

User Guide

PlateSpin® Protect 10.1

November 19, 2012

Novell.

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2009-2011 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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

Online Documentation: To access the latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation/\)](http://www.novell.com/documentation/).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide	7
1 Product Overview	9
1.1 About PlateSpin Protect	9
1.2 Supported Configurations	9
1.2.1 Supported Workloads in VM Containers	9
1.2.2 Supported VM Containers	10
1.2.3 Supported Workloads in Image Containers	11
1.2.4 Supported Image Container Hosts	11
1.3 Security and Privacy	11
1.3.1 Security of Workload Data in Transmission	12
1.3.2 Security of Client/Server Communications	12
1.3.3 Security of Credentials	12
1.3.4 User Authorization and Authentication	12
1.4 Performance	12
1.4.1 About Product Performance Characteristics	12
1.4.2 Data Compression	13
1.4.3 Bandwidth Throttling	13
1.4.4 RPO, RTO, and TTO Specifications	14
1.4.5 Scalability	14
2 Application Configuration	15
2.1 Product Licensing	15
2.1.1 Obtaining a License Activation Code	15
2.1.2 Online License Activation	15
2.1.3 Offline License Activation	16
2.2 Setting Up User Authorization and Authentication	16
2.2.1 About PlateSpin Protect User Authorization and Authentication	17
2.2.2 Managing PlateSpin Protect Access and Permissions	18
2.2.3 Managing PlateSpin Protect Security Groups and Workload Permissions	19
2.3 Access and Communication Requirements across your Protection Network	20
2.3.1 Access and Communication Requirements for Workloads	21
2.3.2 Access and Communication Requirements for Containers	22
2.3.3 Open Port Requirements for PlateSpin Protect Server Hosts	22
2.3.4 Protection Across Public and Private Networks Through NAT	23
2.3.5 Optimizing Data Transfer over WAN Connections (File-Based and VSS Replications)	23
2.3.6 Enabling SSL Communication Between PlateSpin Protect Web Client	24
2.3.7 Requirements for DRS Clusters as Containers	25
2.3.8 Imposing Replication Blackout Windows	25
2.3.9 Configuring the Application to Function Across NAT	25
2.4 Configuring PlateSpin Protect Default Options	26
2.4.1 Setting Up Automatic E-Mail Notifications of Events and Reports	26
2.4.2 Language Setup for International Versions of PlateSpin Protect	28
2.4.3 Configuring the Product Behavior through XML Configuration Parameters	29
2.4.4 Restarting the PlateSpin Protect Server to Apply System Changes	29
3 Up and Running	31
3.1 Launching the PlateSpin Protect Web Client	31

3.2	Elements of the PlateSpin Protect Web Client	32
3.2.1	Navigation Bar	33
3.2.2	Visual Summary Panel	33
3.2.3	Tasks and Events Panel	34
3.3	Workloads and Workload Commands	34
3.3.1	Workload Protection and Recovery Commands	35
3.4	Summary of User Experience Changes from the Portability Suite Client.	36
3.5	Using Workload Protection Features through the PlateSpin Protect Web Services API	36
3.6	Managing Multiple Instances of PlateSpin Protect.	37
3.6.1	Using the PlateSpin Protect Management Console.	37
3.6.2	About PlateSpin Protect Management Console Cards	37
3.6.3	Adding Instances of PlateSpin Protect to the Management Console	38
3.6.4	Managing Cards on the Management Console	39
3.7	Adding Containers	39
3.8	Generating Workload and Workload Protection Reports	41
4	Workload Protection	43
4.1	Basic Workflow for Workload Protection and Recovery	43
4.2	Adding a Workload for Protection	44
4.3	Configuring Protection Details and Preparing the Replication	46
4.3.1	Workload Protection Details	46
4.4	Starting the Workload Protection	48
4.5	Failover	49
4.5.1	Failure Detection	49
4.5.2	Performing a Failover	50
4.5.3	Testing the Recovery Workload and the Failover Functionality.	50
4.6	Failback	51
4.6.1	Automated Failback to a Virtual Machine	51
4.6.2	Semi-Automated Failback to a Physical Machine	54
4.6.3	Semi-Automated Failback to a Virtual Machine.	54
4.7	Advanced Workload Protection Topics	54
4.7.1	Protecting Windows Clusters.	55
4.7.2	Linux Failback to a Paravirtualized VM on Xen-on-SLES	55
5	Workload Image Protection	59
5.1	Protecting a Workload Image.	59
5.1.1	Adding a Workload for Image Protection	59
5.1.2	Configuring Workload Image Protection Details	60
5.2	Deploying a Workload Image	60
5.2.1	Deploying an Image to a Virtual Target	61
5.2.2	Deploying an Image to a Physical Target	62
5.3	Browsing and Extracting Image Files.	63
5.3.1	Starting the Image Browser and Loading Image Files.	63
5.3.2	Sorting and Searching Items in the Image Browser Interface	64
5.3.3	Extracting Items from an Image.	65
5.3.4	Browsing and Extracting Image Files at the Command Line	65
6	Auxiliary Tools for Working with Physical Machines	67
6.1	Analyzing Workloads with PlateSpin Analyzer (Windows).	67
6.2	Managing Device Drivers	68
6.2.1	Packaging Device Drivers for Windows Systems	68
6.2.2	Packaging Device Drivers for Linux Systems	69
6.2.3	Uploading Drivers to the PlateSpin Protect Device Driver Database.	69

7	Essentials of Workload Protection	73
7.1	Guidelines for Workload and Container Credentials	73
7.2	Transfer Methods	74
7.3	Protection Tiers	75
7.4	Recovery Points	76
7.5	Initial Replication Method (Full and Incremental)	76
7.6	Service and Daemon Control	77
7.7	Using Freeze and Thaw Scripts for Every Replication (Linux)	78
7.8	Volumes	78
7.9	Networking	80
7.10	Registering Physical Machines with PlateSpin Protect for Failback.	80
7.10.1	Registering Target Physical Machines	81
8	Troubleshooting	83
8.1	Troubleshooting Workload Inventory (Windows)	83
8.1.1	Performing Connectivity Tests.	84
8.1.2	Disabling AntiVirus Software	86
8.1.3	Enabling File/Share Permissions and Access	86
8.2	Troubleshooting Workload Inventory (Linux)	87
8.3	Troubleshooting Problems during the Prepare Replication Command (Windows)	87
8.3.1	Group Policy and User Rights	87
8.4	Troubleshooting Workload Replication	88
8.5	Generating and Viewing Diagnostic Reports	89
8.6	Post-Protection Workload Cleanup	90
8.6.1	Cleaning Up Windows Workloads	90
8.6.2	Cleaning Up Linux Workloads	90
8.6.3	Removing Workloads.	91
	Glossary	93

About This Guide

This guide provides information about using PlateSpin Protect.

- ♦ [Chapter 1, “Product Overview,” on page 9](#)
- ♦ [Chapter 3, “Up and Running,” on page 31](#)
- ♦ [Chapter 4, “Workload Protection,” on page 43](#)
- ♦ [Chapter 5, “Workload Image Protection,” on page 59](#)
- ♦ [Chapter 6, “Auxiliary Tools for Working with Physical Machines,” on page 67](#)
- ♦ [Chapter 7, “Essentials of Workload Protection,” on page 73](#)
- ♦ [Chapter 8, “Troubleshooting,” on page 83](#)
- ♦ [“Glossary” on page 93](#)

Audience

This guide is intended for IT staff, such as data center administrators and operators, who use PlateSpin Protect in their ongoing workload protection projects.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or submit your comments through the [Novell Documentation Feedback site \(http://www.novell.com/documentation/feedback.html\)](http://www.novell.com/documentation/feedback.html).

Additional Documentation

This guide is part of the PlateSpin Protect documentation set.

For a complete list of publications supporting this release, visit the [PlateSpin Protect 10 Online Documentation Web Site \(http://www.novell.com/documentation/platespin_protect_10\)](http://www.novell.com/documentation/platespin_protect_10).

Documentation Updates

The most recent version of this guide can be found at [PlateSpin Protect 10 Online Documentation Web Site \(http://www.novell.com/documentation/platespin_protect_10\)](http://www.novell.com/documentation/platespin_protect_10).

Additional Resources

We encourage you to use the following additional resources on the Web:

- ♦ [Novell User Forum \(http://forums.novell.com\)](http://forums.novell.com): A Web-based community with a variety of discussion topics.
- ♦ [Novell Knowledgebase \(http://www.novell.com/support\)](http://www.novell.com/support): A collection of in-depth technical articles.

Technical Support

- ♦ Telephone (North America): +1-877-528-3774 (1 87 PlateSpin)
- ♦ Telephone (global): +1-416-203-4799
- ♦ E-mail: support@platespin.com

You can also visit the [PlateSpin Technical Support Web site \(http://www.platespin.com/support\)](http://www.platespin.com/support).

1 Product Overview

- ♦ [Section 1.1, “About PlateSpin Protect,” on page 9](#)
- ♦ [Section 1.2, “Supported Configurations,” on page 9](#)
- ♦ [Section 1.3, “Security and Privacy,” on page 11](#)
- ♦ [Section 1.4, “Performance,” on page 12](#)

1.1 About PlateSpin Protect

PlateSpin Protect is software that replicates and rapidly recovers workloads (operating systems, middleware, and data). If there is a production server outage or disaster, workloads can be rapidly powered on and continue to run as normal until the production environment is restored.

PlateSpin Protect features two different mechanisms for workload protection:

- ♦ **Virtualization:** This mechanism provides you the capability to rapidly recover a workload and requires that you have an existing VM host (a *VM container*).

In this scenario, PlateSpin Protect creates a failover workload (a virtual replica of your production workload) and regularly updates it at configurable intervals. If your production workload goes offline, you can fail it over to the VM replica, which takes over the business services of the failed workload. You can then fail this workload back to either its original or to a completely new infrastructure, physical or virtual.

- ♦ **Imaging:** This mechanism provides you with the capability to recover a workload using a protected image of its volumes. Recovering a workload from a protected image takes longer than recovery from a virtual replica. However, imaging requires no VM hosts; a workload’s image is captured, stored, and regularly updated on almost any host that you designate as an image server. If your production workload goes offline, you can deploy the captured image to run on either physical hardware or, if necessary and available, also on a VM host.

1.2 Supported Configurations

- ♦ [Section 1.2.1, “Supported Workloads in VM Containers,” on page 9](#)
- ♦ [Section 1.2.2, “Supported VM Containers,” on page 10](#)
- ♦ [Section 1.2.3, “Supported Workloads in Image Containers,” on page 11](#)
- ♦ [Section 1.2.4, “Supported Image Container Hosts,” on page 11](#)

1.2.1 Supported Workloads in VM Containers

PlateSpin Protect supports both Windows and Linux workloads.

Table 1-1 Supported Windows Workloads

Operating System	Remarks
Windows 7	Windows 7 Home Edition is not supported
Windows Server 2008 R2	Including domain controller (DC) systems and Small Business Server (SBS) editions
Windows Server 2008	Including domain controller (DC) systems and Small Business Server (SBS) editions
Windows Vista	Business, Enterprise, and Ultimate editions; SP1 and later
Windows Server 2003	Including domain controller (DC) systems and Small Business Server (SBS) editions
Windows XP Professional	
Windows Server 2000	
Windows clusters	

Supported international versions (Windows): French, German, Japanese, Chinese Traditional, and Chinese Simplified

Table 1-2 Supported Linux Workloads

Operating System
Open Enterprise Server 2, SP2 and SP3
Oracle Enterprise Linux (OEL) 5.3, 5.4
SUSE Linux Enterprise Server (SLES) 9, 10, 11
Red Hat Enterprise Linux (RHEL) 4, 5

Supported international versions (Linux): All international versions of these Linux systems are supported.

1.2.2 Supported VM Containers

Table 1-3 Virtualization Platforms Supported as VM Containers

Platform	Notes
VMware DRS Cluster in vSphere 4.1	<ul style="list-style-type: none">♦ The DRS configuration must be either Partially Automated or Fully Automated (it must not be set to Manual)♦ The Cluster can use ESX 4.1, ESXi 4.1, or both
VMware ESX 3.5, 4.0, 4.1, 4.1 Update 1	
VMware ESXi 3.5, 4.0, 4.1, 4.1 Update 1	All ESXi versions must have a paid license; protection is unsupported with these systems if they are operating with a free license.

1.2.3 Supported Workloads in Image Containers

Operating Systems:

- ♦ Windows Server 2008 (including DC and SBS systems)
- ♦ Windows Server 2008 R2
- ♦ Windows Vista
- ♦ Windows Server 2003 (including DC and SBS systems)
- ♦ Windows 2000
- ♦ Windows XP

Supported international versions are: French, German, Japanese, Chinese Traditional, and Chinese Simplified.

1.2.4 Supported Image Container Hosts

Table 1-4 *Supported Image Container Hosts*

Requirement	Details
Operating System	Any of the following: <ul style="list-style-type: none">♦ Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2♦ Microsoft Windows Vista♦ Microsoft Windows Server 2003, Microsoft Windows Server 2003 R2♦ Microsoft Windows 2000
Disk Space	Minimum 100 MB for basic controller software. Additional space requirements depend on the number and size of workload images that you intend to store on a given image server.
Software	<ul style="list-style-type: none">♦ Microsoft .NET Framework 2.0 or later♦ Remote Registry service enabled and started

1.3 Security and Privacy

PlateSpin Protect provides several features to help you safeguard your data and increase security.

- ♦ [Section 1.3.1, “Security of Workload Data in Transmission,” on page 12](#)
- ♦ [Section 1.3.2, “Security of Client/Server Communications,” on page 12](#)
- ♦ [Section 1.3.3, “Security of Credentials,” on page 12](#)
- ♦ [Section 1.3.4, “User Authorization and Authentication,” on page 12](#)

1.3.1 Security of Workload Data in Transmission

To make the transfer of your workload data more secure, you can configure the workload protection to encrypt the data. When encryption is enabled, data replicated over the network is encrypted by using AES (Advanced Encryption Standard).

If necessary, you can configure your PlateSpin Protect Server to use a data encryption algorithm that is compliant with FIPS (Federal Information Processing Standards, Publication 140-2). See [“Enabling Support for FIPS-Compliant Data Encryption Algorithms \(Optional\)”](#) in your *Installation Guide*.

You can enable or disable encryption for each workload protection, with encryption being a parameter of workload protection details. See [“Workload Protection Details”](#) on page 46.

1.3.2 Security of Client/Server Communications

Data transmission between the PlateSpin Protect Server and the PlateSpin Protect Web Client can be configured to use either HTTP (default) or HTTPS (Hypertext Transfer Protocol Secure).

To secure data transmission between the client and the server, enable SSL on your PlateSpin Protect Server host, update the server configuration to reflect the change (see [“Enabling SSL Communication Between PlateSpin Protect Web Client”](#) on page 24), and use HTTPS when specifying the server URL.

1.3.3 Security of Credentials

Credentials that you use to access various systems (such as workloads and failback targets) are stored in the PlateSpin Protect database and are therefore covered by the same security safeguards that you have in place for your PlateSpin Protect Server host.

In addition, credentials are included within diagnostics, which are accessible to accredited users. You should ensure that workload protection projects are handled by authorized staff.

1.3.4 User Authorization and Authentication

PlateSpin Protect provides a comprehensive and secure user authorization and authentication mechanism based on user roles, and controls application access and operations that users can perform. See [Section 2.2, “Setting Up User Authorization and Authentication,”](#) on page 16.

1.4 Performance

- ♦ [Section 1.4.1, “About Product Performance Characteristics,”](#) on page 12
- ♦ [Section 1.4.2, “Data Compression,”](#) on page 13
- ♦ [Section 1.4.3, “Bandwidth Throttling,”](#) on page 13
- ♦ [Section 1.4.4, “RPO, RTO, and TTO Specifications,”](#) on page 14
- ♦ [Section 1.4.5, “Scalability,”](#) on page 14

1.4.1 About Product Performance Characteristics

The performance characteristics of your PlateSpin Protect product depend on a number of factors, including:

- ♦ Hardware and software profiles of your source workloads

- ♦ Hardware and software profiles of your target containers
- ♦ Hardware and software profile of your PlateSpin Protect Server host
- ♦ The specifics of your network bandwidth, configuration, and conditions
- ♦ The number of protected workloads
- ♦ The number of volumes under protection
- ♦ The size of volumes under protection
- ♦ File density (number of files per unit of capacity) on your source workloads' volumes
- ♦ Source I/O levels (how busy your workloads are)
- ♦ The number of concurrent replications
- ♦ Whether data encryption is enabled or disabled
- ♦ Whether data compression is enabled or disabled

For large-scale workload protection plans, you should perform a test protection of a typical workload, run some replications, and use the result as a benchmark, fine-tuning your metrics regularly throughout the project.

1.4.2 Data Compression

If necessary, PlateSpin Protect can compress the workload data before transferring it over the network. This enables you to reduce the overall amount of data transferred during replications.

Compression ratios depend on the type of files on a source workload's volumes, and might vary from approximately 0.9 (100MB of data compressed to 90 MB) to approximately 0.5 (100MB compressed to 50MB).

NOTE: Data compression utilizes the source workload's processor power.

Data Compression can be configured per protection or per Protection Tier. See ["Protection Tiers" on page 75](#).

1.4.3 Bandwidth Throttling

PlateSpin Protect enables you to control the amount of available bandwidth consumed by direct source-to-target communication over the course of workload protection; you can specify a throughput rate for each protection schedule. This provides a way to prevent replication traffic from congesting your production network and reduces the overall load of your PlateSpin Protect Server.

Bandwidth throttling is a parameter of a workload protection contact's Protection Tier. See ["Protection Tiers" on page 75](#).

1.4.4 RPO, RTO, and TTO Specifications

- ♦ **Recovery Point Objective (RPO):** Describes the acceptable amount of data loss measured in time. The RPO is determined by the time between incremental replications of a protected workload and is affected by current utilization levels of PlateSpin Protect, the rate and scope of changes on the workload, and your network speed.
- ♦ **Recovery Time Objective (RTO):** Describes the time required for a failover operation (bringing a workload replica online to temporarily replace a protected production workload).

The RTO for failing a workload over to its virtual replica is affected by the time it takes to configure and execute the failover operation (10 to 45 minutes). See [“Failover” on page 49](#).

The RTO for deploying a protected image as a bootable workload is affected by the target infrastructure (physical or virtual) and the time required for the corresponding image deployment procedure. See [“Deploying a Workload Image” on page 60](#).

- ♦ **Test Time Objective (TTO):** Describes the time required for testing disaster recovery with some confidence of service restoration.

Use the *Test Failover* feature to run through different scenarios and generate benchmark data.

Among factors that have an impact on RPO, RTO, and TTO is the number of required concurrent failover operations; a single failed-over workload has more memory and CPU resources than multiple failed-over workloads, which share the resources of their underlying infrastructure.

You should get average failover times for workloads in your environment by doing test failovers at various times, then use them as benchmark data in your overall data recovery plans. See [“Generating Workload and Workload Protection Reports” on page 41](#).

1.4.5 Scalability

Scalability encompasses (and depends on) the following major characteristics of your PlateSpin Protect product:

- ♦ **Workloads per Server:** The number of workloads per PlateSpin Protect Server per might vary between 5 and 50, depending on several factors, including your RPO requirements and the hardware characteristics of the server host.
- ♦ **Protections per Container:** The maximum number of protections per container is related to (but is not the same as) the VMware specifications pertaining to the maximum number of VMs supported per ESX host. Additional factors include recovery statistics (including concurrent replications and failovers) and hardware vendor specifications.

You should conduct tests, incrementally adjust your capacity numbers, and use them in determining your scalability ceiling.

2 Application Configuration

- ♦ [Section 2.1, “Product Licensing,” on page 15](#)
- ♦ [Section 2.2, “Setting Up User Authorization and Authentication,” on page 16](#)
- ♦ [Section 2.3, “Access and Communication Requirements across your Protection Network,” on page 20](#)
- ♦ [Section 2.4, “Configuring PlateSpin Protect Default Options,” on page 26](#)

2.1 Product Licensing

This section provides information about activating your PlateSpin Protect software.

- ♦ [Section 2.1.1, “Obtaining a License Activation Code,” on page 15](#)
- ♦ [Section 2.1.2, “Online License Activation,” on page 15](#)
- ♦ [Section 2.1.3, “Offline License Activation,” on page 16](#)

2.1.1 Obtaining a License Activation Code

For product licensing, you must have a license activation code. If you do not have a license activation code, request one through the [Novell Customer Center Web site \(http://www.novell.com/customercenter/\)](http://www.novell.com/customercenter/). A license activation code will be e-mailed to you.

The first time you log into PlateSpin Protect, the browser is automatically redirected to the License Activation page. You have two options for activating your product license: [Online License Activation](#) or [Offline License Activation](#).

2.1.2 Online License Activation

For online activation, PlateSpin Protect must have Internet access.

NOTE: HTTP proxies might cause failures during online activation. Offline activation is recommended for users in HTTP proxy environments.

- 1 In the PlateSpin Protect Web Client, click *Settings > Licenses > Add License*. The License Activation page is displayed.

- 2 Select *Online Activation*, specify the e-mail address that you provided when placing your order and the activation code you received, then click *Activate*.

The system obtains the required license over the Internet and activates the product.

2.1.3 Offline License Activation

For offline activation, you obtain a license key over the Internet by using a machine that has Internet access.

NOTE: To obtain a license key, you must have a Novell account. If you are an existing PlateSpin customer and you don't have a Novell account, you must first create one. Use your existing PlateSpin username (a valid e-mail address registered with PlateSpin) as input for your Novell account username.

- 1 Click *Settings > License*, then click *Add license*. The License Activation page is displayed.
- 2 Select *Offline Activation*.
- 3 Use your hardware ID to create a license key file at the [PlateSpin Product Activation Web Site \(http://www.platespin.com/productactivation/ActivateOrder.aspx\)](http://www.platespin.com/productactivation/ActivateOrder.aspx). This also requires a user name, password, the e-mail address that you provided when placing your order and the activation code you received.
- 4 Type the path to the file or browse to its location and click *Activate*.

The License Key file is saved and the product is activated based on this file.

2.2 Setting Up User Authorization and Authentication

- ♦ [Section 2.2.1, "About PlateSpin Protect User Authorization and Authentication," on page 17](#)
- ♦ [Section 2.2.2, "Managing PlateSpin Protect Access and Permissions," on page 18](#)
- ♦ [Section 2.2.3, "Managing PlateSpin Protect Security Groups and Workload Permissions," on page 19](#)

2.2.1 About PlateSpin Protect User Authorization and Authentication

The user authorization and authentication mechanism of PlateSpin Protect is based on user roles, and controls application access and operations that users can perform. The mechanism is based on Integrated Windows Authentication (IWA) and its interaction with Internet Information Services (IIS).

