

PlateSpin. Protect 10.4

User Guide

2013



Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2013 NetIQ Corporation and its affiliates. All Rights Reserved.

For information about NetIQ trademarks, see <https://www.netiq.com/company/legal/>.

Contents

About This Guide	7
1 Product Overview	9
1.1 About PlateSpin Protect	9
1.2 Supported Configurations	9
1.2.1 Supported Windows Workloads	9
1.2.2 Supported Linux Workloads	10
1.2.3 Supported VM Containers	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
2.2.4 Setting Up VMware vCenter Privileges for PlateSpin Access in a Multi-Tenant Architecture	20
2.3 Access and Communication Requirements across your Protection Network	23
2.3.1 Access and Communication Requirements for Workloads	24
2.3.2 Access and Communication Requirements for Containers	25
2.3.3 Open Port Requirements for PlateSpin Protect Server Hosts	25
2.3.4 Protection Across Public and Private Networks Through NAT	25
2.3.5 Optimizing Data Transfer over WAN Connections	26
2.3.6 Enabling SSL Communication with the PlateSpin Server	27
2.3.7 Overriding the Default bash Shell for Executing Commands on Linux Workloads	27
2.3.8 Requirements for VMware DRS Clusters as Containers	28
2.3.9 Configuring the Application to Function Across NAT	28
2.4 Configuring PlateSpin Protect Default Options	28
2.4.1 Setting Up Automatic E-Mail Notifications of Events and Reports	28
2.4.2 Language Setup for International Versions of PlateSpin Protect	32
2.4.3 Configuring the Product Behavior through XML Configuration Parameters	32
3 Up and Running	35
3.1 Launching the PlateSpin Protect Web Interface	35
3.2 Elements of the PlateSpin Protect Web Interface	36

3.2.1	Navigation Bar	37
3.2.2	Visual Summary Panel	37
3.2.3	Tasks and Events Panel	38
3.3	Workloads and Workload Commands	38
3.3.1	Workload Protection and Recovery Commands	39
3.4	Managing Multiple Instances of PlateSpin Protect and PlateSpin Forge	40
3.4.1	Using the PlateSpin Protect Management Console	40
3.4.2	About PlateSpin Protect Management Console Cards	40
3.4.3	Adding Instances of PlateSpin Protect and PlateSpin Forge to the Management Console	41
3.4.4	Managing Cards on the Management Console	42
3.5	Generating Workload and Workload Protection Reports	43
4	Workload Protection	45
4.1	Basic Workflow for Workload Protection and Recovery	45
4.2	Adding Containers (Protection Targets)	46
4.3	Adding Workloads for Protection	47
4.4	Configuring Protection Details and Preparing the Replication	49
4.4.1	Workload Protection Details	49
4.5	Starting the Workload Protection	51
4.6	Aborting Commands	52
4.7	Failover	53
4.7.1	Detecting Offline Workloads	53
4.7.2	Performing a Failover	54
4.7.3	Using the Test Failover Feature	54
4.8	Failback	55
4.8.1	Automated Failback to a VM Platform	55
4.8.2	Semi-Automated Failback to a Physical Machine	58
4.8.3	Semi-Automated Failback to a Virtual Machine	59
4.9	Reprotecting a Workload	59
5	Essentials of Workload Protection	61
5.1	Workload License Consumption	61
5.2	Guidelines for Workload and Container Credentials	62
5.3	Transfer Methods	62
5.4	Protection Tiers	63
5.5	Recovery Points	64
5.6	Initial Replication Method (Full and Incremental)	65
5.7	Service and Daemon Control	66
5.8	Using Freeze and Thaw Scripts for Every Replication (Linux)	66
5.9	Volumes	67
5.10	Networking	69
5.11	Registering Physical Machines with PlateSpin Protect for Failback	69
5.11.1	Registering Target Physical Machines	70
5.12	Advanced Workload Protection Topics	71
5.12.1	Protecting Windows Clusters	72
5.12.2	Linux Failback to a Paravirtualized VM on Xen on SLES	72
5.12.3	Using Workload Protection Features through the PlateSpin Protect Web Services API	75
6	Auxiliary Tools for Working with Physical Machines	77
6.1	Analyzing Device Drivers with PlateSpin Analyzer (Windows)	77
6.2	Managing Device Drivers	78

6.2.1	Packaging Device Drivers for Windows Systems	78
6.2.2	Packaging Device Drivers for Linux Systems	79
6.2.3	Uploading Drivers to the PlateSpin Protect Device Driver Database.	79

7 Troubleshooting 83

7.1	Troubleshooting Workload Inventory (Windows)	83
7.1.1	Performing Connectivity Tests	84
7.1.2	Disabling AntiVirus Software	85
7.1.3	Enabling File/Share Permissions and Access	86
7.2	Troubleshooting Workload Inventory (Linux)	86
7.3	Troubleshooting Problems during the Prepare Replication Command (Windows)	87
7.3.1	Group Policy and User Rights	87
7.4	Troubleshooting Workload Replication	87
7.5	Generating and Viewing Diagnostic Reports	89
7.6	Removing Workloads	90
7.7	Post-Protection Workload Cleanup	90
7.7.1	Cleaning Up Windows Workloads	90
7.7.2	Cleaning Up Linux Workloads	91

Glossary 93

About This Guide

This guide provides information about using PlateSpin Protect.

- ♦ Chapter 1, “Product Overview,” on page 9
- ♦ Chapter 2, “Application Configuration,” on page 15
- ♦ Chapter 3, “Up and Running,” on page 35
- ♦ Chapter 4, “Workload Protection,” on page 45
- ♦ Chapter 5, “Essentials of Workload Protection,” on page 61
- ♦ Chapter 6, “Auxiliary Tools for Working with Physical Machines,” on page 77
- ♦ Chapter 7, “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.

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.netiq.com/documentation/platespin_protect_10/) (http://www.netiq.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.netiq.com/documentation/platespin_protect_10/) (http://www.netiq.com/documentation/platespin_protect_10/).

Additional Resources

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

- ♦ [NetIQ User Community](http://community.netiq.com/) (<http://community.netiq.com/>): A Web-based community with a variety of discussion topics.
- ♦ [NetIQ Support Knowledgebase](https://www.netiq.com/support/) (<https://www.netiq.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 request support through the [NetIQ Support & Services Web site \(https://www.netiq.com/Support/default.asp\)](https://www.netiq.com/Support/default.asp).

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 business continuity and disaster recovery software that protects physical and virtual workloads (operating systems, middleware, and data) by using virtualization technology. If there is a production server outage or disaster, a virtualized replica of a workload can be rapidly powered on within the target *container* (a VM host), and continue to run as normal until the production environment is restored.

PlateSpin Protect enables you to:

- ◆ Quickly recover workloads upon failure
- ◆ Simultaneously protect multiple workloads
- ◆ Test the failover workload without interfering with your production environment
- ◆ Fail back failover workloads to either their original or to completely new infrastructures, physical or virtual
- ◆ Take advantage of existing external storage solutions, such as SANs

1.2 Supported Configurations

- ◆ [Section 1.2.1, “Supported Windows Workloads,” on page 9](#)
- ◆ [Section 1.2.2, “Supported Linux Workloads,” on page 10](#)
- ◆ [Section 1.2.3, “Supported VM Containers,” on page 11](#)

1.2.1 Supported Windows Workloads

PlateSpin Protect supports most Windows-based workloads.

Both file- and block-level replications are supported, with certain restrictions. See [Section 5.3, “Transfer Methods,” on page 62](#).

Table 1-1 Supported Windows Workloads

Operating System	Remarks
Windows Server 2012	
Windows 8	
Windows 7	Professional, Enterprise, and Ultimate editions only
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 R2	Including domain controller (DC) systems and Small Business Server (SBS) editions
Windows Server 2003	Including domain controller (DC) systems and Small Business Server (SBS) editions
Windows XP Professional	
Windows Server 2000	Requires Service Pack 4 with Update Rollup 1.
Windows clusters	See "Protecting Windows Clusters" on page 72 for specific cluster configurations supported.

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

1.2.2 Supported Linux Workloads

PlateSpin Protect supports a number of Linux distributions.

Replication is done at the block level, for which your PlateSpin software requires a `blkwatch` module compiled for a particular Linux distribution being protected.

Some of the supported Linux versions require that you compile the PlateSpin `blkwatch` module for your specific kernel. Those workloads are called out explicitly.

Table 1-2 Supported Linux Workloads

Operating System	Remarks
Red Hat Enterprise Linux (RHEL) 4.0, 5.0-5.5, 6.0-6.2	
RHEL 5.6-5.8, 6.3	You must compile the PlateSpin <code>blkwatch</code> module before inventorying these workloads. See KB Article 7005873 (https://www.netiq.com/support/kb/doc.php?id=7005873) .
SUSE Linux Enterprise Server (SLES) 9, 10, 11 (SP1, SP2)	

Operating System	Remarks
Open Enterprise Server (OES) 11	
OES 2 (SP2 and SP3)	
Oracle Enterprise Linux (OEL)	<ul style="list-style-type: none"> ◆ Same level of support as that for workloads running RHEL. ◆ Workloads using the Unbreakable Enterprise Kernel are not supported.

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

Supported Linux file systems: EXT2, EXT3, EXT4, REISERFS, and NSS (OES 2 workloads).

NOTE: Encrypted volumes of workloads on the source are decrypted in the failover VM.

1.2.3 Supported VM Containers

Table 1-3 Platforms Supported as VM Containers

Container	Notes
VMware DRS Cluster in vSphere 5.1	<ul style="list-style-type: none"> ◆ The DRS configuration must be either Partially Automated or Fully Automated (it must not be set to Manual) ◆ As a VM Container, the DRS Cluster must consist of ESXi 5.1 servers only, and can be managed by vCenter 5.1 only.
VMware DRS Cluster in vSphere 5.0	<ul style="list-style-type: none"> ◆ The DRS configuration must be either Partially Automated or Fully Automated (it must not be set to Manual) ◆ As a VM Container, the DRS Cluster must consist of ESXi 5.0 servers only, and can be managed by vCenter 5.0 only.
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) ◆ As a VM Container, the Cluster, as a container, can use a combination of ESX 4.1 and ESXi 4.1 servers, and can be managed by vCenter 4.1 only.
VMware ESXi 4.1, 5.0, 5.1	ESXi versions must have a paid license; protection is unsupported with these systems if they are operating with a free license.
VMware ESX 4.1	

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 individually for each workload. See [“Workload Protection Details”](#) on page 49.

1.3.2 Security of Client/Server Communications

Data transmission between your Web browser and the PlateSpin Protect Server 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 with the PlateSpin Server”](#) on page 27), 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 individually for each workload or in a Protection Tier. See ["Protection Tiers" on page 63](#).

1.4.3 Bandwidth Throttling

PlateSpin Protect enables you to control the amount of network 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 can be configured individual for each workload or in a Protection Tier. See ["Protection Tiers" on page 63](#).

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, your network speed, and the chosen replication schedule.
- ♦ **Recovery Time Objective (RTO):** Describes the time required for a failover operation (bringing a failover workload 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 53](#).

- ♦ **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. See [“Using the Test Failover Feature” on page 54](#).

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 available to it than multiple failed-over workloads, which share the resources of their underlying infrastructure.

You should determine 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 43](#).

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 might vary between 5 and 40, 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 23
- ♦ Section 2.4, “Configuring PlateSpin Protect Default Options,” on page 28

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 environments that use HTTP proxy.

- 1 In the PlateSpin Protect Web Interface, 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* and copy the hardware ID shown.
- 3 Use a Web browser on a computer that has internet access to navigate to the [PlateSpin Product Activation Web Site \(http://www.platespin.com/productactivation/ActivateOrder.aspx\)](http://www.platespin.com/productactivation/ActivateOrder.aspx). Log in with your Novell username.
- 4 Enter in the appropriate fields:
 - ♦ the activation code that you received
 - ♦ the e-mail address that you provided when placing your order
 - ♦ the hardware ID that you copied in [Step 2](#)
- 5 Click *Activate*.

The system generates a license key file and prompts you to save it.

- 6 Save the generated license key file, transfer it to the product host that does not have internet connectivity, and use it to activate the product.

