

User Guide

Novell® PlateSpin Forge®

2.5

August 24, 2009

www.novell.com



Legal Notices

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

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

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

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

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the [Novell Legal Patents Web page \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide	9
1 Introduction	11
1.1 Overview	11
1.1.1 What Is PlateSpin Forge?	11
1.1.2 Key Product Features	11
1.1.3 New in This Release	12
1.1.4 Platform Support	13
1.1.5 Browser Support	13
1.2 Using This Guide	13
1.3 How Do I Interact with PlateSpin Forge?	13
1.4 How Servers Work with PlateSpin Forge	14
2 Understanding Basic Functionality	15
2.1 Basic PlateSpin Forge Terms and Concepts	15
2.1.1 Role-Based Access	15
2.1.2 Protection Tiers	16
2.1.3 Failover	16
2.1.4 Test Failover	17
2.1.5 Prepare for Failover	17
2.1.6 Failback	18
2.1.7 Recovery Points	18
2.1.8 Consolidated Workload Protection and Recovery	18
2.1.9 Disaster Recovery	19
2.1.10 Supported Transfer Methods	19
2.1.11 Fine-Tuning Data Transfer Performance	21
2.1.12 Terminology	24
2.1.13 Events and Tasks	25
2.2 Web Interface	26
2.2.1 The Dashboard Page	27
2.2.2 The Workloads Page	29
2.2.3 Workload Commands	30
2.2.4 Add Workload	31
2.2.5 Remove Workload	32
2.2.6 Workload Details	33
2.2.7 The Tasks Page	36
2.2.8 The Reports Page	36
2.2.9 Workload Protection	37
2.2.10 Replication History	37
2.2.11 Replication Window	37
2.2.12 Current Protection Status	38
2.2.13 Events and Upcoming Events	38
2.2.14 The Settings Page	38
2.3 Product Expectations	41
2.3.1 RTO	41
2.3.2 RPO	42
2.3.3 Failover	42
2.3.4 Recovery Points	42

3	Using Forge	43
3.1	Managing Role-Based Access	43
3.1.1	Creating Host Appliance Users	43
3.1.2	Creating Security Groups	44
3.1.3	Editing Security Groups	44
3.1.4	Deleting Security Groups	45
3.1.5	Removing Users from Security Groups	45
3.1.6	Removing Workloads from Security Groups	45
3.2	Protecting a Workload	46
3.2.1	Creating a Protection Tier	46
3.2.2	Network Communication Prerequisites for Discovery	47
3.2.3	Adding a Workload	49
3.2.4	Configuring Protection and Preparing Replication	49
3.2.5	Running Replication	50
3.3	Planning for Failure	50
3.3.1	Workload Testing	50
3.3.2	Preparing for Failover	51
3.3.3	Running a Prepared Failover	52
3.3.4	Running an Unprepared Failover	53
3.3.5	Removing a Snapshot After Failover (Optional)	53
3.4	Failback	54
3.4.1	Preparing the Failback	54
3.4.2	Configuring and Running Failback	55
3.4.3	Configuring Reprotect	55
3.5	Importing a Workload into Forge	56
3.6	Adding a SAN LUN to Forge	57
3.7	Running Diagnostics	58
4	Forge Management Console	59
4.1	Overview	59
4.2	Starting the Console	59
4.3	Working with Appliances	60
4.3.1	Adding Appliances	60
4.3.2	Editing Appliance Information	61
4.3.3	Removing Appliances	61
5	SAN Storage	63
5.1	Using Forge with SAN Storage	63
5.2	Adding a SAN LUN to Forge	64
6	Forge Relocation	67
6.1	Forge IP Addresses	67
6.2	Changing IP Addresses	67
6.2.1	Preparing Currently Protected Workloads for the Change	68
6.2.2	Making the Change	69
6.2.3	Reconfiguring Workloads to Reflect the Change	70
7	Troubleshooting	73
7.1	Add Workload - Configuration	73
7.1.1	Network Connectivity Test	74
7.1.2	WMI Connectivity Test	74

7.1.3	Enabling DCOM	75
7.1.4	Ensuring RPC Service is Running	75
7.2	Add Workload - Discovery	76
7.2.1	Disabling Anti-Virus Software	77
7.2.2	Enabling File/Share Permissions and Access	78
7.3	Prepare Replication	78
7.3.1	Group Policy and User Rights	78
7.4	Replication	79
7.4.1	Optimizing File-based Transfers for WAN Connections	80

About This Guide

This *User Guide* introduces PlateSpin Forge[®] 2.5, including its basic administration environment, which is accessed through the PlateSpin Forge Web Interface. The guide provides an overview of the appliance and explains how it administers and manages workloads under protection, as well as how to put workloads under protection. The guide is organized as follows:

- ♦ Chapter 1, “Introduction,” on page 11
- ♦ Chapter 2, “Understanding Basic Functionality,” on page 15
- ♦ Chapter 3, “Using Forge,” on page 43
- ♦ Chapter 4, “Forge Management Console,” on page 59
- ♦ Chapter 5, “SAN Storage,” on page 63
- ♦ Chapter 6, “Forge Relocation,” on page 67
- ♦ Chapter 7, “Troubleshooting,” on page 73

Audience

This documentation is intended for data center managers, and IT or operations administrators. It assumes that users of the product have the following background:

- ♦ General understanding of network operating environments and systems architecture.
- ♦ General virtualization knowledge.
- ♦ Understanding of disaster recovery principles.

The contents of this guide are of interest to IT personnel, data center system administrators or any other persons who are responsible for the day-to-day functionality of the unit.