The role-based access mechanism enables you to implement user authorization and authentication in several ways:

- ♦ Restricting application access to specific users
- ♦ Allowing only specific operations to specific users
- ♦ Granting each user access to specific workloads for performing operations defined by the assigned role

Every PlateSpin Protect instance has the following set of operating system-level user groups that define related functional roles:

- ♦ **Workload Protection Administrators:** Have unlimited access to all features and functions of the application. A local administrator is implicitly part of this group.
- ♦ **Workload Protection Power Users:** Have access to a limited subset of system features and functions, sufficient to maintain day-to-day operation.
- ♦ **Workload Protection Operators:** Have access to most features and functions of the application, with some limitations such as restrictions in the capability to modify system settings related to licensing and security.

When a user attempts to connect to PlateSpin Protect, the credentials provided through the browser are validated by IIS. If the user is not a member of one of the Workload Protection roles, connection is refused. If the user is a local administrator on the PlateSpin Protect Server host, that account is implicitly regarded as a Workload Protection Administrator.

Table 2-1 Workload Protection Roles and Permission Details

Workload Protection Role Details	Administrators	Power Users	Operators
Add Workload	Allowed	Allowed	Denied
Remove Workload	Allowed	Allowed	Denied
Configure Protection	Allowed	Allowed	Denied
Prepare Replication	Allowed	Allowed	Denied
Run (Full) Replication	Allowed	Allowed	Allowed
Run Incremental	Allowed	Allowed	Allowed
Pause/Resume Schedule	Allowed	Allowed	Allowed
Test Failover	Allowed	Allowed	Allowed
Failover	Allowed	Allowed	Allowed
Cancel Failover	Allowed	Allowed	Allowed
Abort	Allowed	Allowed	Allowed
Dismiss (Task)	Allowed	Allowed	Allowed

Workload Protection Role Details	Administrators	Power Users	Operators
Settings (All)	Allowed	Denied	Denied
Run Reports/Diagnostics	Allowed	Allowed	Allowed
Failback	Allowed	Denied	Denied
Reprotect	Allowed	Allowed	Denied

In addition, PlateSpin Protect software provides a mechanism based on *security groups* that define which OS-level users should have access to which workloads in the PlateSpin Protect workload inventory.

Setting up a proper role-based access to PlateSpin Protect involves two tasks:

1. Adding OS-level users to the required user groups detailed in [Table 2-1](#).
2. Creating application-level security groups that associate these users with specified workloads.

2.2.2 Managing PlateSpin Protect Access and Permissions

- [“Adding PlateSpin Protect Users” on page 18](#)
- [“Assigning a Workload Protection Role to a PlateSpin Protect User” on page 18](#)

Adding PlateSpin Protect Users

Use the procedure in this section to add a new PlateSpin Protect user.

If you want to grant specific role permissions to an existing user on the PlateSpin Protect Server host, see [“Assigning a Workload Protection Role to a PlateSpin Protect User” on page 18](#).

- 1 On your PlateSpin Protect Server host, access the systems’s Local Users and Groups console (*Start > Run > lusrmgr.msc > Enter*).
- 2 Right-click the *Users* node, select *New User*, specify the required details, and click *Create*.

You can now assign a workload protection role to the newly created user. See [“Assigning a Workload Protection Role to a PlateSpin Protect User” on page 18](#).

Assigning a Workload Protection Role to a PlateSpin Protect User

Before assigning a role to a user, determine the collection of permissions that best suits that user. See [Table 2-1, “Workload Protection Roles and Permission Details,” on page 17](#).

- 1 On your PlateSpin Protect Server host, access the systems’s Local Users and Groups console (*Start > Run > lusrmgr.msc > Enter*).
- 2 Click the *Users* node, and double-click the required user in the right pane.
- 3 On the *Member Of* tab, click *Add*, find the required Workload Protection group, and assign it to the user.

It might take several minutes for the change to take effect. To attempt applying the changes manually, restart your server. See [“Restarting the PlateSpin Protect Server to Apply System Changes” on page 29](#).

You can now add this user to a PlateSpin Protect security group and associate a specified collection of workloads. See [“Managing PlateSpin Protect Security Groups and Workload Permissions” on page 19](#).

2.2.3 Managing PlateSpin Protect Security Groups and Workload Permissions

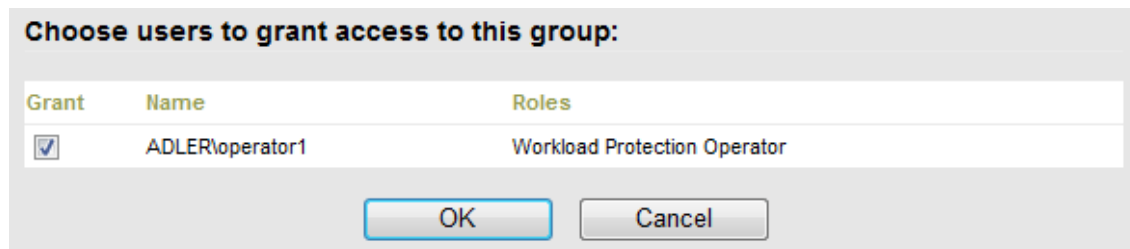
PlateSpin Protect provides a granular application-level access mechanism that allows specific users to carry out specific workload protection tasks on specified workloads. This is accomplished by setting up *security groups*.

- 1 Assign a PlateSpin Protect user a Workload Protection Role whose permissions best suit that role in your organization. See [“Assigning a Workload Protection Role to a PlateSpin Protect User” on page 18](#).
- 2 Access PlateSpin Protect as an administrator by using the PlateSpin Protect Web Client, then click *Settings > Permissions*.

The Security Groups page opens:

- 3 Click *Create Security Group*.
- 4 In the *Security Group Name* field, type a name for your security group.
- 5 Click *Add Users* and select the required users for this security group.

If you want to add a PlateSpin Protect user that was recently added as an OS-level user to the PlateSpin Protect Server host, it might not be immediately available in the user interface. In this case, first click *Refresh User Accounts*.



- 6 Click *Add Workloads* and select the required workloads:

Choose workloads to include in this group:

Include	Workload Name	Security Group
<input checked="" type="checkbox"/>	WIN7-PC	BCM Operators
<input type="checkbox"/>	10.99.161.227	[Unassigned]
<input type="checkbox"/>	AE-W2K3-1	[Unassigned]
<input checked="" type="checkbox"/>	AE-W2K3-3	[Unassigned]
<input checked="" type="checkbox"/>	AE-W2K3-4	[Unassigned]
<input type="checkbox"/>	AE-W2K3-4Y	[Unassigned]
<input type="checkbox"/>	AE-W2K3-5	[Unassigned]
<input type="checkbox"/>	DI-w2k3Dyntar	[Unassigned]

OK Cancel

Only users in this security group will have access to the selected workloads.

7 Click *Create*.

The page reloads and displays the your new group in the list of security groups.

To edit a security group, click its name in the list of security groups.

2.3 Access and Communication Requirements across your Protection Network

- ♦ [Section 2.3.1, “Access and Communication Requirements for Workloads,” on page 21](#)
- ♦ [Section 2.3.2, “Access and Communication Requirements for Containers,” on page 22](#)
- ♦ [Section 2.3.3, “Open Port Requirements for PlateSpin Protect Server Hosts,” on page 22](#)
- ♦ [Section 2.3.4, “Protection Across Public and Private Networks Through NAT,” on page 23](#)
- ♦ [Section 2.3.5, “Optimizing Data Transfer over WAN Connections \(File-Based and VSS Replications\),” on page 23](#)
- ♦ [Section 2.3.6, “Enabling SSL Communication Between PlateSpin Protect Web Client,” on page 24](#)
- ♦ [Section 2.3.7, “Requirements for DRS Clusters as Containers,” on page 25](#)
- ♦ [Section 2.3.8, “Imposing Replication Blackout Windows,” on page 25](#)
- ♦ [Section 2.3.9, “Configuring the Application to Function Across NAT,” on page 25](#)

2.3.1 Access and Communication Requirements for Workloads

The following software, network, and firewall requirements are for workloads that you intend to protect by using PlateSpin Protect.

Table 2-2 Access and Communication Requirements for Workloads

Workload Type	Prerequisites	Required Ports
All workloads	Ping (ICMP echo request and response) capability.	
All Windows workloads	Microsoft .NET Framework version 2.0 or later	
Windows 7; Windows Server 2008; Windows Vista	<ul style="list-style-type: none">◆ Built-in Administrator or domain admin account credentials (membership only in the local Administrators group is insufficient). On Vista, the account must be enabled (it is disabled by default).◆ The Windows Firewall configured with the following Inbound Rules enabled and set to Allow:<ul style="list-style-type: none">◆ File and Printer Sharing (Echo Request - ICMPv4In)◆ File and Printer Sharing (Echo Request - ICMPv6In)◆ File and Printer Sharing (NB-Datagram-In)◆ File and Printer Sharing (NB-Name-In)◆ File and Printer Sharing (NB-Session-In)◆ File and Printer Sharing (SMB-In)◆ File and Printer Sharing (Spooler Service - RPC)◆ File and Printer Sharing (Spooler Service - RPC-EPMAP) <p>These firewall settings are configured by using the Windows Firewall with Advanced Security utility (<code>wf.msc</code>). You can achieve the same result by using the basic Windows Firewall utility (<code>firewall.cpl</code>). Select the <i>File and Printer Sharing</i> item in the list of exceptions.</p>	TCP 3725 NetBIOS 137 - 139 SMB (TCP 139, 445 and UDP 137, 138) TCP 135/445

Workload Type	Prerequisites	Required Ports
Windows Server 2000; Windows XP; Windows NT 4	<ul style="list-style-type: none"> Windows Management Instrumentation (WMI) installed <p>Windows NT Server does not include WMI as part of the default installation. Obtain the WMI Core from the Microsoft Web site. If WMI is not installed, discovery of the workload fails.</p> <p>WMI (RPC/DCOM) can use TCP ports 135 and 445 as well as random or dynamically assigned ports above 1024. If problems occur during the discovery process, consider temporarily placing the workload in a DMZ or temporarily opening the firewalled ports for the discovery process only.</p> <p>For additional information, such as guidance in limiting the port range for DCOM and RPC, see the following Microsoft technical articles.</p> <ul style="list-style-type: none"> Using DCOM with Firewalls (http://msdn.microsoft.com/en-us/library/ms809327.aspx) Configuring RPC dynamic port allocation to work with firewalls (http://support.microsoft.com/default.aspx?scid=kb;en-us;154596) Configuring DCOM to work over a NAT-based firewall (http://support.microsoft.com/kb/248809) 	<p>TCP 3725</p> <p>NetBIOS 137 - 139</p> <p>SMB (TCP 139, 445 and UDP 137, 138)</p> <p>TCP 135/445</p>
All Linux workloads	Secure Shell (SSH) server	TCP 22, 3725

2.3.2 Access and Communication Requirements for Containers

The following software, network, and firewall requirements are for the supported workload containers.

Table 2-3 Access and Communication Requirements for Containers

System	Prerequisites	Required Ports
All containers	Ping (ICMP echo request and response) capability.	
VMware ESX Server 3.5, 4, 4.1 ESXi;	<ul style="list-style-type: none"> VMware account with an Administrator role VMware Web services API and file management API 	<p>HTTPS</p> <p>TCP 443</p>
vCenter Server		

2.3.3 Open Port Requirements for PlateSpin Protect Server Hosts

The following open port requirements are for PlateSpin Protect Server hosts.

Table 2-4 Open Port Requirements for PlateSpin Protect Server Hosts

Port	Remarks
TCP 80	For HTTP communication
TCP 443	For secure HTTP communication (if is enabled)

2.3.4 Protection Across Public and Private Networks Through NAT

In some cases, a source, a target, or PlateSpin Protect itself, might be located in an internal (private) network behind a network address translator (NAT) device, unable to communicate with its counterpart during protection.

PlateSpin Protect enables you to address this issue, depending on which of the following hosts is located behind the NAT device:

- ♦ **PlateSpin Protect Server:** In your server's `web.config` configuration file, record the additional IP addresses assigned to that host. See [“Configuring the Application to Function Across NAT” on page 25](#).
- ♦ **Source Workload:** Supported for failback only, where you can specify an alternative IP address for the recovery workload in [Failback Details \(Workload to VM\) \(page 53\)](#).
- ♦ **Target Container:** When you are attempting to discover a container (such as VMware ESX), specify the public (or external) IP address of that host in the discovery parameters.
- ♦ **Failback Target:** When you are attempting to register a failback target, specify the public (or external) IP address in the discovery/registration parameters.

2.3.5 Optimizing Data Transfer over WAN Connections (File-Based and VSS Replications)

You can optimize data transfer performance and fine tune it for WAN connections. You do this by modifying configuration parameters that the system reads from `*.config` files on your PlateSpin Protect Server host. For the generic procedure, see [“Configuring the Product Behavior through XML Configuration Parameters” on page 29](#).

Use these settings to optimize data transfers across a WAN. These settings are global and affect all replications using the file-based and VSS replications.

- ♦ **Configuration file:** `productinternal.config`
- ♦ **Location:** `\Program Files\PlateSpin Protect Server\Web`

NOTE: Local gigabit LAN replication speeds might be negatively impacted if these values are modified.

[Table 2-5](#) lists the configuration parameters with the defaults and with the values recommended for optimum operation in a high-latency WAN environment.

Table 2-5 Default and Optimized Configuration Parameters in *productinternal.config*

Parameter	Default Value	Optimized Value
<code>fileTransferThreadcount</code>	2	4 to 6
Controls the number of TCP connections opened for file-based data transfer.		
<code>fileTransferMinCompressionLimit</code>	0 (disabled)	max 65536 (64 KB)
Specifies the packet-level compression threshold in bytes.		
<code>fileTransferCompressionThreadsCount</code>	2	N/A
Controls the number of threads used for packet-level data compression. This is ignored if compression is disabled. Because the compression is CPU-bound, this setting might have a performance impact.		
<code>fileTransferSendReceiveBufferSize</code>	0 (8192 bytes)	max 5242880 (5 MB)
TCP/IP window size setting for file transfer connections. It controls the number of bytes sent without TCP acknowledgement, in bytes.		
When the value is set to 0, the default TCP window size is used (8 KB). For custom sizes, specify the size in bytes. Use the following formula to determine the proper value:		
$((\text{LINK_SPEED}(\text{Mbps})/8) * \text{DELAY}(\text{sec})) * 1000 * 1000$		
For example, for a 100 Mbps link with 10 ms latency, the proper buffer size would be:		
$(100/8) * 0.01 * 1000 * 1000 = 125000 \text{ bytes}$		

2.3.6 Enabling SSL Communication Between PlateSpin Protect Web Client

Use these settings to enable communication between the PlateSpin Protect Web Client and the server on which you enabled *after* installing the product. If *was* enabled on the server host at the time of the product's installation, this is not required.

For information on the update procedure, see [“Configuring the Product Behavior through XML Configuration Parameters” on page 29](#).

- **Configuration file:** `Platespin.Config`
- **Location:** `\Program Files\PlateSpin Protect Server\Configs`
- **Value:** Change

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

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


2.3.7 Requirements for DRS Clusters as Containers

To be a valid protection target, your VMware DRS cluster must be added to the set of containers (inventoried) as a VMware Cluster (you should not attempt to add a DRS Cluster as a set of individual ESX servers. See [“Adding Containers” on page 39](#)).

In addition, your VMware DRS cluster must meet the following configuration requirements:

- ♦ DRS is enabled and set to either `Partially Automated` or `Fully Automated`.
- ♦ At least one datastore is shared among all the ESX servers in the VMware Cluster.
- ♦ At least one vSwitch and virtual port-group is common to all the ESX servers in the VMware Cluster.
- ♦ The failover VM for each Protection contract is placed exclusively on datastores, vSwitches and virtual port-groups that are shared among all the ESX servers in the VMware Cluster.

2.3.8 Imposing Replication Blackout Windows

You can impose replication blackout periods to (to suspend scheduled replications during peak utilization hours or to prevent conflicts between VSS-aware Windows applications and the PlateSpin VSS block-level data transfer component). This is done by indicating start times and durations in the configuration file indicated below.

For information on the update procedure, see [“Configuring the Product Behavior through XML Configuration Parameters” on page 29](#).

- ♦ **Configuration file:** `PlateSpin.Protection.Scheduler.Service.dll.config`
- ♦ **Location:** `\Program Files\PlateSpin Protect Server\services\PlateSpinService\Plugins`
- ♦ **Values:** This parameter comprises two values:
 - ♦ `Workload_Scheduling_Blackout_Window_Start`: Defines the time for the start of the suspension. Use the following format:
`HH:MM:SS (HH 00-23, MM 00-59, SS 00-59)`
 - ♦ `Workload_Scheduling_Blackout_Window_Length`: Defines the duration of the suspension period. Use the following format:
`HH:MM:SS (HH 00-23, MM 00-59, SS 00-59)`

2.3.9 Configuring the Application to Function Across NAT

To enable the PlateSpin Protect application to function across NAT-enabled environments, you must record additional IP addresses of your of your PlateSpin Protect Server in a configuration file that the server reads upon startup.

For information on the update procedure, see [“Configuring the Product Behavior through XML Configuration Parameters” on page 29](#).

- ♦ **Configuration file:** `Web.config`
- ♦ **Location:** `\Program Files\PlateSpin Protect Server\Web`
- ♦ **Values:** `<add key="AlternateServerAddresses" value="" />`

Add the additional IP addresses, delimited by a semicolon (;), for example:

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

2.4 Configuring PlateSpin Protect Default Options

- ♦ [Section 2.4.1, “Setting Up Automatic E-Mail Notifications of Events and Reports,” on page 26](#)
- ♦ [Section 2.4.2, “Language Setup for International Versions of PlateSpin Protect,” on page 28](#)
- ♦ [Section 2.4.3, “Configuring the Product Behavior through XML Configuration Parameters,” on page 29](#)
- ♦ [Section 2.4.4, “Restarting the PlateSpin Protect Server to Apply System Changes,” on page 29](#)

2.4.1 Setting Up Automatic E-Mail Notifications of Events and Reports

You can configure PlateSpin Protect to automatically send notifications of events and replication reports to specified e-mail addresses. This functionality requires that you first specify a valid SMTP server for PlateSpin Protect to use.

- ♦ [“SMTP Configuration” on page 26](#)
- ♦ [“Setting Up Automatic Event Notifications by E-Mail” on page 27](#)
- ♦ [“Setting Up Automatic Replication Reports by E-Mail” on page 28](#)

SMTP Configuration

Use the PlateSpin Protect Web Client to configure SMTP (Simple Mail Transfer Protocol) settings for the server used to deliver e-mail notifications of events and replication reports.

Figure 2-1 Simple Mail Transfer Protocol Settings

SMTP Settings		Save
SMTP Server Address:	<input type="text"/>	
Port:	<input type="text" value="25"/>	
Reply Address:	<input type="text"/>	
Username:	<input type="text"/>	
Password:	<input type="password"/>	
Confirm:	<input type="password"/>	

To configure SMTP settings:

- 1 In your PlateSpin Protect Web Client, click *Settings > SMTP*.
- 2 Specify an SMTP server *Address*, an optional *Port* (the default is 25), and a *Reply Address* for receiving e-mail event and progress notifications.
- 3 Type a *Username* and *Password*, then confirm the password.
- 4 Click *Save*.

Setting Up Automatic Event Notifications by E-Mail

- 1 Set up an SMTP server for PlateSpin Protect to use. See [SMTP Configuration](#).
- 2 In your PlateSpin Protect Web Client, click *Settings > Email > Notification Settings*.
- 3 Select the *Enable Notifications* option.
- 4 Click *Edit Recipients*, type the required e-mail addresses separated by commas, then click *OK*.
- 5 Click *Save*.

To delete listed e-mail addresses, click *Delete* next to the address that you want to remove.

The following events trigger e-mail notifications:

Event	Remarks
Workload Online Detected	Generated when the system detects that a previously offline workload is now online. Applies to workloads whose protection schedule's state is not <i>Paused</i> .
Workload Offline Detected	Generated when the system detects that a previously online workload is now offline. Applies to workloads whose protection schedule's state is not <i>Paused</i> .
Incremental Replication Failed	
Full Replication Failed	
Test Failover Completed	Generated upon manually marking a Test Failover operation a success or a failure.
Failover Completed	
Prepare Failover Completed	
Prepare Failover Failed	
Failover Failed	
Incremental Replication Missed	Generated when: <ul style="list-style-type: none">♦ A replication is manually paused while a scheduled incremental replication is due.♦ The system attempts to carry out a scheduled incremental replication while a manually-triggered replication is underway.♦ The system determines that the target has insufficient free disk space.
Full Replication Missed	Similar to the Incremental Replication Missed event above.

Setting Up Automatic Replication Reports by E-Mail

To set up PlateSpin Protect to automatically send out replication reports by e-mail, follow these steps:

- 1 Set up an SMTP server for PlateSpin Protect to use. See [SMTP Configuration](#).
- 2 In your PlateSpin Protect Web Client, click *Settings > Email > Replication Reports Settings*.
- 3 Select the *Enable Replication Reports* option.
- 4 In the *Report Recurrence* section, click *Configure* and specify the required recurrence pattern for the reports.
- 5 In the *Recipients* section, click *Edit Recipients*, type the required e-mail addresses separated by commas, then click *OK*.
- 6 (Optional) In the *Protect Access URL* section, specify a non-default URL for your PlateSpin Protect Server (for example, when your PlateSpin Protect Server host has more than one NIC or if is located behind a NAT server). This URL impacts the title of the report and the functionality of accessing relevant content on the server through hyperlinks within e-mailed reports.
- 7 Click *Save*.

For information on other types of reports that you can generate and view on demand, see [“Generating Workload and Workload Protection Reports” on page 41](#).

2.4.2 Language Setup for International Versions of PlateSpin Protect

PlateSpin Protect provides National Language Support (NLS) for Chinese Simplified, Chinese Traditional, French, German, and Japanese.

To use the PlateSpin Protect Web Client and integrated help in one of these languages, the corresponding language must be added in your Web browser and moved to the top of the order of preference:

- 1 Access the Languages setting in your Web browser:
 - ♦ **Internet Explorer:** Click *Tools > Internet Options > General tab > Languages*.
 - ♦ **Firefox:** Click *Tools > Options > Content tab > Languages*.
- 2 Add the required language and move it up the top of the list.
- 3 Save the settings, then start the client application by connecting to your PlateSpin Protect Server. See [“Launching the PlateSpin Protect Web Client” on page 31](#).

