

PlateSpin[®] Protect 10.4

User Guide

July 31, 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/>.

If this product claims FIPS compliance, it is compliant by use of one or more of the Microsoft cryptographic components listed below. These components were certified by Microsoft and obtained FIPS certificates via the CMVP.

- 893 Windows Vista Enhanced Cryptographic Provider (RSAENH)
- 894 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSSENH)
- 989 Windows XP Enhanced Cryptographic Provider (RSAENH)
- 990 Windows XP Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSSENH)
- 997 Microsoft Windows XP Kernel Mode Cryptographic Module (FIPS.SYS)
- 1000 Microsoft Windows Vista Kernel Mode Security Support Provider Interface (ksecdd.sys)
- 1001 Microsoft Windows Vista Cryptographic Primitives Library (bcrypt.dll)
- 1002 Windows Vista Enhanced Cryptographic Provider (RSAENH)
- 1003 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSSENH)
- 1006 Windows Server 2008 Code Integrity (ci.dll)
- 1007 Microsoft Windows Server 2008 Kernel Mode Security Support Provider Interface (ksecdd.sys)
- 1008 Microsoft Windows Server 2008
- 1009 Windows Server 2008 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSSENH)
- 1010 Windows Server 2008 Enhanced Cryptographic Provider
- 1012 Windows Server 2003 Enhanced Cryptographic Provider (RSAENH)

This product may also claim FIPS compliance by use of one or more of the Open SSL cryptographic components listed below. These components were certified by the Open Source Software Institute and obtained the FIPS certificates as indicated.

918 - OpenSSL FIPS Object Module v1.1.2 - 02/29/2008 140-2 L1

1051 - OpenSSL FIPS Object Module v 1.2 - 11/17/2008 140-2 L1

1111 - OpenSSL FIPS Runtime Module v 1.2 - 4/03/2009 140-2 L1

Note: Windows FIPS algorithms used in this product may have only been tested when the FIPS mode bit was set. While the modules have valid certificates at the time of this product release, it is the user's responsibility to validate the current module status.

EXCEPT AS MAY BE EXPLICITLY SET FORTH IN THE APPLICABLE END USER LICENSE AGREEMENT, NOTHING HEREIN SHALL CONSTITUTE A WARRANTY AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY NETIQ, ITS SUPPLIERS AND LICENSORS.

License Grant

Licenses for PlateSpin Protect 10.4 cannot be used for prior versions of PlateSpin Protect.

Third-Party Software

Please refer to the *PlateSpin Third-Party License Usage and Copyright* (https://www.netiq.com/documentation/platespin_licensing/platespin_licensing_qs/data/platespin_licensing_qs.html) page for information about third party software used in PlateSpin Protect.

Contents

About This Guide	9
1 Product Overview	11
1.1 About PlateSpin Protect	11
1.2 Supported Configurations	11
1.2.1 Supported Windows Workloads	11
1.2.2 Supported Linux Workloads	12
1.2.3 Supported VM Containers	13
1.3 Security and Privacy	13
1.3.1 Security of Workload Data in Transmission	13
1.3.2 Security of Client/Server Communications	14
1.3.3 Security of Credentials	14
1.3.4 User Authorization and Authentication	14
1.4 Performance	14
1.4.1 About Product Performance Characteristics	14
1.4.2 Data Compression	15
1.4.3 Bandwidth Throttling	15
1.4.4 RPO, RTO, and TTO Specifications	15
1.4.5 Scalability	16
2 PlateSpin Protect Application Configuration	17
2.1 Product Licensing	17
2.1.1 Obtaining a License Activation Code	17
2.1.2 Online License Activation	17
2.1.3 Offline License Activation	18
2.2 Setting Up User Authorization and Authentication	18
2.2.1 About PlateSpin Protect User Authorization and Authentication	19
2.2.2 Managing PlateSpin Protect Access and Permissions	20
2.2.3 Managing PlateSpin Protect Security Groups and Workload Permissions	21
2.3 Access and Communication Requirements across your Protection Network	22
2.3.1 Access and Communication Requirements for Workloads	23
2.3.2 Access and Communication Requirements for Containers	24
2.3.3 Open Port Requirements for PlateSpin Server Hosts	24
2.3.4 Protection Across Public and Private Networks Through NAT	25
2.3.5 Overriding the Default bash Shell for Executing Commands on Linux Workloads	25
2.3.6 Requirements for VMware DRS Clusters as Containers	26
2.4 Configuring PlateSpin Protect Default Options	26
2.4.1 Setting Up Automatic E-Mail Notifications of Events and Reports	26
2.4.2 Configuring PlateSpin Server Behavior through XML Configuration Parameters	29
3 Up and Running	33
3.1 Launching the PlateSpin Protect Web Interface	33
3.2 Elements of the PlateSpin Protect Web Interface	34
3.2.1 Navigation Bar	35
3.2.2 Visual Summary Panel	35
3.2.3 Tasks and Events Panel	36
3.3 Workloads and Workload Commands	36
3.3.1 Workload Protection and Recovery Commands	37

3.4	Managing Multiple Instances of PlateSpin Protect and PlateSpin Forge	38
3.4.1	Using the PlateSpin Protect Management Console	38
3.4.2	About PlateSpin Protect Management Console Cards	38
3.4.3	Adding Instances of PlateSpin Protect and PlateSpin Forge to the Management Console	39
3.4.4	Managing Cards on the Management Console	40
3.5	Generating Workload and Workload Protection Reports	41
4	Workload Protection	43
4.1	Basic Workflow for Workload Protection and Recovery	43
4.2	Adding Containers (Protection Targets)	44
4.3	Adding Workloads for Protection	45
4.4	Configuring Protection Details and Preparing the Replication	47
4.4.1	Workload Protection Details	48
4.5	Starting the Workload Protection	49
4.6	Aborting Commands	50
4.7	Failover	51
4.7.1	Detecting Offline Workloads	51
4.7.2	Performing a Failover	52
4.7.3	Using the Test Failover Feature	53
4.8	Failback	53
4.8.1	Automated Failback to a VM Platform	54
4.8.2	Semi-Automated Failback to a Physical Machine	56
4.8.3	Semi-Automated Failback to a Virtual Machine	57
4.9	Reprotecting a Workload	57
5	Essentials of Workload Protection	59
5.1	Workload License Consumption	59
5.2	Guidelines for Workload and Container Credentials	60
5.3	Setting Up Protect Multitenancy on VMware	60
5.3.1	Using Tools to Define VMware Roles	60
5.3.2	Assigning Roles In vCenter	62
5.4	Data Transfer	65
5.4.1	Transfer Methods	65
5.4.2	Data Encryption	66
5.5	Protection Tiers	67
5.6	Recovery Points	68
5.7	Initial Replication Method (Full and Incremental)	68
5.8	Service and Daemon Control	69
5.9	Using Freeze and Thaw Scripts for Every Replication (Linux)	70
5.10	Volumes	70
5.11	Networking	72
5.12	Failback to Physical Machines	72
5.12.1	Downloading the PlateSpin Boot ISO Image	72
5.12.2	Injecting Additional Device Drivers into the Boot ISO Image	72
5.12.3	Registering Physical Machines as Failback Targets with PlateSpin Protect	73
5.13	Advanced Workload Protection Topics	74
5.13.1	Using Workload Protection Features through the PlateSpin Protect Web Services API	74
6	Auxiliary Tools for Working with Physical Machines	75
6.1	Analyzing Device Drivers with PlateSpin Analyzer (Windows)	75
6.2	Managing Device Drivers	76

6.2.1	Packaging Device Drivers for Windows Systems	76
6.2.2	Packaging Device Drivers for Linux Systems	77
6.2.3	Uploading Drivers to the PlateSpin Protect Device Driver Database.	77
6.2.4	Using the Plug and Play (PnP) ID Translator Feature	79
7	Troubleshooting	85
7.1	Troubleshooting Workload Inventory (Windows)	85
7.1.1	Performing Connectivity Tests	86
7.1.2	Disabling AntiVirus Software	87
7.1.3	Enabling File/Share Permissions and Access	88
7.2	Troubleshooting Workload Inventory (Linux)	88
7.3	Troubleshooting Problems during the Prepare Replication Command (Windows)	89
7.3.1	Group Policy and User Rights	89
7.4	Troubleshooting Workload Replication	89
7.5	Generating and Viewing Diagnostic Reports	91
7.6	Removing Workloads	92
7.7	Post-Protection Workload Cleanup	92
7.7.1	Cleaning Up Windows Workloads	92
7.7.2	Cleaning Up Linux Workloads	93
A	Documentation Updates	95
A.1	April 4, 2014	95
A.2	March 26, 2014	95
	Glossary	97

About This Guide

This guide provides information about using PlateSpin Protect.

- ♦ Chapter 1, “Product Overview,” on page 11
- ♦ Chapter 2, “PlateSpin Protect Application Configuration,” on page 17
- ♦ Chapter 3, “Up and Running,” on page 33
- ♦ Chapter 4, “Workload Protection,” on page 43
- ♦ Chapter 5, “Essentials of Workload Protection,” on page 59
- ♦ Chapter 6, “Auxiliary Tools for Working with Physical Machines,” on page 75
- ♦ Chapter 7, “Troubleshooting,” on page 85
- ♦ Appendix A, “Documentation Updates,” on page 95
- ♦ “Glossary” on page 97

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 top and 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 product’s Online Documentation Web Site:

PlateSpin Protect 10 online documentation (http://www.netiq.com/documentation/platespin_protect_10)

Documentation Updates

The most recent version of in this guide can be found at the [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 \(https://www.netiq.com/communities/\)](https://www.netiq.com/communities/): A Web-based community with a variety of discussion topics.

- ♦ [NetIQ Support Knowledgebase \(https://www.netiq.com/support/kb/\)](https://www.netiq.com/support/kb/): A collection of in-depth technical articles.
- ♦ [NetIQ Support Forums \(https://forums.netiq.com/forum.php\)](https://forums.netiq.com/forum.php): A Web location where product users can discuss NetIQ product functionality and advice with other product users.
- ♦ [MyNetIQ \(https://www.netiq.com/f/mynetiq/\)](https://www.netiq.com/f/mynetiq/): A Web site offering PlateSpin product information and services, such as access to premium white papers, webcast registrations, and product trial downloads.

Technical Support

You can learn more about the policies and procedures of NetIQ Technical Support by accessing its [Technical Support Guide \(https://www.netiq.com/Support/process.asp#_Maintenance_Programs_and\)](https://www.netiq.com/Support/process.asp#_Maintenance_Programs_and).

Use these resources for support specific to PlateSpin Protect:

- ♦ Telephone in Canada and the United States: 1-800-858-4000
- ♦ Telephone outside the United States: 1-801-861-4000
- ♦ E-mail: support@netiq.com
- ♦ Product specific information: [PlateSpin Protect Support \(https://www.netiq.com/support/kb/product.php?id=SG_XPLATESPINPROTECT_1_2\)](https://www.netiq.com/support/kb/product.php?id=SG_XPLATESPINPROTECT_1_2)

1 Product Overview

This section includes the following information:

- ♦ [Section 1.1, “About PlateSpin Protect,” on page 11](#)
- ♦ [Section 1.2, “Supported Configurations,” on page 11](#)
- ♦ [Section 1.3, “Security and Privacy,” on page 13](#)
- ♦ [Section 1.4, “Performance,” on page 14](#)

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 11](#)
- ♦ [Section 1.2.2, “Supported Linux Workloads,” on page 12](#)
- ♦ [Section 1.2.3, “Supported VM Containers,” on page 13](#)

1.2.1 Supported Windows Workloads

PlateSpin Protect supports most Windows-based workloads.

Only block-level replications are supported, with certain restrictions. See [Section 5.4, “Data Transfer,” on page 65](#).

Table 1-1 Supported Windows Workloads

Operating System	Remarks
Windows 7	Professional, Enterprise, and Ultimate editions only
Windows Server 2008 R2	Including domain controllers (DC) and Small Business Server (SBS) editions
Windows Server 2008	Including domain controllers (DC) and Small Business Server (SBS) editions
Windows Vista	Business, Enterprise, and Ultimate editions; SP1 and later
Windows Server 2003 R2	Including domain controllers (DC) and Small Business Server (SBS) editions

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)	NOTE: Kernel version 3.0.13 of SLES 11 SP2 (32-bit) is not supported. Upgrade to kernel version 3.0.27 or later before inventorying the workload.
Novell Open Enterprise Server (OES) 11, OES 11 SP1	
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 Linux file systems: EXT2, EXT3, EXT4, REISERFS, and NSS (OES 2 and OES 11 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 13](#)
- ◆ [Section 1.3.2, “Security of Client/Server Communications,” on page 14](#)
- ◆ [Section 1.3.3, “Security of Credentials,” on page 14](#)
- ◆ [Section 1.3.4, “User Authorization and Authentication,” on page 14](#)

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 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 48](#).

1.3.2 Security of Client/Server Communications

Because the PlateSpin Server installation enables SSL on the PlateSpin Server host, secure data transmission between your Web browser and the PlateSpin Server is already configured to HTTPS (Hypertext Transfer Protocol Secure). The installation also adds a self signed certificate if no valid certificates are found.

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 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 18](#).

1.4 Performance

- ♦ [Section 1.4.1, “About Product Performance Characteristics,” on page 14](#)
- ♦ [Section 1.4.2, “Data Compression,” on page 15](#)
- ♦ [Section 1.4.3, “Bandwidth Throttling,” on page 15](#)
- ♦ [Section 1.4.4, “RPO, RTO, and TTO Specifications,” on page 15](#)
- ♦ [Section 1.4.5, “Scalability,” on page 16](#)

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 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 67](#).

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 contract. This provides a way to prevent replication traffic from congesting your production network and reduces the overall load of your PlateSpin Server.

Bandwidth throttling can be configured individual for each workload or in a Protection Tier. See ["Protection Tiers" on page 67](#).

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 51](#).
- ♦ **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 53](#).

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 41](#).

1.4.5 Scalability

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

- ♦ **Workloads per Server:** The number of workloads per PlateSpin 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 PlateSpin Protect Application Configuration

This section includes information about the following:

- ♦ [Section 2.1, “Product Licensing,” on page 17](#)
- ♦ [Section 2.2, “Setting Up User Authorization and Authentication,” on page 18](#)
- ♦ [Section 2.3, “Access and Communication Requirements across your Protection Network,” on page 22](#)
- ♦ [Section 2.4, “Configuring PlateSpin Protect Default Options,” on page 26](#)

2.1 Product Licensing

This section provides information about activating your PlateSpin Protect software.