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
- ♦ [Section 2.2.4, "Setting Up VMware vCenter Privileges for PlateSpin Access in a Multi-Tenant Architecture,"](#) on page 20

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 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.
- ♦ **Workload Protection Operators:** Have access to a limited subset of system features and functions, sufficient to maintain day-to-day operation.

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.

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
Settings (All)	Allowed	Denied	Denied

Workload Protection Role Details	Administrators	Power Users	Operators
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 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 users to the required user groups detailed in [Table 2-1](#) (see your Windows documentation).
2. Creating application-level security groups that associate these users with specified workloads (see [“Managing PlateSpin Protect Security Groups and Workload Permissions”](#) on page 19).

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 system’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 system’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 33.

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 Interface, 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 to the PlateSpin Protect Server host, it might not be immediately available in the user interface. In this case, first click *Refresh User Accounts*.

Choose users to grant access to this group:

Grant	Name	Roles
<input checked="" type="checkbox"/>	ADLER\operator1	Workload Protection Operator

OK Cancel

- 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.

2.2.4 Setting Up VMware vCenter Privileges for PlateSpin Access in a Multi-Tenant Architecture

The VMware privileges required by PlateSpin Protect for full functionality are enumerated in the role definition file `PlateSpinRole.xml`. This file is shipped with the `PlateSpin.VMwareRoleTool` utility and embedded in the `PlateSpin.Athens.VMware` assembly. The enumerated privileges are the minimal set required to perform a full protection lifecycle. This file contains definitions for three separate roles: `PlateSpin Virtual Machine Manager`, `PlateSpin Infrastructure Manager` and `PlateSpin User`.

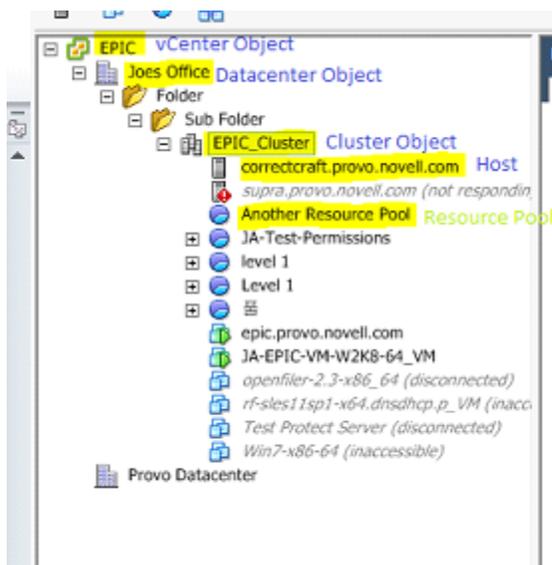
The shipped `PlateSpin.VMwareRoleTool` can be used to create/update the PlateSpin roles in a target vCenter environment.

Table 2-2 Role Assignment in a Multi-Tenant VMware Architecture

For each ...	Required Protect User Role	Remarks
Root of the vCenter inventory tree	PlateSpin Infrastructure Manager (or equivalent)	Required To: Monitor tasks being performed by the Protect software; end any stale VMware sessions. Notes: This permission should be defined as non-propagating.
All datacenter objects	PlateSpin Infrastructure Manager (or equivalent)	Required To: Allow access to the datacenter's datastores for uploading/downloading files. Notes: This permission should be defined as non-propagating.
Cluster	PlateSpin Infrastructure Manager (or equivalent)	Required To: Add a cluster to Protect as a container. Notes: Each host contained in the cluster must also have the PlateSpin Infrastructure Manager (or equivalent) role assigned. See below.
Each ESX host in cluster	PlateSpin Infrastructure Manager (or equivalent)	Required To: Add a cluster-member host to Protect as a container. Notes: This can be achieved by propagating the permission from the cluster object, or creating an additional permission on each cluster host. If the role is assigned on the cluster object and is propagated, then no further changes would be necessary when adding a new host to the cluster. However, propagating this permission will have security implications. See "Security Implications" on page 22 for more information.
Resource Pool	PlateSpin Virtual Machine Manager (or equivalent)	Required To: Access a resource pool to perform protection lifecycle operations. Notes: The administrator may assign access to any number of Resource Pools in any location in the tree, though the Protect user must have been granted the PlateSpin Virtual Machine Manager (or equivalent) role to at least one Resource Pool.

For each ...	Required Protect User Role	Remarks
VM Folder	PlateSpin Virtual Machine Manager (or equivalent)	<p>Required To: Access a folder to perform protection lifecycle operations.</p> <p>Notes: The administrator may assign access to any number of VM Folders in any location in the tree, though the Protect user must have been granted the PlateSpin Virtual Machine Manager (or equivalent) role to at least one folder.</p>
Network	PlateSpin Virtual Machine Manager (or equivalent)	<p>Required To: Access a network to perform protection lifecycle operations.</p> <p>Notes: The Protect user must have been granted the PlateSpin Virtual Machine Manager (or equivalent) role to at least one network. For Distributed Virtual Networks, both the dvSwitch and the dvPortgroup must have the PlateSpin Virtual Machine Manager (or equivalent) role assigned. In order to assign the correct role to the dvSwitch, either the role on the Datacenter must be propagated (resulting in additional object receiving this role), or the dvSwitch must be placed in a folder and the role assigned on that folder. For standard portgroups, every host in the cluster must have a definition for a given portgroup in order for it to be included in the list of available networks.</p>
Datastore, Datastore Cluster	PlateSpin Virtual Machine Manager (or equivalent)	<p>Required To: Access a datastore or a datastore cluster to perform protection lifecycle operations.</p> <p>Notes: The Protect user must have been granted the PlateSpin Virtual Machine Manager (or equivalent) role to at least one datastore or datastore cluster. For Datastore Clusters, the permission must be propagated to the contained datastores. Not providing access to an individual member of the cluster causes both prepare and full replications to fail.</p>

Figure 2-1 Figure 1 The objects in blue have the Infrastructure Manager role assigned, the objects in Green use the Virtual Machine Manager. Not pictured are the VM folders, networks and datastores. These objects would also have the Virtual Machine Manager Role.



Security Implications

It is assumed that the Protect User will only be used by the PlateSpin software to perform protection lifecycle operations. Thus, from a RaaS provider's point of view, the end user will never have access to the Protect User's credential and will not be able to access the same set of VMware resources. However, with multiple Protect servers configured to use the same vCenter environment, the possibilities for cross client access must be protected against. The major security implications that have been identified thus far are (keeping in mind that in these cases the different Protect Users are, in fact, different instances of the PlateSpin software):

- ◆ With the PlateSpin Infrastructure Manager role assigned to the vCenter object, every Protect User will be able to see (but NOT affect) the tasks performed by every other user.
- ◆ Because there is no way to set permissions on datastore folders/subfolders, all Protect Users with permissions on a datastore would have access to all other Protect Users' disks stored on that datastore.
- ◆ With the PlateSpin Infrastructure Manager role assigned to the cluster object, every Protect User will be able to turn off/on HA or DRS on the entire cluster.
- ◆ With the PlateSpin role assigned at the storage cluster object, every Protect User will be able to turn off/on SDRS for the entire cluster.
- ◆ Setting the PlateSpin Infrastructure Manager Role on the DRS Cluster object and propagating this role will allow the Protect User to see all VMs placed in the default resource pool and/or default VM folder. Also, propagation will require the administrator to explicitly set the Protect User to have a no-access role on every resource pool/vm folder that he should not have access to.
- ◆ Setting the PlateSpin Infrastructure Manager Role on the vCenter object will allow the Protect User to end sessions of any other user connected to the vCenter.

Best Practices

When setting up a RaaS environment it is expected that the RaaS provider will provision a single Protect server per RaaS customer. This Protect server will be assigned a Protect User, with the VMware roles configured as specified above, that will be used to create a Protect Container. This Protect User's credentials will be maintained by the RaaS provider and will not be disclosed to the RaaS customer. The RaaS customer will be provided with a user that is a member of the PlateSpin Administrators group on the PlateSpin Protect server. This user will also need to be available on the vCenter server. This user should be granted all the desired permissions on the resource pool (s) and folder(s) where the customer's VMs will be created.

A possible set of permissions could be (these permissions are encapsulated in the pre-defined PlateSpin User role):

- ◆ Change CPU Count
- ◆ Memory
- ◆ Modify Device Settings
- ◆ Settings
- ◆ Console interaction
- ◆ Power Off
- ◆ Power On
- ◆ Reset
- ◆ Suspend
- ◆ Revert to snapshot

If the user will be granted the ability to change the resources used by the VM (i.e. networks, CD iso images, etc), this user will need to be granted the necessary permissions on those resources. For instance, if the user will be given the ability to change the network their VM is attached to, then the user will need to be assigned the Read-only role (or better) on all of the networks being made accessible to the user.

2.3 Access and Communication Requirements across your Protection Network

- ◆ [Section 2.3.1, “Access and Communication Requirements for Workloads,” on page 24](#)
- ◆ [Section 2.3.2, “Access and Communication Requirements for Containers,” on page 25](#)
- ◆ [Section 2.3.3, “Open Port Requirements for PlateSpin Protect Server Hosts,” on page 25](#)
- ◆ [Section 2.3.4, “Protection Across Public and Private Networks Through NAT,” on page 25](#)
- ◆ [Section 2.3.5, “Optimizing Data Transfer over WAN Connections,” on page 26](#)
- ◆ [Section 2.3.6, “Enabling SSL Communication with the PlateSpin Server,” on page 27](#)
- ◆ [Section 2.3.7, “Overriding the Default bash Shell for Executing Commands on Linux Workloads,” on page 27](#)
- ◆ [Section 2.3.8, “Requirements for VMware DRS Clusters as Containers,” on page 28](#)
- ◆ [Section 2.3.9, “Configuring the Application to Function Across NAT,” on page 28](#)

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 2-3 *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 3.5 SP1	

Workload Type	Prerequisites	Required Ports
Windows 7; Windows Server 2008; Windows Vista	<ul style="list-style-type: none"> ◆ Built-in Administrator or domain administrator 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 to allow <i>File and Printer Sharing</i>. Use one of these options: <ul style="list-style-type: none"> ◆ Option 1, using Windows Firewall: Use the basic <i>Windows Firewall Control Panel</i> item (<code>firewall.cpl</code>) and select <i>File and printer Sharing</i> in the list of exceptions. - OR - ◆ Option 2, using Firewall with Advanced Security: Use the <i>Windows Firewall with Advanced Security</i> utility (<code>wf.msc</code>) with the following <i>Inbound Rules</i> enabled and set to Allow: <ul style="list-style-type: none"> ◆ <i>File and Printer Sharing (Echo Request - ICMPv4In)</i> ◆ <i>File and Printer Sharing (Echo Request - ICMPv6In)</i> ◆ <i>File and Printer Sharing (NB-Datagram-In)</i> ◆ <i>File and Printer Sharing (NB-Name-In)</i> ◆ <i>File and Printer Sharing (NB-Session-In)</i> ◆ <i>File and Printer Sharing (SMB-In)</i> ◆ <i>File and Printer Sharing (Spooler Service - RPC)</i> ◆ <i>File and Printer Sharing (Spooler Service - RPC-EPMAP)</i> 	TCP 3725 NetBIOS 137 - 139 SMB (TCP 139, 445 and UDP 137, 138) TCP 135/ 445
Windows Server 2000; Windows XP	<ul style="list-style-type: none"> ◆ Windows Management Instrumentation (WMI) installed <p>WMI (RPC/DCOM) can use TCP ports 135 and 445 as well as random or dynamically assigned ports above 1024. If problems occur when adding the workload, consider temporarily placing the workload in a DMZ or temporarily opening the firewalled ports while adding the workload to PlateSpin Protect.</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) 	TCP 3725 NetBIOS 137 - 139 SMB (TCP 139, 445 and UDP 137, 138) TCP 135/ 445
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 2-4 Access and Communication Requirements for Containers

System	Prerequisites	Required Ports
All containers	Ping (ICMP echo request and response) capability.	
VMware ESX/ESXi 4.1	◆ VMware account with an Administrator role	HTTPS
VMware ESXi 5.0	◆ VMware Web services API and file management API	TCP 443
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 2-5 Open Port Requirements for PlateSpin Protect Server Hosts

Port	Remarks
TCP 80	For HTTP communication
TCP 443	For HTTPS communication (if SSL 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 28](#).
- ◆ **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.
- ◆ **Workload:** When you are attempting to add a workload, specify the public (external) IP address of that workload in the discovery parameters.
- ◆ **Failed-over VM:** During failback, you can specify an alternative IP address for the failed-over workload in [Failback Details \(Workload to VM\) \(page 57\)](#).
- ◆ **Failback Target:** During an attempt to register a failback target, when prompted to provide the IP address of the PlateSpin Server, provide either the local address of the Protect Server host or one of its public (external) addresses recorded in the Server's `web.config` configuration file (see “PlateSpin Protect Server” above).