NOTE: (For users of Chinese Traditional and Chinese Simplified versions) Attempting to connect to the PlateSpin Protect Server with a browser that does not have a specific version of Chinese added might result in Web server errors. For correct operation, use your browser’s configuration settings to add a specific Chinese language (for example, Chinese [zh-cn] or Chinese [zh-tw]). Do not use the culture-neutral Chinese [zh] language.

The language of a small portion of system messages generated by the PlateSpin Protect Server depends on the operating system interface language selected in your PlateSpin Protect Server host:

- 1 Access your PlateSpin Protect Server host.
- 2 Start the Regional and Language Options applet (click *Start > Run*, type `intl.cpl`, and press Enter), then click the *Languages* (Windows Server 2003) or *Keyboards and Languages* (Windows Server 2008) tab, as applicable.

- 3 If it is not already installed, install the required language pack. You might need access to your OS installation media.
- 4 Select the required language as the interface language of the operating system. When you are prompted, log out or restart the system.

2.4.3 Configuring the Product Behavior through XML Configuration Parameters

Some aspects of your PlateSpin Protect Server's behavior are controlled by configuration parameters that are read from *.config files on your PlateSpin Protect Server host.

Under normal circumstances you should not need to modify these settings unless you are advised to do so by PlateSpin Support. This section provides a number of common use cases along with information on the required procedure.

Use the following procedure for changing and applying any *.config parameters:

- 1 On your PlateSpin Protect Server host, go to the indicated directory.
- 2 Use a text editor to open the *.config file.
- 3 Locate the required parameter in the *.config file and change its value, which is enclosed in quotation marks (""). Do not remove the quotation marks. Use acceptable values indicated in this section or as advised by PlateSpin Support.
- 4 Save and close the *.config file.
- 5 Restart the PlateSpin Protect Server. See ["Restarting the PlateSpin Protect Server to Apply System Changes" on page 29](#).

The following topics provide information on commonly used configuration files and values that affect the behavior of your PlateSpin Protect Server.

2.4.4 Restarting the PlateSpin Protect Server to Apply System Changes

- 1 Go to the PlateSpin Protect Server's bin\RestartPlateSpinServer subdirectory.
- 2 Double-click the RestartPlateSpinServer.exe executable.
A command prompt window opens, requesting confirmation.
- 3 Confirm by typing Y and pressing Enter.

3 Up and Running

This section provides information about the essential features of PlateSpin Protect and its interface.

- ♦ [Section 3.1, “Launching the PlateSpin Protect Web Client,” on page 31](#)
- ♦ [Section 3.2, “Elements of the PlateSpin Protect Web Client,” on page 32](#)
- ♦ [Section 3.3, “Workloads and Workload Commands,” on page 34](#)
- ♦ [Section 3.4, “Summary of User Experience Changes from the Portability Suite Client,” on page 36](#)
- ♦ [Section 3.5, “Using Workload Protection Features through the PlateSpin Protect Web Services API,” on page 36](#)
- ♦ [Section 3.6, “Managing Multiple Instances of PlateSpin Protect,” on page 37](#)
- ♦ [Section 3.7, “Adding Containers,” on page 39](#)
- ♦ [Section 3.8, “Generating Workload and Workload Protection Reports,” on page 41](#)

3.1 Launching the PlateSpin Protect Web Client

Most of your interaction with PlateSpin Protect takes place through the browser-based PlateSpin Protect Web Client.

The supported browsers are:

- ♦ Microsoft Internet Explorer 7 and later
- ♦ Mozilla Firefox (on Windows) 3.6 and later

JavaScript (Active Scripting) must be enabled in your browser:

- ♦ **Internet Explorer:** Click *Tools > Internet Options > Security > Internet zone > Custom level*, then select the *Enable* option for the Active Scripting feature.
- ♦ **Firefox:** Click *Tools > Options > Content*, then select the *Enable JavaScript* option.

To use the PlateSpin Protect Web Client and integrated help in one of the supported languages, see [Section 2.4.2, “Language Setup for International Versions of PlateSpin Protect,” on page 28](#).

To launch the PlateSpin Protect Web Client:

- 1 Open a Web browser and go to:

`http://<hostname | IP_address>/Protect`

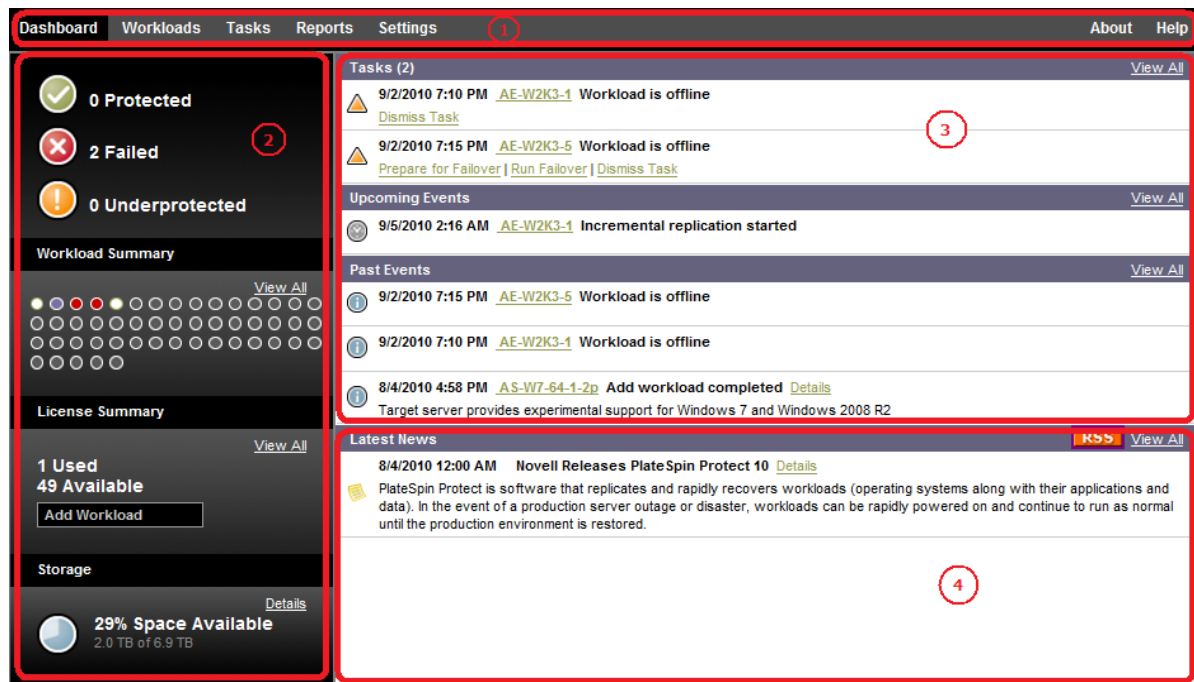
Replace `<hostname | IP_address>` with the hostname or the IP address of your PlateSpin Protect Server host.

If `s` is enabled, use `https` in the URL.

3.2 Elements of the PlateSpin Protect Web Client

The default interface of the PlateSpin Protect Web Client is the Dashboard page, which contains elements for navigating to different functional areas of the interface and carrying out workload protection and recovery operations.

Figure 3-1 The Default Dashboard Page of the PlateSpin Protect Web Client



The Dashboard page consists of the following elements:

- ♦ **Navigation bar:** Found on most pages of the PlateSpin Protect Web Client.
- ♦ **Visual Summary panel:** Provides a high-level view of the overall state of the PlateSpin Protect workload inventory,
- ♦ **Tasks and Events panel:** Provides information about events and tasks requiring user attention.
- ♦ **Latest News panel:** Provides information on product and related updates through RSS. To subscribe to the PlateSpin Protect news feed, click RSS.

The following topics provide more details:

- ♦ [Section 3.2.1, “Navigation Bar,” on page 33](#)
- ♦ [Section 3.2.2, “Visual Summary Panel,” on page 33](#)
- ♦ [Section 3.2.3, “Tasks and Events Panel,” on page 34](#)

3.2.1 Navigation Bar

The Navigation bar provides the following links:

- ♦ **Dashboard:** Displays the default Dashboard page.
- ♦ **Workloads:** Displays the Workloads page. See [“Workloads and Workload Commands” on page 34](#).
- ♦ **Tasks:** Displays the Tasks page, which lists items requiring user intervention.
- ♦ **Reports:** Displays the Reports page. See [“Generating Workload and Workload Protection Reports” on page 41](#).
- ♦ **Settings:** Displays the Settings page, which provides access to the following configuration options:
 - ♦ **Protection Tiers:** See [“Protection Tiers” on page 75](#).
 - ♦ **Permissions:** See [“Setting Up User Authorization and Authentication” on page 16](#).
 - ♦ **Containers:** See [“Adding Containers” on page 39](#).
 - ♦ **Email/SMTP:** See [“Setting Up Automatic E-Mail Notifications of Events and Reports” on page 26](#).
 - ♦ **Licenses/License Designations:** See [“Product Licensing” on page 15](#).

3.2.2 Visual Summary Panel

The Visual Summary panel provides a high-level view of all licensed workloads and the amount of available storage on the appliance.

Inventoried workloads are represented by three categories:

- ♦ **Protected:** Indicates the number of workloads under active protection.
- ♦ **Failed:** Indicates the number of protected workloads that the system has rendered as failed according to that workload’s Protection Tier.
- ♦ **Underprotected:** Indicates the number of protected workloads that require user attention.

The area in the center of the left panel represents a graphical summary of the Workloads page. It uses the following dot icons to represent workloads in different states:

Table 3-1 Dot Icon Workload Representation

● Unprotected	● Underprotected
○ Unprotected – Error	● Failed
● Protected	● Expired
● Unused	

The icons are shown in alphabetical order according to workload name. Mouse over a dot icon to display the workload name, or click the icon to display the corresponding Workload Details page.

Storage provides information about storage space available to PlateSpin Protect.

3.2.3 Tasks and Events Panel

The Tasks and Events panel shows the most recent Tasks, the most recent Past Events, and the next Upcoming Events.

Events are logged whenever something relevant to the system or to the workload occurs. For example, an event could be the addition of a new protected workload, the replication of a workload starting or failing, or the detection of the failure of a protected workload. Some events generate automatic notifications by e-mail if SMTP is configured. See [“Setting Up Automatic E-Mail Notifications of Events and Reports”](#) on page 26.

Tasks are special commands that are tied to events that require user intervention. For example, upon completion of a Test Failover command, the system generates an event associated with two tasks: Mark Test as Success and Mark Test as Failure. Clicking either task results in the Test Failover operation being canceled and a corresponding event being written in the history. Another example is the FullReplicationFailed event, which is shown coupled with a StartFull task. You can view a complete list of current tasks on the *Tasks* tab.

In the Tasks and Events panel on the dashboard, each category shows a maximum of three entries. To see all tasks or to see past and upcoming events, click *View All* in the appropriate section.

3.3 Workloads and Workload Commands

The Workloads page displays a table with a row for each inventoried workload. Click a workload name to display a Workload Details page for viewing or editing configurations relevant to the workload and its state.

Figure 3-2 *The Workloads Page*

Tasks	Online Workload	Protection Tier	Schedule	Replication Status	Last Replication	Next Replication	Last Test Failover
<input type="checkbox"/>	Yes DI-RHEL5-1x64.platespin.com	Custom	Active	Running Incremental	6/3/2010 12:55 PM	--	--
<input type="checkbox"/>	Yes DI-Sles10-SP3.platespin.com	Custom	Active	Idle	6/3/2010 1:15 PM	6/3/2010 2:00 PM	6/1/2010 2:55 PM
<input type="checkbox"/>	Yes DI-machine.platespin.com	Custom	Active	Idle	6/3/2010 1:20 PM	6/3/2010 2:00 PM	--
<input type="checkbox"/>	Yes DI-Sles11-sro-multi.platespin.com	Custom	Active	Idle	6/3/2010 1:17 PM	6/3/2010 2:00 PM	--
<input type="checkbox"/>	Yes RS-W2K3SP12NDDI	Custom	Active	Running Incremental	6/3/2010 12:56 PM	--	--
<input type="checkbox"/>	-- DI-RHEL5u4.platespin.com	Custom	--	Ready For Failback	6/3/2010 12:14 PM	6/3/2010 2:00 PM	--
<input type="checkbox"/>	Yes failback	Custom	Active	Idle	6/3/2010 1:21 PM	6/3/2010 2:00 PM	--
<input type="checkbox"/>	Yes doris	Custom	Active	Idle	6/3/2010 11:24 AM	--	--

[Select All](#) [Deselect All](#)

Workload Commands

[Configure](#) [Prepare Replication](#) [Run Replication](#) [Run Incremental](#) [Pause Schedule](#) [Resume Schedule](#)

[Test Failover](#) [Prepare for Failover](#) [Run Failover](#) [Cancel Failover](#) [Failback / Deploy](#) [Remove Workload](#)

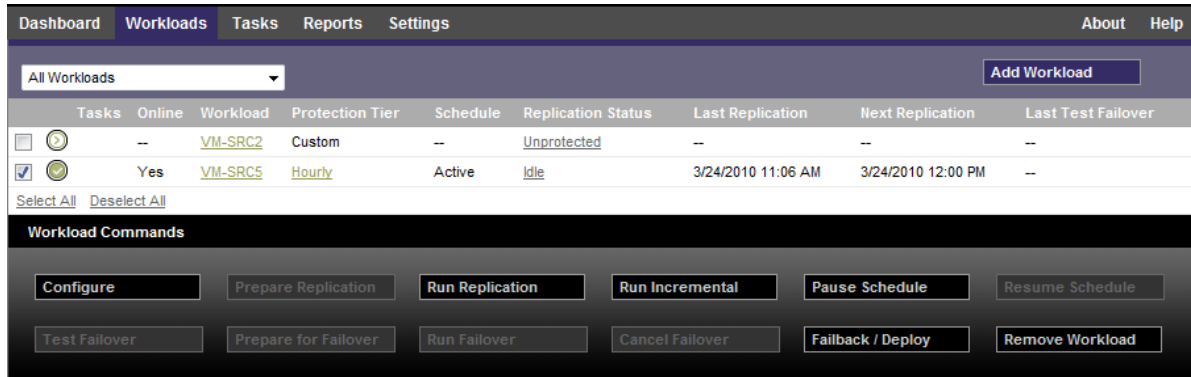
Thursday, June 03, 2010 1:28 PM - Eastern Daylight Time

NOTE: All time stamps reflect the time zone of the PlateSpin Protect Server host. This might be different from the time zone of the protected workload or the time zone of the host on which you are running the PlateSpin Protect Web Client. A display of the server date and time appears at the bottom right of the client window.

3.3.1 Workload Protection and Recovery Commands

Commands reflect the workflow of workload protection and recovery. To perform a command for a workload, select the corresponding check box at the left. Applicable commands depend on the current state of a workload.

Figure 3-3 Workload Commands



The following table summarizes workload commands along with their functional descriptions.

Table 3-2 Workload Protection and Recovery Commands

Workload Command	Description
<i>Configure</i>	Starts the workload protection configuration with parameters applicable to an inventoried workload.
<i>Prepare Replication</i>	Installs required data transfer software on the source and creates a failover VM in preparation of workload replication.
<i>Run Replication</i>	Starts replicating the source workload and according to specified parameters.
<i>Run Incremental</i>	Performs an individual transfer of changed data from the source to the target outside the workload protection schedule.
<i>Pause Schedule</i>	Suspends the protection and pauses data transfers from the protected workload.
<i>Resume Schedule</i>	Resumes the protection according to saved protection settings.
<i>Test Failover</i>	Brings the recovery workload online in an isolated environment within the container for testing purposes.
<i>Prepare for Failover</i>	Boots the recovery workload in preparation for a failover operation.
<i>Run Failover</i>	Boots and configures the recovery workload, which takes over the business services of a failed workload.
<i>Cancel Failover</i>	Aborts the failover process.
<i>Failback / Deploy</i>	Following a failover operation, fails the recovery workload back to its original infrastructure or to a new infrastructure (virtual or physical).
<i>Remove Workload</i>	Removes a workload from the inventory.

3.4 Summary of User Experience Changes from the Portability Suite Client

The following table contains a quick reference for users of the discontinued Portability Suite Client.

Table 3-3 *User Experience Differences between the Portability Suite Client and the Web Client*

Feature	Portability Suite Client (old)	Web Client (new)
Client Startup	<i>Start > Programs > PlateSpin Portability Suite Client</i>	Launch browser > Navigate to <code>http://<server_home>/protect</code>
Portability Suite network	UI option in server connection settings	Discontinued
Discovery (sources)	<i>Servers view > Right-click in white space > Discover Details</i>	Dashboard > <i>Add Workload</i> command
Discovery (targets)	<i>Servers view > Right-click in white space > Discover Details</i>	<i>Settings > Containers > Add Container</i>
Transfer Scope selection (full vs Server Sync)	Start a migration job and select <i>Server Sync (Changes only)</i> as the Transfer Scope.	Start configuring the relevant operation (such as <i>Add Workload</i> or <i>Failback</i>), and for the <i>Initial Replication</i> method, select <i>Incremental</i> .
Viewing Job Lists	Dedicated <i>Jobs</i> view	<i>Reports > Events</i>
Updating Workload credentials	<i>Save</i> command in <i>Discover Details</i> or <i>Refresh</i> dialog box.	<ul style="list-style-type: none">♦ Containers: <i>Settings > Containers > click <container_name></i>♦ Workloads: Edit protection details (click a discovered workload name)

3.5 Using Workload Protection Features through the PlateSpin Protect Web Services API

You can use workload protection functionality programmatically, through the `protection.webservices` API from within your applications. You can use any programming or scripting language that supports Web services.

`http://<hostname | IP_address>/protection.webservices`

Replace `<hostname | IP_address>` with the hostname or the IP address of your PlateSpin Protect Server host.

To script common workload protection operations, use the referenced samples written in Python as guidance. A Microsoft Silverlight application, along with its source code, is also provided for reference purposes.

3.6 Managing Multiple Instances of PlateSpin Protect

PlateSpin Protect includes a Web-based client application, the PlateSpin Protect Management Console, that provides centralized access to multiple instances of PlateSpin Protect.

In a data center with more than one instance of PlateSpin Protect, you can designate one of the instances as the manager and run the management console from there. Other instances are added under the Manager, providing a single point of control and interaction.

- [Section 3.6.1, “Using the PlateSpin Protect Management Console,” on page 37](#)
- [Section 3.6.2, “About PlateSpin Protect Management Console Cards,” on page 37](#)
- [Section 3.6.3, “Adding Instances of PlateSpin Protect to the Management Console,” on page 38](#)
- [Section 3.6.4, “Managing Cards on the Management Console,” on page 39](#)

3.6.1 Using the PlateSpin Protect Management Console

- 1 Open a Web browser on a machine that has access to your PlateSpin Protect instances and navigate to the following URL:

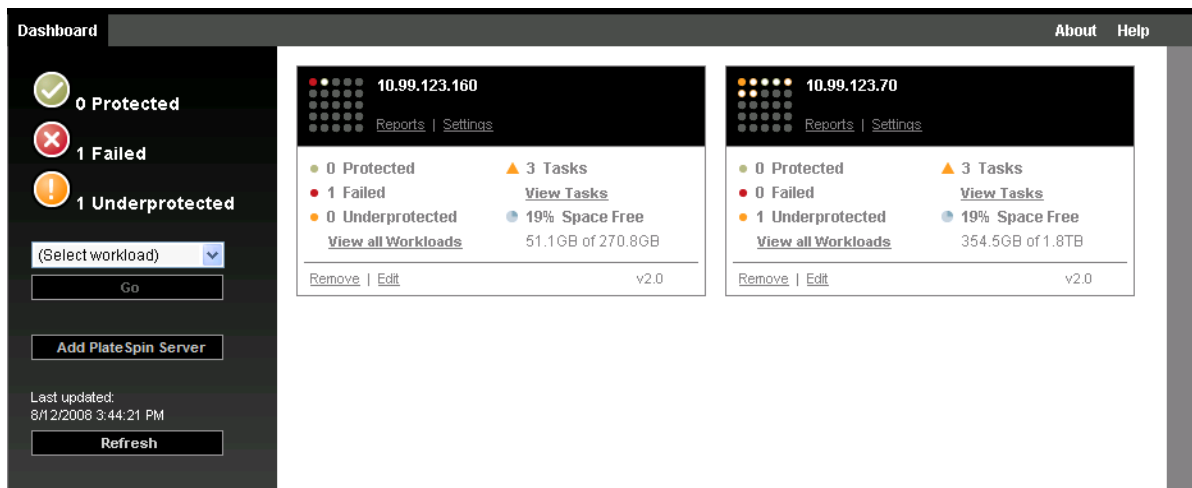
`http://<IP_address | hostname>/console`

Replace `<IP_address | hostname>` with either the IP address or the hostname of the PlateSpin Protect Server host that is designated as the Manager.

- 2 Log in with your username and password.

The console’s default Dashboard page is displayed.

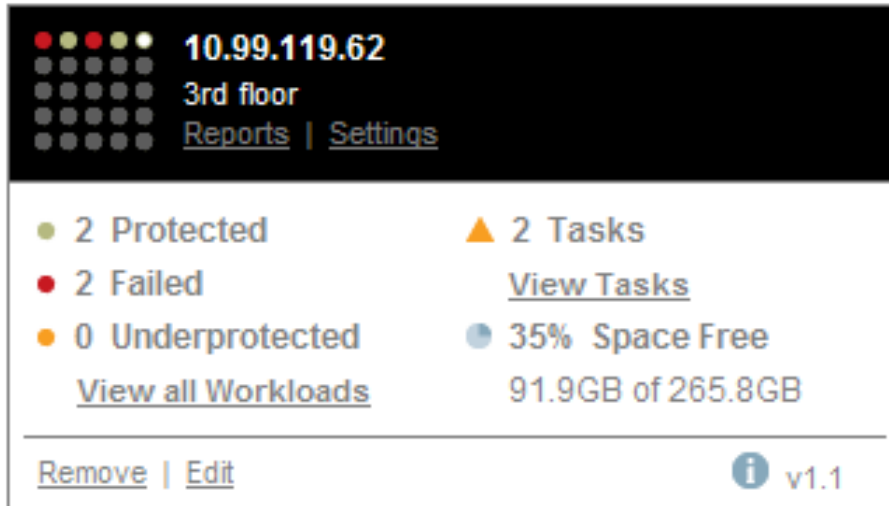
Figure 3-4 The Management Console’s Default Dashboard Page



3.6.2 About PlateSpin Protect Management Console Cards

Individual instances of PlateSpin Protect, when added to the Management Console, are represented by cards.