- ♦ [Section 2.1.1, “Obtaining a License Activation Code,” on page 17](#)
- ♦ [Section 2.1.2, “Online License Activation,” on page 17](#)
- ♦ [Section 2.1.3, “Offline License Activation,” on page 18](#)

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

The following information is included in this section:

- ♦ [Section 2.2.1, "About PlateSpin Protect User Authorization and Authentication," on page 19](#)
- ♦ [Section 2.2.2, "Managing PlateSpin Protect Access and Permissions," on page 20](#)
- ♦ [Section 2.2.3, "Managing PlateSpin Protect Security Groups and Workload Permissions," on page 21](#)

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 21).

2.2.2 Managing PlateSpin Protect Access and Permissions

The following sections provide more information:

- ♦ [“Adding PlateSpin Protect Users”](#) on page 20
- ♦ [“Assigning a Workload Protection Role to a PlateSpin Protect User”](#) on page 20

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 Server host, see [“Assigning a Workload Protection Role to a PlateSpin Protect User”](#) on page 20.

- 1 On your PlateSpin 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 20.

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 19.

- 1 On your PlateSpin 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 by following these steps:

- 1 Go to the PlateSpin 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`.

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 21](#).

2.2.3 Managing PlateSpin Protect Security Groups and Workload Permissions

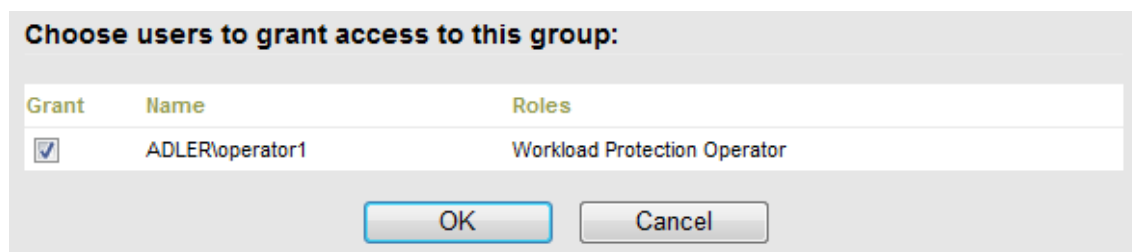
PlateSpin Protect provides a granular application-level access mechanism that allows specific users to carry out specific workload protection tasks on specified workloads. This is accomplished by setting up *security groups*.

- 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 20](#).
- 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 Server host, it might not be immediately available in the user interface. In this case, first click *Refresh User Accounts*.



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

Choose workloads to include in this group:

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

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

7 Click *Create*.

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

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

2.3 Access and Communication Requirements across your Protection Network

This section includes the following information:

- ♦ [Section 2.3.1, “Access and Communication Requirements for Workloads,” on page 23](#)
- ♦ [Section 2.3.2, “Access and Communication Requirements for Containers,” on page 24](#)
- ♦ [Section 2.3.3, “Open Port Requirements for PlateSpin Server Hosts,” on page 24](#)
- ♦ [Section 2.3.4, “Protection Across Public and Private Networks Through NAT,” on page 25](#)
- ♦ [Section 2.3.5, “Overriding the Default bash Shell for Executing Commands on Linux Workloads,” on page 25](#)
- ♦ [Section 2.3.6, “Requirements for VMware DRS Clusters as Containers,” on page 26](#)

2.3.1 Access and Communication Requirements for Workloads

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

Table 2-2 Access and Communication Requirements for Workloads

Workload Type	Prerequisites	Required Ports (Defaults)
All workloads	Ping (ICMP echo request and response) support	
All Windows workloads	Microsoft .NET Framework version 2.0 or 3.5 SP1	
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</i> Control Panel 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 2003 (including SP1 Standard, SP2 Enterprise, and R2 SP2 Enterprise)	<p>NOTE: After enabling the required ports, run the following command at the server prompt to enable PlateSpin remote administration:</p> <pre>netsh firewall set service RemoteAdmin enable</pre> <p>For more information about netsh, see the Microsoft TechNet article, http://technet.microsoft.com/en-us/library/cc785383%28v=ws.10%29.aspx. (http://technet.microsoft.com/en-us/library/cc785383%28v=ws.10%29.aspx).</p>	<ul style="list-style-type: none"> ◆ TCP: 3725, 135, 139, 445 ◆ UDP: 137, 138, 139

Workload Type	Prerequisites	Required Ports (Defaults)
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) 	<p>TCP 3725</p> <p>NetBIOS 137 - 139</p> <p>SMB (TCP 139, 445 and UDP 137, 138)</p> <p>RPC (TCP 135)</p>
All Linux workloads	Secure Shell (SSH) server	TCP 22, 3725

2.3.2 Access and Communication Requirements for Containers

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

Table 2-3 Access and Communication Requirements for Containers

System	Prerequisites	Required Ports (Defaults)
All containers	Ping (ICMP echo request and response) capability.	
VMware ESX/ESXi 4.1	<ul style="list-style-type: none"> VMware account with an Administrator role 	HTTPS (TCP 443)
VMware ESXi 5.0	<ul style="list-style-type: none"> VMware Web services API and file management API 	
vCenter Server	The user with access must be assigned the appropriate roles and permissions. Refer to the pertinent release of VMware documentation for more information.	HTTPS (TCP 443)

2.3.3 Open Port Requirements for PlateSpin Server Hosts

The following open port requirements are for PlateSpin Server hosts.

Table 2-4 Open Port Requirements for PlateSpin Server Hosts

Port (Default)	Remarks
TCP 80	For HTTP communication

Port (Default)	Remarks
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 Server:** In your server's *PlateSpin Server Configuration* tool, record the additional IP addresses assigned to that host. See [“Configuring the Application to Function through NAT” on page 25](#).
- ♦ **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 \(Workload to VM\) \(page 55\)](#).
- ♦ **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 *PlateSpin Server Configuration* tool (see *PlateSpin Server* above).

Configuring the Application to Function through NAT

To enable the PlateSpin Server to function across NAT-enabled environments, you must record additional IP addresses of your PlateSpin Server in the *PlateSpin Server Configuration* tool's database that the server reads upon startup.

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

2.3.5 Overriding the Default bash Shell for Executing Commands on Linux Workloads

By default, the PlateSpin 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 Server.

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

2.3.6 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 44](#).

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.

2.4 Configuring PlateSpin Protect Default Options

This section includes the following information:

- ♦ [Section 2.4.1, “Setting Up Automatic E-Mail Notifications of Events and Reports,” on page 26](#)
- ♦ [Section 2.4.2, “Configuring PlateSpin Server Behavior through XML Configuration Parameters,” on page 29](#)

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

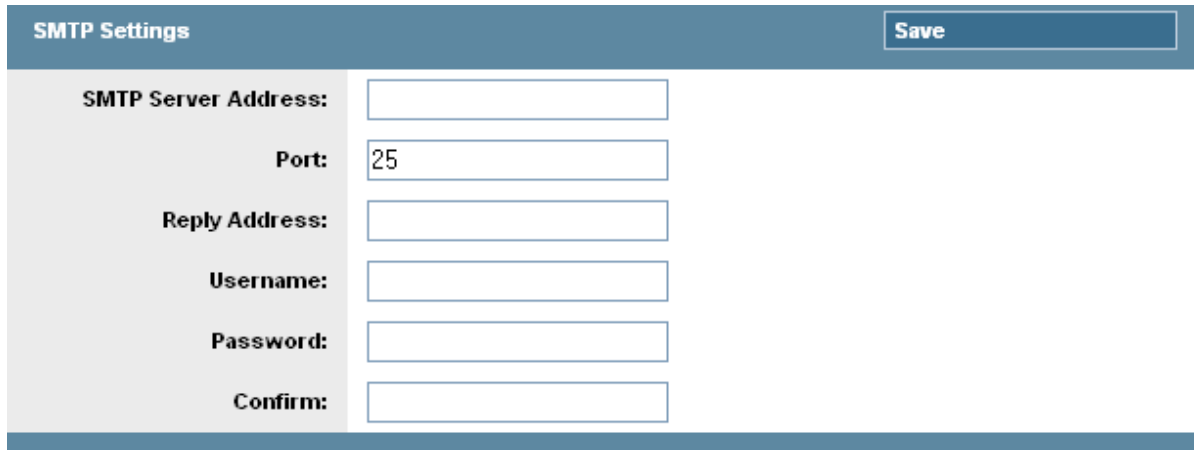
You can configure PlateSpin Protect to automatically send notifications of events and replication reports to specified e-mail addresses. This functionality requires that you first specify a valid SMTP server for PlateSpin Protect to use.

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

SMTP Configuration

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

Figure 2-1 Simple Mail Transfer Protocol Settings



SMTP Settings Save

SMTP Server Address:

Port:

Reply Address:

Username:

Password:

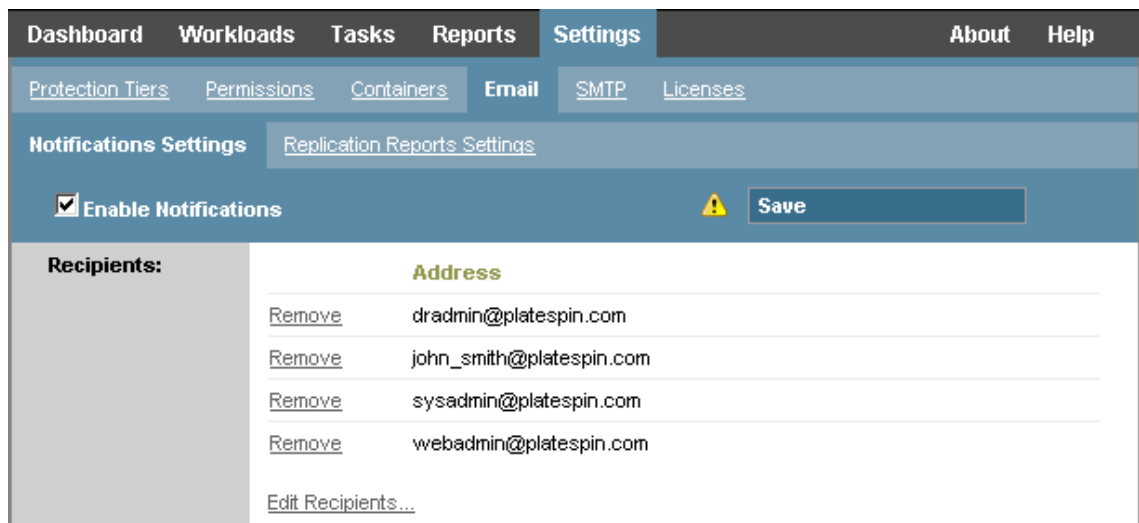
Confirm:

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 26.
- 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*.



Dashboard **Workloads** **Tasks** **Reports** **Settings** **About** **Help**

[Protection Tiers](#) [Permissions](#) [Containers](#) **Email** [SMTP](#) [Licenses](#)

Notifications Settings [Replication Reports Settings](#)

Enable Notifications ⚠ Save

Recipients:	Address
Remove	dradmin@platespin.com
Remove	john_smith@platespin.com
Remove	sysadmin@platespin.com
Remove	webadmin@platespin.com
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 contract'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 contract'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 \(page 26\)](#).
- 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*.

The screenshot shows the 'Settings' page for 'Replication Reports'. The 'Enable Replication Reports' checkbox is checked. The 'Report Recurrence' is set to 'Every day at 12:00 AM'. The 'Recipients' list includes three email addresses: 'admin@platespin.com', 'john_smith@platespin.com', and 'operator@platespin.com'. The 'Protect Access URL' is set to 'http://localhost:80'. A 'Save' button is visible in the top right corner of the settings area.

- 6 (Optional) In the *Protect Access URL* section, specify a non-default URL for your PlateSpin Server (for example, when your PlateSpin 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 41.

2.4.2 Configuring PlateSpin Server Behavior through XML Configuration Parameters

Some aspects of your PlateSpin Server’s behavior are controlled by configuration parameters that you set on a configuration Web page residing your PlateSpin Server host (https://Your_PlateSpin_Server/platespinconfiguration/).

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 configuration parameters:

- 1 From any Web browser, open the https://Your_PlateSpin_Server/platespinconfiguration/tool.
- 2 Locate the required server parameter and change its value.
- 3 Save and your settings and exit the page.

No reboot or restart of services is required after the change is made in the configuration tool.

The following topics provide information on specific situations, in which you might need to change product behavior using an XML configuration value.

- ◆ [“Optimizing Data Transfer over WAN Connections” on page 30](#)

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 settings you make in a configuration tool residing on your PlateSpin Server host. For the generic procedure, see [“Configuring PlateSpin Server Behavior through XML Configuration Parameters” on page 29](#).