2.3.5 Optimizing Data Transfer over WAN Connections

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 32.](#)

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: If these values are modified, replication times on high-speed networks, such as Gigabit Ethernet, might be negatively impacted. Before modifying any of these parameters, consider consulting PlateSpin Support first.

[Table 2-6](#) lists the configuration parameters with the defaults and with the values recommended for optimum operation in a high-latency WAN environment.

Table 2-6 Default and Optimized Configuration Parameters in productinternal.config

Parameter	Default Value	Optimized Value
fileTransferThreadcount	2	4 to 6
Controls the number of TCP connections opened for file-based data transfer.		
fileTransferMinCompressionLimit	0 (disabled)	max 65536 (64 KB)
Specifies the packet-level compression threshold in bytes.		
fileTransferCompressionThreadsCount	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.		
fileTransferSendReceiveBufferSize	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 with the PlateSpin Server

Use these settings to enable communication between your Web browser and the PlateSpin server, on which you enabled SSL *after* installing the product. If SSL 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 32](#).

- ◆ **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 Overriding the Default bash Shell for Executing Commands on Linux Workloads

By default, the PlateSpin Protect Server uses the `/bin/bash` shell when executing commands on a Linux source workload.

If required, you can override the default shell by modifying the corresponding registry key on the PlateSpin Protect Server.

See KB Article [KB Article 7010676 \(https://www.netiq.com/support/kb/doc.php?id=7010676\)](https://www.netiq.com/support/kb/doc.php?id=7010676).

2.3.8 Requirements for VMware 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 \(Protection Targets\)” on page 46](#).

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, or vNetwork Distributed Switch, is common to all the ESX servers in the VMware Cluster.
- ◆ The failover workloads (VMs) 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.

2.3.9 Configuring the Application to Function Across NAT

To enable the PlateSpin Protect Server to function across NAT-enabled environments, you must record additional IP addresses 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 32.

- ◆ **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 28
- ◆ [Section 2.4.2, “Language Setup for International Versions of PlateSpin Protect,”](#) on page 32
- ◆ [Section 2.4.3, “Configuring the Product Behavior through XML Configuration Parameters,”](#) on page 32

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 29
- ◆ [“Setting Up Automatic Event Notifications by E-Mail”](#) on page 29
- ◆ [“Setting Up Automatic Replication Reports by E-Mail”](#) on page 31

SMTP Configuration

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

Figure 2-2 Simple Mail Transfer Protocol Settings

The screenshot shows the 'SMTP Settings' form. It has a dark blue header with the title 'SMTP Settings' on the left and a 'Save' button on the right. Below the header, there are six rows of labels and input fields: 'SMTP Server Address:' with an empty text box; 'Port:' with a text box containing '25'; 'Reply Address:' with an empty text box; 'Username:' with an empty text box; 'Password:' with an empty text box; and 'Confirm:' with an empty text box.

To configure SMTP settings:

- 1 In your PlateSpin Protect Web Interface, click *Settings > SMTP*.
- 2 Specify an SMTP server *Address*, a *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” on page 29.
- 2 In your PlateSpin Protect Web Interface, 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*.

The screenshot shows the 'Notification Settings' page. At the top, there are navigation tabs: 'Dashboard', 'Workloads', 'Tasks', 'Reports', 'Settings', 'About', and 'Help'. Under 'Settings', there are sub-tabs: 'Protection Tiers', 'Permissions', 'Containers', 'Email', 'SMTP', and 'Licenses'. The 'Email' sub-tab is active, and 'Notification Settings' is selected. Below this, there is a section for 'Replication Reports Settings'. A checkbox labeled 'Enable Notifications' is checked. To the right of this checkbox is a yellow warning icon and a 'Save' button. Below this section is a table of recipients. The table has a 'Recipients:' label on the left and an 'Address' header. There are four rows of recipients, each with a 'Remove' link and an email address: 'dradmin@platespin.com', 'john_smith@platespin.com', 'sysadmin@platespin.com', and 'webadmin@platespin.com'. At the bottom of the table is a link labeled 'Edit Recipients...'.

- 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> .
Full Replication Successfully Completed	
Full Replication Failed	
Full Replication Missed	Similar to the Incremental Replication Missed event.
Incremental Replication Successfully Completed	
Incremental Replication Failed	
Incremental Replication Missed	Generated when any of the following applies: <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.
Test Failover Completed	Generated upon manually marking a Test Failover operation a success or a failure.
Prepare Failover Completed	
Prepare Failover Failed	
Failover Completed	
Failover Failed	

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 \(page 29\)](#).
- 2 In your PlateSpin Protect Web Interface, 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 it is located behind a NAT server). This URL affects 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 43.

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 Interface 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 Lanuguages 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 Interface”](#) on page 35.

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 33](#).

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 Interface,” on page 35](#)
- ♦ [Section 3.2, “Elements of the PlateSpin Protect Web Interface,” on page 36](#)
- ♦ [Section 3.3, “Workloads and Workload Commands,” on page 38](#)
- ♦ [Section 3.4, “Managing Multiple Instances of PlateSpin Protect and PlateSpin Forge,” on page 40](#)
- ♦ [Section 3.5, “Generating Workload and Workload Protection Reports,” on page 43](#)

3.1 Launching the PlateSpin Protect Web Interface

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

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 Interface and integrated help in one of the supported languages, see [Section 2.4.2, “Language Setup for International Versions of PlateSpin Protect,” on page 32](#).

To launch the PlateSpin Protect Web Interface:

- 1 Open a Web browser and go to:

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

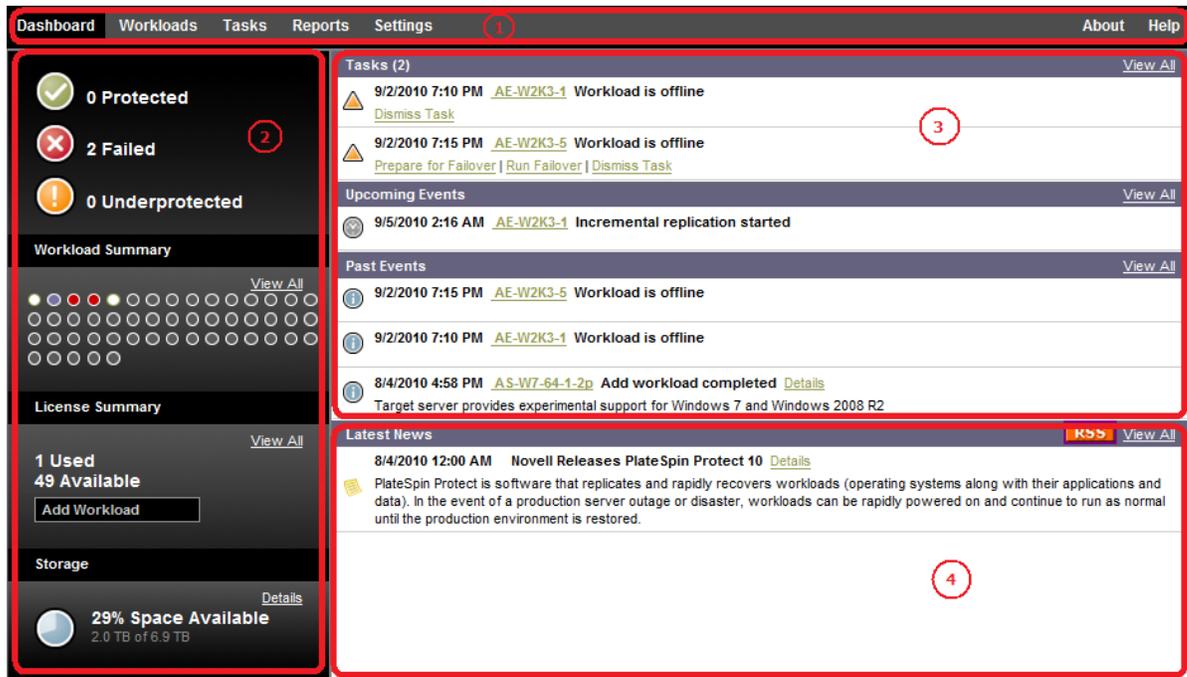
Replace `<hostname | IP_address>` with the hostname or the IP address of your PlateSpin Protect Server host.

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

3.2 Elements of the PlateSpin Protect Web Interface

The default interface of the PlateSpin Protect Web Interface 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 Interface



The Dashboard page consists of the following elements:

1. **Navigation bar:** Found on most pages of the PlateSpin Protect Web Interface.
2. **Visual Summary panel:** Provides a high-level view of the overall state of the PlateSpin Protect workload inventory,
3. **Tasks and Events panel:** Provides information about events and tasks requiring user attention.
4. **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 37](#)
- ♦ [Section 3.2.2, “Visual Summary Panel,” on page 37](#)
- ♦ [Section 3.2.3, “Tasks and Events Panel,” on page 38](#)

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 38](#).
- ◆ **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 43](#).
- ◆ **Settings:** Displays the Settings page, which provides access to the following configuration options:
 - ◆ **Protection Tiers:** See [“Protection Tiers” on page 63](#).
 - ◆ **Permissions:** See [“Setting Up User Authorization and Authentication” on page 16](#).
 - ◆ **Containers:** See [“Adding Containers \(Protection Targets\)” on page 46](#).
 - ◆ **Email/SMTP:** See [“Setting Up Automatic E-Mail Notifications of Events and Reports” on page 28](#).
 - ◆ **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.

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 container 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 28.

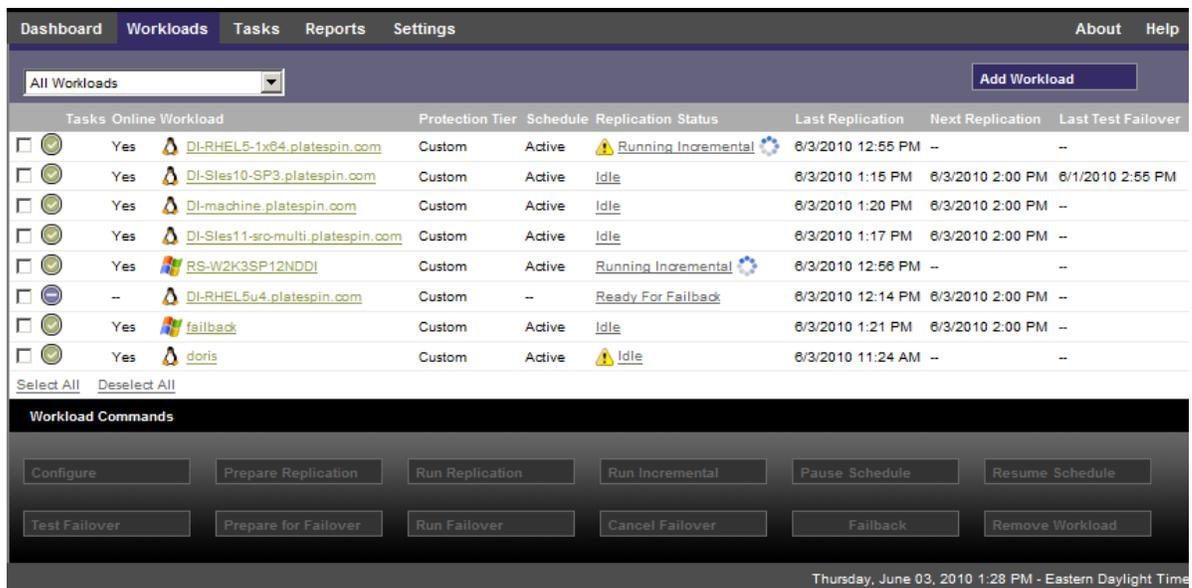
Tasks are special commands that are tied to events that require user intervention. For example, upon completion of a Test Failover command, the system generates an event associated with two tasks: Mark Test as Success and Mark Test as Failure. Clicking either task results in the Test Failover operation 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*

