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-Adaptoren 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 [Wissensdatenbankartikel 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:

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

## 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.

### 9.9.1 Bereinigen von Windows-Workloads

Komponente	Entfernungsanweisung
Blockbasierte PlateSpin-Übertragungskomponente	Weitere Informationen hierzu finden Sie im <a href="#">Knowledgebase-Artikel 7005616</a> .
Blockbasierte Übertragungskomponente eines Drittanbieters (eingestellt)	<ol style="list-style-type: none"><li>1. Windows Software-Applet verwenden (<code>appwiz.cpl</code> ausführen) und die Komponenten entfernen. Abhängig vom Ursprung haben Sie eine der folgenden Versionen:<ul style="list-style-type: none"><li>◆ SteelEye Data Replication for Windows v6 Update2</li><li>◆ SteelEye DataKeeper For Windows v7</li></ul></li><li>2. Booten Sie den Computer neu.</li></ol>
Dateibasierte Übertragungskomponente	Auf Root-Ebene für jedes geschützte Volume alle Dateien namens <code>PlateSpinCatalog*.dat</code> entfernen.
Workload-Inventarisierungssoftware	Im Windows-Verzeichnis des Workloads: <ul style="list-style-type: none"><li>◆ Alle Dateien namens <code>machinediscovery*</code> entfernen.</li><li>◆ Unterverzeichnis <code>platespin</code> entfernen.</li></ul>
Controller-Software	<ol style="list-style-type: none"><li>1. Eine Eingabeaufforderung öffnen und das aktuelle Verzeichnis ändern in:<ul style="list-style-type: none"><li>◆ <code>\Programme\platespin*</code> (32-Bit-Systeme)</li><li>◆ <code>\Programme (x86)\platespin*</code> (64-Bit-Systeme)</li></ul></li><li>2. Führen Sie den folgenden Befehl aus: <code>ofxcontroller.exe /uninstall</code></li><li>3. Verzeichnis <code>platespin*</code> entfernen.</li></ol>

### 9.9.2 Bereinigen von Linux-Workloads

Komponente	Entfernungsanweisung
Controller-Software	<ul style="list-style-type: none"><li>◆ Diese Prozesse stoppen:<ul style="list-style-type: none"><li>◆ <code>pkill -9 ofxcontrollerd</code></li><li>◆ <code>pkill -9 ofxjobexec</code></li></ul></li><li>◆ Das OFX-Controller-rpm-Package entfernen: <code>rpm -e ofxcontrollerd</code></li><li>◆ Im Dateisystem des Workloads das Verzeichnis <code>/usr/lib/ofx</code> mit Inhalt entfernen.</li></ul>