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

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

Table 2-5 *Default and Optimized Configuration Parameters in `https://Your_PlateSpin_Server/platespinconfiguration/`*

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

Parameter	Default Value	Optimized Value
fileTransferSendReceiveBufferSize	0 (8192 bytes)	max 5242880 (5 MB)
<p>TCP/IP window size setting for file transfer connections. It controls the number of bytes sent without TCP acknowledgement, in bytes.</p> <p>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:</p> $((\text{LINK_SPEED}(\text{Mbps})/8) * \text{DELAY}(\text{sec})) * 1000 * 1000$ <p>For example, for a 100 Mbps link with 10 ms latency, the proper buffer size would be:</p> $(100/8) * 0.01 * 1000 * 1000 = 125000 \text{ bytes}$		

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 33](#)
- ♦ [Section 3.2, “Elements of the PlateSpin Protect Web Interface,” on page 34](#)
- ♦ [Section 3.3, “Workloads and Workload Commands,” on page 36](#)
- ♦ [Section 3.4, “Managing Multiple Instances of PlateSpin Protect and PlateSpin Forge,” on page 38](#)
- ♦ [Section 3.5, “Generating Workload and Workload Protection Reports,” on page 41](#)

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 launch the PlateSpin Protect Web Interface:

- 1 Open a Web browser and go to:

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

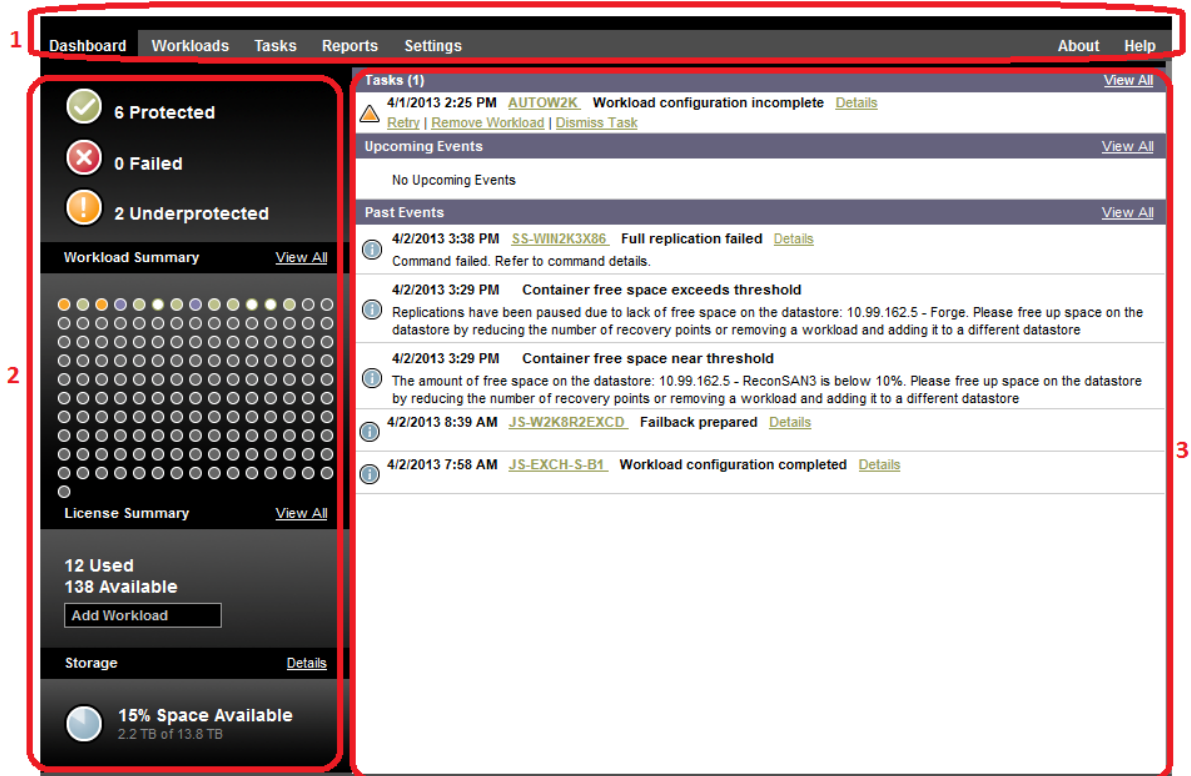
Replace *<hostname | IP_address>* with the hostname or the IP address of your PlateSpin Server host.

If SSL is not enabled, use `http` 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.

The following topics provide more details:

- ♦ Section 3.2.1, "Navigation Bar," on page 35
- ♦ Section 3.2.2, "Visual Summary Panel," on page 35
- ♦ Section 3.2.3, "Tasks and Events Panel," on page 36

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 36](#).
- ◆ **Tasks:** Displays the Tasks page, which lists items requiring user intervention.
- ◆ **Reports:** Displays the Reports page. See [“Generating Workload and Workload Protection Reports” on page 41](#).
- ◆ **Settings:** Displays the Settings page, which provides access to the following configuration options:
 - ◆ **Protection Tiers:** See [“Protection Tiers” on page 67](#).
 - ◆ **Permissions:** See [“Setting Up User Authorization and Authentication” on page 18](#).
 - ◆ **Containers:** See [“Adding Containers \(Protection Targets\)” on page 44](#).
 - ◆ **Email/SMTP:** See [“Setting Up Automatic E-Mail Notifications of Events and Reports” on page 26](#).
 - ◆ **Licenses/License Designations:** See [“Product Licensing” on page 17](#).

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 26.

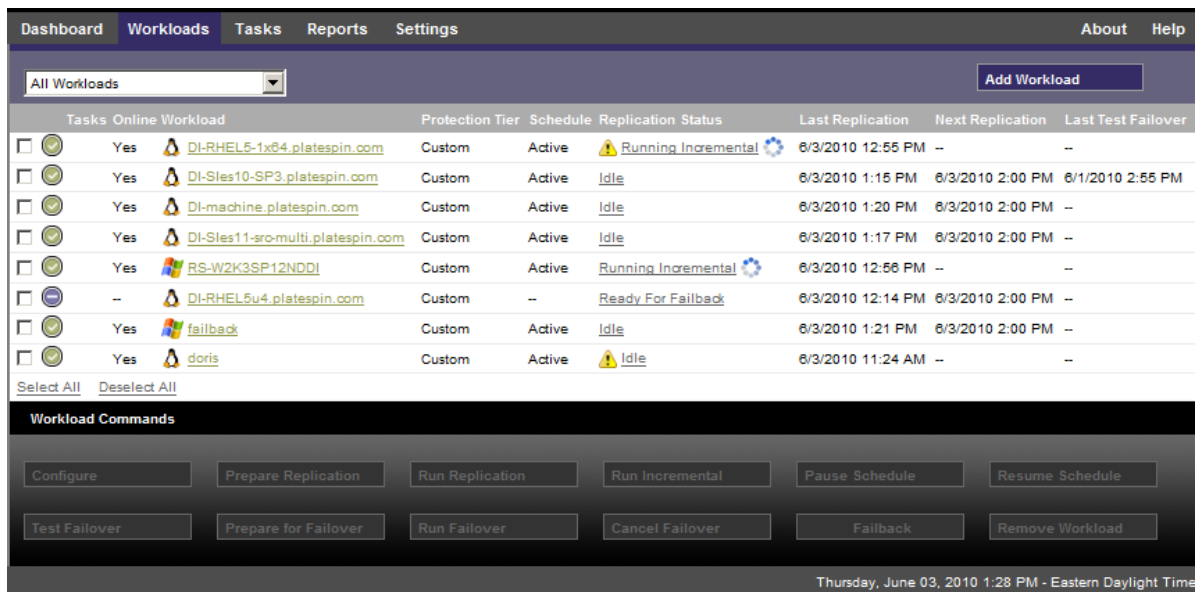
Tasks are special commands that are tied to events that require user intervention. For example, upon completion of a Test Failover command, the system generates an event associated with two tasks: Mark Test as Success and Mark Test as Failure. Clicking either task results in the Test Failover operation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

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

3.3 Workloads and Workload Commands

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

Figure 3-2 *The Workloads Page*

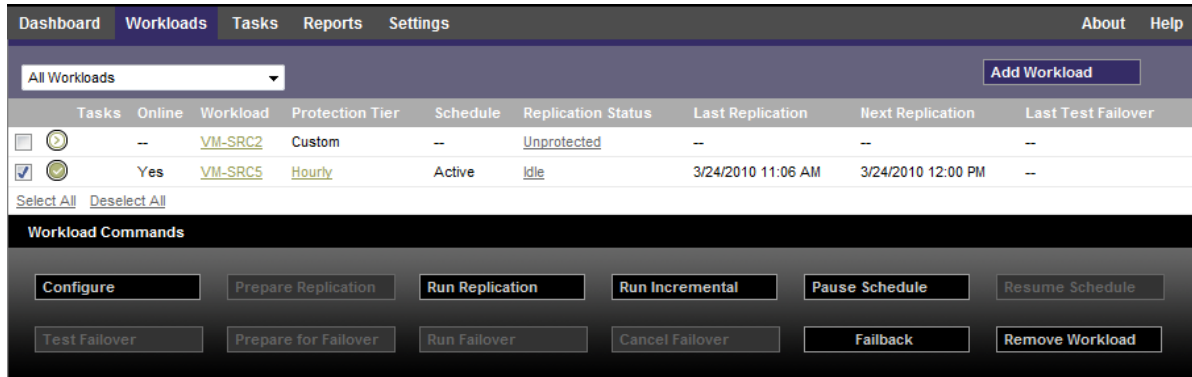


NOTE: All time stamps reflect the time zone of the PlateSpin Server host. This might be different from the time zone of the protected workload or the time zone of the host on which you are running the PlateSpin Protect Web Interface. A display of the server date and time appears at the bottom right of 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 contract.
<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 38
- ♦ Section 3.4.2, “About PlateSpin Protect Management Console Cards,” on page 38
- ♦ Section 3.4.3, “Adding Instances of PlateSpin Protect and PlateSpin Forge to the Management Console,” on page 39
- ♦ Section 3.4.4, “Managing Cards on the Management Console,” on page 40

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:

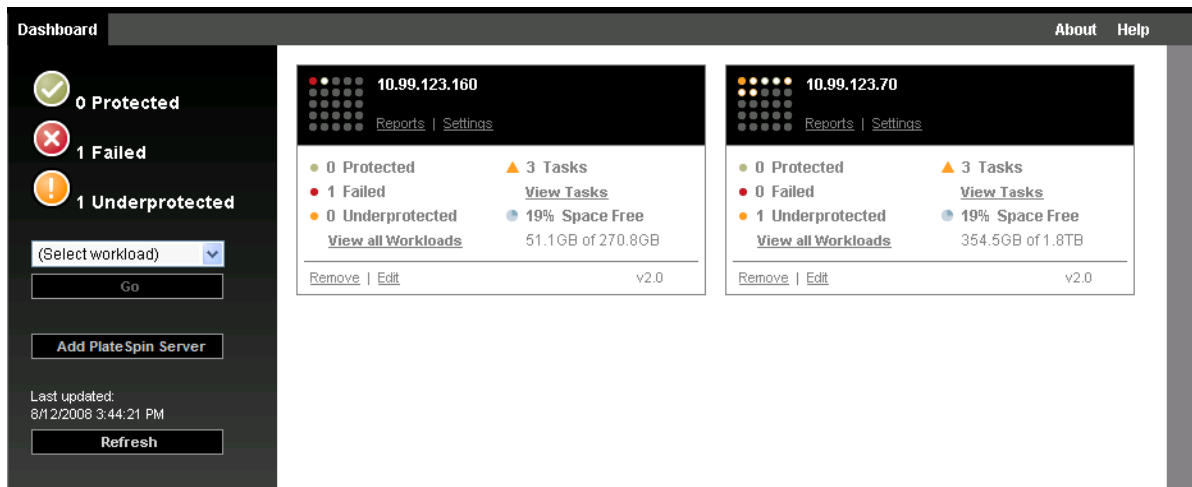
```
https://<IP_address | hostname>/console
```

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

- 2 Log in with your username and password.

The console’s default Dashboard page is displayed.

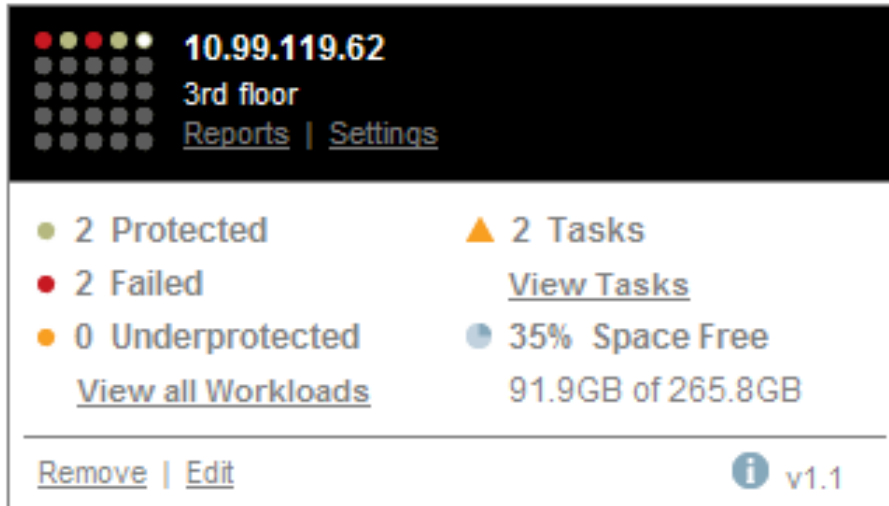
Figure 3-4 The Management Console’s Default Dashboard Page



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 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 contracts 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 43
- ♦ Section 4.2, “Adding Containers (Protection Targets),” on page 44
- ♦ Section 4.3, “Adding Workloads for Protection,” on page 45
- ♦ Section 4.4, “Configuring Protection Details and Preparing the Replication,” on page 47
- ♦ Section 4.5, “Starting the Workload Protection,” on page 49
- ♦ Section 4.6, “Aborting Commands,” on page 50
- ♦ Section 4.7, “Failover,” on page 51
- ♦ Section 4.8, “Failback,” on page 53
- ♦ Section 4.9, “Reprotecting a Workload,” on page 57

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 11.
 - 1b** Make sure that your workloads and containers meet access and network prerequisites.
See “[Access and Communication Requirements across your Protection Network](#)” on page 22.
 - 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 70](#).
- 2 Inventory:** This step involves adding workloads and containers to the PlateSpin 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 contract requires a defined workload and container that were inventoried by the PlateSpin Server. See [“Adding Containers \(Protection Targets\)” on page 44](#) and [“Adding Workloads for Protection” on page 45](#).
 - 3 Definition of the protection contract:** In this step, you define the details and specifications of a protection contract and prepare the replication.
See [“Configuring Protection Details and Preparing the Replication” on page 47](#).
 - 4 Initiating the Protection:** This step commences the protection contract according to your requirements.
See [“Starting the Workload Protection” on page 49](#).
 - 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 contract, 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 51](#).
 - 7 Failback:** This step corresponds to the business resumption phase after you have addressed any problems with your production workload. See [“Failback” on page 53](#).
 - 8 Reprotection:** This step enables you to redefine the original protection contract for your workload. See [“Reprotecting a Workload” on page 57](#)

Most of these steps are represented by workload commands on the Workloads page. See [“Workloads and Workload Commands” on page 36](#).

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 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 13.

- ◆ **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 60.
- ◆ **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 Server.

To add a workload:

- 1 Follow the required preparatory steps.
See [Step 1](#) in “[Basic Workflow for Workload Protection and Recovery](#)” on page 43.
- 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 60.