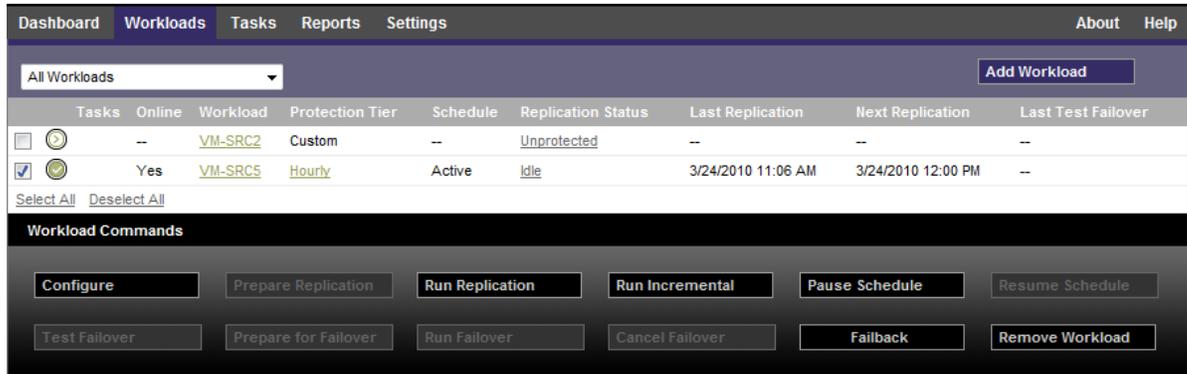


NOTE: All time stamps reflect the time zone of the PlateSpin Protect Server host. This might be different from the time zone of the protected workload or the time zone of the host on which you are running the PlateSpin Protect Web Interface. A display of the server date and time appears at the bottom 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 workload (a virtual machine) on the target container in preparation for workload replication.
<i>Run Replication</i>	Starts replicating the workload according to specified parameters (full replication).
<i>Run Incremental</i>	Performs an incremental transfer of changed data from the source to the target outside the workload protection schedule.
<i>Pause Schedule</i>	Suspends the protection; all scheduled replications are skipped until the schedule is resumed.
<i>Resume Schedule</i>	Resumes the protection according to saved protection settings.
<i>Test Failover</i>	Boots and configures the failover workload in an isolated environment within the container for testing purposes.
<i>Prepare for Failover</i>	Boots the failover workload in preparation for a failover operation.
<i>Run Failover</i>	Boots and configures the failover workload, which takes over the business services of a failed workload.
<i>Cancel Failover</i>	Aborts the failover process.
<i>Failback</i>	Following a failover operation, fails the failover 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 Managing Multiple Instances of PlateSpin Protect and PlateSpin Forge

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

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 3.4.1, “Using the PlateSpin Protect Management Console,” on page 40
- ♦ Section 3.4.2, “About PlateSpin Protect Management Console Cards,” on page 40
- ♦ Section 3.4.3, “Adding Instances of PlateSpin Protect and PlateSpin Forge to the Management Console,” on page 41
- ♦ Section 3.4.4, “Managing Cards on the Management Console,” on page 42

3.4.1 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:

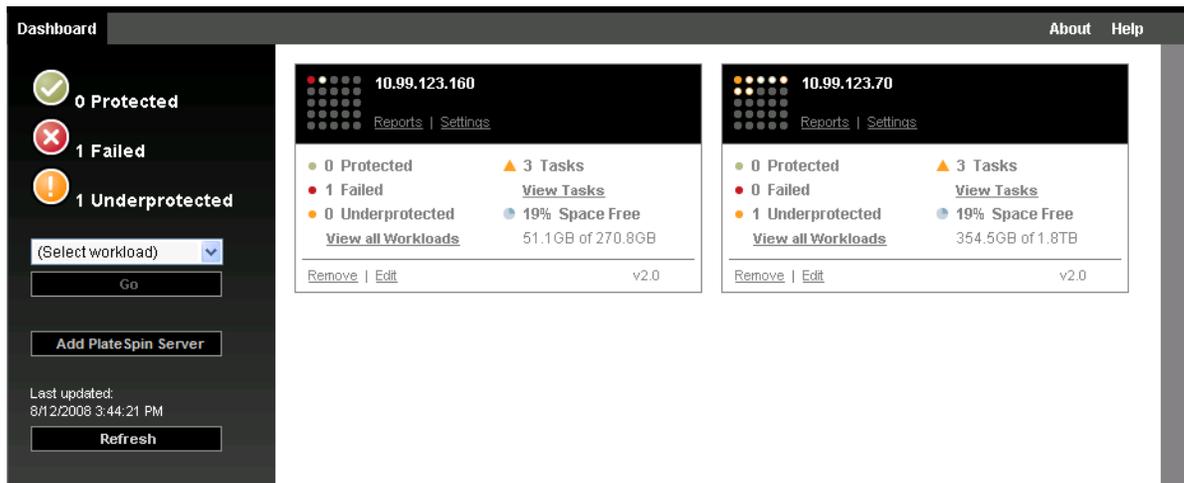
```
http://<IP_address | hostname>/console
```

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.

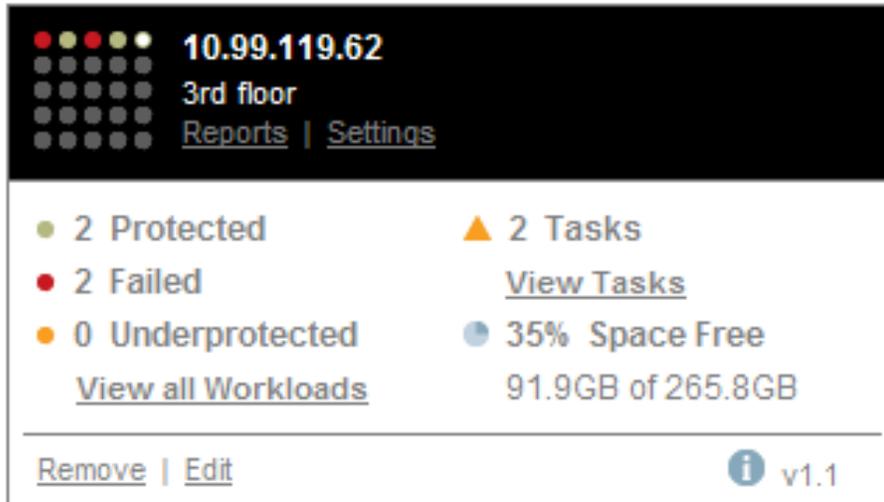
Figure 3-4 The Management Console’s Default Dashboard Page



3.4.2 About PlateSpin Protect Management Console Cards

Individual instances of PlateSpin Protect and PlateSpin Forge, 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 or PlateSpin Forge, 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.

3.4.3 Adding Instances of PlateSpin Protect and PlateSpin Forge to the Management Console

Adding a PlateSpin Protect or Forge 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 running on an instance of PlateSpin Protect or PlateSpin Forge, that instance is not automatically added to the console. It must be manually added.

To add a PlateSpin Protect or Forge instance to the console:

- 1 On the console's main dashboard, click *Add PlateSpin Server*.
The *Add/Edit* page is displayed.
- 2 Specify the URL of the PlateSpin Protect Server host or Forge VM. Use HTTPS if SSL is enabled.
- 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 instance of PlateSpin Protect or PlateSpin Forge 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.

3.4.4 Managing Cards on the Management Console

You can modify the details of a 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 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 card is removed from the dashboard.

3.5 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

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

To generate a report:

- 1 In your PlateSpin Protect Web Interface, 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.

- ♦ [Section 4.1, “Basic Workflow for Workload Protection and Recovery,” on page 45](#)
- ♦ [Section 4.2, “Adding Containers \(Protection Targets\),” on page 46](#)
- ♦ [Section 4.3, “Adding Workloads for Protection,” on page 47](#)
- ♦ [Section 4.4, “Configuring Protection Details and Preparing the Replication,” on page 49](#)
- ♦ [Section 4.5, “Starting the Workload Protection,” on page 51](#)
- ♦ [Section 4.6, “Aborting Commands,” on page 52](#)
- ♦ [Section 4.7, “Failover,” on page 53](#)
- ♦ [Section 4.8, “Failback,” on page 55](#)
- ♦ [Section 4.9, “Reprotecting a Workload,” on page 59](#)

4.1 Basic Workflow for Workload Protection and Recovery

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

- 1 Preparation:** This step involves preparatory steps to ensure that your workloads, containers, and environment meet the required criteria.
 - 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 23](#).
 - 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 \(https://www.netiq.com/support/kb/doc.php?id=7005873\)](https://www.netiq.com/support/kb/doc.php?id=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 \(https://www.netiq.com/support/kb/doc.php?id=7005872\)](https://www.netiq.com/support/kb/doc.php?id=7005872).

- ♦ (Optional) Prepare your `freeze` and `thaw` scripts to execute on your source workload upon each replication.
See [“Using Freeze and Thaw Scripts for Every Replication \(Linux\)”](#) on page 66.
- 2 Inventory:** This step involves adding workloads and containers to the PlateSpin Protect Server database.

Workloads that you want to protect and containers that host failover workloads must be properly inventoried. You can add workloads and containers in any order; however, every protection schedule requires a defined workload and container that were inventoried by the PlateSpin Protect Server. See [“Adding Containers \(Protection Targets\)”](#) on page 46 and [“Adding Workloads for Protection”](#) on page 47.
 - 3 Definition of the Protection Schedule:** In this step, you define the details and specifications of a protection schedule and prepare the replication.

See [“Configuring Protection Details and Preparing the Replication”](#) on page 49.
 - 4 Initiating the Protection:** This step commences the protection schedule according to your requirements.

See [“Starting the Workload Protection”](#) on page 51.
 - 5 Optional Steps in the Protection Lifecycle:** These steps are outside the automated replication schedule but are often useful in different situations or might be dictated by your business continuity strategy.
 - ♦ *Manual incremental.* You can run an incremental replication manually, outside the workload protection schedule, by clicking *Run Incremental*.
 - ♦ *Testing.* You can test failover functionality in a controlled manner and environment. See [Using the Test Failover Feature](#).
 - 6 Failover:** This step carries out a failover of your protected workload to its replica running in your VM container. See [“Failover”](#) on page 53.
 - 7 Failback:** This step corresponds to the business resumption phase after you have addressed any problems with your production workload. See [“Failback”](#) on page 55.
 - 8 ReProtection:** This step enables you to redefine the original protection schedule for your workload. See [“Reprotecting a Workload”](#) on page 59

Except for Steps 1, 8, and 9, these are represented by workload commands on the Workloads page. See [“Workloads and Workload Commands”](#) on page 38.

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

4.2 Adding Containers (Protection Targets)

A container is a protection infrastructure that acts as the host of a protected workload’s regularly-updated replica. That infrastructure can be either a VMware ESX Server or a VMware DRS Cluster.

To be able to protect a workload, you must have a a workload and a container inventoried by (or *added to*) the PlateSpin Protect Server.

To add a container:

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

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 X735Q @ 2.93GHz	31.2 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* or *VMware DRS Cluster*). Make sure the container is supported.

For more information, see [“Supported VM Containers”](#) 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 administrator-level credentials for accessing the required host. See [“Guidelines for Workload and Container Credentials”](#) on page 62.
- ◆ **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.

4.3 Adding Workloads for Protection

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

To protect a workload, you must have a workload and a container inventoried by (or *added to*) the PlateSpin Protect Server.

To add a workload:

- 1 Follow the required preparatory steps.
See [Step 1](#) in “[Basic Workflow for Workload Protection and Recovery](#)” on page 45.
- 2 On the Dashboard or Workloads page, click *Add Workload*.

The PlateSpin Protect Web Interface 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: [masked] Test Credentials

Workload Commands Add Workload Add and New

- 3 Specify the required workload details:
 - ♦ **Workload Settings:** Specify your workload’s hostname or IP address, the operating system, administrator-level credentials.

Use the required credential format. See “[Guidelines for Workload and Container Credentials](#)” on page 62.

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

- 4 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, and the new workload becomes available on the Workloads page.

If you haven’t added a container yet, add one to prepare for protecting the workload, otherwise, skip to “[Configuring Protection Details and Preparing the Replication](#)” on page 49

4.4 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 45), relevant settings are read from the protection details.