Figure 3-5 PlateSpin Protect Instance Card



A card displays basic information about the specific instance of PlateSpin Protect, such as:

- ♦ IP address/hostname
- ♦ Location
- ♦ Version number
- ♦ Workload count
- ♦ Workload status
- ♦ Storage capacity
- ♦ Remaining free space

Hyperlinks on each card allow you to navigate to that particular instance's Workloads, Reports, Settings, and Tasks pages. There are also hyperlinks that allow you to edit a card's configuration or remove a card from the display.

3.6.3 Adding Instances of PlateSpin Protect to the Management Console

Adding a PlateSpin Protect instance to the Management Console results in a new card on the Management Console's dashboard.

NOTE: When you log in to the Management Console on a PlateSpin Protect instance, that instance is not automatically added to the console. It must be manually added.

To add a PlateSpin Protect instance to the console:

- 1 On the console's main dashboard, click *Add*.
The *Add/Edit* page is displayed.
- 2 Specify the URL of the PlateSpin Protect Server host. Both HTTP and HTTPS protocols are supported.
- 3 (Optional) Enable the *Use Management Console Credentials* check box to use the same credentials as those used by the console. When it is selected, the console automatically populates the *Domain \Username* field.

- 4 In the *Domain\Username* field, type a domain name and a username valid for the PlateSpin Protect instance that you are adding. In the *Password* field, type the corresponding password.
- 5 (Optional) Specify a descriptive or identifying *Display Name* (15 characters max), a *Location* (20 characters max), and any *Notes* you might require (400 characters max).
- 6 Click *Add/Save*.

A new card is added to the dashboard.

3.6.4 Managing Cards on the Management Console

You can modify the details of a PlateSpin Protect card on the Management Console.

- 1 Click the *Edit* hyperlink on the card that you want to edit.
The console's *Add/Edit* page is displayed.
- 2 Make any desired changes, then click *Add/Save*.
The updated console dashboard is displayed.

To remove a PlateSpin Protect card from the Management Console:

- 1 Click the *Remove* hyperlink on the card you want to remove.
A confirmation prompt is displayed.
- 2 Click *OK*.
The individual appliance card is removed from the dashboard.

3.7 Adding Containers

A container is a protection infrastructure that acts as the host of a protected workload's regularly-updated replica. There are two categories of protection infrastructure: virtualization and imaging.

Virtualization technology	VMware ESX Server
	VMware DRS cluster
Imaging technology	PlateSpin Image Server

To be able to protect a workload, you must add a container either beforehand, or during the process of adding the workload that you want to protect.

To add a container:

- 1 In your PlateSpin Protect Web Client, click *Settings > Containers > Add Container*.

Dashboard	Workloads	Tasks	Reports	Settings	About	Help
Protection Tiers	Permissions	Containers	Email	SMTP	Licenses	
Containers						
Name	Description	Purpose	CPU	Memory	Free Space	Last Refresh
comp129	VMware ESX Server 4.0.0.261974	Protection	8 x Intel(R) Xeon(R) CPU X5355 @ 2.66GHz	15.6 GB	--	60 Day(s) ago Remove
Comp164	VMware ESX Server 3.5.0.207095	Failback/Deployment	32 x Intel(R) Xeon(R) CPU X7350 @ 2.93GHz	31.2 GB	--	60 Day(s) ago Remove
NOVELL-AD80B2AE	PlateSpin Image Container 9.0.2.7860	Protection	2 x Intel(R) Pentium(R) III Xeon processor	3.8 GB	--	60 Day(s) ago Remove
Add Container						
Monday, April 18, 2011 4:22 PM - Eastern Daylight Time						

2 Specify the following parameters:

- ♦ **Type:** Select the type of the container (*VMware ESX Server*, *VMware DRS Cluster*, or *PlateSpin Image Server*). Make sure the container is supported. For more information, see:
 - ♦ [“Supported VM Containers” on page 10](#)
 - ♦ [“Supported Image Container Hosts” on page 11](#)
 - ♦ **Hostname or IP:** Type the container’s hostname or IP address.
 - ♦ **vCenter Hostname or IP:** (DRS clusters only) Type the vCenter server’s hostname or IP address.
 - ♦ **Cluster Name:** (DRS clusters only) Type the name of the required DRS cluster.
- When you attempt to add or refresh a DRS cluster, the underlying discovery operation might fail if:
- ♦ A cluster contains no ESX hosts.
 - ♦ A cluster name is not unique across the vCenter server (even if it has a unique inventory path).
 - ♦ None of the cluster members are accessible (for example, because the vCenter server is in maintenance mode).
- ♦ **Username/Password:** Provide admin-level credentials for accessing the required host. See [“Guidelines for Workload and Container Credentials” on page 73](#)
 - ♦ **Purpose:** (VM containers only) Select the required item (*Protection*, *Failback/Deployment*, or both). Selecting both (*Protection* and *Failback/Deployment*) results in that container being available for selection as a target in both protection and failback/deployment operations.

3 Click *Add*.

PlateSpin Protect reloads the Containers page and displays a process indicator for the container being added . On completion, the process indicator icon turns into a *Refresh* icon .

To refresh a container, click the *Refresh* icon next to the container you want to refresh. This performs a re-inventory of the container.

To remove a container, click *Remove* next the container that you want to remove.

3.8 Generating Workload and Workload Protection Reports

PlateSpin Protect enables you to generate reports that provide analytical insight into your workload protection schedules over time.

The following report types are supported:

- ♦ **Workload Protection:** Reports replication events for all workloads over a selectable time window.
- ♦ **Replication History:** Reports replication type, size, time, and transfer speed per selectable workload over a selectable time window.
- ♦ **Replication Window:** Reports the dynamics of full and incremental replications that can be summarized by *Average*, *Most Recent*, *Sum*, and *Peak* perspectives.
- ♦ **Current Protection Status:** Reports *Target RPO*, *Actual RPO*, *Actual TTO*, *Actual RTO*, *Last Test Failover*, *Last Replication*, and *Test Age* statistics.
- ♦ **Events:** Reports system events for all workloads over a selectable time window.
- ♦ **Scheduled Events:** Reports only upcoming workload protection events.

Figure 3-6 Options for a Replication History Report

The screenshot shows the 'Reports' tab in the PlateSpin Protect web client. The 'Replication History' report is selected. The interface includes a navigation bar with 'Dashboard', 'Workloads', 'Tasks', 'Reports', 'Settings', 'About', and 'Help'. Below the navigation bar, there is a header for 'Replication History' with a sub-header 'What are the replication events relevant to my workload?'. The main content area contains a form with a 'Custom' dropdown menu, a date range from '4/4/2011 12:00:00 AM' to '4/18/2011 4:15:41 PM', a 'Workload' dropdown menu set to 'SES-2K8-1', and a checkbox for 'All Replication Events' with a link to 'Diagnostics View'. Below the form is a table with the following data:

Date	Replication Event	Total Time	Transfer Time	Transfer Size	Transfer Speed
4/17/2011 4:01 AM	Incremental replication did not run as scheduled because the workload was busy	--	--	.0 MB	0.00 Mbps
4/17/2011 4:00 AM	Incremental replication did not run as scheduled because the workload was busy	--	--	.0 MB	0.00 Mbps
4/10/2011 4:01 AM	Incremental replication did not run as scheduled because the workload was busy	--	--	.0 MB	0.00 Mbps
4/10/2011 4:00 AM	Incremental replication did not run as scheduled because the workload was busy	--	--	.0 MB	0.00 Mbps

At the bottom of the table, there are links for 'Printable View' and 'Export To Xml'. The footer of the page shows the date and time: 'Monday, April 18, 2011 4:15 PM - Eastern Daylight Time'.

To generate a report:

- 1 In your PlateSpin Protect Web Client, click *Reports*.
A list of the report types is displayed.
- 2 Click the name of the required report type.

4 Workload Protection

PlateSpin Protect creates a replica of your production workload and regularly updates that replica based on a schedule that you define.

The replica, or the *failover workload*, is a virtual machine in the VM container of PlateSpin Protect that takes over the business function of your production workload in case of a disruption at the production site.

In addition to workload protection through virtualization, PlateSpin Protect provides workload image protection through volume imaging. See [“Workload Image Protection” on page 59](#).

- ♦ [Section 4.1, “Basic Workflow for Workload Protection and Recovery,” on page 43](#)
- ♦ [Section 4.2, “Adding a Workload for Protection,” on page 44](#)
- ♦ [Section 4.3, “Configuring Protection Details and Preparing the Replication,” on page 46](#)
- ♦ [Section 4.4, “Starting the Workload Protection,” on page 48](#)
- ♦ [Section 4.5, “Failover,” on page 49](#)
- ♦ [Section 4.6, “Failback,” on page 51](#)
- ♦ [Section 4.7, “Advanced Workload Protection Topics,” on page 54](#)

4.1 Basic Workflow for Workload Protection and Recovery

PlateSpin Protect defines the following workflow for workload protection and recovery:

1 Preparatory step:

1a Make sure that PlateSpin Protect supports your workload.

See [“Supported Configurations” on page 9](#).

1b Make sure that your workloads and containers meet access and network prerequisites.

See [“Access and Communication Requirements across your Protection Network” on page 20](#).

1c (Linux only)

- ♦ (Conditional) If you plan to protect a supported Linux workload that has a non-standard, customized, or newer kernel, rebuild the PlateSpin `blkwatch` module, which is required for block-level data replication.

See [KB Article 7005873 \(http://www.novell.com/support/viewContent.do?externalId=7005873\)](http://www.novell.com/support/viewContent.do?externalId=7005873).

- ♦ (Recommended) Prepare LVM snapshots for block-level data transfer. Ensure that each volume group has sufficient free space for LVM snapshots (at least 10 % of the sum of all partitions).

See [KB Article 7005872 \(http://www.novell.com/support/viewContent.do?externalId=7005872\)](http://www.novell.com/support/viewContent.do?externalId=7005872).

- ♦ (Optional) Determine and prepare any custom scripts that you want to execute on your source workload upon each replication.
See [“Using Freeze and Thaw Scripts for Every Replication \(Linux\)” on page 78](#).
- 2 Add a container.
See [“Adding Containers” on page 39](#).
- 3 Add a workload.
See [“Adding a Workload for Protection” on page 44](#).
- 4 Configure protection details and prepare the replication.
See [“Configuring Protection Details and Preparing the Replication” on page 46](#).
- 5 Start the workload protection schedule.
See [“Starting the Workload Protection” on page 48](#).
- 6 (Optional) Manually run an incremental.
- 7 (Optional) Test the failover functionality.
See [Testing the Recovery Workload and the Failover Functionality](#).
- 8 Perform a failover.
See [“Failover” on page 49](#).
- 9 Perform a failback.
See [“Failback” on page 51](#).
- 10 (Optional) Reprotect a workload after failback.

Except for Steps 1, 8, and 9, these are represented by workload commands on the Workloads page. See [“Workloads and Workload Commands” on page 34](#).

A *Reprotect* command becomes available following a successful Failback operation.

4.2 Adding a Workload for Protection

- 1 Follow the required preparatory steps.
See [Step 1 in “Basic Workflow for Workload Protection and Recovery” on page 43](#).
- 2 Add a VM container.
See [“Adding Containers” on page 39](#).
- 3 On the Dashboard or Workloads page, click *Add Workload*.
The PlateSpin Protect Web Client displays the Add Workload page.

Dashboard
Workloads
Tasks
Reports
Settings
About
Help

Add Workload

ADD WORKLOAD
CONFIGURE PROTECTION
PREPARE REPLICATION
RUN REPLICATION

Workload Settings

Hostname or IP: 10.99.123.170

Workload Type:
☐ Windows
☒ Linux

Credentials:
User Name: root
Password:
Test Credentials

Security Group: All Workloads

Replication Settings

Initial Replication Method:
☒ Full Replication
☐ Incremental Replication

Protection Target: comp213 (VMware ESXi Server 4.1.0.260247)

Name	Description	CPU	Memory	Free Space	Last Refresh
comp129	VMware ESX Server 4.0.0.261974	8 x Intel(R) Xeon(R) CPU X5355 @ 2.66GHz	15.6 GB	--	48 Day(s) ago Remove
comp213	VMware ESXi Server 4.1.0.260247	16 x Intel(R) Xeon(R) CPU E5530 @ 2.40GHz	32.0 GB	1.9 TB	0 Hour(s) ago Remove

Add Container

Workload Commands

Add Workload
Add and New

4 Specify the required workload details:


- ◆ **Workload Settings:** Specify your workload's hostname or IP address, the operating system, admin-level credentials, and a security group to assign the workload to. See [“Managing PlateSpin Protect Security Groups and Workload Permissions”](#) on page 19.

Use the required credential format. See [“Guidelines for Workload and Container Credentials”](#) on page 73.

To make sure that PlateSpin Protect can access the workload, click *Test Credentials*.

- ◆ **Replication Settings:** Select the required replication settings. See [“Initial Replication Method \(Full and Incremental\)”](#) on page 76.
- ◆ **Protection Target:** Select the required protection target. This is either the target container or, if you have selected *Incremental Replication* as the initial replication method, a prepared workload. See [“Initial Replication Method \(Full and Incremental\)”](#) on page 76.

5 Click *Add Workload*.

PlateSpin Protect reloads the Workloads page and displays a process indicator for the workload being added . Wait for the process to complete. Upon completion, a *Workload Added* event is shown on the Dashboard.

4.3 Configuring Protection Details and Preparing the Replication

Protection details control the workload protection and recovery settings and behavior over the entire life cycle of a workload under protection. At each phase of the protection and recovery workflow (see [“Basic Workflow for Workload Protection and Recovery” on page 43](#)), relevant settings are read from the protection details.

To configure your workload’s protection details:

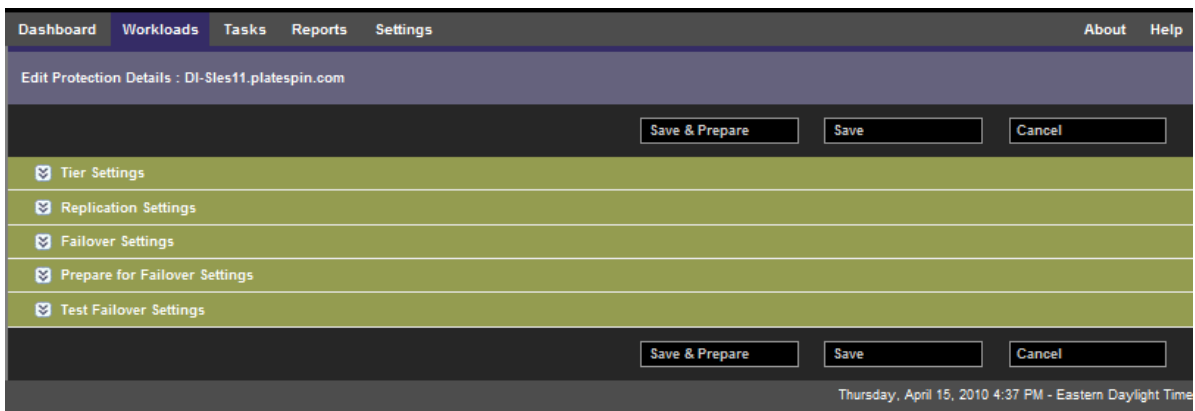
- 1 Add a workload. See [“Adding a Workload for Protection” on page 44](#).
- 2 On the Workloads page, select the required workload and click *Configure*.
The PlateSpin Protect Web Client displays the workload’s Protection Details page.
- 3 Configure the protection details in each set of settings as dictated by your business continuity needs. See [“Workload Protection Details” on page 46](#).
- 4 Correct any validation errors.
- 5 Click *Save*.

Alternately, click *Save & Prepare*. This saves the settings and simultaneously executes the *Prepare Replication* command (installing data transfer drivers on the source workload if necessary and creating the initial VM replica of your workload).

Wait for the process to complete. Upon completion, a *Workload configuration completed* event is shown on the Dashboard.

4.3.1 Workload Protection Details

Workload protection details are represented by five sets of parameters:



You can expand or collapse each parameter set by clicking the ☒ icon at the left.

The following are the details of the five parameter sets:

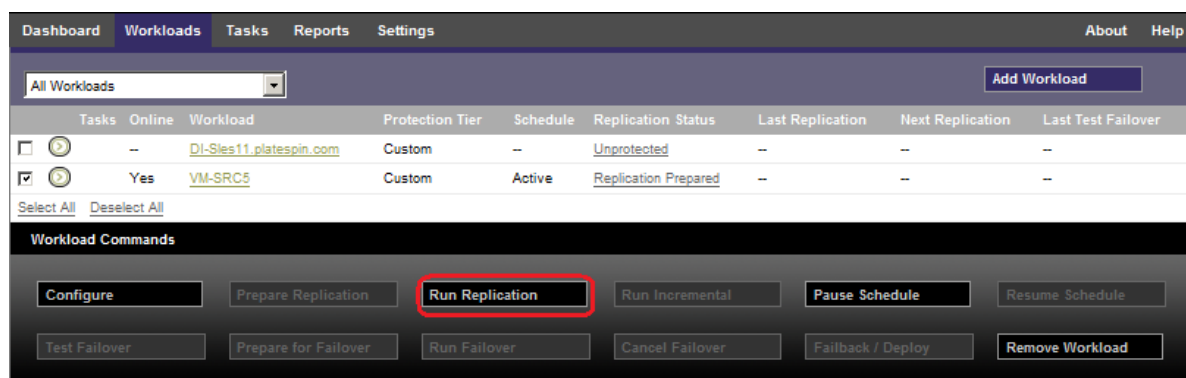
Table 4-1 Workload Protection Details

Parameter Set (Settings)	Details
Tier	Indicates the Protection Tier that the current protection uses. See “Protection Tiers” on page 75 .
Replication	<p>Transfer Encryption: To enable encryption, select the <i>Encrypt Data Transfer</i> option. See “Security and Privacy” on page 11.</p> <p>Transfer Method: (Windows) Enables you to select a data transfer mechanism and security through encryption. See “Transfer Methods” on page 74.</p> <p>Source Credentials: Required for accessing the workload. See “Guidelines for Workload and Container Credentials” on page 73.</p> <p>Number of CPUs: Enables you to specify the required number of vCPUs assigned to the recovery workload.</p> <p>Replication Network: Enables you to separate replication traffic based on virtual networks defined on your VM container. See “Networking” on page 80.</p> <p>Recovery Point Datastore: Enables you to select a datastore associated with your VM container for storing Recovery Points. See “Recovery Points” on page 76.</p> <p>Protected Volumes: Use these options to select volumes for protection and to assign their replicas to specific datastores on your VM container. You can also select for protection:</p> <ul style="list-style-type: none"> ♦ Linux workloads: logical volumes and volume groups ♦ OES 2 workloads: EVMS volumes <p>See “Volumes” on page 78.</p> <p>Thin Disk option: Enables the thin-provisioned virtual disk feature, whereby a virtual disk appears to the VM to have a set size, but only consumes the amount of disk space that is required by that disk.</p> <p>Services/Daemons to Stop During Replication: Enables you to select Windows services or Linux Daemons that are automatically stopped during the replication. See “Service and Daemon Control” on page 77.</p>
Failover	<p>VM Memory: Enables you to specify the amount of memory allocated to the failover VM.</p> <p>Hostname and Domain/Workgroup affiliation: Use these options to control the identity and domain/workgroup affiliation of the failover workload when it is live. For domain affiliation, domain admin credentials are required.</p> <p>Network Connections: Use these options to control the LAN settings of the failover workload. See “Networking” on page 80.</p> <p>Service/Daemon States to Change: Enables you to control the startup state of specific application services (Windows) or daemons (Linux). See “Service and Daemon Control” on page 77.</p>
Prepare for Failover	Enables you to control the temporary network settings of the failover workload during the optional Prepare for Failover operation. See “Networking” on page 80 .

Parameter Set (Settings)	Details
Test Failover	<p>VM Memory: Enables you to assign the required RAM to the temporary workload.</p> <p>Hostname: Enables you to assign a hostname to the temporary workload.</p> <p>Domain/Workgroup: Enables you to affiliate the temporary workload with a domain or a workgroup. For domain affiliation, domain admin credentials are required.</p> <p>Network Connections: Controls the LAN settings of the temporary workload. See “Networking” on page 80.</p> <p>Service/Daemon States to Change: Enables you to control the startup state of specific application services (Windows) or daemons (Linux). See “Service and Daemon Control” on page 77.</p>

4.4 Starting the Workload Protection

Workload protection is started by the *Run Replication* command:



You can execute the Run Replication command after:

- Adding a workload.
- Configuring the workload’s protection details.
- Preparing the initial replication.

When you are ready to proceed:

- 1 On the Workloads page, select the required workload, then click *Run Replication*.
- 2 Click *Execute*.

PlateSpin Protect starts the execution and displays a process indicator for the *Copy data* step .

NOTE: After a protection contract is established:

- Changing the size of a volume that is under block-level protection invalidates the protection. The appropriate procedure is to 1. remove the contract, 2. resize the volumes as required. 3. re-establish the protection.
- Any significant modification of the protected workload requires that the protection be re-established. Examples include adding volumes or network cards to the workload under protection.

4.5 Failover

Failover is when the business function of a failed workload is taken over by a recovery workload within a PlateSpin Protect VM container.