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 47

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 43), 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 45.
- 2 Add a container. See [“Adding Containers \(Protection Targets\)”](#) on page 44.
- 3 On the Workloads page, select the required workload and click *Configure*.

Alternatively, you can click the name of the workload.

NOTE: If the PlateSpin Protect inventory doesn’t have a container yet, the system prompts you to add one; do so by clicking *Add Container* at the bottom.

- 4 Select an *Initial Replication Method*. This indicates whether you want volume data transferred entirely from your workload to the failover VM or synchronized with volumes on an existing VM. See [“Initial Replication Method \(Full and Incremental\)”](#) on page 68.
- 5 Assign a protection target. 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 68.

NOTE: If your inventory has only one container, your workload is automatically assigned to it.

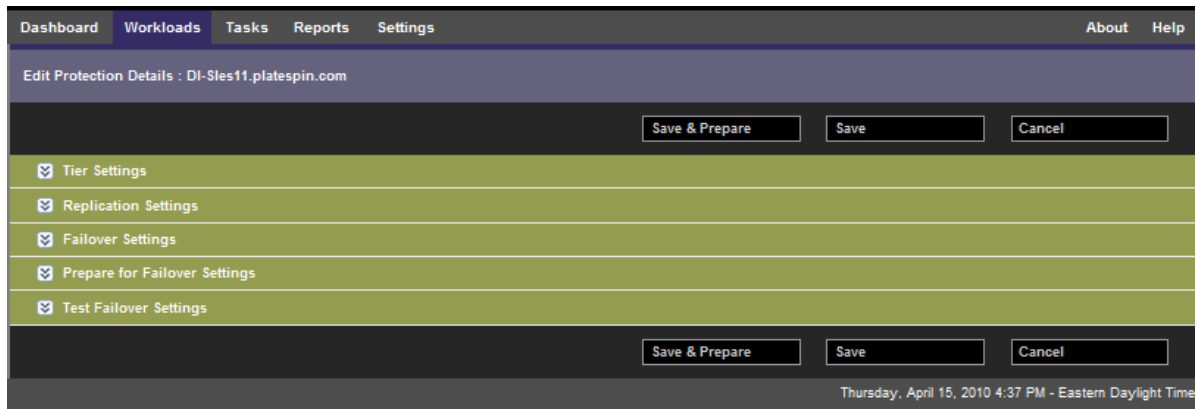
- 6 Configure the protection details in each set of settings as dictated by your business continuity needs. See [“Workload Protection Details”](#) on page 48.
- 7 Correct any validation errors, if displayed by the PlateSpin Protect Web Interface.
- 8 Click *Save*.

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:

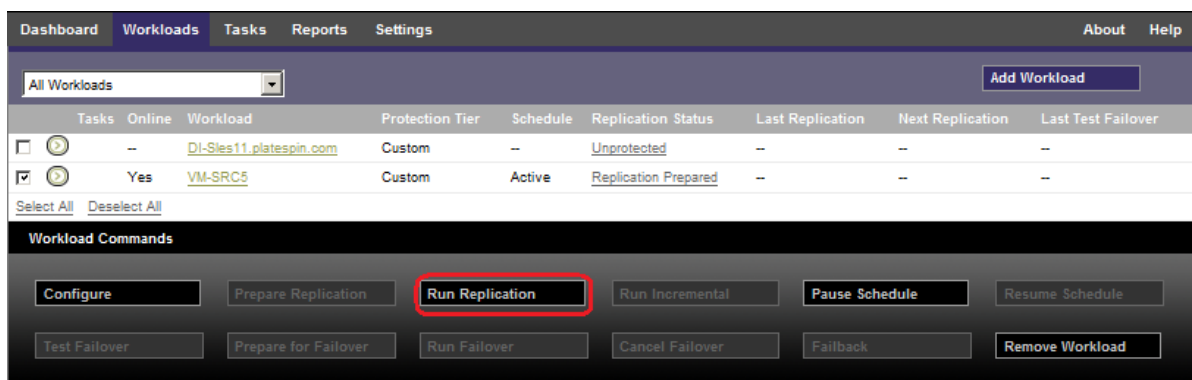
Table 4-1 Workload Protection Details

Parameter Set (Settings)	Details
Tier	Indicates the Protection Tier that the current protection uses. See “Protection Tiers” on page 67.
Replication	<p>Transfer Method: (Windows) Enables you to select a data transfer mechanism and security through encryption. See “Data Transfer” on page 65.</p> <p>Transfer Encryption: To enable encryption, select the <i>Encrypt Data Transfer</i> option. See “Security and Privacy” on page 13.</p> <p>Source Credentials: Required for accessing the workload. See “Guidelines for Workload and Container Credentials” on page 60.</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 72.</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 68.</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 69.</p>

Parameter Set (Settings)	Details
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 72.</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 69.</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 72 .
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 72.</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 69.</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.

<input type="checkbox"/>			No	 CL-2K8R2-VM1	Custom	Active	 Idle	3/5/2012 12:23 AM	4/11/2012 12:00 AM	--
<input type="checkbox"/>			Yes	 DL-Sies11x64-Src	every 4 hours	Active	Failover Prepared	3/29/2012 8:13 AM	4/9/2012 12:00 PM	3/23/2012 3:32 PM
<input type="checkbox"/>			--	 ma-cl-slessp2_site	every 4 hours	--	Live	3/15/2012 2:49 PM	--	3/9/2012 2:44 PM
<input type="checkbox"/>			Yes	 VISTACLIENT	Custom	Active	 Running Incremental 	3/28/2012 10:21 AM	4/9/2012 12:00 PM	3/23/2012 5:14 PM
<input type="checkbox"/>			--	 CL-VISTASP1-SRC	every 4 hours	--	Live	2/22/2012 2:55 PM	--	--
<input type="checkbox"/>			Yes	 CL-XPX64-SRC	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:

Running Incremental

Status: ⚠ Running 🔄

Duration: 3d 21h 31m 37s

Step: Copy data (2%)

Setting Up Controller (1%)

Last Full Replication: 2/17/2012 3:53 PM
 Last Incremental Replication: 3/26/2012 10:21 AM
 Last Test Failover: 3/23/2012 5:14 PM
 Schedule: Active
 Replication History: [View](#)
 Tasks: --

Command Summary

Events:	Event	Details	User	Date
	Incremental replication started		DEV-MORTAZAA\PlateSpin	4/5/2012 2:00 PM

Status: Running 🔄

⚠ Controller installation has not finished in a timely fashion. A controller has already been installed on 10.99.123.164.

Start Time: 4/5/2012 2:00 PM

Duration: 3d 21h 31m 37s

Steps:

Step	Status	Start Time	End Time	Duration	Diagnostics
Revert to snapshot	Completed	4/5/2012 2:00 PM	4/5/2012 2:01 PM	1m 7s	--
i Copy data	⚠ Running (2%) 🔄	4/5/2012 2:01 PM	--	3d 21h 30m 30s	--

Diagnostics: [Generate](#)

Workload Commands

Abort Configure Pause Schedule

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 51](#)
- ♦ [Section 4.7.2, “Performing a Failover,” on page 52](#)
- ♦ [Section 4.7.3, “Using the Test Failover Feature,” on page 53](#)

4.7.1 Detecting Offline Workloads

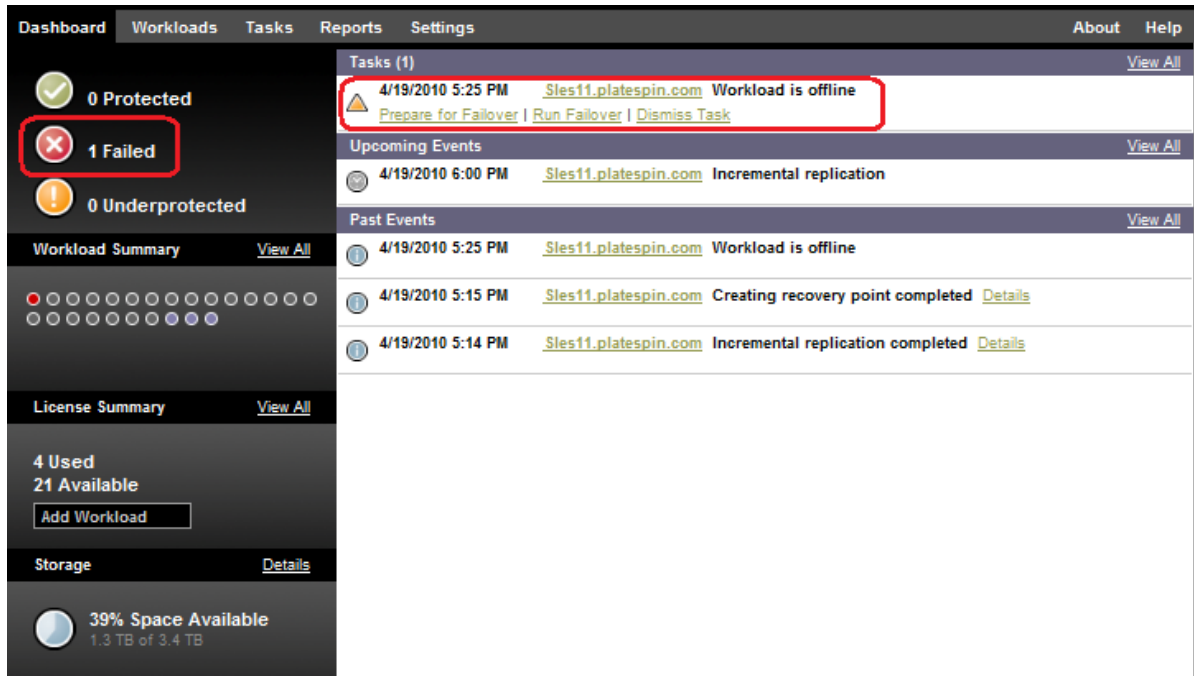
PlateSpin Protect constantly monitors your protected workloads. If an attempt to monitor a workload fails for a predefined number of times, PlateSpin Protect generates a *Workload is offline* event. Criteria that determine and log a workload failure are part of a workload protection’s Tier settings (see the [Tier](#) row in “[Workload Protection Details](#)” on page 48).

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

If a workload failure is detected while the status of the replication is *Idle*, you can proceed to the *Run Failover* command. If a workload fails while an incremental is underway, the job stalls. In this case, abort the command (see “[Aborting Commands](#)” on page 50), and then proceed to the *Run Failover* command. See “[Performing a Failover](#)” on page 52.

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 48.

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 68). 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 53.

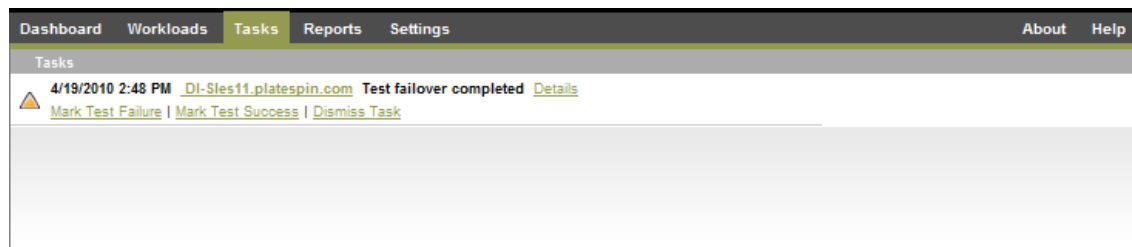
4.7.3 Using the Test Failover Feature

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 48).

- 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 68), 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 54](#)
- ♦ [Section 4.8.2, “Semi-Automated Failback to a Physical Machine,” on page 56](#)
- ♦ [Section 4.8.3, “Semi-Automated Failback to a Virtual Machine,” on page 57](#)

4.8.1 Automated Failback to a VM Platform

The following containers are supported as automated failback targets:

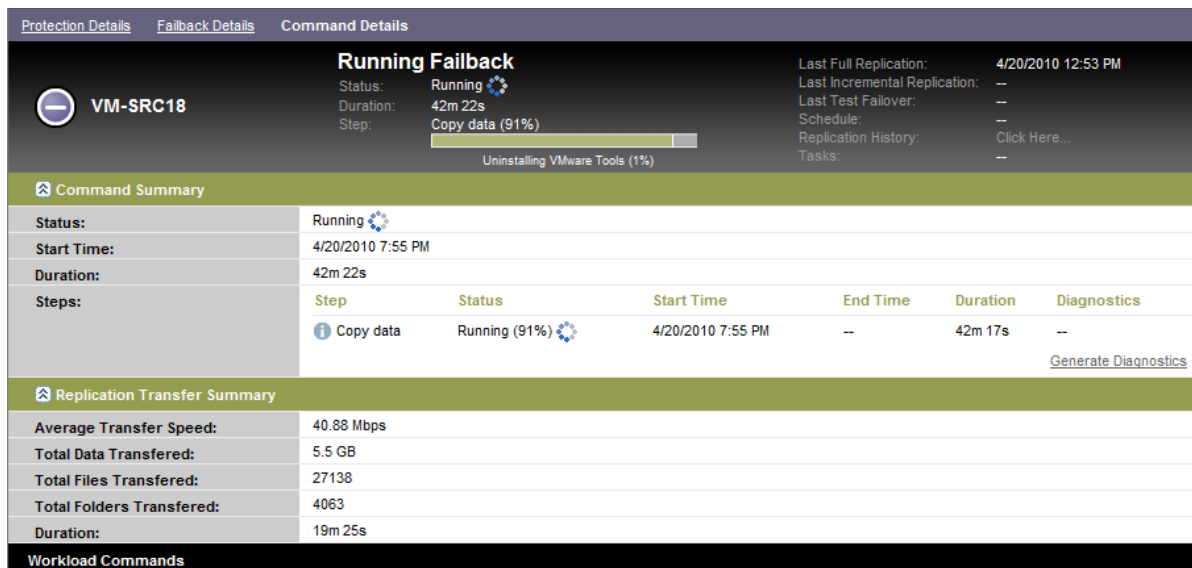
Target	Notes
VMware DRS Cluster in vSphere 5.1	<ul style="list-style-type: none">♦ The DRS configuration must be either Partially Automated or Fully Automated (it must not be set to Manual)♦ As a VM Container, the DRS Cluster must consist of ESXi 5.1 servers only, and can be managed by vCenter 5.1 only.
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*.
The system prompts you to make the following selections
- 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 60](#)).
 - ♦ **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 68](#).
 - ♦ **Target Type:** Select *Virtual Target*. If you don’t yet have a failback container, click *Add Container* and inventory a supported container.
- 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 55](#).