To configure your workload’s protection details:

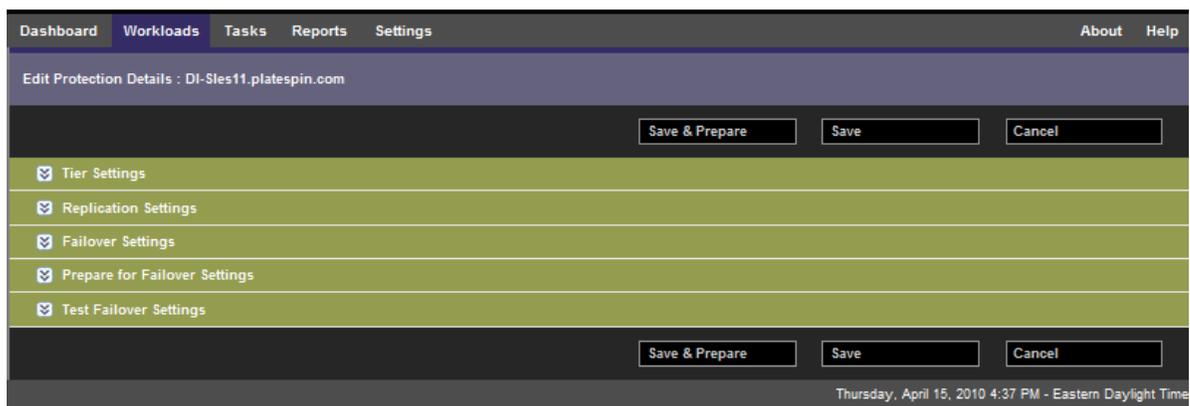
- 1 Add a workload. See [“Adding Workloads for Protection”](#) on page 47.
- 2 On the Workloads page, select the required workload and click *Configure*.
Alternatively, you can click the name of the workload.
- 3 Select the required replication settings.
See [“Initial Replication Method \(Full and Incremental\)”](#) on page 65.
- 4 Select a Protection Target (Container). This can be either a 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 65.
- 5 Configure the protection details in each set of settings as dictated by your business continuity needs. See [“Workload Protection Details”](#) on page 49.
- 6 Correct any validation errors, if displayed by the PlateSpin Protect Web Interface.
- 7 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.

4.4.1 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:

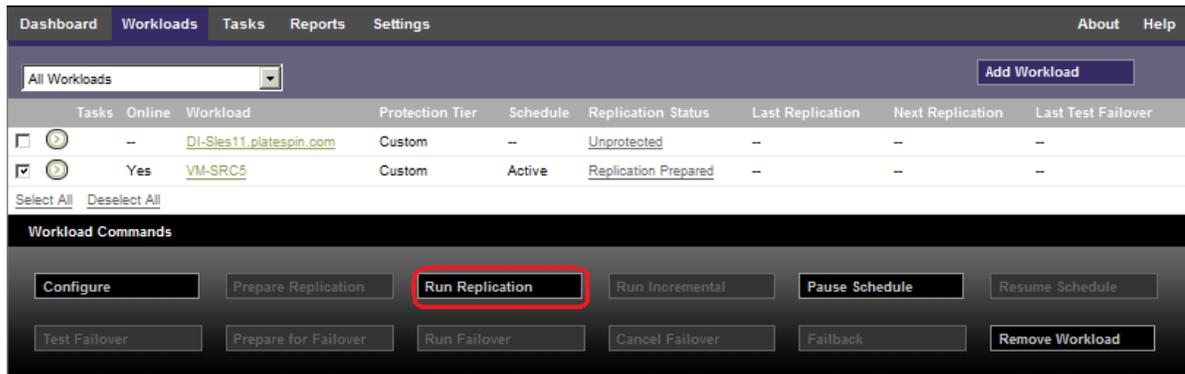
Table 4-1 Workload Protection Details

Parameter Set (Settings)	Details
Tier	Indicates the Protection Tier that the current protection uses. See “Protection Tiers” on page 63 .
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 62.</p> <p>Source Credentials: Required for accessing the workload. See “Guidelines for Workload and Container Credentials” on page 62.</p> <p>Number of CPUs: Enables you to specify the required number of vCPUs assigned to the failover workload (applicable only when the selected method of initial replication is <i>Full</i>).</p> <p>Replication Network: Enables you to separate replication traffic based on virtual networks defined on your VM container. See “Networking” on page 69.</p> <p>Configuration File Datastore: Enables you to select a datastore associated with your VM container for storing VM configuration files. See “Recovery Points” on page 64.</p> <p>Protected Volumes: Use these options to select volumes for protection and to assign their replicas to specific datastores on your VM container.</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 actually required by data on 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 66.</p>
Failover	<p>VM Memory: Enables you to specify the amount of memory allocated to the failover workload.</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 administrator credentials are required.</p> <p>Network Connections: Use these options to control the LAN settings of the failover workload. See “Networking” on page 69.</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 66.</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 69 .

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 administrator credentials are required.</p> <p>Network Connections: Controls the LAN settings of the temporary workload. See “Networking” on page 69.</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 66.</p>

4.5 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 workload has been protected:

- ♦ Changing the size of a volume that is under block-level protection invalidates the protection. The appropriate procedure is to 1. remove the workload from protection, 2. resize the volumes as required. 3. re-establish the protection by re-adding the workload, configuring its protection details, and starting replications.
- ♦ 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.

4.6 Aborting Commands

You can abort a command after executing it and while it is underway, on the Command Details page of that particular command.

To access the Command Details page of any command that is underway:

- 1 Go to the Workloads page.
- 2 Locate the required workload and click the link representing the command currently executing on that workload.

Workload	Protection	Command	Status	Command	Start Time	Last Run	Next Run
CL-2K8R2-VM1	No	Custom	Active	Idle	3/5/2012 12:23 AM	4/11/2012 12:00 AM	--
DI-Sles11x64-Src	Yes	every 4 hours	Active	Fallover Prepared	3/29/2012 8:13 AM	4/9/2012 12:00 PM	3/23/2012 3:32 PM
ma-cl-slessp2_site	--	every 4 hours	--	Live	3/15/2012 2:49 PM	--	3/9/2012 2:44 PM
VISTACLIENT	Yes	Custom	Active	Running Incremental	3/28/2012 10:21 AM	4/9/2012 12:00 PM	3/23/2012 5:14 PM
CL-VISTASP1-SRC	--	every 4 hours	--	Live	2/22/2012 2:55 PM	--	--
CL-XPX64-SRC	Yes	Custom	Active	Idle	4/9/2012 10:17 AM	4/9/2012 12:00 PM	3/23/2012 5:15 PM

The PlateSpin Protect Web Interface displays the appropriate Command Details page:

The screenshot shows the 'Command Details' page for a 'Running Incremental' command. The status is 'Running' with a warning icon. The duration is '3d 21h 31m 37s'. The step is 'Copy data (2%)'. The command summary shows 'Setting Up Controller (1%)'. The events table shows 'Incremental replication started' at '4/5/2012 2:00 PM'. The workload commands section has an 'Abort' button highlighted with a red box.

- 3 Click *Abort*.

4.7 Failover

A *Failover* results in the business function of a failed workload being taken over by a failover workload within a PlateSpin Protect VM container.

- ◆ [Section 4.7.1, “Detecting Offline Workloads,” on page 53](#)
- ◆ [Section 4.7.2, “Performing a Failover,” on page 54](#)
- ◆ [Section 4.7.3, “Using the Test Failover Feature,” on page 54](#)

4.7.1 Detecting Offline Workloads

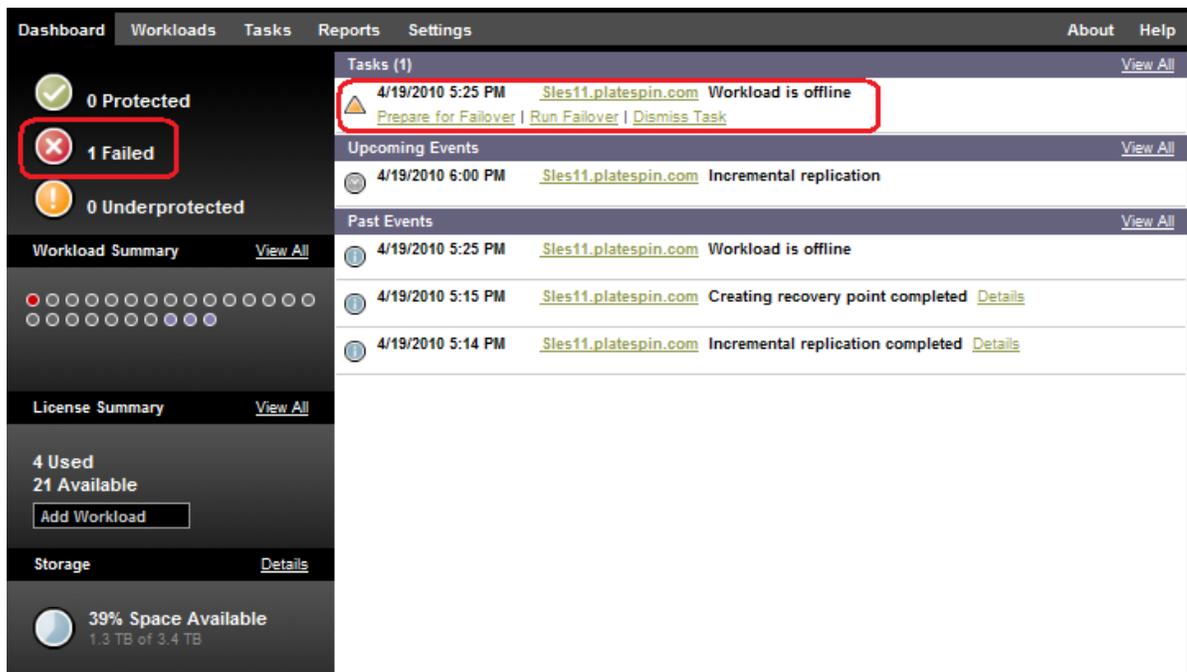
PlateSpin Protect constantly monitors your protected workloads. If an attempt to monitor a workload fails for a predefined number of times, PlateSpin Protect generates a *Workload is offline* event. Criteria that determine and log a workload failure are part of a workload protection’s Tier settings (see the [Tier](#) row in [“Workload Protection Details” on page 49](#)).

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 28](#).

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 (see [“Aborting Commands” on page 52](#)), and then proceed to the *Run Failover* command. See [“Performing a Failover” on page 54](#).

The following figure shows the PlateSpin Protect Web Interface’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 (‘Workload Offline’)



4.7.2 Performing a Failover

Failover settings, including the failover 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 49.

You can use the following methods to perform a failover:

- ◆ Select the required workload on the Workloads page and click *Run Failover*.
- ◆ Click the corresponding command hyperlink of the *Workload is offline* event in the Tasks and Events pane. See [Figure 4-1](#).
- ◆ Run a *Prepare for Failover* command to boot the failover VM ahead of time. You still have the option to cancel the failover (useful in staged failovers).

Use one of these methods to start the failover process and select a recovery point to apply to the failover workload (see "Recovery Points" on page 64). Click *Execute* and monitor the progress. Upon completion, the replication status of the workload should indicate *Live*.

For testing the failover workload or testing the failover process as part of a planned disaster recovery exercise, see "Using the Test Failover Feature" on page 54.

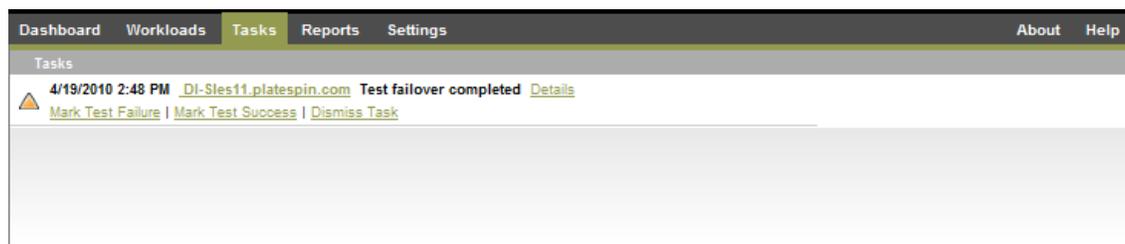
4.7.3 Using the Test Failover Feature

PlateSpin Protect provides you with the capability to test the failover functionality and the integrity of the failover workload. This is done by using the *Test Failover* command, which boots the failover 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 failover workload (see the [Test Failover](#) row in "Workload Protection Details" on page 49).