- ♦ [Section 4.5.1, “Failure Detection,” on page 49](#)
- ♦ [Section 4.5.2, “Performing a Failover,” on page 50](#)
- ♦ [Section 4.5.3, “Testing the Recovery Workload and the Failover Functionality,” on page 50](#)

4.5.1 Failure Detection

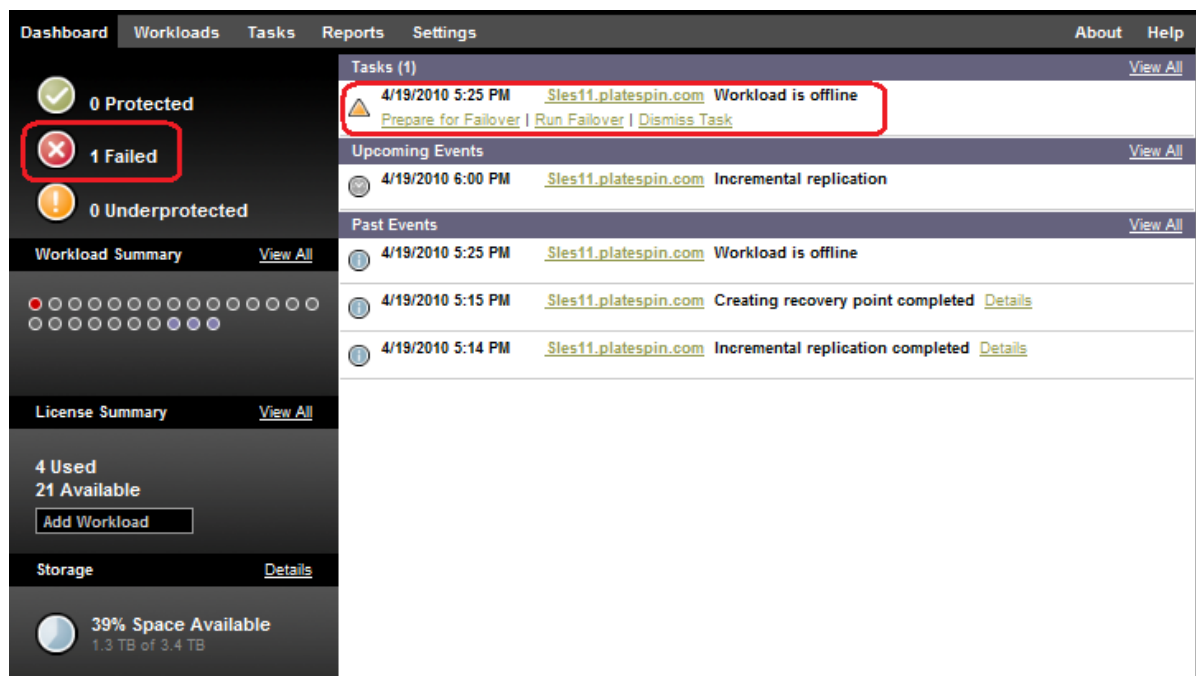
If an attempt to detect a workload fails for a predefined number of times, PlateSpin Protect generates a *Workload is offline* event. Criteria that determine and log a workload failure are part of a workload protection’s Tier settings (see the [Tier](#) row in [“Workload Protection Details” on page 46](#)).

If notifications are configured along with SMTP settings, PlateSpin Protect simultaneously sends a notification e-mail to the specified recipients. See [“Setting Up Automatic E-Mail Notifications of Events and Reports” on page 26](#).

If a workload failure is detected while the status of the replication is *Idle*, you can proceed to the *Run Failover* command. If a workload fails while an incremental is underway, the job stalls. In this case, abort the command, and then proceed to the *Run Failover* command. See [“Performing a Failover” on page 50](#).

The following figure shows the PlateSpin Protect Web Client’s Dashboard page upon detecting a workload failure. Note the applicable tasks in the Tasks and Events pane:

Figure 4-1 The Dashboard Page upon Workload Failure Detection



4.5.2 Performing a Failover

Failover settings, including the recovery workload's network identity and LAN settings, are saved together with the workload's protection details at configuration time. See the [Failover](#) row in "Workload Protection Details" on page 46.

You can use the following methods to perform a failover:

- Selecting the required workload on the Workloads page and clicking *Run Failover*. You can use the optional *Prepare for Failover* command for applying your saved failover settings to the recovery workload and booting it in advance of a full failover. Consider a separate *Prepare for Failover* operation to make sure that your production workload has indeed failed. This saves time when running a full *Failover* command.
- Clicking the appropriate command hyperlink of the *Workload is offline* event in the Tasks and Events pane. See [Figure 4-1](#).
- Manually booting the recovery workload by using the VMware vSphere Client. When using this method, use the vSphere Client's Snapshot Manager to select a snapshot (a recovery point). See your VMware documentation.

NOTE: When performing a failover manually, the system applies failover settings as saved upon the workload's replication.

Use one of these methods to start the failover process and select a recovery point to apply to the recovery workload (see "[Recovery Points](#)" on page 76). Click *Execute* and monitor the progress. Upon completion, the replication status of the workload should indicate *Live*.

For testing the recovery workload or testing the failover process as part of a planned disaster recovery exercise, see "[Testing the Recovery Workload and the Failover Functionality](#)" on page 50.

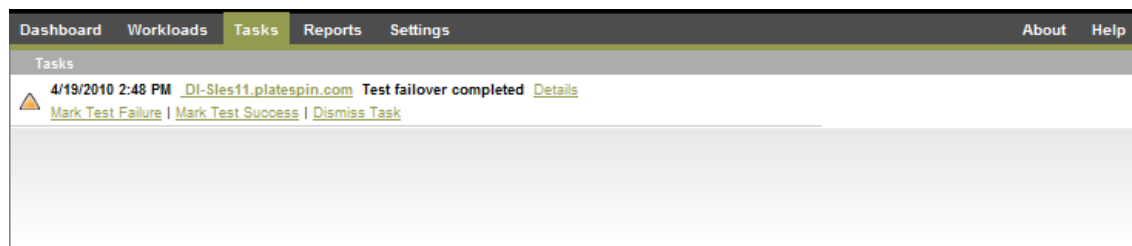
4.5.3 Testing the Recovery Workload and the Failover Functionality

PlateSpin Protect provides you with the capability to test the failover functionality and the integrity of the recovery workload. This is done by using the *Test Failover* command, which boots the recovery workload in a restricted network environment for testing.

When you execute the command, PlateSpin Protect applies the Test Failover Settings, as saved in the workload protection details, to the recovery workload (see the [Test Failover](#) row in "Workload Protection Details" on page 46).

- 1 Define an appropriate time window for testing and make sure that there are no replications underway. The replication status of the workload must be *Idle*.
- 2 On the Workloads page, select the required workload, click *Test Failover*, select a recovery point (see "[Recovery Points](#)" on page 76), and then click *Execute*.

Upon completion, PlateSpin Protect generates a corresponding event and a task with a set of applicable commands:



- 3 Verify the integrity and business functionality of the recovery workload. Use the VMware vSphere Client to access the recovery workload in the VM container.
- 4 Mark the test as a failure or a success. Use the corresponding commands in the task (*Mark Test Failure*, *Mark Test Success*). The selected action is saved in the history of events associated with the workload. *Dismiss Task* discards the task and the event.

Upon completion of the *Mark Test Failure* or *Mark Test Success* tasks, PlateSpin Protect discards temporary settings that were applied to the recovery workload, and the protection returns to its pre-test state.

4.6 Failback

A Failback operation is the next logical step after a failover; it transfers the failover workload to its original infrastructure or, if necessary, a new one.

Failback methods differ according to the target infrastructure type and the degree of automation of the failback process:

- ♦ **Automated Failback to a Virtual Machine:** Supported for VMware ESX platforms.
- ♦ **Semi-Automated Failback to a Physical Machine:** Supported for all physical machines.
- ♦ **Semi-Automated Failback to a Virtual Machine:** Supported for Xen on SLES and Microsoft Hyper-V platforms.

The following topics provide more information:

- ♦ [Section 4.6.1, “Automated Failback to a Virtual Machine,” on page 51](#)
- ♦ [Section 4.6.2, “Semi-Automated Failback to a Physical Machine,” on page 54](#)
- ♦ [Section 4.6.3, “Semi-Automated Failback to a Virtual Machine,” on page 54](#)

4.6.1 Automated Failback to a Virtual Machine

The following containers are supported as automated failback targets:

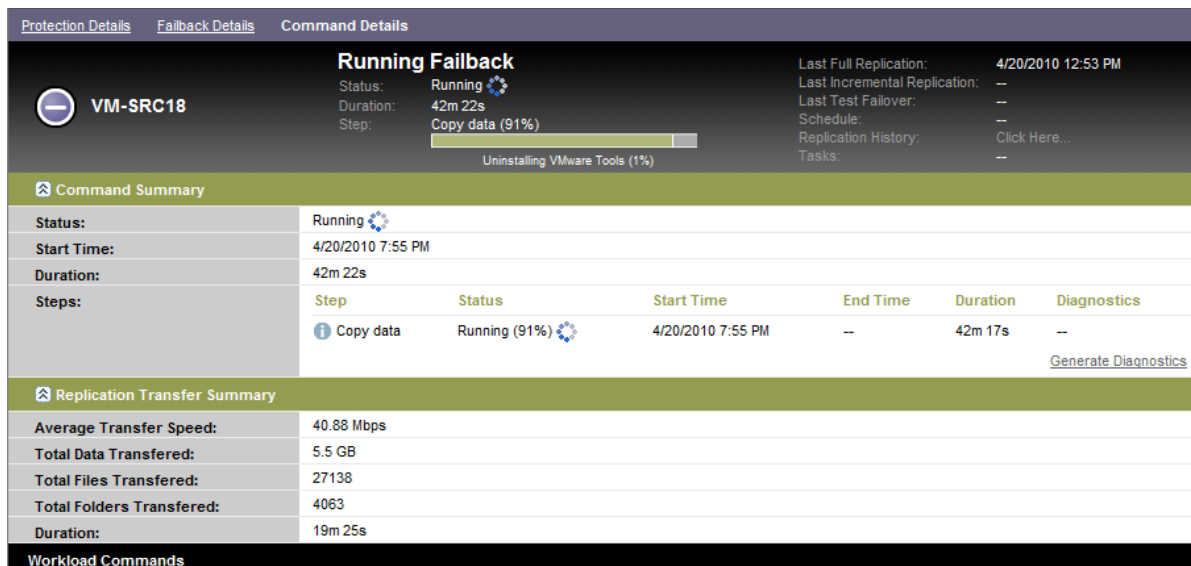
Platform	Notes
VMware DRS Cluster in vSphere 4.1	<ul style="list-style-type: none"> ♦ The DRS configuration must be either Partially Automated or Fully Automated (it must not be set to Manual) ♦ The Cluster can use ESX 4.1, ESXi 4.1, or both
VMware ESX 3.5, 4.0, 4.1, 4.1 Update 1	
VMware ESXi 3.5, 4.0, 4.1, 4.1 Update 1	All ESXi versions must have a paid license; protection is unsupported with these systems if they are operating with a free license.

Use these steps to do an automated failback of a failover workload to a target VMware container.

- 1 Following a failover, select the workload on the Workloads page and click *Failback / Deploy*.
- 2 Specify the following sets of parameters:
 - ♦ **Workload Settings:** Specify the recovery workload’s hostname or IP address and provide admin-level credentials. Use the required credential format (see [“Guidelines for Workload and Container Credentials” on page 73](#)).

- ♦ **Failback Target Settings:** Specify the the following parameters:
 - ♦ **Replication Method:** Select the scope of data replication. If you select *Incremental*, you must prepare a target. See [“Initial Replication Method \(Full and Incremental\)”](#) on page 76.
 - ♦ **Target Type:** Select *Virtual Target*. If you don’t yet have a failback container, click *Add Container* and inventory a supported VM host using root-level credentials.
- 3 Click *Save and Prepare* and monitor the progress on the Command Details screen.
 Upon successful completion, PlateSpin Protect loads the Ready for Failback screen, prompting you to specify the details of the failback operation.
- 4 Configure the failback details. See [“Failback Details \(Workload to VM\)”](#) on page 53.
- 5 Click *Save and Failback* and monitor the progress on the Command Details page. See [Figure 4-2](#).
 PlateSpin Protect executes the command. If you selected *Reprotect after Failback* in the Post-Failback parameter set, a *Reprotect* command is shown in the PlateSpin Protect Web Client.

Figure 4-2 Failback Command Details



Failback Details (Workload to VM)

Failback details are represented by three sets of parameters that you configure when you are performing a workload failback operation to a virtual machine.

Table 4-2 Failback Details (VM)

Parameter Set (Settings)	Details
Failback	<p>Transfer Method: (Windows) Enables you to select a data transfer mechanism and security through encryption. See “Transfer Methods” on page 74.</p> <p>Failback Network: Enables you to direct failback traffic over a dedicated network based on virtual networks defined on your VM container. See “Networking” on page 80.</p> <p>VM Datastore: Enables you to select a datastore associated with your failback container for the target workload.</p> <p>Volumes to Copy: Enables you to select the volumes for re-creating on the target and assigning to a specific datastore.</p> <p>Services/Daemons to stop: Enables you to select Windows services or Linux daemons that are automatically stopped during the failback. See “Service and Daemon Control” on page 77.</p> <p>Alternative Address for Source: Accepts input of an additional IP address for the source workload if applicable. See “Protection Across Public and Private Networks Through NAT” on page 23.</p>
Workload	<p>Number of CPUs: Enables you to specify the required number of vCPUs assigned to the target workload.</p> <p>VM Memory: Enables you to assign the required RAM to the target workload .</p> <p>Hostname, Domain/Workgroup: Use these options to control the identity and domain/workgroup affiliation of the target workload. For domain affiliation, domain admin credentials are required.</p> <p>Network Connections: Use these options to specify the network mapping of the target workload based on the virtual networks of the underlying VM container.</p> <p>Service States to Change: Enables you to control the startup state of specific application services (Windows) or daemons (Linux). See “Service and Daemon Control” on page 77.</p>
Post-Failback	<p>Reprotect Workload: Use this option if you plan to re-create the protection contract for the target workload after deployment. This maintains a continuous event history for the workload and auto-assigns/designates a workload license.</p> <ul style="list-style-type: none">♦ Reprotect after Failback: Select this option if you intend to re-create a protection contract for the target workload.♦ No reprotect: Select this option if you don’t intend to re-create a protection contract for the target workload.

4.6.2 Semi-Automated Failback to a Physical Machine

Use these steps to fail a workload back to a physical machine after a failover. The physical machine might be either the original infrastructure or a new one.

- 1 Register the required physical machine with your PlateSpin Protect Server. See [“Registering Physical Machines with PlateSpin Protect for Failback” on page 80](#).
- 2 (Optional: Windows platforms) Run the PS Analyzer tool to determine whether any drivers are missing. See [“Analyzing Workloads with PlateSpin Analyzer \(Windows\)” on page 67](#).
- 3 If the PS Analyzer reports missing or incompatible drivers, upload the required drivers to the PlateSpin Protect device driver database. See [“Managing Device Drivers” on page 68](#).
- 4 Following a failover, select the workload on the Workloads page and click *Failback / Deploy*.
- 5 Specify the following sets of parameters:
 - ♦ **Workload Settings:** Specify the recovery workload’s hostname or IP address and provide admin-level credentials. Use the required credential format (see [“Guidelines for Workload and Container Credentials” on page 73](#)).
 - ♦ **Failback Target Settings:** Specify the following parameters:
 - ♦ **Replication Method:** Select the scope of data replication.
See [“Initial Replication Method \(Full and Incremental\)” on page 76](#).
 - ♦ **Target Type:** Select the *Physical Target* option and then select the physical machine you registered in [Step 1](#).
- 6 Click *Save and Prepare* and monitor the progress on the Command Details screen.
Upon successful completion, PlateSpin Protect loads the Ready for Failback screen, prompting you to specify the details of the failback operation.
- 7 Configure the failback details, then click *Save and Failback*.
Monitor the progress on the Command Details screen.

4.6.3 Semi-Automated Failback to a Virtual Machine

This failback type follows a process similar to the [Semi-Automated Failback to a Physical Machine](#) for a VM target other than a natively-supported VMware container. During this process, you direct the system to regard a VM target as a physical machine.

A semi-automated failback to a VM is supported for the following target VM platforms:

- ♦ Xen on SLES 10, 11
- ♦ Microsoft Hyper-V

4.7 Advanced Workload Protection Topics

- ♦ [Section 4.7.1, “Protecting Windows Clusters,” on page 55](#)
- ♦ [Section 4.7.2, “Linux Failback to a Paravirtualized VM on Xen-on-SLES,” on page 55](#)

4.7.1 Protecting Windows Clusters

PlateSpin Protect supports the protection of a Microsoft Windows cluster's business services. The supported clustering technologies are:

- ♦ Windows 2003 Server-based Windows Cluster Server (*Single-Quorum Device Cluster* model)
- ♦ Windows 2008 Server-based Microsoft Failover Cluster (*Node and Disk Majority* and *No Majority: Disk Only* models)

Protection of a cluster is achieved through incremental replications of changes on the active node streamed to a virtual single-node cluster, which you can use while troubleshooting the source infrastructure.

The scope of support for cluster migrations in the current release is subject to the following conditions:

- ♦ When you perform an *Add Workload* operation, you must identify the active node—the node that currently owns the quorum resource of the cluster—identified by the cluster's IP address (*virtual IP address*). Specifying the IP address of an individual node results in that node being inventoried as a regular, cluster-unaware Windows workload.
- ♦ A cluster's quorum resource must be collocated with the cluster's resource group (service) being protected.

If a node failover occurs between incremental replications of a protected cluster, PlateSpin Protect generates a protection event. If the new active node's profile is similar to the failed active node, the protection schedule continues; otherwise, the command fails. The profiles of cluster nodes are considered similar if:

- ♦ They have the same number of volumes
- ♦ Each volume is exactly the same size on each node
- ♦ They have an identical number of network connections

To protect a Windows cluster, follow the normal workload protection workflow (see [“Basic Workflow for Workload Protection and Recovery” on page 43](#)).

On failback, PlateSpin Protect provides validation that helps you ensure that shared volume layouts are preserved on the target. Make sure you map the volumes correctly.

4.7.2 Linux Failback to a Paravirtualized VM on Xen-on-SLES

You can do a failback to a paravirtualized VM on Xen-on-SLES (version 10 only). This is done indirectly, through a two-stage process. The paravirtualized VM needs to be transformed into a fully virtualized VM first and later transformed back. A utility (`xmps`), included in your PlateSpin boot ISO image, is used to transform the VM.

The procedure varies slightly, depending on whether the target is a new or an existing paravirtualized VM.

- ♦ [“Linux Failback to a New Paravirtualized VM” on page 56](#)
- ♦ [“Linux Failback to an Existing Paravirtualized VM” on page 57](#)

Linux Failback to a New Paravirtualized VM

- 1 Copy the PlateSpin Linux boot ISO to the target Xen/SLES server. See [Table 7-2, “ISO Boot Images for Target Physical Machines,”](#) on page 80.
- 2 Start the Virtual Machine manager and create a fully virtualized VM:
 - 2a Select the *I need to install an operating system* option.
 - 2b Choose a suitable size for the disk image (the disk size should be equal to or bigger than that of the source machine).
 - 2c Select the boot ISO as the installation source.

The VM boots into the PlateSpin OS environment, used in *failback to physical machine* settings.

- 3 Complete the failback procedure. See [“Semi-Automated Failback to a Physical Machine”](#) on page 54.

Upon completion, the VM should be fully functional as a fully virtualized machine.

- 4 Reboot the VM, making sure that it still boots into the PlateSpin OS environment.

```
Available boot options (type the name to boot into):

ps          - PlateSpin Linux for Taking Control (press ENTER to boot into)
ps64        - PlateSpin Linux(x86_64) for Taking Control
ps64_512m   - PlateSpin Linux(x86_64) for Taking Control a Virtual Machine
              which has more than 512M memory
next        - Boot from Next Boot Device Set in BIOS (timeout)
debug       - PlateSpin Linux for Trouble Shooting
switch      - PlateSpin Linux for switching kernel to Xen PV

When no key is pressed for 20 seconds, it will boot from the next boot device.

boot: switch_
```

- 5 At the boot : prompt, type switch and press Enter.

This reconfigures the operating system to be bootable as a paravirtualized machine. Upon completion, the output should look similar to the one shown below:

```
about to find other volumes in native off-line OS
kjournal starting. Commit interval 5 seconds
EXT3-fs: mounted filesystem with ordered data mode.
found volume /boot in off-line OS
found other 1 volume(s)
mount all the system volumes
kjournal starting. Commit interval 5 seconds
EXT3 FS on hda1, internal journal
EXT3-fs: mounted filesystem with ordered data mode.
volume /boot has been mounted.
all the system volumes are mounted
Switching to Xen kernel for Para-virt machine....
unmount all the system volumes for clean up.
volume /boot has been unmounted
volume / has been unmounted

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

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

#####

[DB1]$ _
```


Note the bootloader arguments in the final segment of the output:

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

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

These are used by the `xmps` utility to set up the location of the kernel and the `initrd` image, from which the paravirtualized machine boots from.

6 Power off the virtual machine:

```
[DB]$ poweroff
```

7 Login to the XEN/SLES server as `root` and mount the PlateSpin Linux boot ISO (the command example assumes that the ISO has been copied under the `/root` directory):

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

8 Run the `xmps` utility to create a paravirtualized VM based on the configuration of the fully virtualized VM:

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

The utility takes as input:

- ♦ The name of the fully virtualized VM on which the configuration of the paravirtualized machine will be based (SLES10-FV)
- ♦ The name of the virtual machine to create (SLES10-PV)
- ♦ The paravirtualized machine's bootloader arguments `--bootloader_args` (shown at [Step 5](#))

If a VM with the same name as the one passed as `new_vm_name` already exists, the `xmps` utility fails.

The newly created paravirtualized VM (SLES10-PV) should now be available in the Virtual Machine Manager, ready to be turned on. The corresponding fully virtualized machine is retired and will fail to boot. This VM can be deleted safely (only the VM configuration will be removed).

9 Unmount the PlateSpin Linux boot ISO:

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

Linux Failback to an Existing Paravirtualized VM

1 Copy the PlateSpin Linux boot ISO to the target Xen/SLES server. See [Table 7-2, “ISO Boot Images for Target Physical Machines,”](#) on page 80.

2 Log in to the XEN/SLES server as `root` and mount the PlateSpin Linux boot ISO:

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

3 Run the `xmps` utility to create a fully virtualized VM based on the configuration of the paravirtualized VM (the intended failback target):

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

The utility takes as input:

- ♦ The name of the existing paravirtualized machine (SLES10-PV), which is the intended failback target

- ♦ The name of the temporary fully virtualized machine (SLES10-FV) to be created for the two-stage failback operation
- ♦ The full path of the boot ISO (assuming that the ISO file is located under `/root: /root/booxofxx2p.iso`)

If a VM with the same name as the one passed as `new_vm_name` already exists, the `xmps` utility fails.

The newly created fully virtualized machine (SLES10-FV) should now be available in the Virtual Machine Manager.

- 4 Turn on the newly created fully virtualized machine (SLES10-FV).

The VM boots into the PlateSpin OS environment, used in *failback to physical machine* settings.

- 5 Complete the failback procedure. See [“Semi-Automated Failback to a Physical Machine” on page 54](#).
- 6 Reboot the VM, run `switch`, and reconfigure the workload as described in [“Linux Failback to a New Paravirtualized VM” on page 56](#) (from [Step 4](#) to [Step 9](#) only).

5 Workload Image Protection

Imaging is one of the two workload protection infrastructures of PlateSpin Protect. For information about the virtualization infrastructure, see [“Workload Protection” on page 43](#).

A PlateSpin Image is a static stored copy of the state of a physical or virtual machine (including volume data and the configuration details of the workload’s hardware profile, operating system, and network identity), captured at a specific point in time and regularly updated at intervals you specify in the workload’s protection settings.

Upon failure of the protected workload, you can deploy the captured image to run on physical hardware or in a VM host.