- 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 “Data Transfer” on page 65.</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 72.</p> <p>VM Datastore: Enables you to select a datastore associated with your failback container for the target workload.</p> <p>Volume Mapping: When the initial replication method is specified as “incremental”, enables you to select source volumes and map to volumes on the failback target for synchronization.</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 69.</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>

Parameter Set (Settings)	Details
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 69.</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 Server. See [“Failback to Physical Machines” on page 72](#).
- 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 75](#).
- 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 76](#).
- 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 60](#)).
 - ◆ **Failback Target Settings:** Specify the following parameters:
 - ◆ **Replication Method:** Select the scope of data replication. See [“Initial Replication Method \(Full and Incremental\)” on page 68](#).
 - ◆ **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 in the PlateSpin Protect Web Interface. The interface is divided into three main sections: 'Workload Settings', 'Failback Target Settings', and 'Workload Commands'. In 'Workload Settings', the 'Hostname or IP' is 'MA--Rhel5u3', 'User Name' is 'root', and 'Password' is masked with dots. In 'Failback Target Settings', 'Replication Method' is 'Full Replication', 'Target type' is 'Physical Targets', and 'Failback Target' is currently empty with a message 'No physical targets available.' and a note about adding physical targets. At the bottom, there is 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)

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 53](#).

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 59](#)
- ◆ [Section 5.2, “Guidelines for Workload and Container Credentials,” on page 60](#)
- ◆ [Section 5.3, “Setting Up Protect Multitenancy on VMware,” on page 60](#)
- ◆ [Section 5.4, “Data Transfer,” on page 65](#)
- ◆ [Section 5.5, “Protection Tiers,” on page 67](#)
- ◆ [Section 5.6, “Recovery Points,” on page 68](#)
- ◆ [Section 5.7, “Initial Replication Method \(Full and Incremental\),” on page 68](#)
- ◆ [Section 5.8, “Service and Daemon Control,” on page 69](#)
- ◆ [Section 5.9, “Using Freeze and Thaw Scripts for Every Replication \(Linux\),” on page 70](#)
- ◆ [Section 5.10, “Volumes,” on page 70](#)
- ◆ [Section 5.11, “Networking,” on page 72](#)
- ◆ [Section 5.12, “Failback to Physical Machines,” on page 72](#)
- ◆ [Section 5.13, “Advanced Workload Protection Topics,” on page 74](#)

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 17](#).

5.2 Guidelines for Workload and Container Credentials

PlateSpin Protect must have administrator-level access to workloads and appropriate role configuration for 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>
All Linux workloads	Root-level username and password	Non-root accounts must be properly configured to use <code>sudo</code> . See KB Article 7920711 .
VMware ESX/ESXi 4.1; ESXi 5.0	VMware account with an appropriate role configuration. See Section 5.3.1, “Using Tools to Define VMware Roles,” on page 60.	If ESX is configured for Windows domain authentication, you can also use your Windows domain credentials.
VMware vCenter Server	VMware account with an appropriate role configuration. See Section 5.3.1, “Using Tools to Define VMware Roles,” on page 60.	

5.3 Setting Up Protect Multitenancy on VMware

PlateSpin Protect includes unique user roles (and a tool for creating them in a VMware datacenter) that make it possible non-administrative VMware users (or “enabled users”) to perform Protect lifecycle operations in the VMware environment. These roles makes it possible for you, as a service provider, to segment your VMware cluster to allow multitenancy: where multiple Protect containers are instantiated in your datacenter to accommodate Protect customers or “tenants” who want to keep their data and evidence of their existence separate from and inaccessible to other customers who also use your datacenter.

This section includes the following information:

- ◆ [Section 5.3.1, “Using Tools to Define VMware Roles,”](#) on page 60
- ◆ [Section 5.3.2, “Assigning Roles In vCenter,”](#) on page 62

5.3.1 Using Tools to Define VMware Roles

PlateSpin Protect requires certain privileges to access and perform tasks in the VMware Infrastructure (that is, VMware “containers”), making the Protect workflow and functionality possible in that environment. Because there are many of these required privileges, NetIQ has created a file that defines the minimum required privileges and aggregates them respectively into three VMware custom roles:

- ◆ PlateSpin Virtual Machine Manager

- ◆ PlateSpin Infrastructure Manager
- ◆ PlateSpin User

This definition file, `PlateSpinRole.xml`, is included in the PlateSpin Protect Server installation. An accompanying executable, `PlateSpin.VMwareRoleTool.exe`, accesses the file to enable the creation of these custom PlateSpin roles in a target vCenter environment.

This section includes the following information:

- ◆ [“Basic Command Line Syntax” on page 61](#)
- ◆ [“Additional Command Line Parameters and Flags” on page 61](#)
- ◆ [“Tool Usage Example” on page 61](#)
- ◆ [“\(Option\) Manually Defining the PlateSpin Roles in vCenter” on page 62](#)

Basic Command Line Syntax

From the location where the role tool was installed, run the tool from the command line, using this basic syntax:

```
PlateSpin.VMwareRoleTool.exe /host=[host name/IP] /user=[user name] /role=[the
role definition file name and location] /create
```

NOTE: By default, the role definition file is located in the same folder with the role definition tool.

Additional Command Line Parameters and Flags

Apply the following parameters as needed when you use `PlateSpin.VMwareRoleTool.exe` to create or update roles in vCenter:

<code>/create</code>	(mandatory) Creates the roles defined by the <code>/role</code> parameter
<code>/get_all_privileges</code>	Display all server-defined privileges

Optional Flags

<code>/interactive</code>	Run the tool with interactive options that allow you to choose to create individual roles, check role compatibility, or list all compatible roles.
<code>/password=[password]</code>	Provide the VMware password (bypasses the password prompt)
<code>/verbose</code>	Display detailed information

Tool Usage Example

Usage: `PlateSpin.VMwareRoleTool.exe /host=houston_sales /user=pedrom /role=PlateSpinRole.xml /create`

Resulting Actions:

1. The role definition tool runs on the `houston_sales` vCenter server, which has an administrator with the user name `pedrom`.

2. In the absence of the `/password` parameter, the tool prompts for the user password, which you enter.
3. The tool accesses the role definition file, `PlateSpinRole.xml`, which is located in the same directory as the tool executable (there was no need to further define its path).
4. The tool locates the definition file and is instructed (`/create`) to create the roles defined in the contents of that file in the vCenter environment.
5. The tool accesses the definition file and creates the new roles (including the appropriate minimum privileges for defined, limited access) inside vCenter.

The new custom roles are to be [assigned to users later in vCenter](#).

(Option) Manually Defining the PlateSpin Roles in vCenter

You use the vCenter client to manually create and assign the PlateSpin custom roles. This requires creating the roles with the enumerated privileges as defined in `PlateSpinRole.xml`. When you create manually, there is no restriction on the name of the role. The only restriction is that the role names you create as equivalents to those in the definition file have all of the appropriate minimum privileges from the definition file.

For more information about how to create custom roles in vCenter, see [Managing VMWare VirtualCenter Roles and Permissions](#) (http://www.vmware.com/pdf/vi3_vc_roles.pdf) in the VMware Technical Resource Center.

5.3.2 Assigning Roles In vCenter

As you set up a multitenancy environment, you need to provision a single Protect server per customer or “tenant.” You assign this Protect server an enabled user with special Protect VMware roles. This enabled user creates the Protect container. As service provider, you maintain this user’s credentials and do not disclose them to your tenant customer.

The following table lists the roles you need to define for the enabled user. It also includes more information about the purpose of the role:

vCenter Container for Role Assignment	Role Assignment Specifics	Propagate Instructions	More Information
Root of vCenter inventory tree.	Assign the enabled user the <i>PlateSpin Infrastructure Manager</i> (or equivalent) role.	For security reasons, define the permission as non-propagating.	This role is needed to monitor tasks being performed by the Protect software and to end any stale VMware sessions.
All datacenter objects where the enabled user needs access	Assign the enabled user the <i>PlateSpin Infrastructure Manager</i> (or equivalent) role.	For security reasons, define the permission as non-propagating.	This role is needed to allow access to the datacenter’s datastores for file upload/download. Define the permission as non-propagating.

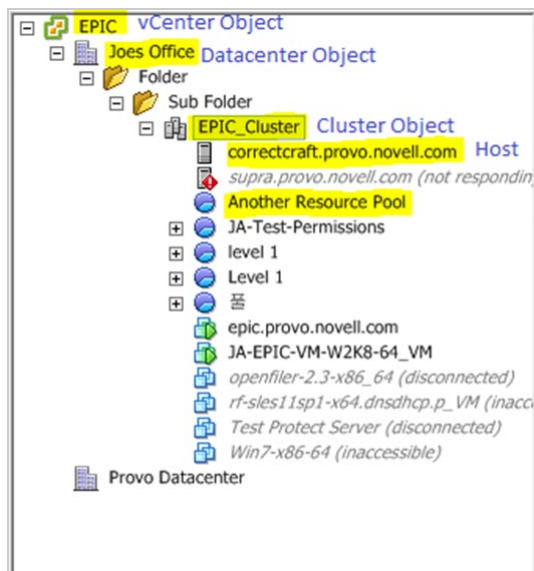
vCenter Container for Role Assignment	Role Assignment Specifics	Propagate Instructions	More Information
Each cluster to be added to Protect as a container, and each host contained in the cluster	Assign the enabled user the <i>PlateSpin Infrastructure Manager</i> (or equivalent) role.	Propagation is at the discretion of the VMware administrator.	To assign to a host, propagate the permission from the cluster object or create an additional permission on each cluster host. If the role is assigned on the cluster object and is propagated, no further changes are necessary when you add a new host to the cluster. However, propagating this permission has security implications.
Each Resource Pool where the enabled user needs access.	Assign the enabled user the <i>PlateSpin Virtual Machine Manager</i> (or equivalent) role.	Propagation is at the discretion of the VMware administrator.	Although you can assign access to any number of Resource Pools in any location in the tree, you must assign the enabled user this role on at least one Resource Pool.
Each VM folder where the enabled user needs access	Assign the enabled user the <i>PlateSpin Virtual Machine Manager</i> (or equivalent) role.	Propagation is at the discretion of the VMware administrator.	Although you can assign access to any number of VM Folders in any location in the tree, you must assign the enabled user this role on at least one folder.
Each Network where the enabled user needs access. Distributed Virtual Networks with a dvSwitch and a dvPortgroup	Assign the enabled user the <i>PlateSpin Virtual Machine Manager</i> (or equivalent) role.	Propagation is at the discretion of the VMware administrator.	Although you can assign access to any number of networks in any location in the tree, you must assign the enabled user this role on at least one folder. <ul style="list-style-type: none"> ◆ To assign the correct role to the dvSwitch, propagate the role on the Datacenter (resulting in an additional object receiving the role) or place the dvSwitch in a folder and assign the role on that folder. ◆ For a standard portgroup to be listed as an available network in the Protect UI, create a definition for it on every host in the cluster.
Each Datastore and Datastore Cluster where the enabled user needs access	Assign the enabled user the <i>PlateSpin Virtual Machine Manager</i> (or equivalent) role.	Propagation is at the discretion of the VMware administrator.	The enabled user must have been assigned this role on 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

The following table shows the role you can assign to the customer or tenant user.

vCenter Container for Role Assignment	Role Assignment Specifics	Propagate Instructions	More Information
Each resource pool(s) and folder(s) where the customer's VMs will be created.	Assign the tenant user the <i>PlateSpin User</i> (or equivalent) role.	Propagation is at the discretion of the VMware administrator.	<p>This tenant is a member of the PlateSpin Administrators group on the PlateSpin Protect server and is also on the vCenter server.</p> <p>If the tenant will be granted the ability to change the resources used by the VM (that is, networks, ISO images, and so forth), grant this user the necessary permissions on those resources. For example, if you want to allow the customer to change the network where their VM is attached, this user should be assigned the Read-only role (or better) on all of the networks being made accessible to the customer.</p>

The figure below illustrates a Virtual Infrastructure in the vCenter console. The objects labeled in blue are assigned the Infrastructure Manager role. The objects labeled in green are assigned the Virtual Machine Manager role. The tree does not show VM folders, Networks and Datastores. Those objects are assigned the *PlateSpin Virtual Machine Manager* role.

Figure 5-1 Roles assigned in vCenter



Security Implications of Assigning VMware Roles

PlateSpin software uses an enabled user only to perform protection lifecycle operations. From your perspective as a service provider, an end user never has access to the enabled user's credentials and is unable to access the same set of VMware resources. In an environment where multiple Protect servers are configured to use the same vCenter environment, Protect prevents possibilities for cross-client access. The major security implications include:

- ♦ With the *PlateSpin Infrastructure Manager* role assigned to the vCenter object, every enabled user can see (but not affect) the tasks performed by every other user.
- ♦ Because there is no way to set permissions on datastore folders/subfolders, all enabled users with permissions on a datastore have access to all other enabled users' disks stored on that datastore.
- ♦ With the *PlateSpin Infrastructure Manager* role assigned to the cluster object, every enabled user is able to turn off/on HA or DRS on the entire cluster
- ♦ With the *PlateSpin User* role assigned at the storage cluster object, every enabled user is 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 allows the enabled user to see all VMs placed in the default resource pool and/or default VM folder. Also, propagation requires the administrator to explicitly set the enabled user to have a "no-access" role on every resource pool/VM folder that he or she should not have access to.
- ♦ Setting the *PlateSpin Infrastructure Manager Role* on the vCenter object allows the enabled user to end sessions of any other user connected to the vCenter.

NOTE: Remember, in these scenarios, different enabled users are actually different instances of the PlateSpin software.

5.4 Data Transfer

The following topics provide information about the mechanisms and options of data transfer from your workloads to their replicas.

- ♦ [Section 5.4.1, "Transfer Methods," on page 65](#)
- ♦ [Section 5.4.2, "Data Encryption," on page 66](#)

5.4.1 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.

Transfer Methods Supported for Windows Workloads

For Windows workloads, PlateSpin Protect provides mechanisms to transfer workload volume data at either block or file level.