- 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 64), 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 failover workload. Use the VMware vSphere Client to access the failover 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 and is retrievable by reports. *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 failover workload, and the protection returns to its pre-test state.

4.8 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.

Supported failback methods depend on the target infrastructure type and the degree of automation of the failback process:

- ♦ **Automated Failback to a Virtual Machine:** Supported for VMware ESX platforms and VMware DRS Clusters.
- ♦ **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 4.8.1, “Automated Failback to a VM Platform,” on page 55](#)
- ♦ [Section 4.8.2, “Semi-Automated Failback to a Physical Machine,” on page 58](#)
- ♦ [Section 4.8.3, “Semi-Automated Failback to a Virtual Machine,” on page 59](#)

4.8.1 Automated Failback to a VM Platform

The following containers are supported as automated failback targets:

Target	Notes
VMware DRS Cluster in vSphere 5.1	<ul style="list-style-type: none"> ♦ The DRS configuration must be either Partially Automated or Fully Automated (it must not be set to Manual) ♦ As a VM Container, the DRS Cluster must consist of ESXi 5.1 servers only, and can be managed by vCenter 5.1 only.
VMware DRS Cluster in vSphere 5.0	<ul style="list-style-type: none"> ♦ The DRS configuration must be either Partially Automated or Fully Automated (it must not be set to Manual) ♦ As a VM Container, the DRS Cluster must consist of ESXi 5.0 servers only, and can be managed by vCenter 5.0 only.
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) ♦ As a VM Container, the Cluster, as a container, can use a combination of ESX 4.1 and ESXi 4.1 servers, and can be managed by vCenter 4.1 only
VMware ESXi 4.1, 5.0, 5.1	ESXi versions must have a paid license; protection is unsupported with these systems if they are operating with a free license.
VMware ESX 4.1	

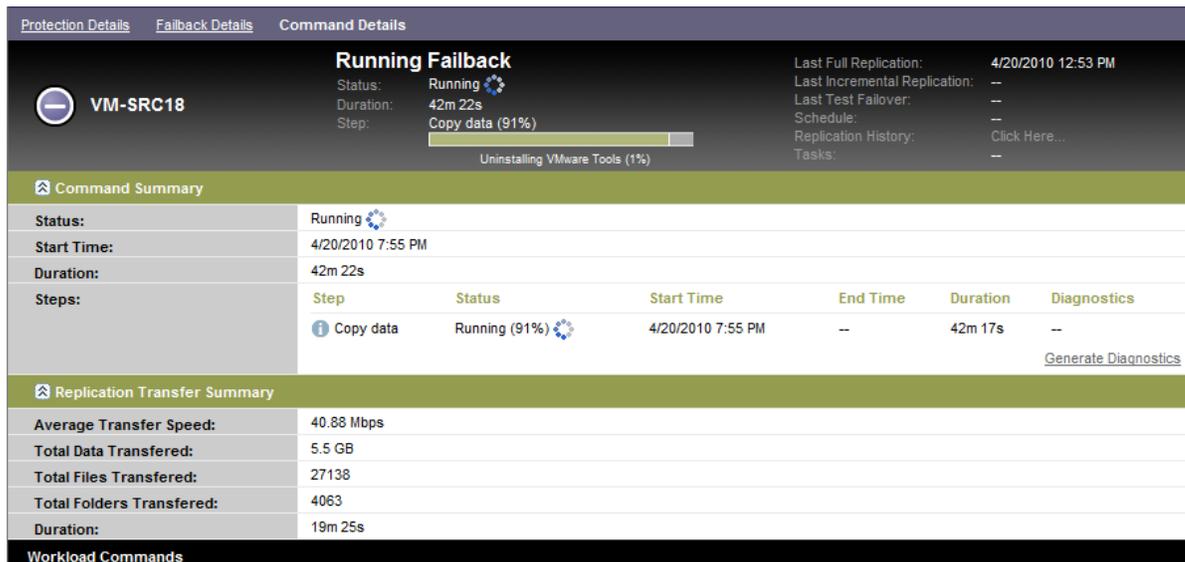
Use these steps to do an automated failback of a failover workload to a target VMware container.

- 1 Following a failover, select the workload on the Workloads page and click *Failback*.
- 2 Specify the following sets of parameters:
 - ♦ **Workload Settings:** Specify the failover workload’s hostname or IP address and provide administrator-level credentials. Use the required credential format (see “[Guidelines for Workload and Container Credentials](#)” on page 62).
 - ♦ **Failback Target Settings:** Specify 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 65.
 - ♦ **Target Type:** Select *Virtual Target*. If you don’t yet have a failback container, click *Add Container* and inventory a supported VM host using administrator-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 57.
- 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 Interface.

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: Enables you to select a data transfer mechanism and security through encryption. See “Transfer Methods” on page 62.</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 69.</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 66.</p> <p>Alternative Address for Source: Accepts input of an additional IP address for the failed-over VM if applicable. See “Protection Across Public and Private Networks Through NAT” on page 25.</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 administrator 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 66.</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. When the failback is complete, a <i>Reprotect</i> command will be available in the PlateSpin Protect Web Interface for the failed-back workload.◆ No reprotect: Select this option if you don’t intend to re-create a protection contract for the target workload. To protect the failed-back workload upon completion, you will have to re-inventory that workload and reconfigure its protection details.

4.8.2 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 69.
- 2 (Optional: Windows platforms) Run the PS Analyzer tool to determine whether any drivers are missing. See [“Analyzing Device Drivers with PlateSpin Analyzer \(Windows\)”](#) on page 77.
- 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 78.
- 4 Following a failover, select the workload on the Workloads page and click *Failback*.
- 5 Specify the following sets of parameters:
 - ♦ **Workload Settings:** Specify the failover workload’s hostname or IP address and provide administrator-level credentials. Use the required credential format (see [“Guidelines for Workload and Container Credentials”](#) on page 62).
 - ♦ **Failback Target Settings:** Specify the following parameters:
 - ♦ *Replication Method:* Select the scope of data replication. See [“Initial Replication Method \(Full and Incremental\)”](#) on page 65.
 - ♦ *Target Type:* Select the *Physical Target* option and then select the physical machine you registered in [Step 1](#).

The screenshot shows the 'CONFIGURE FAILBACK' step of a wizard. The interface is divided into three main sections: 'PREPARE FAILBACK', 'CONFIGURE FAILBACK', and 'RUN FAILBACK'. The 'CONFIGURE FAILBACK' section is active and contains two main configuration areas: 'Workload Settings' and 'Failback Target Settings'.
Under 'Workload Settings', there is a 'Hostname or IP:' field with the value 'MA--Rhel5u3'. Below it are 'Credentials:' fields for 'User Name:' (containing 'root') and 'Password:' (masked with dots). A 'Test Credentials' link is visible below the password field.
Under 'Failback Target Settings', there are three fields: 'Replication Method:' with radio buttons for 'Full Replication' (selected) and 'Incremental Replication'; 'Target type:' with radio buttons for 'Virtual Targets' and 'Physical Targets' (selected); and 'Failback Target:' which shows a dropdown menu with the text '[Selection required below]' and a red 'x' icon. Below this field, a message states 'No physical targets available.'
At the bottom of the configuration area, there is a note: 'Note: To add a physical target, boot up and register the physical server with PlateSpin Failback ISO Image. To download, visit the [PlateSpin Resource Centre](#).'
The bottom of the screen features a dark 'Workload Commands' bar with a 'Save and Prepare' button.

- 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.

4.8.3 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 SP2
- ♦ Microsoft Hyper-V Server 2008 (*not* R2)

NOTE: You can also do a semi-automated failback to a container, for which there is fully-automated failback support (VMware ESX and DRS Cluster targets).

4.9 Reprotecting a Workload

A *Reprotect* operation, the next logical step after a *Failback*, completes the workload protection lifecycle and starts it anew. Following a successful Failback operation, a *Reprotect* command becomes available in the PlateSpin Protect Web Interface interface, and the system applies the same protection details as those indicated during the initial configuration of the protection contract.

NOTE: The *Reprotect* command becomes available only if you selected the *Reprotect* option in the Failback details. See [“Failback” on page 55](#).

The rest of the workflow covering the protection lifecycle is the same as that in normal workload protection operations; you can repeat it as many times as required.

5 Essentials of Workload Protection

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

- ◆ [Section 5.1, “Workload License Consumption,” on page 61](#)
- ◆ [Section 5.2, “Guidelines for Workload and Container Credentials,” on page 62](#)
- ◆ [Section 5.3, “Transfer Methods,” on page 62](#)
- ◆ [Section 5.4, “Protection Tiers,” on page 63](#)
- ◆ [Section 5.5, “Recovery Points,” on page 64](#)
- ◆ [Section 5.6, “Initial Replication Method \(Full and Incremental\),” on page 65](#)
- ◆ [Section 5.7, “Service and Daemon Control,” on page 66](#)
- ◆ [Section 5.8, “Using Freeze and Thaw Scripts for Every Replication \(Linux\),” on page 66](#)
- ◆ [Section 5.9, “Volumes,” on page 67](#)
- ◆ [Section 5.10, “Networking,” on page 69](#)
- ◆ [Section 5.11, “Registering Physical Machines with PlateSpin Protect for Failback,” on page 69](#)
- ◆ [Section 5.12, “Advanced Workload Protection Topics,” on page 71](#)

5.1 Workload License Consumption

Your PlateSpin Protect product license entitles you to a specific number of workloads for protection through workload licensing. Every time you add a workload for protection, the system consumes a single workload license from your license pool. You can recover a consumed license, if you remove a workload, up to a maximum of five times.

For information about product licensing and license activation, see [“Product Licensing” on page 15](#).

5.2 Guidelines for Workload and Container Credentials

PlateSpin Protect must have administrator-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 5-1 Workload and Container Credentials

To Discover	Credentials	Remarks
All Windows workloads	Local or domain administrator 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 administrator credentials	
All Linux workloads	Root-level username and password	Non-root accounts must be properly configured to use <code>sudo</code> . See KB Article 7920711 (https://www.netiq.com/support/kb/doc.php?id=7920711) .
VMware ESX 4.1, ESXi 5.0	ESX account with administrator role.	If ESX is configured for Windows domain authentication, you can also use your Windows domain credentials.

5.3 Transfer Methods

A transfer method describes the way data is replicated from a source workload 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 and 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 and leverages LVM snapshots if available (this is the default and recommended option). See [KB Article 7005872](https://www.netiq.com/support/kb/doc.php?id=7005872) (<https://www.netiq.com/support/kb/doc.php?id=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](https://www.netiq.com/support/kb/doc.php?id=7005873) (<https://www.netiq.com/support/kb/doc.php?id=7005873>).

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

- ◆ **File-level:** Data is replicated on a file-by-file basis (Windows only). Supported with or without VSS, but using VSS is highly recommended.

NOTE: Not all workloads support VSS, and in some cases supported transfer methods are determined by a Service Pack level. For further information, see [KB Article 7005870](https://www.netiq.com/support/kb/doc.php?id=7005870).

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.

5.4 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 to encrypt data transmission
- ◆ 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 offline (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 Interface, 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: The blackout start and end times are based on the system clock on your PlateSpin Protect Server.</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 64 .
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.

5.5 Recovery Points

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

Each protected workload has at least one recovery point and may have a maximum of 32 recovery points.

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

5.6 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 failover workload), or from a failover workload to its original virtual or physical infrastructure.
- ♦ **Incremental:** Only differences are transferred from a source to its target, provided that they have similar operating system and volume profiles.
 - ♦ 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 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 58).

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 Interface displays the Prepare for Incremental Replication page.

Name	Description	CPU	Memory	Free Space	Last Refresh
comp212	VMware ESX Server 4.0.0.175825	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 changes detected by the block-based component while it is monitoring a running workload.

5.7 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 workload is replicated 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 66](#).

- ♦ **Target startup state/run level control:** You can select the startup state (Windows) or the run level (Linux) of services/daemons on the failover VM. 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.

5.8 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.