Komponente	Entfernungsanweisung
Software für den Datentransfer auf Blockebene	<ol style="list-style-type: none"> <li>Prüfen Sie, ob der Treiber aktiv ist:  <code>lsmod   grep blkwatch</code>  Wenn der Treiber immer noch im Arbeitsspeicher geladen ist, sollte das Ergebnis eine Zeile wie die folgende enthalten:  <code>blkwatch_7616 70924 0</code></li> <li>(Bedingt) Wenn der Treiber noch geladen ist, entfernen Sie ihn aus dem Arbeitsspeicher:  <code>rmmmod blkwatch_7616</code></li> <li>Entfernen Sie den Treiber aus der Boot-Sequenz:  <code>blkconfig -u</code></li> <li>Entfernen Sie die Treiberdateien, indem Sie das folgende Verzeichnis mitsamt Inhalt löschen:  <code>/lib/modules/[Kernel-Version]/Platespin</code></li> <li>Löschen Sie die folgende Datei:  <code>/etc/blkwatch.conf</code></li> </ol>
LVM-Snapshots	<p>LVP-Snapshots, die bei fortlaufenden Reproduktionen verwendet werden, werden entsprechend einer <i>Volume-Name-PS-snapshot</i>-Konvention benannt. Beispiel: Ein Snapshot eines LogVol01-Volumes wird LogVol01-PS-snapshot genannt.</p> <p>So entfernen Sie diese LVM-Snapshots:</p> <ol style="list-style-type: none"> <li>Erstellen Sie anhand einer der folgenden Methoden eine Liste der Snapshots auf dem erforderlichen Workload: <ul style="list-style-type: none"> <li>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 -</li> <li>Führen Sie am erforderlichen Linux-Workload den folgenden Befehl aus, um eine Liste aller Volumes und Snapshots anzuzeigen:  <code># lvdisplay -a</code></li> </ul> </li> <li>Notieren Sie sich die Namen und Standorte der Snapshots, die entfernt werden sollen.</li> <li>Entfernen Sie die Snapshots mit dem folgenden Befehl:  <code>lvremove <i>Snapshot-Name</i></code></li> </ol>
Bitmap-Dateien	Bei jedem geschützten Volume im Volume-Stamm die entsprechende <code>.blocks_bitmap</code> -Datei entfernen.
Werkzeuge	Im Ursprungs-Workload unter <code>/sbin</code> folgende Dateien entfernen: <ul style="list-style-type: none"> <li><code>bmaputil</code></li> <li><code>blkconfig</code></li> </ul>

## 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 [Wissensdatenbankartikel 7006458](#) finden Sie Angaben zum Speicherort und den verfügbaren Optionen für dieses Werkzeug, mit denen Sie Offline-Datenbankvorgänge ausführen können.

---

# 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 127](#)
- ♦ [Abschnitt A.2, „PlateSpin Forge Vorkompilierter „blkwatch“-Treiber \(Linux\)“ auf Seite 128](#)

## A.1 Analysieren Ihres Linux-Workloads

Bevor Sie feststellen können, ob PlateSpin Forge einen `blkwatch`-Treiber für Ihre Verteilung umfasst, benötigen Sie weitere Informationen über den Kernel Ihres Linux-Workloads, so dass 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 127](#)
- ♦ [Abschnitt A.1.2, „Ermitteln der Architektur“ auf Seite 127](#)

### 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, um zu ermitteln, ob die Version und Architektur des Kernels Ihres Linux-Workloads mit einer unterstützten Verteilung in der Liste übereinstimmt. 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 Wissensdatenbankartikel [KB 7005873](#) beschriebenen Schritte aus.

### 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-bigsm` für die 32-Bit-(x86)-Architektur wird das Element in folgendem Format aufgeführt:

```
SLES9-SP1-2.6.5-7.139-bigsm-x86
```

### Liste der Verteilungen

Eine Liste der unterstützten Kernel-Distributionen finden Sie unter „[Liste der Verteilungen](#)“ 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 des lokalen Clusterknoten-Speichers.

## 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 11.1. 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 131](#)
- ♦ [Abschnitt C.2, „Anpassen des Produktnamens an das Markenbild in der Windows-Registrierungsdatenbank“ auf Seite 135](#)

## 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/](https://Ihr_PlateSpin-Server/platespinconfiguration/)) festlegen. Mit diesen Parametern verleihen Sie der PlateSpin Forge-Weboberfläche das unverkennbare Erscheinungsbild Ihres eigenen Unternehmens. In diesem Abschnitt finden Sie Informationen zum Ausführen dieser Anpassungen an das Marktbild.

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

- 1 Öffnen Sie [https://Ihr\\_PlateSpin-Server/platespinconfiguration/](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.