- ❑ **Windows Block-level Replication:** Data is replicated at a volume's block level. For this transfer method, PlateSpin Protect provides two mechanisms that differ by their continuity impact and performance. You can toggle between these mechanisms as required.
 - ◆ **Replication using the Block-Based Component:** This option uses a dedicated software component for block-level data transfer and leverages the Microsoft Volume Snapshot Service (VSS) with applications and services that support VSS. The installation of the component on your protected workload is automatic.

NOTE: Installation and uninstallation of the block-based component requires a reboot of your protected workload. When you are configuring workload protection details, you can opt to install the component at a later time, deferring the required reboot until the time of the first replication.

- ◆ **Replication without the Block-Based Component:** This option uses an internal 'hashing' mechanism in combination with Microsoft VSS to track changes on the protected volumes. This option requires no reboot, but its performance is inferior to that of the block-based component.

Transfer Methods Supported for Linux Workloads

For Linux workloads, PlateSpin Protect provides a mechanism to transfer workload volume data at block level only. Data transfer is powered by a block-level data transfer component that 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.

5.4.2 Data Encryption

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 (see “[Enabling Support for FIPS-Compliant Data Encryption Algorithms \(Optional\)](#)” in your *Installation and Upgrade Guide*).

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

5.5 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	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). 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. NOTE: The blackout start and end times are based on the system clock on your PlateSpin Server.
Compression Level	These settings control whether and how workload data is compressed before transmission. See " Data Compression " on page 15. 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.
Bandwidth Throttling	These settings control bandwidth throttling. See " Bandwidth Throttling " on page 15. To throttle replications to a specified rate, specify the required throughput value in Mbps and indicate the time pattern.
Recovery Points to Keep	Specify the number of recovery points to keep for workloads that use this Protection Tier. See " Recovery Points " on page 68.

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.

5.6 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.

5.7 Initial Replication Method (Full and Incremental)

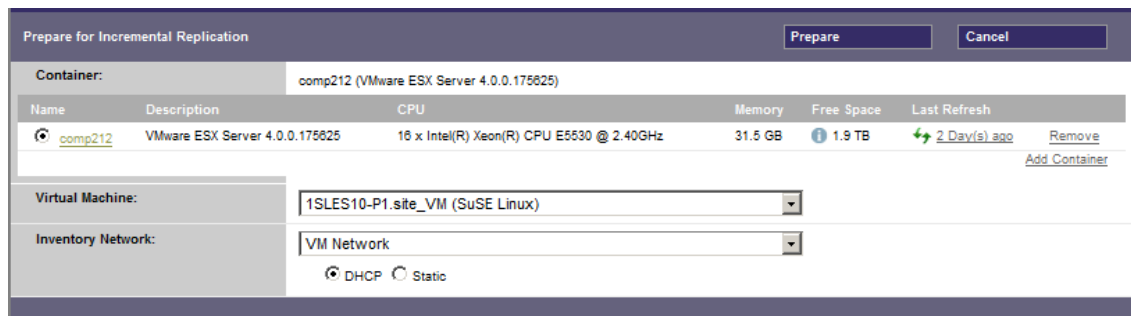
In workload protection and failback operations, the Initial Replication parameter determines the scope of data transferred from a source to a target.

- ◆ **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 56).

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 *Configure (Protection Details)* 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.



- 4 Select the required container, the virtual machine, and the inventory network to use for communicating with the VM. If the specified target container is a VMware DRS Cluster, you can also specify a target Resource Pool for the system to assign the workload to.
- 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.

5.8 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 70.

- ♦ **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.