The `freeze` script 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 66](#)). 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
```

5.9 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 Interface for you to specify the volumes you require for protection.

PlateSpin Protect supports several types of storage, including Windows dynamic disks, LVM (version 2 only), RAID, and SAN.

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

- ♦ Non-volume storage, such as a swap partition that is associated with the source workload, is recreated in the failover 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 show the Replication Settings parameter set for a Linux workload with multiple volumes and two logical volumes in a volume group.

Figure 5-1 Volumes, Logical Volumes, and Volume Groups of a Protected Linux Workload

<input checked="" type="checkbox"/> Tier Settings				
<input checked="" type="checkbox"/> Replication Settings				
Encrypt Data Transfer:	No			
Source Credentials:	root			
Number of CPUs:	1			
Replication Network:	DHCP - VM Network			
Recovery Point Datastore:	Storage2 (669.7 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:	--			
<input checked="" type="checkbox"/> Failover Settings				
<input checked="" type="checkbox"/> Prepare for Failover Settings				
<input checked="" type="checkbox"/> Test Failover Settings				
<input checked="" type="checkbox"/> Recovery Points				
<input checked="" type="checkbox"/> 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 failover workload:

Figure 5-2 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/NEWPOOL (NSSFS)	23.3 MB	999.6 MB	NEWPOOL	
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	Datastore	Thin Disk
	<input checked="" type="checkbox"/>	/dev/evms/sda1	dev-comp124:storage	70.6 MB	dev-comp124:storage	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	NEWPOOL	dev-comp124:storage	1023.0 MB	dev-comp124:storage	<input type="checkbox"/>
Daemons to Stop During Replication:	Add Daemons					

5.10 Networking

PlateSpin Protect enables you to control your failover 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 failover 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 failover workload during a Test Failover stage.

5.11 Registering Physical Machines with PlateSpin Protect for Failback

If the required target infrastructure for a failback 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 PlateSpin boot ISO image.

You can download the PlateSpin boot ISO image from the [PlateSpin Protect area of Novell Downloads \(http://download.novell.com\)](#) by doing a search with the following parameters:

- ♦ *Product or Technology:* PlateSpin Protect
- ♦ *Select Version:* PlateSpin Protect 10.4
- ♦ *Date Range:* All Dates

Use the image appropriate to your target machine:

Table 5-2 Boot ISO Images for Target Physical Machines

Filename	Remarks
<<NEW BOOT ISO IMAGE NAME>>	<<WINDOWS/LINUX; details>>
<<discard>>WindowsFailback.iso	Windows
<<discard>>WindowsFailback-WinPE3.iso	For use with hardware not supported by WindowsFailback.zip
<<discard>>LinuxFailback.iso	Linux systems
<<?>>WindowsFailback-Cisco.iso	Windows systems on Cisco hardware
<<?>>WindowsFailback-Dell.iso	Windows systems on Dell hardware
<<?>>WindowsFailback-Fujitsu.iso	Windows systems on Fujitsu hardware

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

- ♦ [Section 5.11.1, “Registering Target Physical Machines,” on page 70](#)

5.11.1 Registering Target Physical Machines

<<Section needs an update to reflect the removal of WinPE>>

- 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 “<<[Injecting Device Drivers Using the Recovery Tool Command Line Utility \(Windows\)>>](#)” on page 70.

- 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 hostname or the IP address of your PlateSpin Protect Server host.

- 7 Provide your administrator-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 When prompted to indicate whether to use HTTPS, enter `Y` if you have enabled SSL, and `N` if you have not.

After a few minutes, the physical machine should be available in the failback settings of the PlateSpin Protect Web Interface.

<<Injecting Device Drivers Using the Recovery Tool Command Line Utility (Windows)>>

<<This section needs to be removed (or the tool ported to Mono)>>

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 70](#)).

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



```
C:\ 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 (for x86 systems: 2.6.32.54-0.3-pae, for x64 systems: 2.6.32.54-0.3-default) and are appropriate for the target architecture. See also [KB Article 7005990](#).

- 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 unmount <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.

5.12 Advanced Workload Protection Topics

- ♦ [Section 5.12.1, “Protecting Windows Clusters,” on page 72](#)
- ♦ [Section 5.12.2, “Linux Failback to a Paravirtualized VM on Xen on SLES,” on page 72](#)
- ♦ [Section 5.12.3, “Using Workload Protection Features through the PlateSpin Protect Web Services API,” on page 75](#)

5.12.1 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 45](#)).

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.

5.12.2 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 (`xmpsadministrator-`), 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 73](#)
- ♦ [“Linux Failback to an Existing Paravirtualized VM” on page 74](#)

Linux Failback to a New Paravirtualized VM

- 1 Copy the PlateSpin Linux boot ISO to the target Xen on SLES server. See [Table 5-2, “Boot ISO Images for Target Physical Machines,”](#) on page 69.
- 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 failover VM).
 - 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 58.
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
kjournald 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
kjournald 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'