Similar to workload protection functionality with virtualization, image deployment allows for key workload configuration options, such as those for managing the workload’s disk layout, volume sizes, network identity, and domain or workgroup affiliation.

- [Section 5.1, “Protecting a Workload Image,” on page 59](#)
- [Section 5.2, “Deploying a Workload Image,” on page 60](#)
- [Section 5.3, “Browsing and Extracting Image Files,” on page 63](#)

5.1 Protecting a Workload Image

This section provides information about workload image protection.


- [Section 5.1.1, “Adding a Workload for Image Protection,” on page 59](#)
- [Section 5.1.2, “Configuring Workload Image Protection Details,” on page 60](#)

5.1.1 Adding a Workload for Image Protection

Protecting a workload image captures the specified workload’s volume data in PlateSpin Flexible Image format and establishes an ongoing protection of the image through incremental updates at specified intervals.

- 1 Make sure your workload is supported for image protection.
See [“Supported Workloads in Image Containers” on page 11](#).
- 2 Add an Image Container.
See [“Adding Containers” on page 39](#).
- 3 In the PlateSpin Protect Web Client, click *Add Workload*.
- 4 Specify the required information about the workload.
See [“Guidelines for Workload and Container Credentials” on page 73](#).
- 5 Select the required image server as the protection target.


- 6 Click *Add Workload*.

PlateSpin Protect reloads the Workloads page and displays a process indicator for the workload being added . Wait for the process to complete. Upon completion, a *Workload Added* event is shown on the Dashboard.

5.1.2 Configuring Workload Image Protection Details

Image protection settings determine how often a workload image is synchronized with changes on the workload's volumes, what transfer mechanism is used during replications, and which volumes of the workload are selected for protection.

- 1 Add a workload for image protection. See [“Adding a Workload for Image Protection” on page 59](#).
- 2 On the Workloads page, select the required workload and click *Configure*.
- 3 Configure the required Protection Tier settings. See [“Protection Tiers” on page 75](#).
- 4 Configure the image replication settings:
 - ♦ **Transfer Method and Encryption:** See [“Transfer Methods” on page 74](#).
 - ♦ **Source Credentials:** Specify admin-level credentials for the source workload. See [“Guidelines for Workload and Container Credentials” on page 73](#).
 - ♦ **Protected Volumes:** Select the volumes of the workload for which you require image protection.
 - ♦ **Datastore:** Select the datastore for workload image data.
 - ♦ **Services to Stop During Replication:** See [“Service and Daemon Control” on page 77](#).
- 5 Click *Save*.
- 6 To start the operation, click *Run Replication*, then confirm by clicking *Execute*.

PlateSpin Protect reloads the Workloads page and displays a process indicator for the workload being replicated .

5.2 Deploying a Workload Image

If a workload with a protected image fails, you can deploy the protected image that is stored on your image server as a bootable workload onto a physical or virtual infrastructure. Criteria that determine and log a workload failure are part of a workload image protection contract's Tier settings (see [“Protection Tiers” on page 75](#)).

If notifications are configured along with SMTP settings, PlateSpin Protect simultaneously sends a notification e-mail to the specified recipients. See [“Setting Up Automatic E-Mail Notifications of Events and Reports” on page 26](#).

- ♦ [Section 5.2.1, “Deploying an Image to a Virtual Target,” on page 61](#)
- ♦ [Section 5.2.2, “Deploying an Image to a Physical Target,” on page 62](#)

5.2.1 Deploying an Image to a Virtual Target

Use this procedure to deploy an image as a bootable workload on a virtual machine.

- 1 Add a failback container. See [“Adding Containers” on page 39](#).
- 2 In your PlateSpin Protect Web Client, select the required workload, then click *Failback / Deploy*. Select *Virtual* as the Target Type, and select your failback container as the target.
- 3 Click *Save and Prepare*. When you are prompted, specify the complete parameters for the operation:

Parameter Set (Settings)	Details
Deployment	<p>Transfer Method: (Windows) Enables you to select a data transfer mechanism and security through encryption. See “Transfer Methods” on page 74.</p> <p>Failback Network: Enables you to direct failback traffic over a dedicated network based on virtual networks defined on your VM container. See “Networking” on page 80.</p> <p>VM Datastore: Enables you to select a datastore associated with your failback container for the target workload.</p> <p>Volumes to Copy: Enables you to select the protected volumes for deployment on the selected target and to assign them to specific datastores.</p>
Workload	<p>Number of CPUs: Enables you to specify the required number of vCPUs assigned to the target workload.</p> <p>VM Memory: Enables you to assign the required RAM to the target workload.</p> <p>Hostname, Domain/Workgroup: Use these options to control the identity and domain/workgroup affiliation of the target workload. For domain affiliation, domain admin credentials are required.</p> <p>Network Connections: Use these options to specify the network mapping of the target workload based on the virtual networks of the underlying VM container.</p> <p>Service States to Change: Enables you to control the startup state of specific application services. See “Service and Daemon Control” on page 77.</p>
Post-Failback	<p>Reprotect Workload: Use this option if you plan to re-create the image protection contract for the target workload after deployment. This maintains a continuous event history for the workload.</p> <ul style="list-style-type: none">♦ <i>Turn off Deployed Workload:</i> If this option is selected, the target VM is powered off upon completion of the deployment.

- 4 Click *Run Deployment* and monitor the progress.
Upon completion, PlateSpin Protect reports the status of the command as *Deployment completed*.
- 5 Access the target target physical machine and verify its functionality and integrity.

Deployment Details (Image to VM)

Deployment details are represented by three sets of parameters that you configure when you are performing a workload image deployment to a virtual machine.

5.2.2 Deploying an Image to a Physical Target

Use this procedure to deploy an image as a bootable workload on a physical machine.

- 1 Register the required physical machine with your PlateSpin Protect Server.
See [“Registering Physical Machines with PlateSpin Protect for Failback” on page 80](#).
- 2 Run the PlateSpin Analyzer tool to determine whether any drivers are missing.
See [“Analyzing Workloads with PlateSpin Analyzer \(Windows\)” on page 67](#).
- 3 If the PlateSpin Analyzer reports missing or incompatible drivers, upload the required drivers to the PlateSpin Protect device driver database.
See [“Managing Device Drivers” on page 68](#).
- 4 In your PlateSpin Protect Web Client, select the required workload, then click *Failback / Deploy*. Select *Physical* as the Target Type, and select your physical machine as the target.
- 5 Click *Save and Prepare*. When you are prompted, specify the complete parameters for the operation:

Parameter Set (Settings)	Details
Failback	<p>Transfer Method: (Windows) Enables you to select a data transfer mechanism and security through encryption. See “Transfer Methods” on page 74.</p> <p>Volumes to Copy: Enables you to select the protected volumes for deployment on the selected target.</p>
Workload	<p>Hostname, Domain/Workgroup: Use these options to control the identity and domain/workgroup affiliation of the target workload. For domain affiliation, domain admin credentials are required.</p> <p>Network Connections: Use these options to specify the LAN settings of the target workload.</p> <p>Service States to Change: Enables you to control the startup state of specific application services. See “Service and Daemon Control” on page 77.</p> <p>Partitions to Preserve: Enables you to preserve any existing partitions on the target.</p> <p>Service States to Change: Enables you to control the startup state of specific application services. See “Service and Daemon Control” on page 77.</p>
Post-Failback	<p>Reprotect Workload: Use this option if you plan to re-create the image protection contract for the target workload after deployment. This maintains a continuous event history for the workload.</p> <ul style="list-style-type: none">♦ Turn off Deployed Workload: If this option is selected, the target VM is powered off upon completion of the deployment.

- 6 Click *Run Deployment* and monitor the progress.
Upon completion, PlateSpin Protect reports the status of the command as *Deployment completed*.
- 7 Access the target physical machine and verify its functionality and integrity.

Deployment Details (Image to Physical)

Deployment details are represented by three sets of parameters that you configure when you are performing a workload image deployment to a physical machine.

5.3 Browsing and Extracting Image Files

During a disaster recovery effort or a business continuity exercise you can selectively restore files in your workload's file system by using backup versions of those files that are stored in images.

To do this, you can use the Image Browser utility, which enables you to browse, search, sort, and extract files from an image file or a specific image increment file.

You can work with both base images and image increments by loading either of the following:

- ♦ A base image's corresponding binary file (*volume-x.pkg*) or text configuration file (*image_name.xml*).
- ♦ An image increment's binary (*image_increment.pkg*) file. You cannot use an increment's text configuration file (*image_increment_name.xml*).

The utility enables you to work with image files in a Windows Explorer-like environment. A command line version enables you to extract files at the command line.

- ♦ [Section 5.3.1, "Starting the Image Browser and Loading Image Files," on page 63](#)
- ♦ [Section 5.3.2, "Sorting and Searching Items in the Image Browser Interface," on page 64](#)
- ♦ [Section 5.3.3, "Extracting Items from an Image," on page 65](#)
- ♦ [Section 5.3.4, "Browsing and Extracting Image Files at the Command Line," on page 65](#)

5.3.1 Starting the Image Browser and Loading Image Files

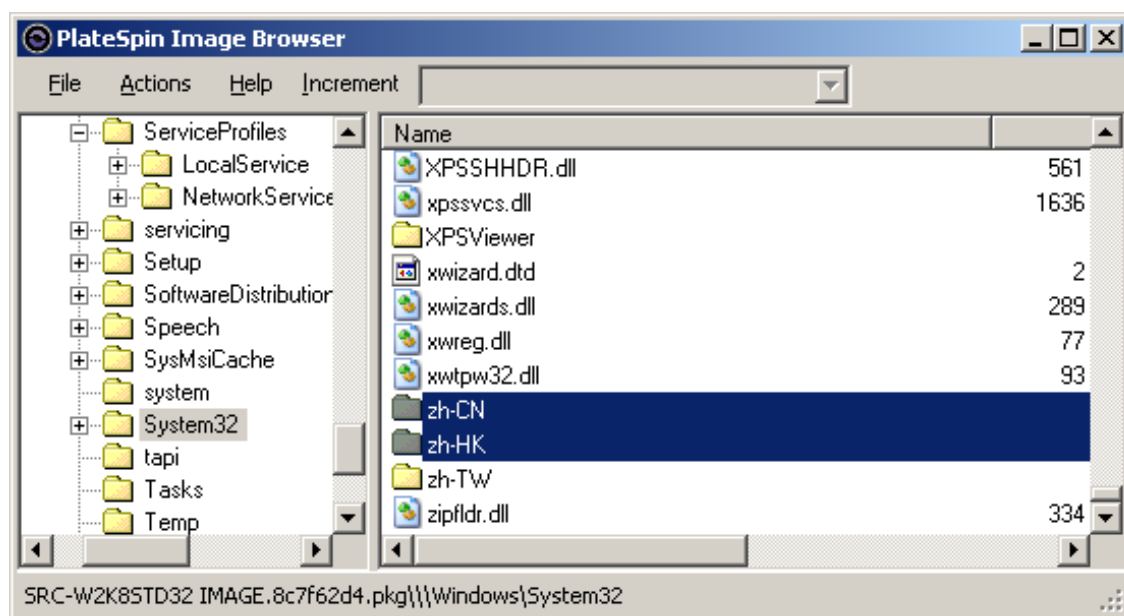
- 1 Start the Image Browser program (*ImageBrowser.exe*), which is located on your image server host, in the following directory:

`\Program Files\PlateSpin Image Server\ImageOperations`

The utility starts and displays the Open dialog box. At any time after the program's initial startup, you can load an image file by clicking *File > Open*.

- 2 In the Open dialog box, select the file type, navigate to and select the required image or image increment file, then click *OK*.

The utility loads the required file and displays its contents in a two-pane interface.



Depending on the size of the image, it might take a few seconds to several minutes for the utility to load the required file.

5.3.2 Sorting and Searching Items in the Image Browser Interface

You can sort the contents of a selected directory by name, size, type, date last modified, and by file attribute. To sort items in a selected view, click the corresponding bar at the top of the right pane.

You can search for a specific directory name or filename. You can use alphanumeric text, wildcards, and regular expressions. Regular expression search patterns that you specify must adhere to the Microsoft .NET Framework regular expression syntax requirements. See the [Microsoft .NET Framework Regular Expressions page on MSDN \(http://msdn.microsoft.com/en-us/library/hs600312.aspx\)](http://msdn.microsoft.com/en-us/library/hs600312.aspx).

To search for an item:

- 1 Load the required image or image increment.
- 2 In the left pane, select a volume or a subdirectory.
- 3 On the *Actions* menu, click *Search*.

Alternately, you can right-click the required volume or subdirectory in the left pane and click *Search* in the context menu.

The Image Browser Search window opens.

- 4 Specify the name of the file you are searching. If you are using a regular expression, select the corresponding option.
- 5 Click *Search*.

The results are shown in the right pane.

5.3.3 Extracting Items from an Image

- 1 Load the required image or image increment.
- 2 Locate and select the required file or directory. You can select multiple files and directories in the right pane.
- 3 On the *Actions* menu, click *Extract*.
Alternately, you can right-click the required item and click *Extract* in the context menu.
The Browse for Folder dialog box opens.
- 4 Browse to the required destination, then click *OK*.
The selected items are extracted to the specified destination.

NOTE: Files that you choose to overwrite are deleted if you interrupt the extraction process.

5.3.4 Browsing and Extracting Image Files at the Command Line

To browse and extract files from images and image increments at the command line, you can use the `ImageBrowser.Console` utility.

To start the utility:

- 1 On your Flexible Image Server host, open a command interpreter (`cmd.exe`) and change the current directory to `\Program Files\PlateSpin Image Server\ImageOperations`.
- 2 At the command prompt, type `ImageBrowser.Console`, then press Enter.
For command syntax and usage details, type `ImageBrowser.Console /help`, then press Enter.

6 Auxiliary Tools for Working with Physical Machines

Your PlateSpin Protect distribution includes tools for use when working with physical machines as failback or image deployment targets.

- ♦ [Section 6.1, “Analyzing Workloads with PlateSpin Analyzer \(Windows\),” on page 67](#)
- ♦ [Section 6.2, “Managing Device Drivers,” on page 68](#)

6.1 Analyzing Workloads with PlateSpin Analyzer (Windows)

Before running a workload failback or image deployment operation to a physical machine, use the PlateSpin Analyzer to identify potential driver problems and correct them beforehand.

NOTE: PlateSpin Analyzer currently supports only Windows workloads.

- 1 On your PlateSpin Protect Server host, start the `Analyzer.Client.exe` program, located in the following directory:
`\Program Files\PlateSpin Protect Server\PlateSpin Analyzer`
- 2 Make sure that the network selection is *Default*, then select the required machine in the *All Machines* drop-down list.
- 3 (Optional) To reduce the analysis time, limit the scope of machines to a specific language.
- 4 Click *Analyze*.

Depending on the number of inventoried workloads you select, the analysis might take a few seconds to several minutes.

Analyzed servers are listed in the left pane. Select a server to view test results in the right pane. Test results can be any combination of the following:

Table 6-1 *Status Messages in PlateSpin Analyzer Test Results*

Result	Description
Passed	The machine passed the PlateSpin Analyzer tests.
Warning	One or more tests returned warnings for the machine, indicating potential migration issues. Click the hostname to see the details.
Failed	One or more tests failed for this machine. Click the hostname to see the details and obtain more information.

The *Summary* tab provides a listing of the number of machines analyzed and not checked, as well as those that passed the test, failed the test, or were assigned a warning status.

The *Test Results* tab provides the following information:

Table 6-2 *PlateSpin Analyzer Test Results Tab*

Section	Details
<i>System Test</i>	Validates that the machine fulfills minimum hardware and operating system requirements.
<i>Hardware Support</i>	Checks the workload for hardware compatibility.
<i>Target Hardware Support</i>	Checks hardware compatibility for use as a target physical machine.
<i>Software Test</i>	Checks for applications that must be shut down for Live Transfer, and databases that should be shut down during Live Transfer to guarantee transactional integrity.
<i>Incompatible Application Test</i>	Verifies that applications known to interfere with the migration process are not installed on the system. These applications are stored in the Incompatible Application Database. To add, delete or edit entries in this database, select <i>Incompatible Application</i> from the <i>Tools</i> menu.

The *Properties* tab provides detailed information about a selected machine.

6.2 Managing Device Drivers

PlateSpin Protect ships with a library of device drivers and automatically installs the appropriate ones on target workloads. To determine if the required drivers are available, use the PlateSpin Analyzer utility. See [“Analyzing Workloads with PlateSpin Analyzer \(Windows\)” on page 67](#).

If PlateSpin Analyzer encounters missing or incompatible drivers, or if you require specific drivers for a target infrastructure, you might need to add (upload) drivers to the PlateSpin Protect driver database.

- ♦ [Section 6.2.1, “Packaging Device Drivers for Windows Systems,” on page 68](#)
- ♦ [Section 6.2.2, “Packaging Device Drivers for Linux Systems,” on page 69](#)
- ♦ [Section 6.2.3, “Uploading Drivers to the PlateSpin Protect Device Driver Database,” on page 69](#)

6.2.1 Packaging Device Drivers for Windows Systems

To package your Windows device drivers for uploading to the PlateSpin Protect driver database:

- 1 Prepare all interdependent driver files (*.sys, *.inf, *.dll, etc.) for your target infrastructure and device. If you have obtained manufacturer-specific drivers as a .zip archive or an executable, extract them first.
- 2 Save the driver files in separate folders, with one folder per device.

The drivers are now ready for upload. See [“Uploading Drivers to the PlateSpin Protect Device Driver Database” on page 69](#).

NOTE: For problem-free operation of your protection job and the target workload, upload only digitally signed drivers for:

- ♦ All 64-bit Windows systems
 - ♦ 32-bit versions of Windows Vista and Windows Server 2008, and Windows 7 systems
-

6.2.2 Packaging Device Drivers for Linux Systems

To package your Linux device drivers for uploading to the PlateSpin Protect driver database, you can use a custom utility included in your Linux Take Control ISO boot image. See [Table 7-2, “ISO Boot Images for Target Physical Machines,” on page 80](#).

- 1 On a Linux workstation, create a directory for your device driver files. All the drivers in the directory must be for the same kernel and architecture.
- 2 Download the boot image and mount it.

For example, assuming that the ISO has been copied under the `/root` directory, issue these commands:

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

- 3 From the `/tools` subdirectory of the mounted ISO image, copy the `packageModules.tar.gz` archive into a another working directory and extract it.

For example, with the `.gz` file is inside your current working directory, issue this command:

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

- 4 Enter the working directory and execute the following command:

```
./PackageModules.sh -d <path_to_driver_dir> -o <package name>
```

Replace `<path_to_driver_dir>` with the actual path to the directory where you saved you driver files, and `<package name>` with the actual package name, using the following format:

```
Drivername-driverversion-dist-kernelversion-arch.pkg
```

For example, `bnx2x-1.48.107-RHEL4-2.6.9-11.EL-i686.pkg`

The package is now ready for uploading. See [“Uploading Drivers to the PlateSpin Protect Device Driver Database” on page 69](#).

6.2.3 Uploading Drivers to the PlateSpin Protect Device Driver Database

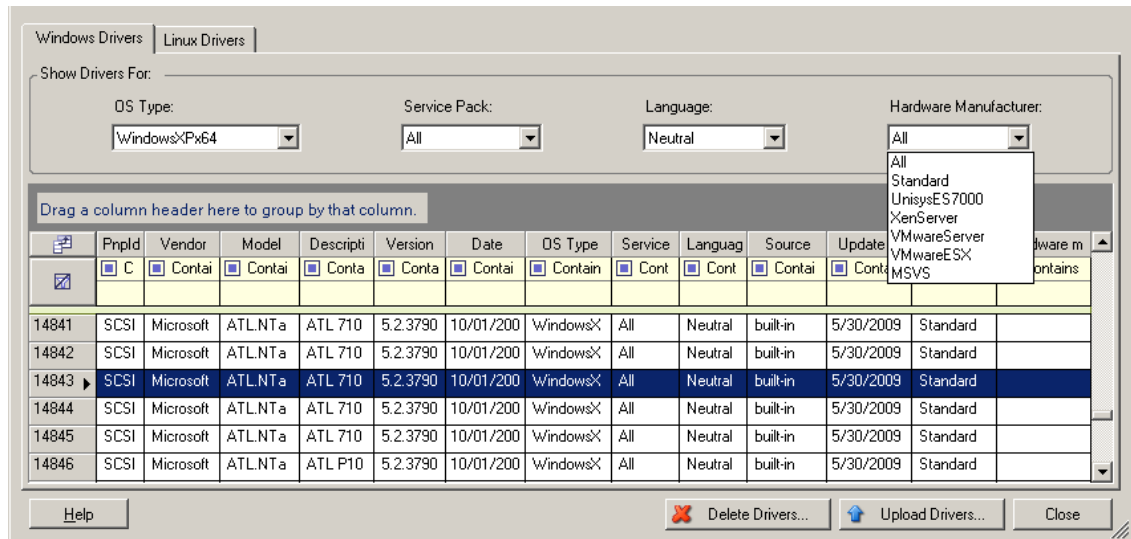
Use the PlateSpin Driver Manager to upload device drivers to the driver database.

NOTE: On upload, PlateSpin Protect does not validate drivers against selected operating system types or their bit specifications; make sure that you only upload drivers that are appropriate for your target infrastructure.

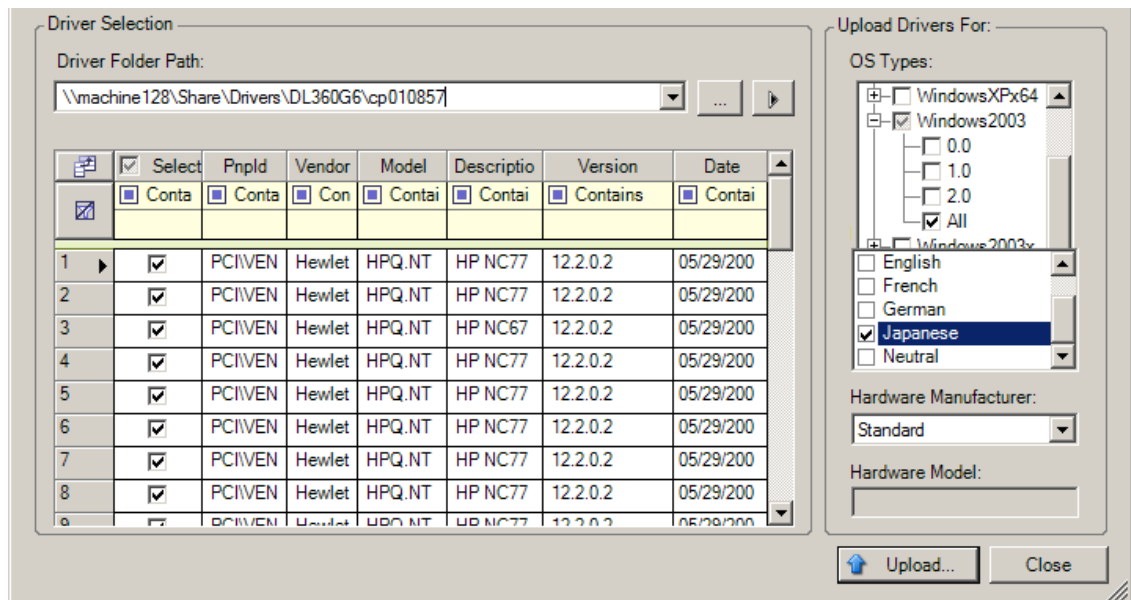
- ♦ [“Device Driver Upload Procedure \(Windows\)” on page 70](#)
- ♦ [“Device Driver Upload Procedure \(Linux\)” on page 71](#)

Device Driver Upload Procedure (Windows)

- 1 Obtain and prepare the required device drivers. See [Packaging Device Drivers for Windows Systems](#).
- 2 On your PlateSpin Protect Server host, under \Program Files\PlateSpin Protect Server\DriverManager, start the `DriverManager.exe` program and select the *Windows Drivers* tab.