5.9 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 69](#)). 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
```

5.10 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 5-2 Volumes, Logical Volumes, and Volume Groups of a Protected Linux Workload

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

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

Figure 5-3 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/NEVPPOOL (NSSFS)	23.3 MB	999.6 MB	NEVPPOOL	
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"/>	NEVPPOOL	dev-comp124:storage	1023.0 MB	dev-comp124:storage	<input type="checkbox"/>
Daemons to Stop During Replication:	Add Daemons					

5.11 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.

5.12 Failback to Physical Machines

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.

- ♦ [Section 5.12.1, "Downloading the PlateSpin Boot ISO Image," on page 72](#)
- ♦ [Section 5.12.2, "Injecting Additional Device Drivers into the Boot ISO Image," on page 72](#)
- ♦ [Section 5.12.3, "Registering Physical Machines as Failback Targets with PlateSpin Protect," on page 73](#)

5.12.1 Downloading the PlateSpin Boot ISO Image

You can download a .zip file containing the PlateSpin boot ISO image (`bootofx.x2.iso`) from the PlateSpin Protect area of [Novell Downloads](http://download.novell.com) (<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

5.12.2 Injecting Additional Device Drivers into the Boot ISO Image

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 *.ko driver files appropriate for the target hardware manufacturer.

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 `umount <mount_point>`).
- 4 Create another working directory for the required driver files and save them in that directory.
- 5 In the directory where you saved the `rebuildiso.sh` script, run the following command as root:


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

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

5.12.3 Registering Physical Machines as Failback Targets with PlateSpin Protect

- 1 Burn the PlateSpin boot ISO 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*.
- 3 Use the boot CD to boot the target physical machine, then wait for the command prompt window to open.
- 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 Server host.
- 7 Provide your administrator-level credentials for the PlateSpin 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.

5.13 Advanced Workload Protection Topics

This section includes the following information:

- ◆ [Section 5.13.1, “Using Workload Protection Features through the PlateSpin Protect Web Services API,” on page 74](#)

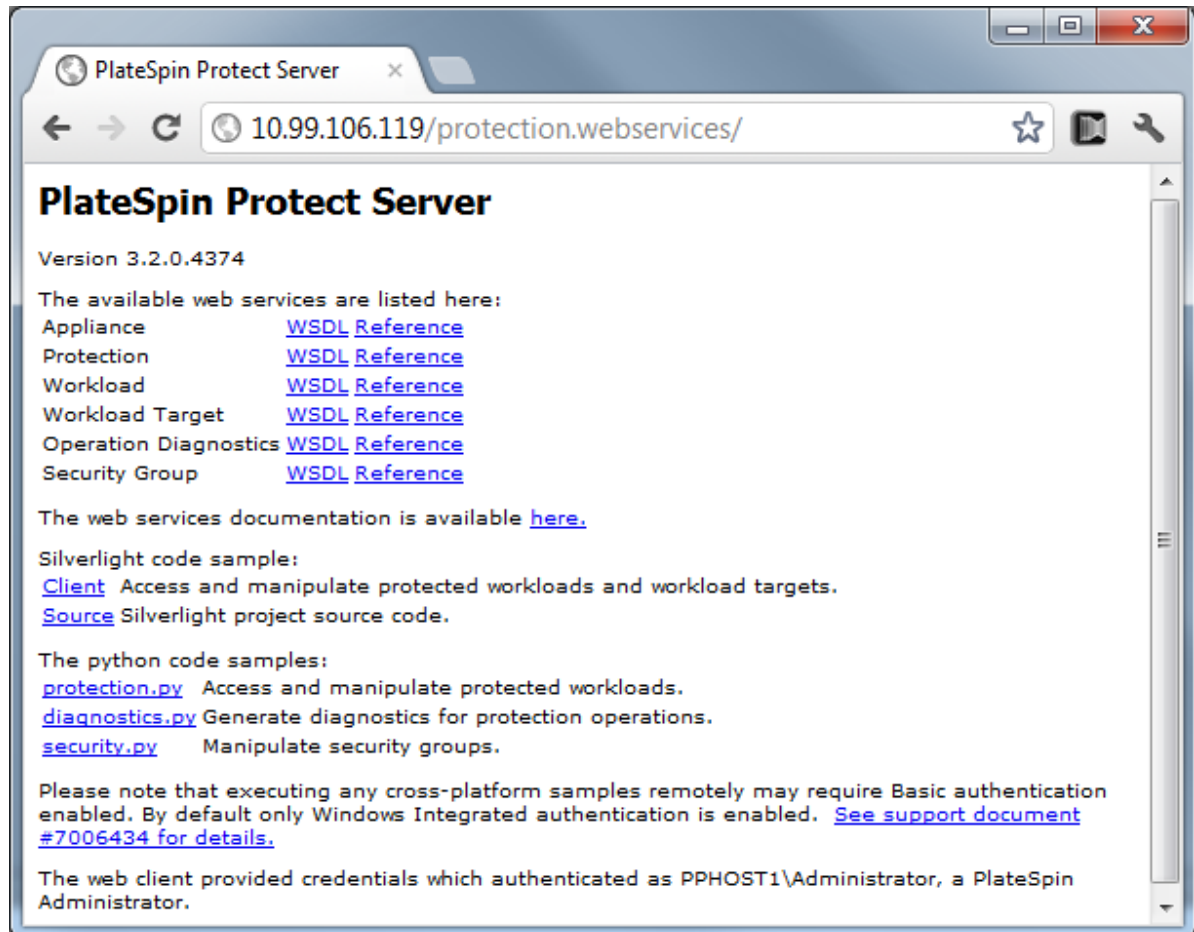
5.13.1 Using Workload Protection Features through the PlateSpin Protect Web Services API

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.

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

Replace `<hostname | IP_address>` with the hostname or the IP address of your PlateSpin Server host. If SSL is not enabled, use `http` in the URI.

Figure 5-4 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 75](#)
- ◆ [Section 6.2, “Managing Device Drivers,” on page 76](#)

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 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 75.

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.

The following sections provide more details:

- ♦ [Section 6.2.1, “Packaging Device Drivers for Windows Systems,”](#) on page 76
- ♦ [Section 6.2.2, “Packaging Device Drivers for Linux Systems,”](#) on page 77
- ♦ [Section 6.2.3, “Uploading Drivers to the PlateSpin Protect Device Driver Database,”](#) on page 77
- ♦ [Section 6.2.4, “Using the Plug and Play \(PnP\) ID Translator Feature,”](#) 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 77](#).

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 PlateSpin boot ISO image.

- 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 77](#).

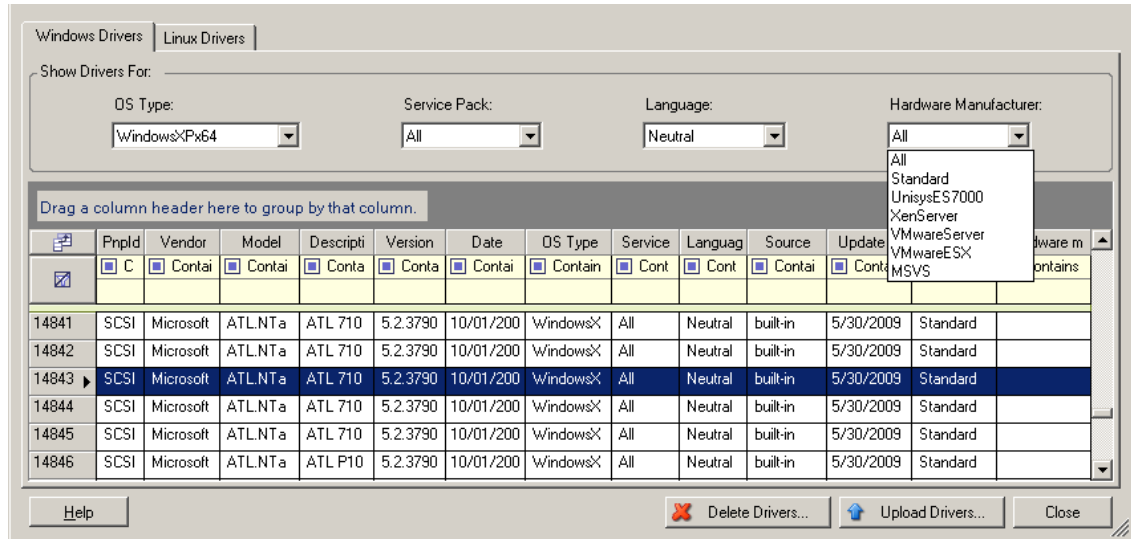
6.2.3 Uploading Drivers to the PlateSpin Protect Device Driver Database

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

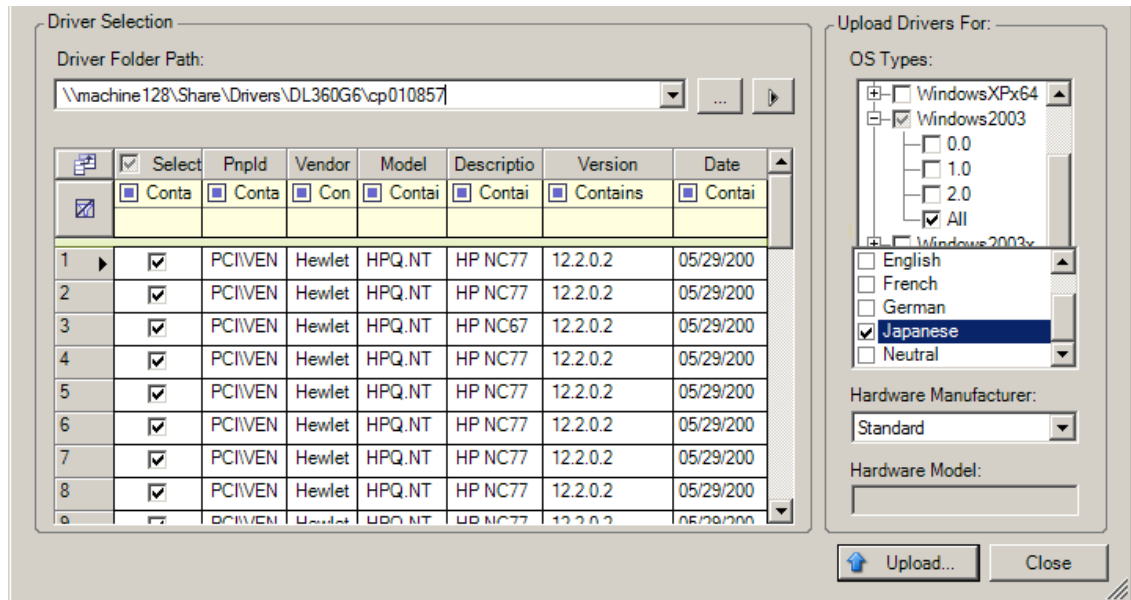
NOTE: On upload, PlateSpin Protect does not validate drivers against selected operating system types or their bit specifications; make sure that you only upload drivers that are appropriate for your target infrastructure.

Device Driver Upload Procedure (Windows)

- 1 Obtain and prepare the required device drivers. See [Packaging Device Drivers for Windows Systems](#).
- 2 On your PlateSpin 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.

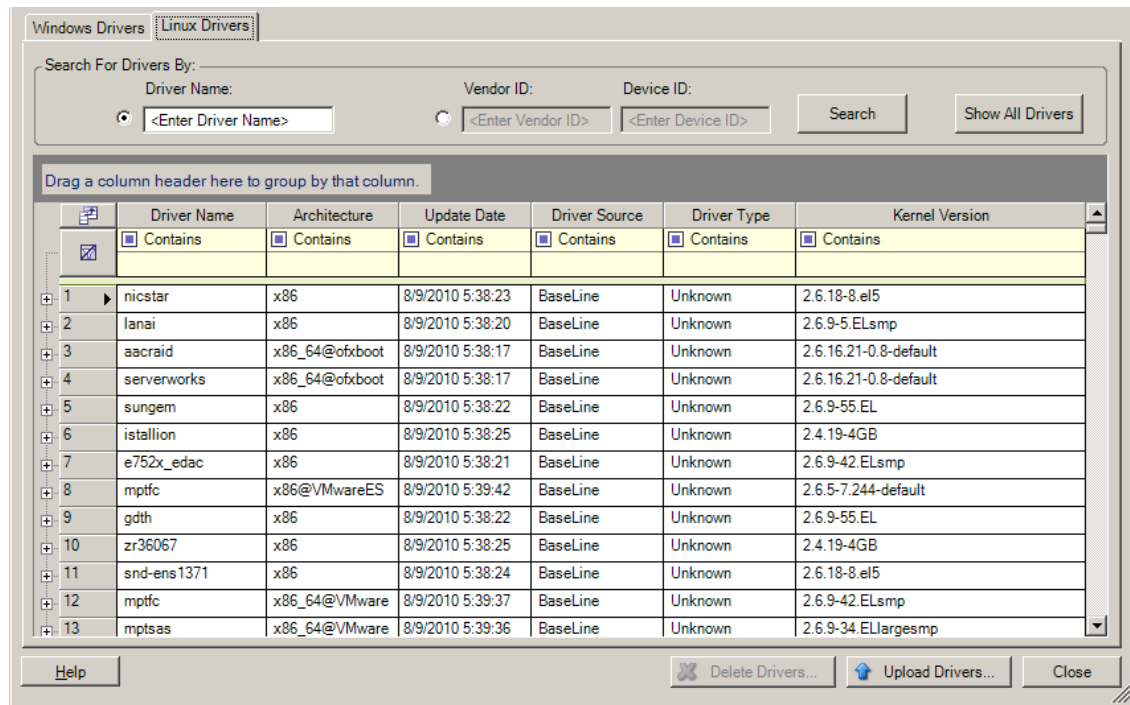


Select *Standard* as the *Hardware Manufacturer* option, unless your drivers are designed specifically for any of the target environments listed.

- 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.

6.2.4 Using the Plug and Play (PnP) ID Translator Feature

“Plug and Play” (PnP) refers to Windows operating system functionality that supports connectivity, configuration, and management with native plug and play devices. In Windows, the feature facilitates discovery of PnP compliant hardware devices attached to a PnP compliant bus. PnP compliant devices are assigned a set of Device Identification Strings by their manufacturer. These strings are programmed into the device when it is built. These strings are fundamental to how PnP works: they are part of the Windows' information source used to match the device with a suitable driver.

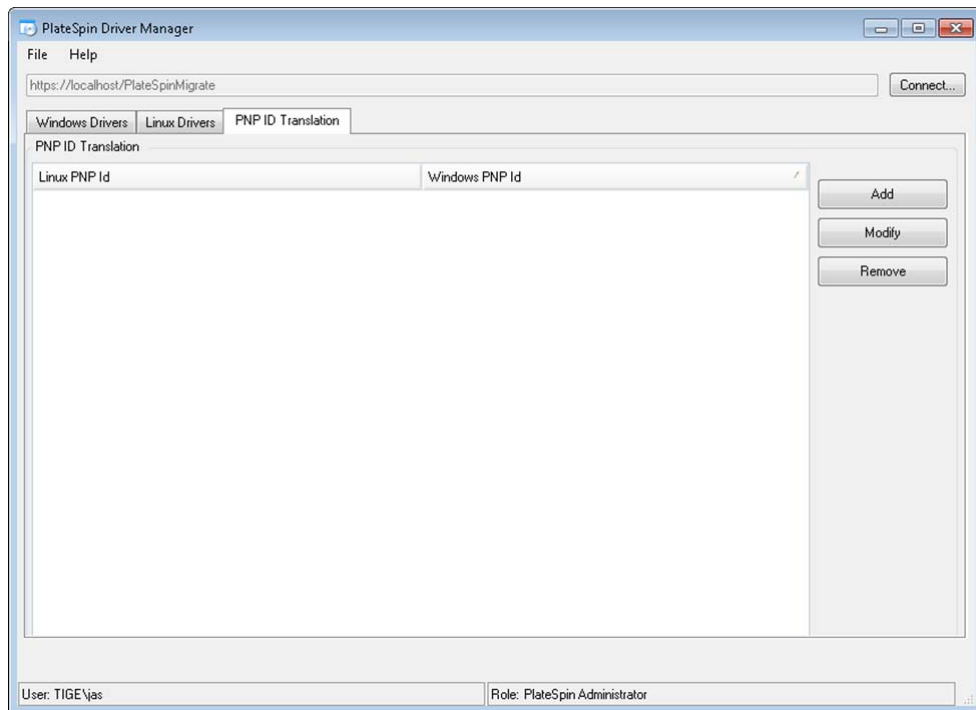
When the PlateSpin Server discovers workloads and their available hardware, the discovery includes these PnP IDs and the storage of that data as part of the workload's details. PlateSpin uses the IDs to determine which, if any, drivers need to be injected during a failover/failback operation. The

PlateSpin Server maintains a database of PnP IDs for the associated drivers of each of the supported operating systems. Because Windows and Linux use different formats for PnP IDs, a Windows workload discovered by the Protect Linux RAM disk contains Linux-style PnP IDs.

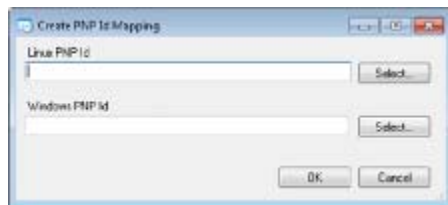
These IDs are formatted consistently, so PlateSpin can apply a standard transformation to each of them to determine its corresponding Windows PnP ID. The translation occurs automatically within the PlateSpin product. The feature lets you or a support technician add, edit or remove custom PnP mappings.

Follow these steps to use the PnP ID Translation feature:

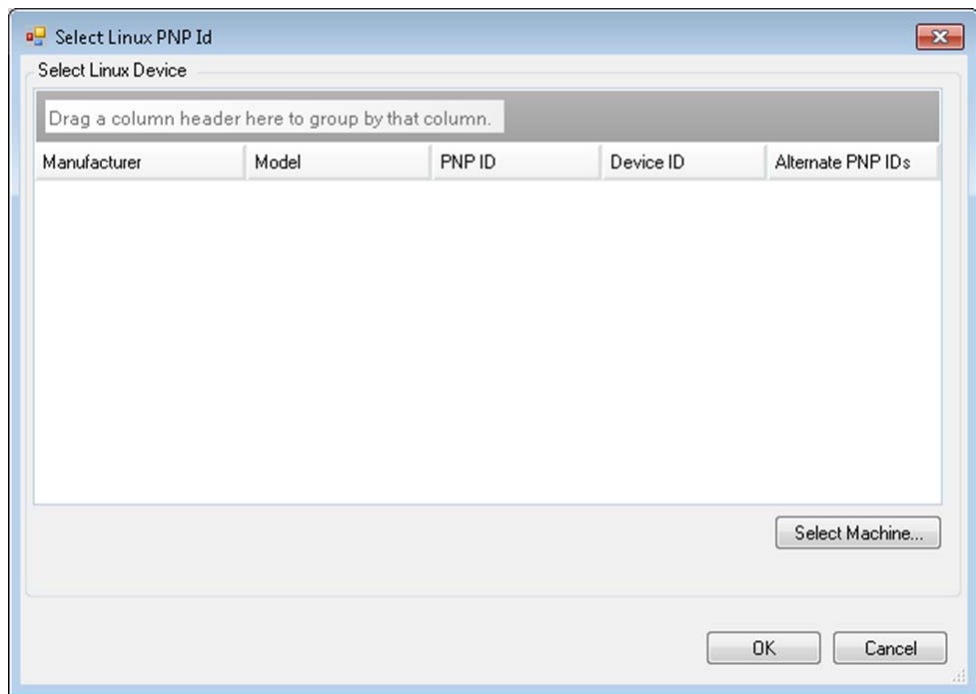
- 1 Launch the PlateSpin Driver Manager tool and connect to the PlateSpin Server.
- 2 In the Driver Manager tool, select the PNP ID Translation tab to open the *PNP ID Translation* list, which includes the currently known custom PnP ID mappings.



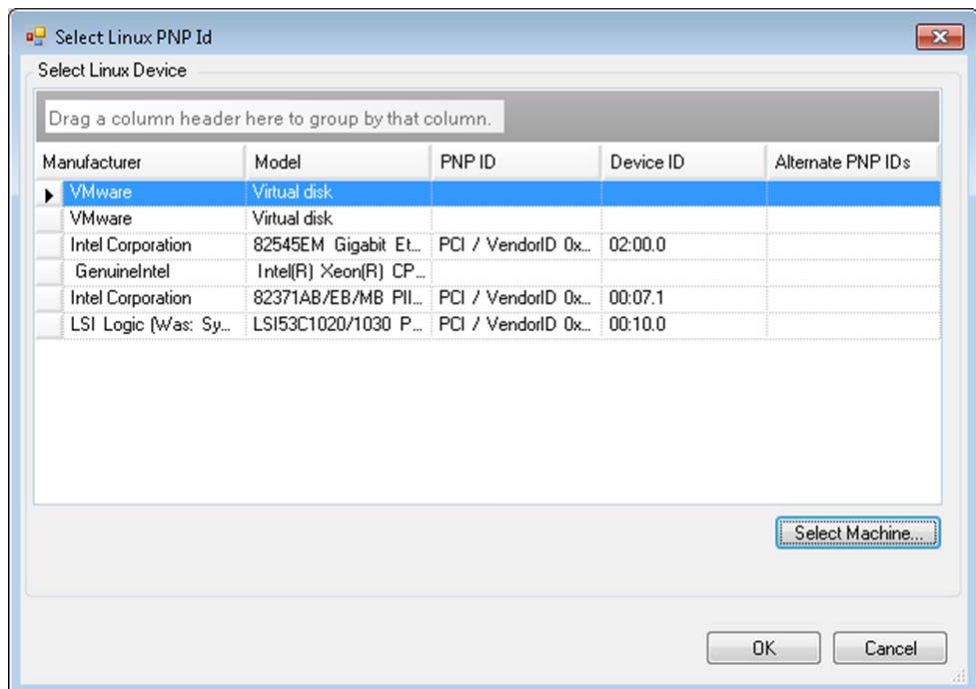
- 3 On the list page, click *Add* to display the Create PNP ID Mapping dialog box.



- 4 In the *Linux PnP ID* field, add a Linux PnP ID.
 - 4a (Conditional) If you know it, type the Linux PnP ID you want to use.
or
 - 4b (Conditional) Select an ID from a previously discovered workload:
 - 4b1 Adjacent to the *Linux PnP ID* field, click *Select* to open the Select Linux PnP ID dialog box.



- 4b2** On the dialog box, click *Select Machine* to display a list of the machines previously discovered by the PlateSpin Linux RAM disk.
- 4b3** Highlight one of the devices in the list, then click *Select* to populate the list in the Select Linux PnP ID dialog box.



- 4b4** Select a device on the list, then click *OK* to apply the standard transformation to the PnP ID and display it in the Create PnP ID Mapping dialog box.

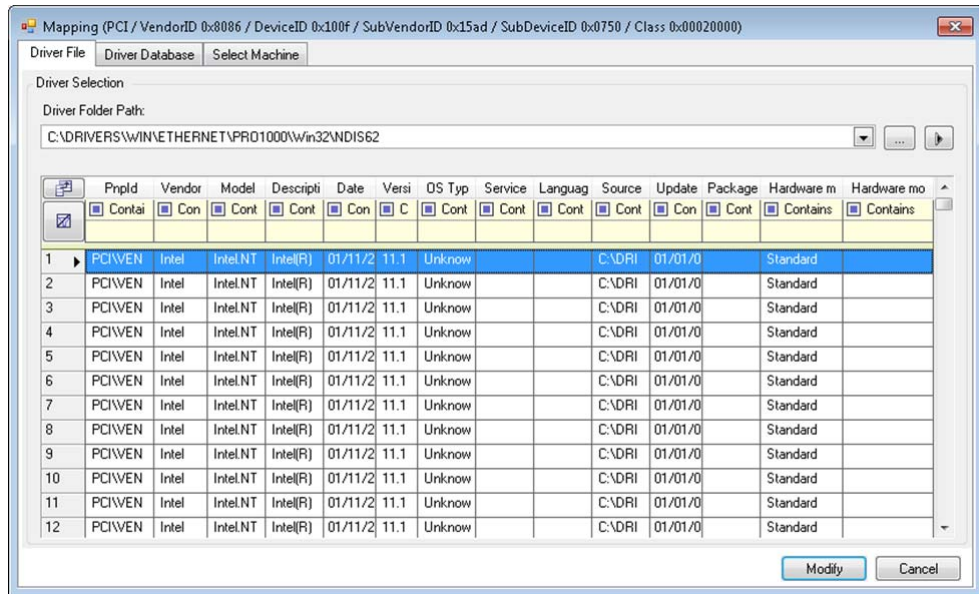
5 In the *Windows PNP ID* field, add a Windows PnP ID:

5a (Conditional) If you know it, type the Windows PnP ID you want to use.

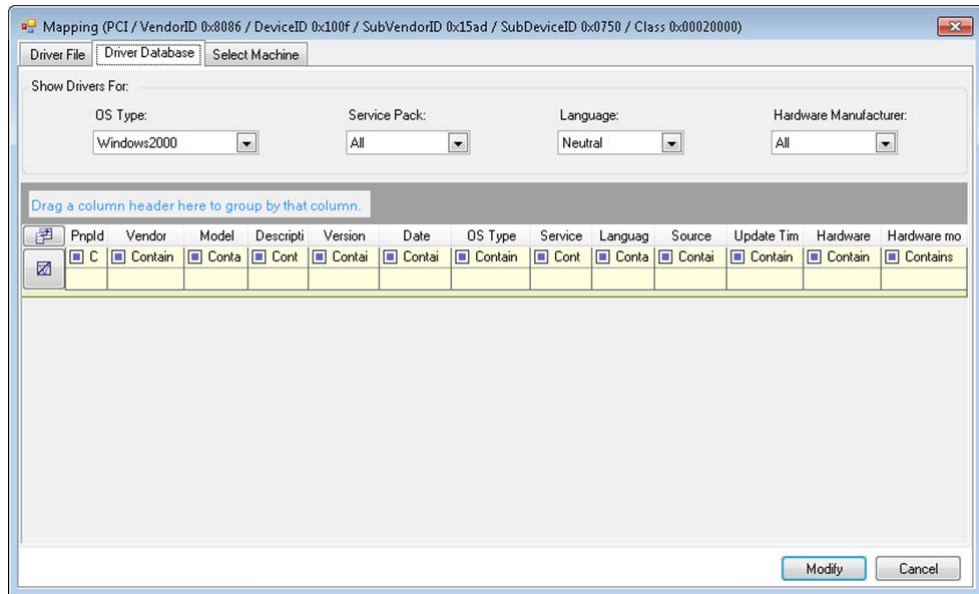
OR

5b (Conditional) Adjacent to the *Windows PNP ID* field, click *Select* to open a mapping tool that presents three methods for helping you map a the Windows PnP ID:

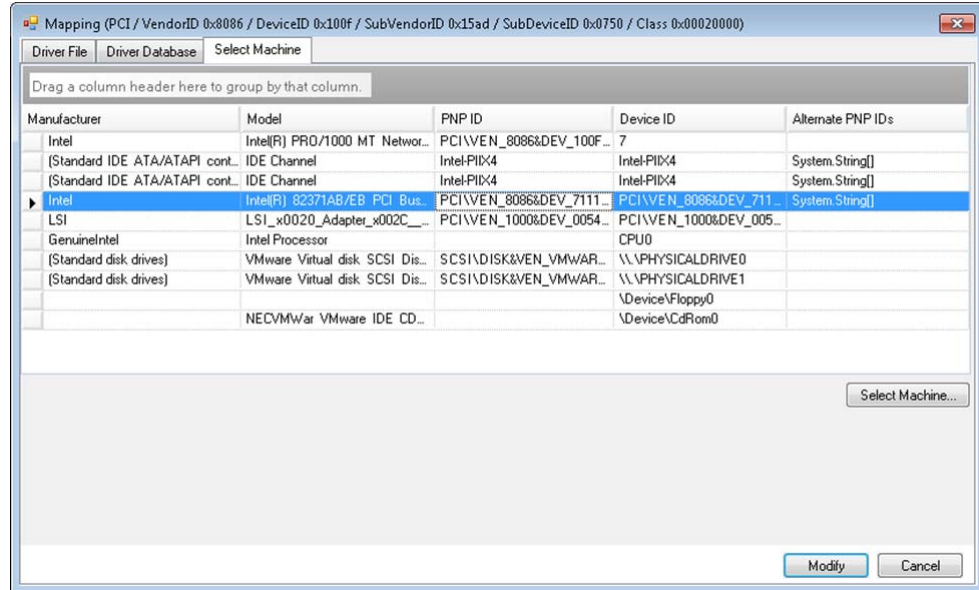
- ♦ Under the *Driver File* tab, browse to and select a Windows driver file (that is, a file with the *.inf extension), select the desired PnP ID, then click *Modify*.



- ♦ Under the *Driver Database* tab, browse to and select the existing driver database, select the correct PnP ID, then select *Modify*.

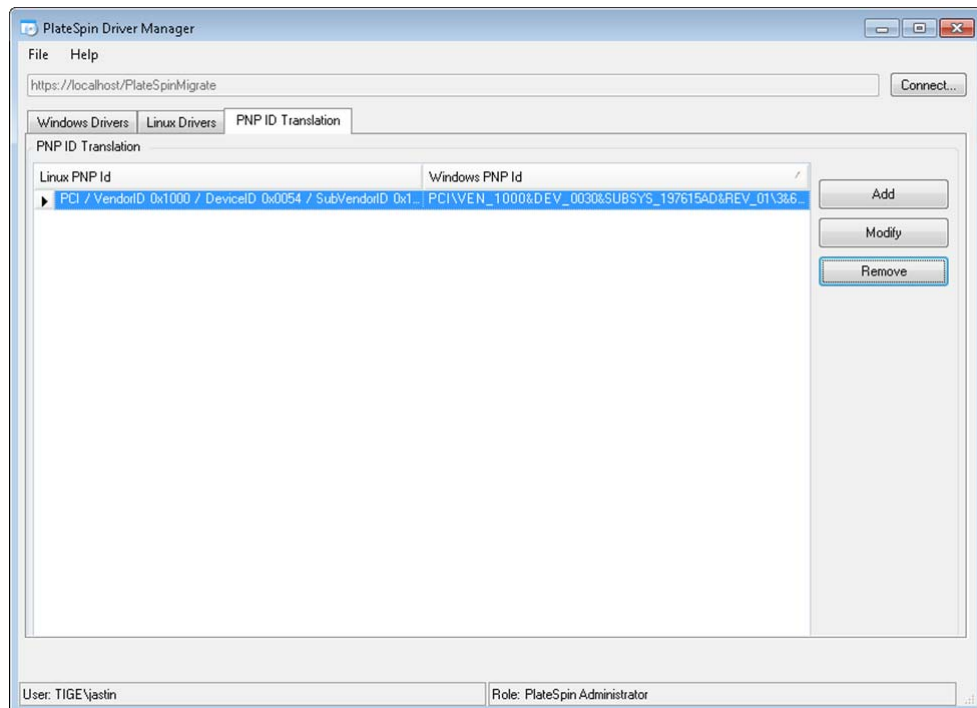


- Under the *Select Machine* tab, click *Select Machine*, then, from the list of Windows machines discovered using live discovery, select a machine, click *OK* to display its devices, select the desired PnP ID, then click *Modify*.



IMPORTANT: Selecting a Windows PnP ID that does not have an associated driver package installed might result in a failure at failover/failback time.

- In the Create PnP Id Mapping dialog box, confirm that the correct Linux PnP ID and the correct Windows PnP are selected, then click *OK* to display the PNP ID Translation page of the PlateSpin Driver Manager.



- 7** (Optional) To modify or remove the mapping in the PNP ID Translation list, select the mapping pattern, then click *Remove* or *Modify*, depending on the operation you want to perform.

Remove simply deletes the mapping (after displaying a confirmation dialog box).

To modify,

7a Click *Modify* to open the Create PNP id Mapping dialog box.

7b Repeat [Step 5 on page 82](#) to modify the Windows PnP ID.

NOTE: You cannot select or modify the Linux PnP ID.

7 Troubleshooting

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 86 again. If the test succeeds, try adding the workload again.</p> <ul style="list-style-type: none">◆ “Troubleshooting DCOM Connectivity” on page 87◆ “Troubleshooting RPC Service Connectivity” on page 87
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 86. If a test fails, ensure that PlateSpin Protect and the workload are on the same network. Reconfigure the network and try again.</p>
D:\discover Server Details {hostname}” Failed Progress: 0% Status: NotStarted	<p>This error can occur for several reasons and each has a unique solution:</p> <ul style="list-style-type: none">◆ For environments using a local proxy with authentication, bypass the proxy or add the proper permissions. See KB Article 7920339 (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).

Problems or Messages	Solutions
Workload Discovery fails with error message	There are several possible reasons for the Could not find file output.xml error:
Could not find file output.xml or Network path not found	<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 87. ◆ 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 88. ◆ 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.

The following sections provide more troubleshooting information on Windows workloads:

- ◆ [Section 7.1.1, “Performing Connectivity Tests,” on page 86](#)
- ◆ [Section 7.1.2, “Disabling AntiVirus Software,” on page 87](#)
- ◆ [Section 7.1.3, “Enabling File/Share Permissions and Access,” on page 88](#)

7.1.1 Performing Connectivity Tests

- ◆ [“Network Connectivity Test” on page 86](#)
- ◆ [“WMI Connectivity Test” on page 86](#)
- ◆ [“Troubleshooting DCOM Connectivity” on page 87](#)
- ◆ [“Troubleshooting RPC Service Connectivity” on page 87](#)

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 Server host.
- 2 Open a command prompt and ping your workload:

```
ping workload_ip
```

WMI Connectivity Test

- 1 Go to your PlateSpin 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 22).

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 Server host:

- 1 Go to your PlateSpin 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 22.</p>
Access denied	<p>This authentication problem indicates either an invalid username or password. For information on proper workload access credentials, see “Guidelines for Workload and Container Credentials” on page 60.</p>

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 89.
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 85.

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.	<p>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.</p>
Slow network speeds over 1 MB.	<p>Measure the latency by running the following command from the source workload:</p> <pre>ping ip-t (replace ip with the IP address of your PlateSpin Server host).</pre> <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 30.</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> <p>Run <code>netstat -ano</code> 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 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 Server host.</p>

Problems or Messages**Solutions**

Replication job does not start (stuck at 0%)

This error can occur for different reasons and each has a unique solution:

- ◆ For environments using a local proxy with authentication, bypass the proxy or add proper permissions to resolve this problem. See [KB Article 20339 \(https://www.netiq.com/support/kb/doc.php?id=7920339\)](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 \(https://www.netiq.com/support/kb/doc.php?id=7920862\)](https://www.netiq.com/support/kb/doc.php?id=7920862).

This is a common issue when PlateSpin Server host is affiliated with a domain and the domain policies are applied with restrictions. See “[Group Policy and User Rights](#)” on page 89.

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.

The screenshot shows the PlateSpin Protect Web Interface. The top navigation bar includes 'Dashboard', 'Workloads', 'Tasks', 'Reports', 'Settings', 'About', and 'Help'. Below the navigation bar, there are tabs for 'Protection Details' and 'Command Details'. The main content area displays the details for a command named 'Running First Replication' on the host 'DI-Sies11.platespin.com'. The status is 'Running' with a progress bar at 80%. The duration is 14h 49m 6s. The current step is 'Copy data (80%)'. A 'Generate Diagnostics' link is highlighted with a red box. Below the command details, there is a 'Command Summary' section with a table showing the command's status, start time, duration, and a table of steps. The 'Generate Diagnostics' link is also present in this section. Below the command summary, there is a 'Replication Transfer Summary' section with a table showing the average transfer speed, total data transferred, and duration. At the bottom, there is a 'Workload Commands' section.

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

Property	Value
Average Transfer Speed:	298.80 Mbps
Total Data Transferred:	3.7 GB
Duration:	1m 42s

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.

The following sections include more information:

- ♦ [Section 7.7.1, “Cleaning Up Windows Workloads,” on page 92](#)
- ♦ [Section 7.7.2, “Cleaning Up Linux Workloads,” on page 93](#)

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.

Component	Removal Instructions
File-based Transfer Component	At root level for each volume under protection, remove all files named PlateSpinCatalog*.dat
Workload Inventory software	In the workload's Windows directory: <ul style="list-style-type: none"> ◆ Remove all files named machinediscovery*. ◆ Remove the subdirectory named platespin.
Controller software	<ol style="list-style-type: none"> 1. Open a command prompt and change the current directory to: <ul style="list-style-type: none"> ◆ \Program Files\platespin* (32-bit systems) ◆ \Program Files (x86)\platespin* (64-bit systems) 2. Run the following command: <pre>ofxcontroller.exe /uninstall</pre> 3. 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"> 1. Check if the driver is active: <pre>lsmod grep blkwatch</pre> <p>If the driver is still loaded in memory, the result should contain a line, similar to the following:</p> <pre>blkwatch_7616 70924 0</pre> 2. (Conditional) If the driver is still loaded, remove it from memory: <pre>rmmmod blkwatch_7616</pre> 3. Remove the driver from the boot sequence: <pre>blkconfig -u</pre> 4. Remove the driver files by deleting the following directory with its contents: <pre>/lib/modules/[Kernel_Version]/Platespin</pre> 5. Delete the following file: <pre>/etc/blkwatch.conf</pre>

Component	Removal Instructions
LVM snapshots	<p>LVP snapshots used by ongoing replications are named according to a <code>volume_name-PS-snapshot</code> convention. For example, a snapshot of a <code>LogVol101</code> volume will be named <code>LogVol101-PS-snapshot</code>.</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 <code>.blocks_bitmap</code> file.</p>
Tools	<p>On the source workload, under <code>/sbin</code>, remove the following files:</p> <ul style="list-style-type: none"> ◆ <code>bmaputil</code> ◆ <code>blkconfig</code>

A Documentation Updates

This section contains information on documentation content changes that were made in this *User Guide* after the initial release of NetIQ PlateSpin Protect 10.4. The changes are listed according to the date they were published.

The documentation for this product is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the changes listed in this section.

If you need to know whether a copy of the PDF documentation that you are using is the most recent, the PDF document includes a publication date on the title page.

The documentation was updated on the following dates:

- ♦ [Section A.1, “April 4, 2014,” on page 95](#)
- ♦ [Section A.2, “March 26, 2014,” on page 95](#)

A.1 April 4, 2014

Updates were made to the following sections:

Location	Update
Section 5.13, “Advanced Workload Protection Topics,” on page 74	<p>The subsection titled <i>Protecting Windows Clusters</i> has been removed from this section.</p> <p>PlateSpin Protect does not support the protection of a Microsoft Windows Cluster’s business services in this release.</p>

A.2 March 26, 2014

Updates were made to the following sections:

Location	Update
Section 5.13, “Advanced Workload Protection Topics,” on page 74	<p>The subsection titled <i>Linux Failback to a Paravirtualized VM on Xen on SLES</i> has been removed from this section.</p> <p>Because PlateSpin Protect now uses the Linux RAM Disk, supporting SLES XEN as a failback target is no longer practical.</p>

Glossary

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

Event. A PlateSpin 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.