#####

[DB]$_
```

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 on 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 on SLES server. See [Table 5-2, “Boot ISO Images for Target Physical Machines,”](#) on page 69.

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/linuxfailback.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 58](#).
- 6 Reboot the VM, run `switch`, and reconfigure the workload as described in [“Linux Failback to a New Paravirtualized VM” on page 73](#) (from [Step 4](#) to [Step 9](#) only).

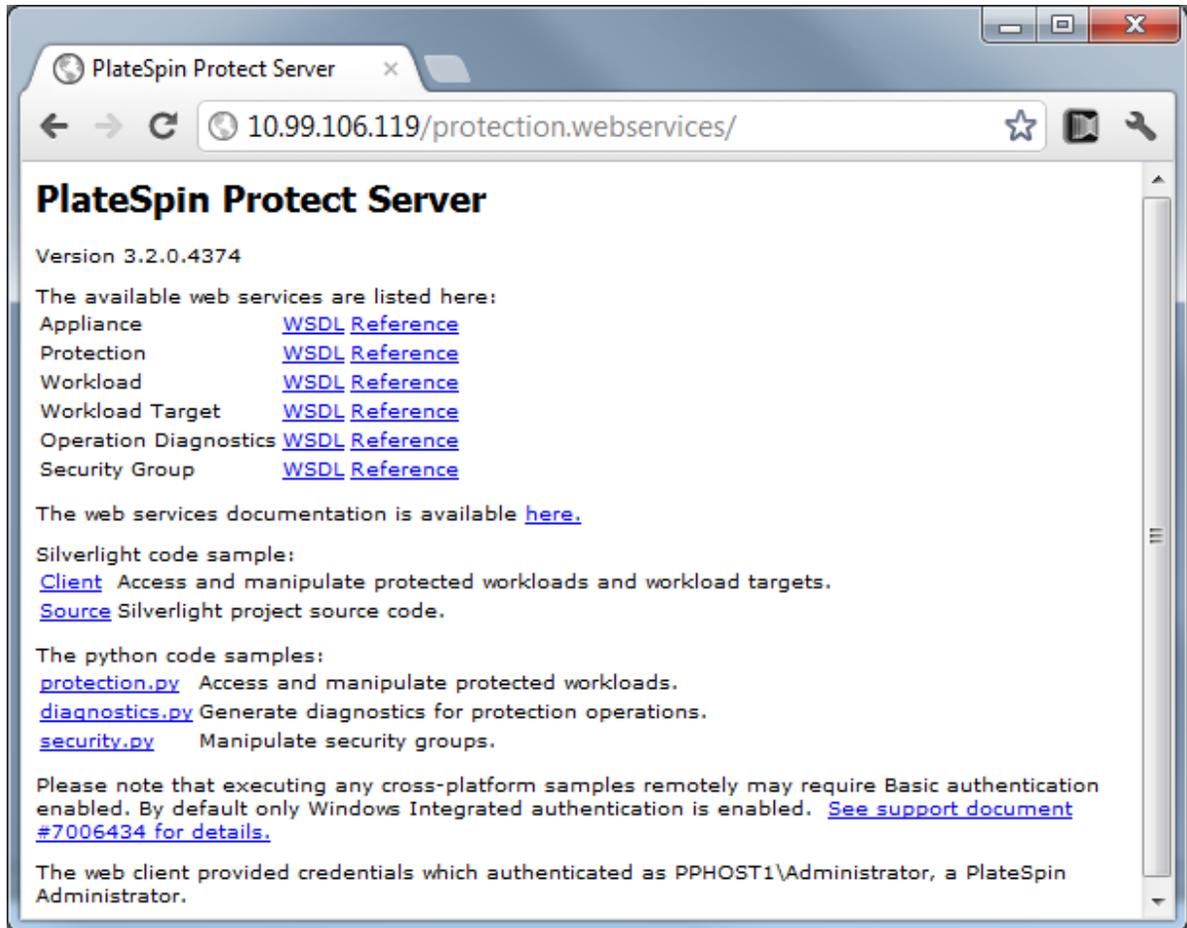
5.12.3 Using Workload Protection Features through the PlateSpin Protect Web Services API

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.

Figure 5-3 The Front Page of the Protection Web Services API



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.

6 Auxiliary Tools for Working with Physical Machines

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

- ♦ [Section 6.1, “Analyzing Device Drivers with PlateSpin Analyzer \(Windows\),” on page 77](#)
- ♦ [Section 6.2, “Managing Device Drivers,” on page 78](#)

6.1 Analyzing Device Drivers with PlateSpin Analyzer (Windows)

Before running a workload failback 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 Device Drivers with PlateSpin Analyzer \(Windows\)” on page 77](#).

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 78](#)
- ◆ [Section 6.2.2, “Packaging Device Drivers for Linux Systems,” on page 79](#)
- ◆ [Section 6.2.3, “Uploading Drivers to the PlateSpin Protect Device Driver Database,” on page 79](#)

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 79](#).

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 boot ISO image. See [Table 5-2, “Boot ISO Images for Target Physical Machines,” on page 69](#).

- 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 79](#).

6.2.3 Uploading Drivers to the PlateSpin Protect Device Driver Database

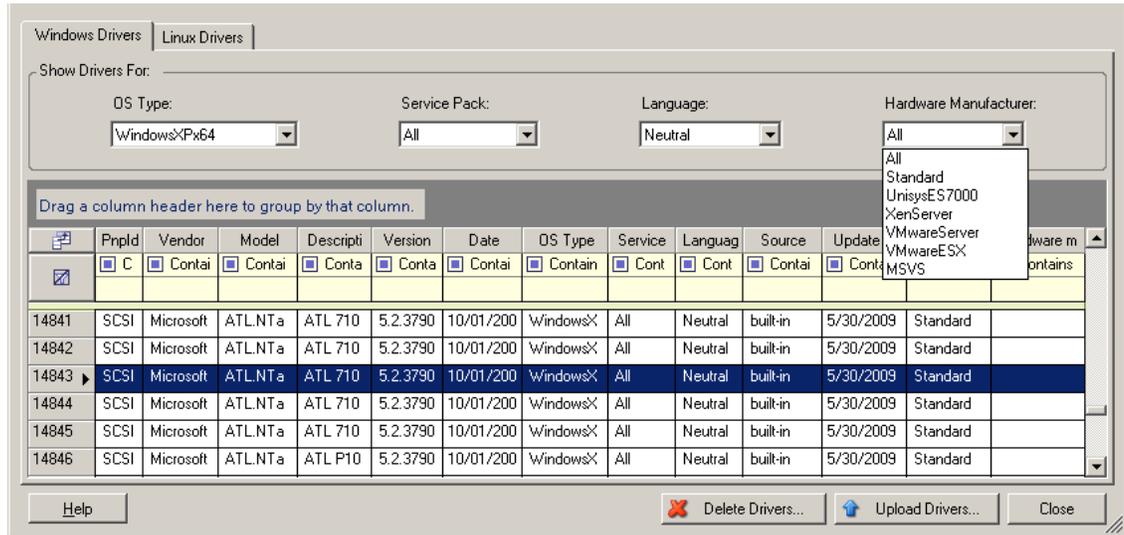
Use the PlateSpin Driver Manager to upload device drivers to the driver database.

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.

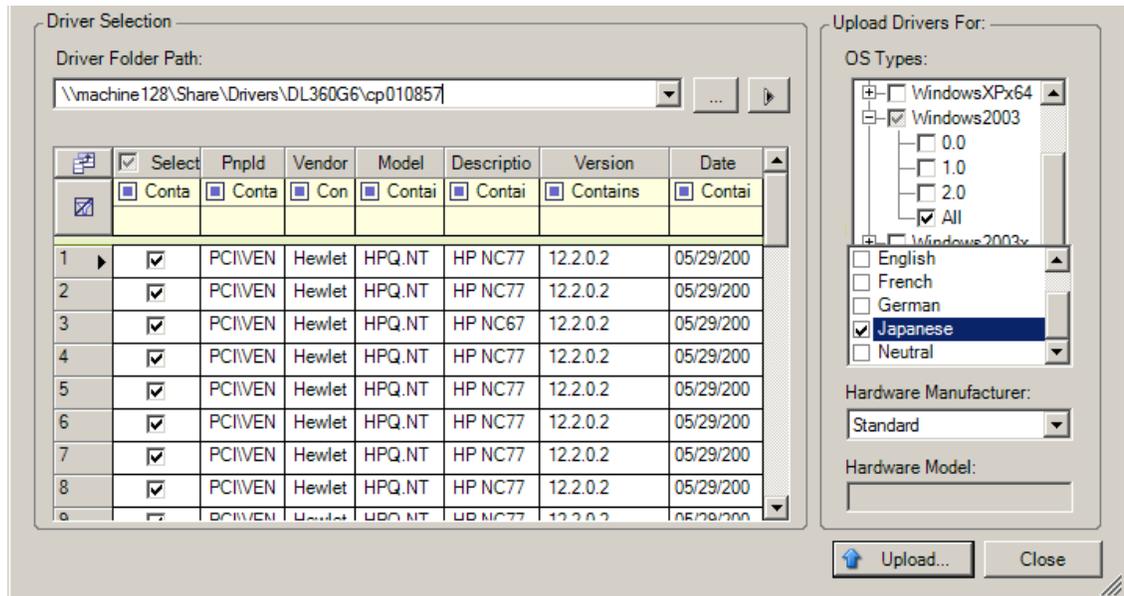
- ♦ [“Device Driver Upload Procedure \(Windows\)” on page 80](#)
- ♦ [“Device Driver Upload Procedure \(Linux\)” on page 81](#)

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.

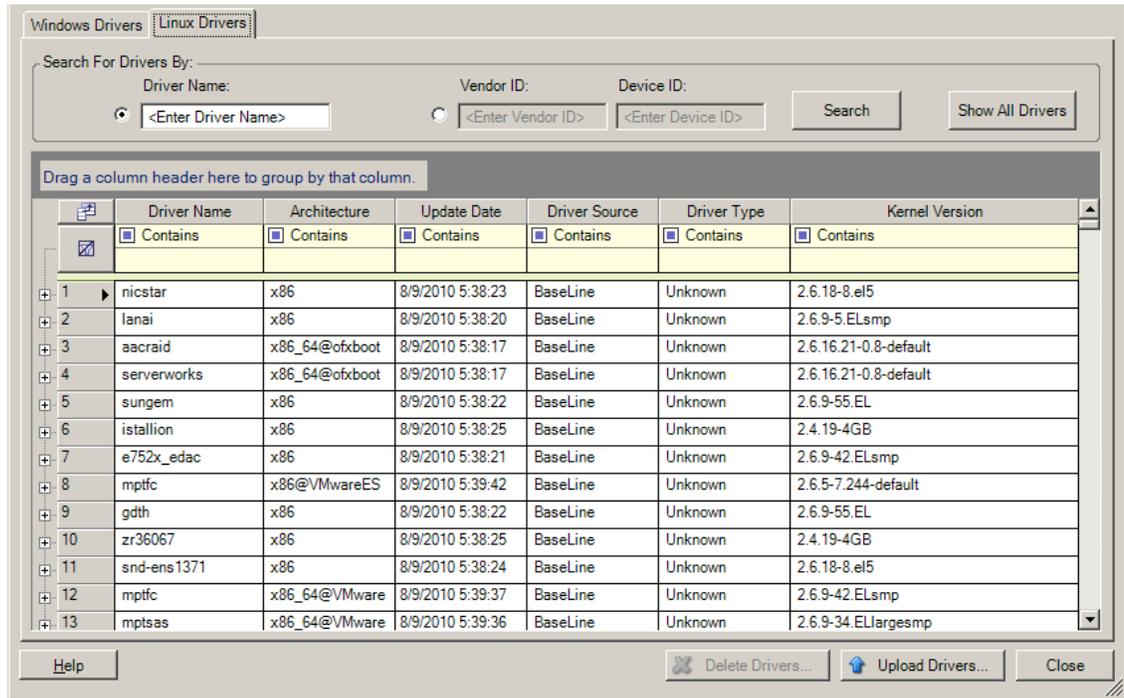


Select *Standard* as the *Hardware Manufacturer* option, unless your drivers are designed specifically for any of the target environments listed.

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

Device Driver Upload Procedure (Linux)

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



- 3 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 Troubleshooting

- ◆ [Section 7.1, “Troubleshooting Workload Inventory \(Windows\),” on page 83](#)
- ◆ [Section 7.2, “Troubleshooting Workload Inventory \(Linux\),” on page 86](#)
- ◆ [Section 7.3, “Troubleshooting Problems during the Prepare Replication Command \(Windows\),” on page 87](#)
- ◆ [Section 7.4, “Troubleshooting Workload Replication,” on page 87](#)
- ◆ [Section 7.5, “Generating and Viewing Diagnostic Reports,” on page 89](#)
- ◆ [Section 7.6, “Removing Workloads,” on page 90](#)
- ◆ [Section 7.7, “Post-Protection Workload Cleanup,” on page 90](#)

7.1 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 administrator account with the credential format <code>hostname\LocalAdmin</code></p> <p>Or, try the discovery by using a domain administrator account with the credential format <code>domain\DomainAdmin</code></p>
Unable to connect to Windows server...Access is denied	<p>A non-account was used when trying to add a workload. Use an administrator 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 84 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	This error can occur for several reasons and each has a unique solution: <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 (https://www.netiq.com/support/kb/doc.php?id=7920339) for more details. ◆ If local or domain policies restrict required permissions, follow the steps outlined in KB Article 7920862 (https://www.netiq.com/support/kb/doc.php?id=7920862).
Workload Discovery fails with error message Could not find file output.xml or Network path not found or (upon attempting to discover a Windows cluster) Inventory failed to discover. Inventory result returned nothing.	There are several possible reasons for the Could not find file output.xml error: <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 85. ◆ File and Printer Sharing for Microsoft Networks might not be enabled. Enable it under the Network Interface Card properties. ◆ The 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. ◆ 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.

7.1.1 Performing Connectivity Tests

- ◆ ["Network Connectivity Test" on page 84](#)
- ◆ ["WMI Connectivity Test" on page 84](#)
- ◆ ["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:
 - ♦ For Windows systems (XP/Vista/2003/2008/7), 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.
 - ♦ On a Windows 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.
- 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 network 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 23).

7.1.2 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.

7.1.3 Enabling File/Share Permissions and Access

To successfully protect a workload, PlateSpin Protect needs to successfully deploy and install software within the workload. 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 administrator 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 *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>\Admin$`, 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.

7.2 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 23.</p>

Problems or Messages	Solutions
Access denied	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 62.

7.3 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.	The account used to add a workload needs to be allowed by this policy. See “Group Policy and User Rights” on page 87.
Failure to determine whether .NET Framework is installed (with exception The trust relationship between this workstation and the primarydomain failed).	Check whether the Remote Registry service on the source is enabled and started. See also “Troubleshooting Workload Inventory (Windows)” on page 83.

7.3.1 Group Policy and User Rights

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.

You can refresh the policy immediately by using `gpupdate /force` (for Windows 2003/XP) or `secedit /refreshpolicy machine_policy /enforce` (for Windows 2000).

7.4 Troubleshooting Workload Replication

Problems or Messages	Solutions
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> .	This problem occurs when the server is under load and the process is taking longer than expected. Wait until the replication is complete.

Problems or Messages	Solutions
Workload issue requires user intervention	<p>Several types of issues might cause this message. In most cases the message should contain further specifics about the nature of the problem and the problem area (such as connectivity, credentials, . After troubleshooting, wait for a few minutes.</p> <p>If the message persists, contact PlateSpin Support.</p>
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" on page 26.</p>
<p>The file transfer cannot begin - port 3725 is already in use</p> <p>or</p> <p>3725 unable to connect</p>	<p>Ensure that the port is open and listening:</p> <pre>Run netstat -ano</pre> <p>on the workload.</p> <p>Check the firewall.</p> <p>Retry the replication.</p>
<p>Controller connection not established</p> <p>Replication fails at the <i>Take Control of Virtual Machine</i> step.</p>	<p>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.</p> <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 (https://www.netiq.com/support/kb/doc.php?id=7920339) for more details. If local or domain policies restrict required permissions, follow the steps outlined in KB Article 7920862 (https://www.netiq.com/support/kb/doc.php?id=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>

7.5 Generating and Viewing Diagnostic Reports

In the PlateSpin Protect Web Interface, 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.

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.

7.6 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 Interface 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.

7.7 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.

7.7.1 Cleaning Up Windows Workloads

Component	Removal Instructions
PlateSpin Block-Based Transfer Component	See KB Article 7005616 (https://www.netiq.com/support/kb/doc.php?id=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>.

Component	Removal Instructions
Controller software	<ol style="list-style-type: none"> Open a command prompt and change the current directory to: <ul style="list-style-type: none"> \Program Files\platespin* (32-bit systems) \Program Files (x86)\platespin* (64-bit systems) Run the following command: <pre>ofxcontroller.exe /uninstall</pre> Remove the platespin* directory

7.7.2 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>pkill -9 ofxcontrollerd</code> <code>pkill -9 ofxjobexec</code> remove the OFX controller rpm package: <pre>rpm -e ofxcontrollerd</pre> In the workload's file system, remove the <code>/usr/lib/ofx</code> directory with its contents.
Block-level data transfer software	<ol style="list-style-type: none"> 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> (Conditional) If the driver is still loaded, remove it from memory: <pre>rmmmod blkwatch_7616</pre> Remove the driver from the boot sequence: <pre>blkconfig -u</pre> Remove the driver files by deleting the following directory with its contents: <pre>/lib/modules/[Kernel_Version]/Platespin</pre> Delete the following file: <pre>/etc/blkwatch.conf</pre>

Component	Removal Instructions
LVM snapshots	<p>LVP snapshots used by ongoing replications are named according to a <i>volume_name-PS-snapshot</i> convention. For example, a snapshot of a LogVol01 volume will be named LogVol01-PS-snapshot.</p> <p>To remove these LVM snapshots:</p> <ol style="list-style-type: none"> 1. Generate a list of snapshot on the required workload by using one of the following ways: <ul style="list-style-type: none"> ◆ Use the PlateSpin Protect Web Interface to generate a Job Report for the failed job. The report should contain information about LVM snapshots and their names. - OR - ◆ On the required Linux workload, run the following command to display a list of all volumes and snapshots: <pre># lvdisplay -a</pre> 2. Note the names and locations of the snapshots you want to remove. 3. Remove the snapshots by using the following command: <pre>lvremove <i>snapshot_name</i></pre>
Bitmap files	<p>For each volume under protection, at the root of the volume, remove the corresponding <i>.blocks_bitmap</i> file.</p>
Tools	<p>On the source workload, under <i>/sbin</i>, remove the following files:</p> <ul style="list-style-type: none"> ◆ <i>bmaputil</i> ◆ <i>blkconfig</i>

Glossary

Container. PlateSpin Protect's workload protection infrastructure, such as a VM host.

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 failover workload within PlateSpin Protect is no longer required.

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

Failover Workload. A protected workload's bootable virtual replica.

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

Protection Contract. A collection of currently-active settings pertaining to the complete lifecycle of a workload's protection (*Add-inventory*, initial and ongoing *Replications*, *Failover*, *Failback*, and *Reprotect*).

Recovery Point. A point-in-time snapshot, allowing a replicated workload 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.

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

Replication. 1. *Initial Replication*, the creation of an initial base copy of a workload. Can be carried out as a *Full Replication* (all workload data is transferred to a 'blank' failover VM), or as an *Incremental Replication* (see [Incremental](#) (2)).

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 failover workload in the container.

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 failover 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.

See also [Source](#).

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