- 3 Click *Upload Drivers*, browse to the folder that contains the required driver files, and select applicable OS type, language, and hardware manufacturer options.

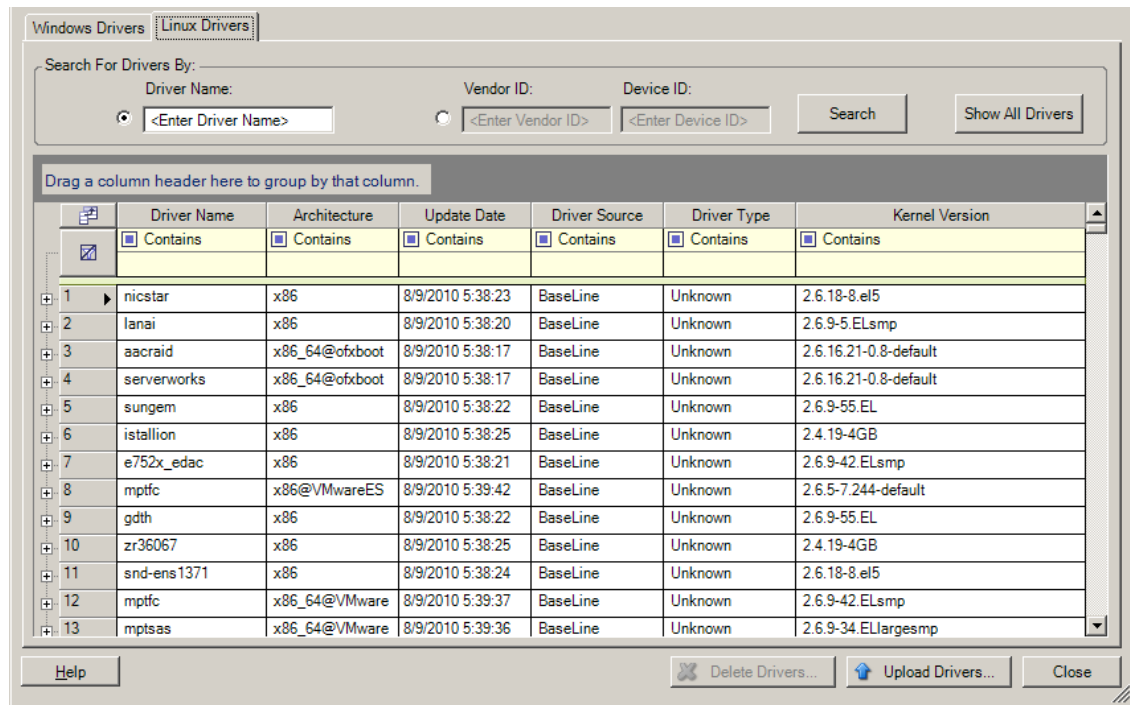


Select *Standard* as the *Hardware Manufacturer* option, unless your drivers are designed specifically for any of the target environments listed.

- Click *Upload* and confirm your selections when prompted.
The system uploads the selected drivers to the driver database.

Device Driver Upload Procedure (Linux)

- Obtain and prepare the required device drivers. See [Packaging Device Drivers for Linux Systems](#).
- Click *Tools > Manage Device Drivers* and select the *Linux Drivers* tab:



- Click *Upload Drivers*, browse to the folder that contains the required driver package (*.pkg), and click *Upload All Drivers*.
The system uploads the selected drivers to the driver database.

7 Essentials of Workload Protection

This section provides information about the different functional areas of a workload protection contract.

- ♦ Section 7.1, “Guidelines for Workload and Container Credentials,” on page 73
- ♦ Section 7.2, “Transfer Methods,” on page 74
- ♦ Section 7.3, “Protection Tiers,” on page 75
- ♦ Section 7.4, “Recovery Points,” on page 76
- ♦ Section 7.5, “Initial Replication Method (Full and Incremental),” on page 76
- ♦ Section 7.6, “Service and Daemon Control,” on page 77
- ♦ Section 7.7, “Using Freeze and Thaw Scripts for Every Replication (Linux),” on page 78
- ♦ Section 7.8, “Volumes,” on page 78
- ♦ Section 7.9, “Networking,” on page 80
- ♦ Section 7.10, “Registering Physical Machines with PlateSpin Protect for Failback,” on page 80

7.1 Guidelines for Workload and Container Credentials

PlateSpin Protect must have admin-level access to workloads and containers. Throughout the workload protection and recovery workflow, PlateSpin Protect prompts you to specify credentials that must be provided in a specific format.

Table 7-1 Workload and Container Credentials

To Discover	Credentials	Remarks
All Windows workloads Image Server Containers	Local or domain admin credentials.	For the username, use this format: <ul style="list-style-type: none">♦ For domain member machines: <i>authority\principal</i>♦ For workgroup member machines: <i>hostname\principal</i>
Windows Clusters	Domain admin credentials	Use the cluster's virtual IP address. If you use the IP address of an individual Windows cluster node, that node is discovered as a regular (cluster-unaware) Windows workload.
All Linux workloads	Root-level username and password	Non-root accounts must be properly configured to use <code>sudo</code> . See KB Article 7920711 (http://www.novell.com/support/viewContent.do?externalId=7920711) .

To Discover	Credentials	Remarks
VMware ESX hosts (4.0 and earlier)	ESX account with admin role.	
VMware ESX 4.1	ESX account with admin role.	If the ESX Server 4.1 is configured for Windows domain authentication, you can also use your Windows domain credentials.

7.2 Transfer Methods

A transfer method describes the way data is replicated from a source to a target. PlateSpin Protect provides different data transfer capabilities, which depend on the protected workload's operating system:

- ♦ **Block-level:** Data is replicated at a volume's block level. For this transfer method, PlateSpin Protect uses a driver to monitor changes on the source workload.
 - ♦ **Windows systems:** For Windows systems, PlateSpin Protect uses a block-based component that leverages the Microsoft Volume Snapshot Service (VSS) with applications and services that support VSS. The automatic installation of the block-based component requires a reboot of the source workload (no reboot is required when you are protecting Windows clusters with block-level data transfer). When you are configuring workload protection details, you can select the timing of the component's installation. Similarly, when removing a workload, uninstallation of the block-based component requires a reboot.

- ♦ **Linux systems:** For block-level transfer of Linux systems, PlateSpin Protect uses a block-level data transfer component that leverages LVM snapshots if available (this is the default and recommended option). See [KB Article 7005872](http://www.novell.com/support/viewContent.do?externalId=7005872) (<http://www.novell.com/support/viewContent.do?externalId=7005872>).

The Linux block-based component included in your PlateSpin Protect distribution is precompiled for the standard, non-debug kernels of the supported Linux distributions. If you have a non-standard, customized, or newer kernel, you can rebuild the block-based component for your specific kernel. See [KB Article 7005873](http://www.novell.com/support/viewContent.do?externalId=7005873) (<http://www.novell.com/support/viewContent.do?externalId=7005873>).

Deployment or removal of the component is transparent, has no continuity impact, and requires no intervention.

- ♦ **File-level:** Data is replicated on a file-by-file basis (Windows only). Supported with or without VSS.

In image protection and deployment operations, data is replicated at the file level without requiring explicit selection.

To make the transfer of workload data more secure, PlateSpin Protect enables you to encrypt data replication. When encryption is enabled, over-the-network data transfer from the source to the target is encrypted by using AES (Advanced Encryption Standard) or 3DES if FIPS-compliant encryption is enabled.

NOTE: Data encryption has a performance impact and might significantly slow down the data transfer.

7.3 Protection Tiers

A Protection Tier is a customizable collection of workload protection parameters that define the following:

- ♦ The frequency and recurrence pattern of replications
- ♦ Whether and how to apply data compression
- ♦ Whether to throttle available bandwidth to a specified throughput rate during data transfer
- ♦ Criteria for the system to consider a workload as failed

A Protection Tier is an integral part of every workload protection contract. During the configuration stage of a workload protection contract, you can select one of several built-in Protection Tiers and customize its attributes as required by that specific protection contract.

You can also create custom Protection Tiers in advance:

- 1 In your PlateSpin Protect Web Client, click *Settings > Protection Tiers > Create Protection Tier*.
- 2 Specify the parameters for the new Protection Tier:

Name	Type the name you want to use for the tier.
Incremental Recurrence	Specify the frequency of incremental replications and the incremental recurrence pattern. You can type directly in the <i>Start of recurrence</i> field, or click the calendar icon to select a date. Select <i>None</i> as the Recurrence Pattern to never use incremental replication.
Full Recurrence	Specify the frequency of full replications and the full recurrence pattern.
Blackout Window	<p>Use these settings to force a replication blackout (for suspending scheduled replications during peak utilization hours or to prevent conflicts between VSS-aware software and the PlateSpin VSS block-level data transfer component).</p> <p>To specify a blackout window, click <i>Edit</i>, then select a blackout recurrence pattern (daily, weekly, etc.), and the blackout period's start and end times.</p> <p>Note: At the start of a blackout window, the system aborts any replications that have not finished.</p>
Compression Level	<p>These settings control whether and how workload data is compressed before transmission. See "Data Compression" on page 13.</p> <p>Select one of the available options. <i>Fast</i> consumes the least CPU resources on the source but yields a lower compression ratio, <i>Maximum</i> consumes the most, but yields a higher compression ratio. <i>Optimal</i>, the middle ground, is the recommended option.</p>
Bandwidth Throttling	<p>These settings control bandwidth throttling. See "Bandwidth Throttling" on page 13.</p> <p>To throttle replications to a specified rate, specify the required throughput value in Mbps and indicate the time pattern.</p>
Recovery Points to Keep	Specify the number of recovery points to keep for workloads that use this Protection Tier. See "Recovery Points" on page 76 . A 0 value disables this feature.

Workload Failure	Specify the number of workload detection attempts before it is considered failed.
Workload Detection	Specify the time interval (in seconds) between workload detection attempts.

7.4 Recovery Points

A recovery point is a point-in-time snapshot of a workload or a workload image. It allows a replicated workload or a workload image to be restored to a specific state.

For each protected workload, you can keep up to 32 recovery points.

For each protected image, you can keep up to 100 recovery points.

Recovery points that accumulate over time might cause your PlateSpin Protect storage to run out of space.

7.5 Initial Replication Method (Full and Incremental)

In workload protection and failback operations, the Initial Replication parameter determines the scope of data transferred from a source to a target.

- ♦ **Full:** A full volume transfer takes place from a production workload to its replica (the recovery workload), or from a failover workload to its original virtual or physical infrastructure.
- ♦ **Incremental:** Only differences are transferred from a selected operation's source to its target, provided that they have a similar operating system and volume profile.
 - ♦ During protection: The production workload is compared with an existing VM in the VM container. The existing VM might be one of the following:
 - ♦ A previously-protected workload's recovery VM (when a *Remove Workload* command's *Delete VM* option is deselected).
 - ♦ A VM that is manually imported into the VM container, such as a workload VM physically moved on portable media from the production site to a remote recovery site (for VMware ESX 3.5 and later only).

For details, see your VMware documentation.
 - ♦ During failback to a virtual machine: The failover workload is compared with an existing VM in a failback container.
 - ♦ During failback to a physical machine: The failover workload is compared with a workload on the target physical machine, if the physical machine is registered with PlateSpin Protect (see [“Semi-Automated Failback to a Physical Machine”](#) on page 54).

During workload protection and failback to a VM host, selecting *Incremental* as the initial replication method requires that you browse, locate, and prepare the target VM for synchronization with the selected operation's source.

- 1 Proceed with the required workload command, such as *Add Workload* or *Failback*.
- 2 For the *Initial Replication Method* option, select *Incremental Replication*.
- 3 Click *Prepare Workload*.

The PlateSpin Protect Web Client displays the Prepare for Incremental Replication page.

Prepare for Incremental Replication

Container: comp212 (VMware ESX Server 4.0.0.175625)

Name	Description	CPU	Memory	Free Space	Last Refresh
comp212	VMware ESX Server 4.0.0.175625	16 x Intel(R) Xeon(R) CPU E5530 @ 2.40GHz	31.5 GB	1.9 TB	2 Day(s) ago

Virtual Machine: 1SLES10-P1.site_VM (SuSE Linux)

Inventory Network: VM Network

☒ DHCP ☐ Static

- 4 Select the required container, the virtual machine, and the inventory network to use for communicating with the VM.
- 5 Click *Prepare*.
Wait for the process to complete and for the user interface to return to the original command, then select the prepared workload.

NOTE: (Block-level data replications only) An initial incremental replication takes significantly longer than subsequent replications. This is because the system must compare the volumes on the source and the target block by block. Subsequent replications rely on data already polled by the block-based component while it is monitoring a source.

7.6 Service and Daemon Control

PlateSpin Protect enables you to control services and daemons:

- ♦ **Source service/daemon control:** During data transfer, you can automatically stop Windows services or Linux daemons that are running on your source workload. This ensures that the source workload is transferred to the recovery workload in a more consistent state than if you leave them running.

For example, for Windows workloads, consider stopping antivirus software services or services of third-party VSS-aware backup software.

For additional control of Linux sources during replication, consider the capability to run custom scripts on your Linux workloads during each replication. See [“Using Freeze and Thaw Scripts for Every Replication \(Linux\)”](#) on page 78.

- ♦ **Target startup state/run level control:** You can select the startup state (Windows) or the run level (Linux) of services/daemons on the target workload. When you perform a Failover or Test Failover operation, you can specify which services or daemons you want to be running or stopped when the failover workload has gone live.

Common services that you might want to assign a disabled startup state are vendor-specific services that are tied to their underlying physical infrastructure and are not required in a virtual machine.

7.7 Using Freeze and Thaw Scripts for Every Replication (Linux)

For Linux systems, PlateSpin Protect provides you with the capability to automatically execute custom scripts, *freeze* and *thaw*, that complement the automatic daemon control feature. *freeze* is executed at the beginning of a replication, and *thaw* is executed at the end of a replication.

Consider using this capability to complement the automated daemon control feature provided through the user interface (see [“Source service/daemon control:” on page 77](#)). For example, you might want to use this feature to temporarily freeze certain daemons instead of shutting them down during replications.

To implement the feature, use the following procedure before setting up your Linux workload protection:

1 Create the following files:

- ♦ `platespin.freeze.sh`: A shell script to execute at the beginning of the replication
- ♦ `platespin.thaw.sh`: A shell script to execute at the end of the replication
- ♦ `platespin.conf`: A text file defining any required arguments, along with a timeout value.

The required syntax for the contents of the `platespin.conf` file is:

```
[ServiceControl]
```

```
FreezeArguments=<arguments>
```

```
ThawArguments=<arguments>
```

```
TimeOut=<timeout>
```

Replace `<arguments>` with the required command arguments, separated by a space, and `<timeout>` with a timeout value in seconds. If a value is not specified, the default timeout is used (60 seconds).

2 Save the scripts, along with the `.conf` file, on your Linux source workload, in the following directory:

```
/etc/platespin
```

7.8 Volumes

Upon adding a workload for protection, PlateSpin Protect inventories your source workload's storage media and automatically sets up options in the PlateSpin Protect Web Client for you to specify the volumes you require for protection.

PlateSpin Protect supports several types of storage, including Windows dynamic disks, LVM, RAID, and SAN.

For Linux workloads, PlateSpin Protect provides the following additional features:

- ♦ Non-volume storage that is associated with the source workload is recreated and assigned to the recovery workload.
- ♦ The layout of volume groups and logical volumes is preserved so that you can re-create it during failback.
- ♦ (OES 2 workloads) EVMS layouts of source workloads are preserved and re-created in the VM container. NSS pools are copied from the source to the recovery VM.

The following figures shows the Replication Settings parameter set for a Linux workload with multiple volumes and two logical volumes in a volume group.

Figure 7-1 Volumes, Logical Volumes, and Volume Groups of a Protected Linux Workload

Tier Settings				
Replication Settings				
Encrypt Data Transfer:	No			
Source Credentials:	root			
Number of CPUs:	1			
Replication Network:	DHCP - VM Network			
Recovery Point Datastore:	Storage2 (889.7 GB free)			
Protected Volumes:	Include	Name	Total Size	Datastore
	<input checked="" type="checkbox"/>	/usr	2.9 GB	Storage2
	<input checked="" type="checkbox"/>	/boot	2.0 GB	Storage2
	<input checked="" type="checkbox"/>	/new2 (EXT3)	151.9 MB	Storage2
Protected Logical Volumes:	Include	Name	Total Size	Volume Group
	<input checked="" type="checkbox"/>	/LogicalVolume1 (EXT3)	484.2 MB	group
	<input checked="" type="checkbox"/>	/LogicalVolume2 (EXT3)	193.7 MB	group
Volume Groups:	Include	Name	Total Size	Datastore
	<input checked="" type="checkbox"/>	group	1016.0 MB	Storage2
Non-volume Storage:	--			
Daemons to Stop During Replication:	--			
Failover Settings				
Prepare for Failover Settings				
Test Failover Settings				
Recovery Points				
Workload Details				

The following figure shows volume protection options of an OES 2 workload with options indicating that the EVMS layout should be preserved and re-created for the recovery workload:

Figure 7-2 Replication Settings, Volume-Related Options (OES 2 Workload)

Protected Logical Volumes:	Include	Name	Used Space	Free Space	Volume Group / EVMS Volume
	<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/novell/nss/mnt/pools/NEVPOOL (NSSFS)	23.3 MB	999.6 MB	NEVPOOL
Non-volume Storage:	Include	Partition	Is Swap	Total Size	Datastore / Volume Group
	<input checked="" type="checkbox"/>	/dev/system/swap	Yes	1.48 GB	system
Volume Groups:	Include	Name	Total Size	Datastore	Thin Disk
	<input checked="" type="checkbox"/>	system	5.9 GB	dev-comp124:storage	<input type="checkbox"/>
EVMS Volumes:	Include	Name	Datastore	Total Size	Thin Disk
	<input checked="" type="checkbox"/>	/dev/evms/sda1	dev-comp124:storage	70.6 MB	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	NEVPOOL	dev-comp124:storage	1023.0 MB	<input type="checkbox"/>
Daemons to Stop During Replication:	Add Daemons				

7.9 Networking

PlateSpin Protect enables you to control your recovery workload’s network identity and LAN settings to prevent replication traffic from interfering with your main LAN or WAN traffic.

You can specify distinct networking settings in your workload protection details for use at different stages of the workload protection and recovery workflow:

- ♦ **Replication:** ([Replication](#) parameter set) For separating regular replication traffic from your production traffic.
- ♦ **Failover:** ([Failover](#) parameter set) For the recovery workload to become part of your production network when it goes live.
- ♦ **Prepare for Failover:** ([Prepare for Failover](#) network parameter) For network settings during the optional Prepare for Failover stage.
- ♦ **Test Failover:** ([Test Failover](#) parameter set) For network settings to apply to the recovery workload during a Test Failover stage.

7.10 Registering Physical Machines with PlateSpin Protect for Failback

If the required target infrastructure for a failback or image deployment operation is a physical machine, you must register it with PlateSpin Protect.

The registration of a physical machine is carried out by booting the target physical machine with the appropriate PlateSpin boot ISO image.

To use a boot ISO image, download it from the [PlateSpin Protect area of Novell Downloads \(http://download.novell.com/Download?buildid=3OpGRMKYpJY~\)](http://download.novell.com/Download?buildid=3OpGRMKYpJY~). Use the image appropriate to your target machine:

Table 7-2 ISO Boot Images for Target Physical Machines

Filename	Remarks
WindowsFailback.zip (contains WindowsFailback.iso)	Windows
LinuxFailback.zip (contains LinuxFailback.iso)	Linux systems
WindowsFailback-Cisco.zip (contains WindowsFailback-Cisco.iso)	Windows systems on Cisco hardware
WindowsFailback-Dell.zip (contains WindowsFailback-Dell.iso)	Windows systems on Dell hardware
WindowsFailback-Fujitsu.zip (contains WindowsFailback-Fujitsu.iso)	Windows systems on Fujitsu hardware

After downloading the required file, unzip and save the extracted ISO file.

- ♦ [Section 7.10.1, “Registering Target Physical Machines,” on page 81](#)

7.10.1 Registering Target Physical Machines

1 Burn the appropriate image on a CD or save it to media from which your target can boot.

2 Ensure that the network switch port connected to the target is set to *Auto Full Duplex*.

Because the Windows version of the boot CD image supports only *Auto Negotiate Full Duplex*, this ensures that there are no conflicts in the duplex settings.

3 Use the boot CD to boot the target physical machine, then wait for the command prompt window to open.

(Windows only) Wait for the *REGISTERMACHINE* and *Recovery Console* command boxes to open. Use the *REGISTERMACHINE* command box. For information on the *Recovery Console* utility, see [“Using the Recovery Tool Command Line Utility \(Windows\)” on page 81](#).

4 (Linux only) For 64-bit systems, at the initial boot prompt, type the following:

- ♦ `ps64` (for systems with up to 512 MB RAM)
- ♦ `ps64_512m` (for systems with more than 512 MB RAM)

5 Press Enter.

6 When you are prompted, enter the following URL:

`http://<hostname | IP_address>/platespinprotect`

Replace `<hostname | IP_address>` with the hostname or the IP address of your PlateSpin Protect Server host.

7 Provide your admin-level credentials for the PlateSpin Protect Server host, specifying an authority. For the user account, use this format:

`domain\username` or `hostname\username`

Available network cards are detected and displayed by their MAC addresses.