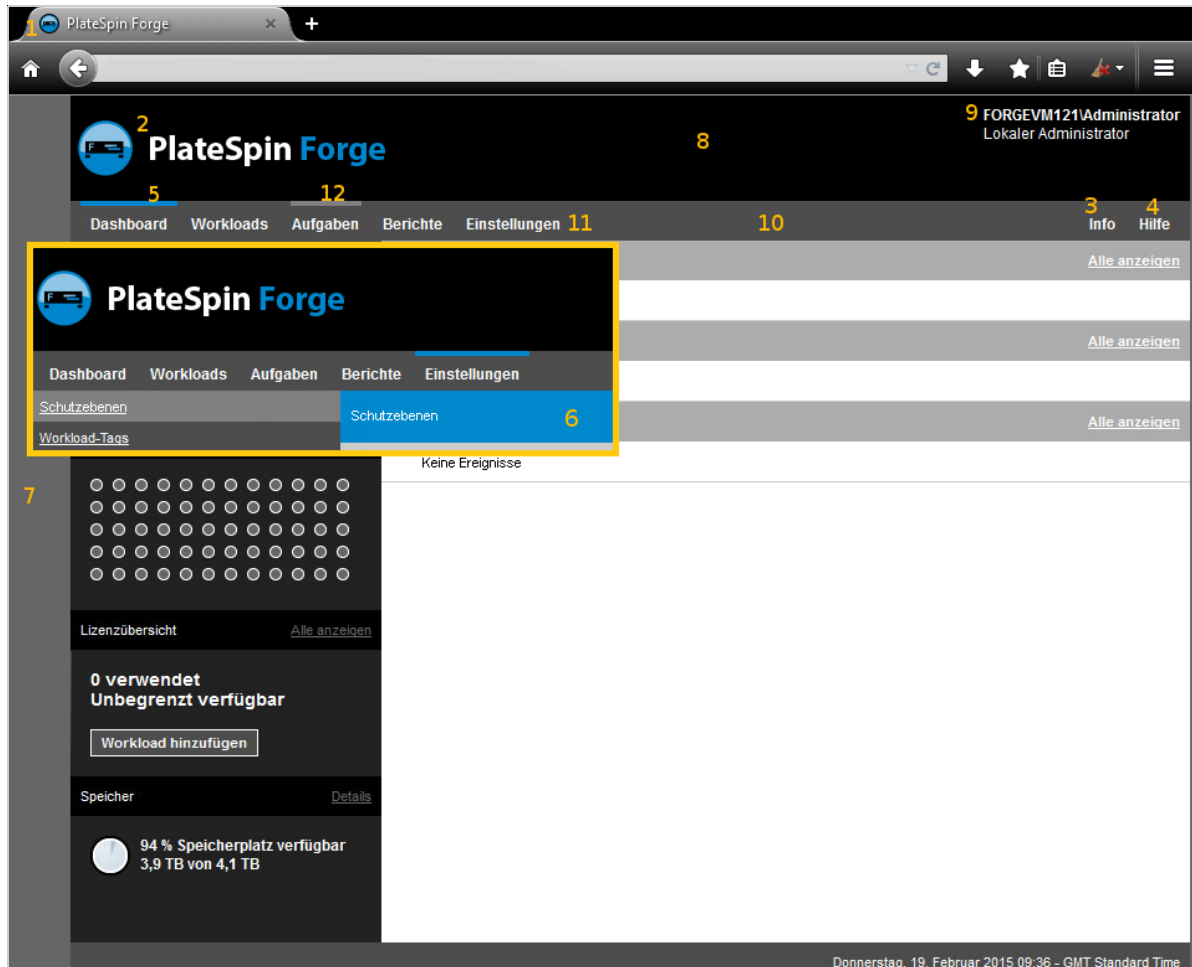
Weitere Informationen finden Sie in [Abbildung C-1](#) sowie unter dem Namen, der Beschreibung und dem Standardwert für die Einstellungen der verschiedenen bearbeitbaren Elemente.

- 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	<p>WebUIFaviconUrl</p> <p>Speicherort einer gültigen <code>.ico</code>-Grafikdatei. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>♦ Gültige URL zur entsprechenden <code>.ico</code>-Datei auf einem anderen Computer.</li> </ul> <p>Beispiel: <code>https://meinserver.beispiel.de/dir1/dir2/icons/meinefirma_favsymbol.ico</code></p> <li>♦ Relativer Pfad unterhalb des Stammverzeichnisses des lokalen Webservers, in das Sie die entsprechende <code>.ico</code>-Datei hochgeladen haben.</li> <p>Sie haben beispielsweise den Pfad <code>\meinefirma\images\icons</code> im Stammverzeichnis des Webservers erstellt, in dem die Grafikdateien für die benutzerdefinierten Symbole gespeichert werden sollen:</p> <pre>~/ \meinefirma\images\icons\meinefirma_favsymb bol.ico</pre> <p>Der tatsächliche Dateisystempfad, in dem sich die Datei befindet, lautet in diesem Beispiel</p> <pre>D:\Programme\PlateSpin Forge Server\PlateSpin Forge\web\meinefirma\images\icons\meinefir ma_favsymbol.ico.</pre>	<p>~/doc/de/favicon.ico <sup>1</sup></p>
2	<p>WebUILogoUrl</p> <p>Speicherort der Grafikdatei mit dem Produktlogo. Wählen Sie eine der folgenden Optionen aus:</p> <ul style="list-style-type: none"> <li>♦ Gültige URL zur entsprechenden Grafikdatei auf einem anderen Computer.</li> </ul> <p>Beispiel: <code>https://meinserver.beispiel.de/dir1/dir2/logos/meinefirma_logo.png</code></p> <li>♦ Relativer Pfad unterhalb des Stammverzeichnisses des lokalen Webservers, in das Sie die entsprechende Grafikdatei hochgeladen haben.</li> <p>Sie haben beispielsweise den Pfad <code>meinefirma\images\logos</code> im Stammverzeichnis des Webservers erstellt, in dem die benutzerdefinierten Logobilder gespeichert werden sollen:</p> <pre>~/meinefirma/images/logos/ meinefirma_logo.png.</pre> <p>Der tatsächliche Dateisystempfad, in dem sich die Datei befindet, lautet in diesem Beispiel</p> <pre>D:\Programme\PlateSpin Forge Server\PlateSpin Forge\web\meinefirma\images\logos\meinefir ma_logo.png.</pre>	<p>~/Resources/forgeLogo.png <sup>2</sup></p>

ID	Name und Beschreibung der Einstellung	Standardwert
3	WebUIShowAboutTab Aktiviert oder deaktiviert die Anzeige der Registerkarte <b>Info</b> ( <b>wahr</b> bzw. <b>falsch</b> ).	Wahr
4	WebUIShowHelpTab Aktiviert oder deaktiviert die Anzeige der Registerkarte <b>Hilfe</b> ( <b>wahr</b> bzw. <b>falsch</b> ).	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

<sup>1</sup> Der tatsächliche Dateipfad lautet D:\Programme\PlateSpin Forge Server\PlateSpin Forge\web\doc\de\favicon.ico.

<sup>2</sup> Der tatsächliche Dateipfad lautet D:\Programme\PlateSpin Forge Server\PlateSpin Forge\web\Resources\forgeLogo.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 Produktnamen 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.





# 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.

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

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

**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-Web-Client:** 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.

**Ausführbare Forge-Installations-/Aufrüstungsdatei.** Die ausführbare Datei, die die Forge-Appliance-Software aufrüstet. Die ausführbare Datei (auch als „Aufrüstungsprogramm“ bezeichnet) ist im *Forge 11.1-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.** Von NetIQ entwickelte PlateSpin-Software für den Schutz eines spezifischen virtuellen Workloads (also das Betriebssystem, die 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 (alle Workload-Daten werden an einen „leeren“ virtuellen Failover-Computer übertragen) oder als eine *Inkrementelle Reproduktion* (weitere Informationen hierzu finden Sie unter dem Punkt [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.

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

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

**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.

**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.

**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 zurückzusetzen.

**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](#).*