8 If DHCP is available on the NIC to be used, press Enter to continue. If DHCP is not available, select the required NIC to configure with a static IP address.

9 Enter a hostname for the physical machine or press the Enter key to accept the default values.

10 Enter *Yes* if you have enabled ; otherwise, enter *No*.


After a few moments, the physical machine should be available in the failback/image deployment settings of the PlateSpin Protect Web Client.

Using the Recovery Tool Command Line Utility (Windows)

The Recovery Console command line utility enables you to dynamically inject Windows device drivers into the target physical machine without restarting the entire physical target registration process.

The utility is loaded in a secondary command box upon the initial attempt to boot from the Windows boot image (see [Step 3 on page 81](#)).

To use the Recovery Tool, enter its command name, `RECOVERYTOOL`, followed by an applicable parameter, in the Recovery Console window.



```
Recovery Console
AM      643,072 SPRING.CORE.DLL
PM      143,360 SPRING.THREADING.DLL
PM      275,456 VIRTUALDISKS.DLL
File(s) 12,075,414 bytes
Dir(s)   0 bytes free
platespin\utility>RECOVERYTOOL /L
```

You can use:

- ♦ /L to list any driver services installed on the target OS
- ♦ /J to inject drivers into the target OS

You can specify whether the drivers are to be downloaded from the PlateSpin Protect Server or from a local path. If you intend to use a local path, you should group multiple drivers for the same device together. If you want to download drivers from the PlateSpin Protect Server, the utility prompts you to specify which driver you want to use (if there is more than one).

Injecting Drivers into a PlateSpin Boot Image (Linux)

You can use a custom utility to package and inject additional Linux device drivers into the PlateSpin boot image before burning it on a CD:

- 1 Obtain or compile the required *.ko driver files.

IMPORTANT: Make sure the drivers are valid for the kernel included with the ISO file (2.6.32.12-0.7-default) and are appropriate for the target architecture.

- 2 Mount the image in any Linux machine (root credentials required). Use the following command syntax:

```
mount -o loop <path-to-ISO> <mount_point>
```

- 3 Copy the rebuildiso.sh script, located in the /tools subdirectory of the mounted ISO file, into a temporary working directory. When you have finished, unmount the ISO file (execute the command `umount <mount_point>`).
- 4 Create another working directory for the required driver files and save them in that directory.
- 5 In the directory where you saved the rebuildiso.sh script, run the following command as root:

```
./rebuildiso.sh -i <ISO_file> -d <driver_dir> -m i586|x86_64
```

On completion, the ISO file is updated with the additional drivers.

8 Troubleshooting

- ♦ [Section 8.1, “Troubleshooting Workload Inventory \(Windows\),” on page 83](#)
- ♦ [Section 8.2, “Troubleshooting Workload Inventory \(Linux\),” on page 87](#)
- ♦ [Section 8.3, “Troubleshooting Problems during the Prepare Replication Command \(Windows\),” on page 87](#)
- ♦ [Section 8.4, “Troubleshooting Workload Replication,” on page 88](#)
- ♦ [Section 8.5, “Generating and Viewing Diagnostic Reports,” on page 89](#)
- ♦ [Section 8.6, “Post-Protection Workload Cleanup,” on page 90](#)

8.1 Troubleshooting Workload Inventory (Windows)

You might need to troubleshoot the following common problems during the workload inventory.

Problems or Messages	Solutions
The domain in the credentials is invalid or blank	<p>This error occurs when the Credential Format is incorrect.</p> <p>Try the discovery by using a local admin account with the credential format <code>hostname\LocalAdmin</code></p> <p>Or, try the discovery by using a domain admin account with the credential format <code>domain\DomainAdmin</code></p>
Unable to connect to Windows server...Access is denied	<p>A non-admin account was used when trying to add a workload. Use an admin account or add the user to the administrators group and try again.</p> <p>This message might also indicate WMI connectivity failure. For each of the following possible resolutions, attempt the solution and then perform the “WMI Connectivity Test” on page 85 again. If the test succeeds, try adding the workload again.</p> <ul style="list-style-type: none">♦ “Troubleshooting DCOM Connectivity” on page 85♦ “Troubleshooting RPC Service Connectivity” on page 85
Unable to connect to Windows server...The network path was not found	<p>Network connectivity failure. Perform the tests in “Performing Connectivity Tests” on page 84. If a test fails, ensure that PlateSpin Protect and the workload are on the same network. Reconfigure the network and try again.</p>

Problems or Messages	Solutions
"Discover Server Details {hostname}" Failed Progress: 0% Status: NotStarted	<p>This error can occur for several reasons and each has a unique solution:</p> <ul style="list-style-type: none"> ◆ For environments using a local proxy with authentication, bypass the proxy or add the proper permissions. See KB Article 7920339 (http://www.novell.com/support/viewContent.do?externalId=7920339) for more details. ◆ If local or domain policies restrict required permissions, follow the steps outlined in KB Article 7920862 (http://www.novell.com/support/viewContent.do?externalId=7920862).
Workload Discovery fails with error message	There are several possible reasons for the Could not find file output.xml error:
Could not find file output.xml	<ul style="list-style-type: none"> ◆ Antivirus software on the source could be interfering with the discovery. Disable the antivirus software to determine whether or not it is the cause of the problem. See "Disabling AntiVirus Software" on page 86.
or	
Network path not found	<ul style="list-style-type: none"> ◆ File and Printer Sharing for Microsoft Networks might not be enabled. Enable it under the Network Interface Card properties.
or (upon attempting to discover a Windows cluster)	<ul style="list-style-type: none"> ◆ The C\$ and/or Admin\$ shares on the source might not be accessible. Ensure that PlateSpin Protect can access those shares. See "Enabling File/Share Permissions and Access" on page 86.
Inventory failed to discover. Inventory result returned nothing.	<ul style="list-style-type: none"> ◆ Change the flag ForceMachineDiscoveryUsingService to true in the web.config file in the \Program Files\PlateSpin Portability Suite Server\Web folder. ◆ The Server or the Workstation service might not be running. If this is the case, enable them and set the startup mode to automatic. ◆ The Windows remote registry service is disabled. Start the service and set the startup type to automatic.

8.1.1 Performing Connectivity Tests

- ◆ ["Network Connectivity Test" on page 84](#)
- ◆ ["WMI Connectivity Test" on page 85](#)
- ◆ ["Troubleshooting DCOM Connectivity" on page 85](#)
- ◆ ["Troubleshooting RPC Service Connectivity" on page 85](#)

Network Connectivity Test

Perform this basic network connectivity test to determine whether PlateSpin Protect can communicate with the workload that you are trying to protect.

- 1 Go to your PlateSpin Protect Server host.
- 2 Open a command prompt and ping your workload:

```
ping workload_ip
```

WMI Connectivity Test

- 1 Go to your PlateSpin Protect Server host.
- 2 Click *Start > Run*, type `Wbemtest` and press Enter.
- 3 Click *Connect*.
- 4 In the *Namespace*, type the name of the workload you are trying to discover with `\root\cimv2` appended to it. For example, if the hostname is `win2k`, type:
`\\win2k\root\cimv2`
- 5 Enter the appropriate credentials, using either the `hostname\LocalAdmin` or `domain\DomainAdmin` format.
- 6 Click *Connect* to test the WMI connection.

If an error message is returned, a WMI connection cannot be established between PlateSpin Protect and your workload.

Troubleshooting DCOM Connectivity

- 1 Log into the workload that you want to protect.
- 2 Click *Start > Run*.
- 3 Type `dcomcnfg` and press Enter.
- 4 Check connectivity:
 - ♦ On a Windows NT/2000 server machine, the DCOM Configuration dialog box is displayed. Click the *Default Properties* tab and ensure that *Enable Distributed COM on this computer* is selected.
 - ♦ For Windows Server 2003, the Component Services window is displayed. In the *Computers* folder of the console tree of the Component Services administrative tool, right-click the computer that you want to check for DCOM connectivity, then click *Properties*. Click the *Default Properties* tab and ensure that *Enable Distributed COM on this computer* is selected.
- 5 If DCOM was not enabled, enable it and either reboot the server or restart the Windows Management Instrumentation Service. Then try adding the workload again.

Troubleshooting RPC Service Connectivity

There are three potential blockages for the RPC service:

- ♦ The Windows Service
- ♦ A Windows firewall
- ♦ A hardware firewall

For the Windows Service, ensure that the RPC service is running on the workload. To access the services panel, run `services.msc` from a command prompt. For a Windows firewall, add an RPC exception. For hardware firewalls, you can try the following strategies:

- ♦ Putting PlateSpin Protect and the workload on the same side of the firewall
- ♦ Opening up specific ports between PlateSpin Protect and the workload (See [“Access and Communication Requirements across your Protection Network”](#) on page 20).

8.1.2 Disabling AntiVirus Software

Antivirus software might occasionally block some of the PlateSpin Protect functionality related to WMI and Remote Registry. In order to ensure that workload inventory is successful, it might be necessary to first disable the antivirus service on a workload. In addition, antivirus software might occasionally lock access to certain files, allowing access only to certain processes or executables. This might occasionally obstruct file-based data replication. In this case, when you configure the workload protection, you can select services to disable, such as services installed and used by antivirus software. These services are only disabled for the duration of the file transfer, and are restarted when the process completes. This is not necessary during block-level data replication.

8.1.3 Enabling File/Share Permissions and Access

To successfully protect a workload, PlateSpin Protect needs to successfully deploy and install the OFX Controller and, if you require block-level replication, a dedicated block-based component. Upon deployment of these components to a workload, as well as during the Add Workload process, PlateSpin Protect uses the workload's administrative shares. PlateSpin Protect needs administrative access to the shares, using either a local administrator account or a domain admin account for this to work.

To ensure that the Administrative shares are enabled:

- 1 Right-click *My Computer* on the desktop and select *Manage*.
- 2 Expand *System Tools > Shared Folders > Shares*
- 3 In the *Shared Folders* directory, you should see *C\$* and *Admin\$*, among other shares.

After confirming that the shares are enabled, ensure that they are accessible from within the PlateSpin Protect Server host:

- 1 Go to your PlateSpin Protect Server host.
- 2 Click *Start > Run*, type `\\<server_host>\C$`, then click *OK*.
- 3 If you are prompted, use the same credentials as those you will use to add the workload to the PlateSpin Protect workload inventory.

The directory is opened and you should be able to browse and modify its contents.

- 4 Repeat the process for all shares with the exception of the *IPC\$* share.

Windows uses the *IPC\$* share for credential validation and authentication purposes. It is not mapped to a folder or file on the workload, so the test always fails; however, the share should still be visible.

PlateSpin Protect does not modify the existing content of the volume; however, it creates its own directory, to which it requires access and permissions.

8.2 Troubleshooting Workload Inventory (Linux)

Problems or Messages	Solutions
Unable to connect neither to the SSH server running on <IP_address> nor to VMware Virtual Infrastructure web-services at <ip_address>/sdk	<p>This message has a number of possible causes:</p> <ul style="list-style-type: none">♦ The workload is unreachable.♦ The workload does not have SSH running.♦ The firewall is on and the required ports have not been opened.♦ The workload's specific operating system is not supported. <p>For network and access requirements for a workload, see "Access and Communication Requirements across your Protection Network" on page 20.</p>
Access denied	<p>This authentication problem indicates either an invalid username or password. For information on proper workload access credentials, see "Guidelines for Workload and Container Credentials" on page 73.</p>

8.3 Troubleshooting Problems during the Prepare Replication Command (Windows)

Problems or Messages	Solutions
Authentication error when verifying the controller connection while setting up the controller on the source.	<p>The account used to add a workload needs to be allowed by this policy. See "Group Policy and User Rights" on page 87.</p>
Failure to determine whether .NET Framework is installed (with exception The trust relationship between this workstation and the primarydomain failed).	<p>Check whether the Remote Registry service on the source is enabled and started. See also "Troubleshooting Workload Inventory (Windows)" on page 83.</p>

8.3.1 Group Policy and User Rights

You can refresh the policy immediately by using `gpupdate /force` (for Windows 2003/XP) or `secedit /refreshpolicy machine_policy /enforce` (for Windows 2000). Because of the way that PlateSpin Protect interacts with the source workload's operating system, it requires the administrator account that is used to add a workload to have certain user rights on the source machine. In most instances, these settings are defaults of group policy; however, if the environment has been locked down, the following user rights assignments might have been removed:

- ♦ Bypass Traverse Checking
- ♦ Replace Process Level Token
- ♦ Act as part of the Operating System

In order to verify that these Group Policy settings have been set, you can run `gpresult /v` from the command line on the source machine, or alternately `RSOP.msc`. If the policy has not been set, or has been disabled, it can be enabled through either the Local Security Policy of the machine or through any of the Domain Group Policies being applied to the machine.

8.4 Troubleshooting Workload Replication

Problems or Messages	Solutions
Workload issue requires user intervention	This problem occurs when the server is under load and the process is taking longer than expected.
Recoverable error during replication either during <i>Scheduling Taking Snapshot of Virtual Machine</i> or <i>Scheduling Reverting Virtual Machine to Snapshot before Starting</i> .	The solution is to wait until the replication is complete.
All workloads go into recoverable errors because you are out of disk space.	Verify the free space. If more space is required, remove a workload.
Slow network speeds under 1 MB.	Confirm that the source machine's network interface card's duplex setting is on and the switch it is connected to has a matching setting. That is, if the switch is set to auto, the source can't be set to 100 MB.
Slow network speeds over 1 MB.	<p>Measure the latency by running the following command from the source workload:</p> <pre>ping ip-t</pre> <p>(replace <i>ip</i> with the IP address of your PlateSpin Protect Server host).</p> <p>Allow it to run for 50 iterations and the average indicates the latency.</p> <p>Also see "Optimizing Data Transfer over WAN Connections (File-Based and VSS Replications)" on page 23.</p>
The file transfer cannot begin - port 3725 is already in use	Ensure that the port is open and listening:
or	Run <code>netstat -ano</code> on the workload.
3725 unable to connect	Check the firewall.
	Retry the replication.
Controller connection not established	This error occurs when the replication networking information is invalid. Either the DHCP server is not available or the replication virtual network is not routable to the PlateSpin Protect Server host.
Replication fails at the <i>Take Control of Virtual Machine</i> step.	<p>Change the replication IP to a static IP or enable the DHCP server.</p> <p>Ensure that the virtual network selected for replication is routable to the PlateSpin Protect Server host.</p>

Problems or Messages	Solutions
Replication job does not start (stuck at 0%)	<p>This error can occur for different reasons and each has a unique solution:</p> <ul style="list-style-type: none"> For environments using a local proxy with authentication, bypass the proxy or add proper permissions to resolve this problem. See KB Article 20339 (http://www.novell.com/support/viewContent.do?externalId=7920339) for more details. If local or domain policies restrict required permissions, follow the steps outlined in KB Article 7920862 (http://www.novell.com/support/viewContent.do?externalId=7920862). <p>This is a common issue when PlateSpin Protect Server host is affiliated with a domain and the domain policies are applied with restrictions. See “Group Policy and User Rights” on page 87.</p>

8.5 Generating and Viewing Diagnostic Reports

In the PlateSpin Protect Web Client, after you have executed a command, you can generate detailed diagnostic reports about the command's details.

- 1 Click *Command Details*, then click the *Generate Diagnostics* link.

The screenshot shows the PlateSpin Protect Web Client interface. The top navigation bar includes links for Dashboard, Workloads, Tasks, Reports, Settings, About, and Help. The main content area is titled 'Running First Replication' and shows the status of a replication job. The job is currently 'Running' with a duration of 14h 49m 6s and a progress of 80%. A 'Generate Diagnostics' link is visible in the bottom right corner of the command details section, highlighted with a red box.

Step	Status	Start Time	End Time	Duration	Diagnostics
Copy data	Running (80%)	3/31/2010 8:24 PM	--	14h 48m 53s	--

After a few moments, the page refreshes and displays a *View* link above the *Generated Diagnostics* link.

- 2 Click *View*.

A new page opens with comprehensive diagnostic information about the current command.

- 3 Save the diagnostics page and have it ready if you need to contact technical support.

8.6 Post-Protection Workload Cleanup

Use these steps to clean up your source workload from all PlateSpin software components when required, such as following an unsuccessful or problematic protection.

8.6.1 Cleaning Up Windows Workloads

Component	Removal Instructions
PlateSpin Block-Based Transfer Component	See KB Article 7005616 (http://www.novell.com/support/viewContent.do?externalId=7005616) .
Third-party Block-based Transfer Component (discontinued)	<ol style="list-style-type: none">1. Use the Windows Add/Remove Programs applet (run <code>appwiz.cpl</code>) and remove the component. Depending on the source, you might have either of the following versions:<ul style="list-style-type: none">◆ SteelEye Data Replication for Windows v6 Update2◆ SteelEye DataKeeper For Windows v72. Reboot the machine.
File-based Transfer Component	At root level for each volume under protection, remove all files named <code>PlateSpinCatalog*.dat</code>
Workload Inventory software	In the workload's Windows directory: <ul style="list-style-type: none">◆ Remove all files named <code>machinediscovery*</code>.◆ Remove the subdirectory named <code>platespin</code>.
Controller software	<ol style="list-style-type: none">1. Open a command prompt and change the current directory to:<ul style="list-style-type: none">◆ <code>\Program Files\platespin*</code> (32-bit systems)◆ <code>\Program Files (x86)\platespin</code> (64-bit systems)2. Run the following command: <code>ofxcontroller.exe /uninstall</code>3. Remove the <code>platespin*</code> directory

8.6.2 Cleaning Up Linux Workloads

Component	Removal Instructions
Controller software	<ul style="list-style-type: none">◆ Kill these processes:<ul style="list-style-type: none">◆ <code>kill -9 ofxcontrollerd</code>◆ <code>kill -9 ofxjobexec</code>◆ remove the OFX controller rpm package: <code>rpm -e ofxcontrollerd</code>◆ In the source workload's file system, remove the <code>/usr/lib/ofx</code> directory with its contents.

Component	Removal Instructions
Block-level data transfer software	<ol style="list-style-type: none"> 1. Check if the driver is active: <pre>lsmod grep blkwatch</pre> <p>If the driver is still loaded in memory, the result should contain a line, similar to the following:</p> <pre>blkwatch_7616 70924 0</pre> 2. (Conditional) If the driver is still loaded, remove it from memory: <pre>rmmod blkwatch_7616</pre> 3. Remove the driver from the boot sequence: <pre>blkconfig -u</pre> 4. Remove the driver files by deleting the following directory with its contents: <pre>/lib/modules/[Kernel_Version]/Platespin</pre> 5. Delete the following file: <pre>/etc/blkwatch.conf</pre>
LVM snapshots	<ol style="list-style-type: none"> 1. In the Jobs view, generate a Job Report for the failed job, then note the name of the snapshot. 2. Remove the snapshot device by using the following command: <pre>lvremove <i>snapshot_name</i></pre>
Bitmap files	For each volume under protection, at the root of the volume, remove the corresponding <code>.blocks_bitmap</code> file.
Tools	<p>On the source workload, under <code>/sbin</code>, remove the following files:</p> <ul style="list-style-type: none"> ♦ <code>bmaputil</code> ♦ <code>blkconfig</code>

8.6.3 Removing Workloads

In some circumstances you might need to remove a workload from the PlateSpin Protect inventory and re-add it later.

- 1 On the Workloads page, select the workload that you want to remove, then click *Remove Workload*.

(Conditional) For Windows workloads previously protected through block-level replication, the PlateSpin Protect Web Client prompts you to indicate whether you also want to remove the Block-Based Components. You can make the following selections:

- ♦ **Do not remove components:** The components will not be removed.
- ♦ **Remove components but do not restart workload:** The components will be removed. However, a reboot of the workload will be required to complete the uninstallation process.
- ♦ **Remove components and restart workload:** The components will be removed, and the workload will be automatically rebooted. Make sure you carry out this operation during scheduled downtime.

- 2 On the Command Confirmation page, click *Confirm* to execute the command.
Wait for the process to complete.

Glossary

container. Either of the two workload protection infrastructures supported by PlateSpin Protect (a VM host or an image server).

Deploy. PlateSpin Protect command that recovers a failed workload by deploying its image, which is under protection on an image server, to run on physical hardware or a VM container.

Event. A PlateSpin Protect Server message that contains information about important steps throughout the workload protection lifecycle.

failback. Restoration of the business function of a failed workload in its original environment when the business function of a temporary recovery workload within PlateSpin Protect is no longer required.

failover. Taking over the business function of a failed workload by a recovery workload within a PlateSpin Protect VM container.

incremental. 1. (noun) An individual scheduled transfer or manual transfer of differences between a protected workload and its replica (the recovery workload).

2. (adjective) Describes the scope of *replication (1)*, in which the initial replica of a workload is created differentially, based on differences between the workload and its prepared counterpart.

Prepare for Failover. A PlateSpin Protect operation that boots the recovery workload in preparation of a full Failover operation.

Protection Tier. A customizable collection of workload protection parameters that define the frequency of replications and criteria for the system to consider a workload as failed.

recovery point. A point-in-time snapshot, allowing a replicated workload or a workload image to be restored to a previous state.

recovery point objective (RPO). Tolerable data loss measured in time and defined by a configurable interval between incremental replications of a protected workload or a protected workload image.

recovery time objective (RTO). A measure of a workload's tolerable downtime defined by the time a failover operation takes to complete.

recovery workload. A protected workload's bootable virtual replica.

replication. 1. The creation of an initial base copy of a workload (*initial replication*).

2. Any transfer of changed data from a protected workload to its replica in the container.

replication schedule. The schedule that is set up to control the frequency and scope of replications.

Reprotect. A PlateSpin Protect command that reestablishes a protection contract for a workload following the failover and failback operations.

source. A workload or its infrastructure that is the starting point of a PlateSpin Protect operation. For example, upon initial protection of a workload, the source is your production workload. In a failback operation, it is the recovery workload in the container.

In image deployment, the source is the image of a workload on a designated image server.

See also [target](#).

target. A workload or its infrastructure that is the outcome of a PlateSpin Protect command. For example, upon initial protection of a workload, the target is the recovery workload in the container. In a failback operation, it is either your production workload's original infrastructure or any supported container that has been inventoried by PlateSpin Protect.

In image deployment, the target is the infrastructure onto which a protected image is deployed to boot.

See also [source](#).

Test Failover. A PlateSpin Protect operation that boots a recovery workload in an isolated networking environment for testing the functionality of the failover and verifying the integrity of the recovery workload.

test time objective (TTO). A measure of the ease with which a disaster recovery plan can be tested. It is similar to RTO, but includes the time needed for a user to test the recovery workload.

workload. The basic object of protection in a data store. An operating system, along with its middleware and data, decoupled from the underlying physical or virtual infrastructure.