Feedback

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

Documentation Updates

For the most recent version of this text, visit the [PlateSpin Forge version 2.5 Web site \(http://www.novell.com/documentation/platespin_forge_25/\)](http://www.novell.com/documentation/platespin_forge_25/).

Additional Documentation

This guide is part of the PlateSpin Forge[®] documentation set. Below is a complete list of the set:

<i>PlateSpin Forge 2.5 Release Notes</i>	Provides late-breaking information, as well as information about known issues and suggested workarounds.
PlateSpin Forge 2.5 Getting Started Guide	Provides information about installing the product and performing the initial configuration.

PlateSpin Forge 2.5 User Guide	Provides information about using the product in your workload protection projects.
<i>PlateSpin Forge 2.5 Upgrade Guide</i>	Provides information on upgrading the forge unit, both from downloaded files and using a PlateSpin Forge USB stick.
PlateSpin Forge 2.5 Integrated Help	The User Guide in compiled HTML help format, integrated with the product.
PlateSpin Forge 2.5 Online Documentation	All product documentation in WebHelp format for browser-based access over the Internet. This distribution should contain the latest updates at all times.

Additional Resources

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

- ◆ [PlateSpin User Forum \(http://forum.platespin.com\)](http://forum.platespin.com): A Web-based community with a variety of discussion topics.
- ◆ [PlateSpin Knowledge Base \(http://support.platespin.com/kb2/\)](http://support.platespin.com/kb2/): A collection of in-depth technical articles.

Technical Support

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

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

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (® , ™ , etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

Introduction

1

Welcome to PlateSpin Forge[®] 2.5. The following sections include general information you need to become acquainted with the product:

- ◆ [Section 1.1, “Overview,” on page 11](#)
- ◆ [Section 1.2, “Using This Guide,” on page 13](#)
- ◆ [Section 1.3, “How Do I Interact with PlateSpin Forge?,” on page 13](#)
- ◆ [Section 1.4, “How Servers Work with PlateSpin Forge,” on page 14](#)

1.1 Overview

The following sections contain information to introduce you to PlateSpin Forge:

- ◆ [Section 1.1.1, “What Is PlateSpin Forge?,” on page 11](#)
- ◆ [Section 1.1.2, “Key Product Features,” on page 11](#)
- ◆ [Section 1.1.3, “New in This Release,” on page 12](#)
- ◆ [Section 1.1.4, “Platform Support,” on page 13](#)
- ◆ [Section 1.1.5, “Browser Support,” on page 13](#)

1.1.1 What Is PlateSpin Forge?

PlateSpin Forge is a consolidated recovery hardware appliance that protects both physical and virtual server workloads by using embedded virtualization technology. If there is a production server outage or disaster, workloads can be rapidly powered on within the PlateSpin Forge recovery environment and continue to run as normal until the production environment is restored.

PlateSpin Forge 2.5 uses its functional components to:

- ◆ Protect from 10 to 25 workloads, depending on which model is installed
- ◆ Perform protection testing without interfering with the production environment
- ◆ Provide quick disaster recovery, including restoration to different hardware
- ◆ Take advantage of existing external storage solutions, such as SANs.

Four different models are available in various configurations. Most of the models ship with prepackaged storage, and all models ship with consolidated recovery software and virtualization technology that is ready to go out-of-the-box. With internal, prepackaged storage, Forge has a total storage capacity of 2.5 terabytes, although the capacity is almost unlimited when external storage configurations are used by adding iSCSI or Fibre Channel cards. The built-in management console provides support for an unlimited number of Forge appliances.

1.1.2 Key Product Features

PlateSpin Forge includes these core features:

- ◆ Whole Workload Replication

- ◆ Block-level and Snapshot Replication
- ◆ Rapid One-click Failover
- ◆ Failback Flexibility
- ◆ Events, Tasks, and Actionable Alerts
- ◆ Protection Tiers
- ◆ Workload Protection Metrics
- ◆ Centralized Management Console
- ◆ Plug In and Protect Workloads
- ◆ Simple Web-Based Management
- ◆ Easy Test Failover
- ◆ Failover Preparation
- ◆ Remote Control

1.1.3 New in This Release

Some of the new features in PlateSpin Forge 2.5 include:

- ◆ Windows Server 2008 & Windows Vista support
 - ◆ Live file-based replication support (VSS-aware)
 - ◆ Live block-based replication support (VSS-aware)
- ◆ Improved Block-Based Transfers
 - ◆ Faster, more robust block-based transfer protocol. Up to 50% faster than previous versions.
 - ◆ Now available for 64-bit workloads.
- ◆ Server Sync Block-Based Transfers
 - ◆ Server Sync now has option of file-based or block-based transfers.
- ◆ Physical Machine Server Sync
 - ◆ Adds support for Server Sync to physical server targets for faster failback scenarios.
- ◆ 24 hour+ replications
 - ◆ Supports block-based replications lasting longer than 24 hours, for customers with extremely large workloads or slow WAN connections.
- ◆ User Interface Enhancements
 - ◆ Integrated failback process: failover from down production server to PlateSpin Forge, then failback to repaired or replaced production server entirely within PlateSpin Forge interface.
 - ◆ Integrated License Release: Change protected workloads entirely within PlateSpin Forge interface.
- ◆ Role-Based Access and Multi-Tenancy
 - ◆ Delegated control through user (workload) groups enables hosting of multiple customers on a single PlateSpin Forge appliance.

- ◆ Appliance Portability
 - ◆ Allows network changes to existing protection contracts.
 - ◆ Enables appliance to be moved within or between networks (e.g., from test to production site).

1.1.4 Platform Support

Forge currently supports these 32-bit and 64-bit Windows systems:

Table 1-1 *Supported Windows Systems*

Operating System	32-bit	64-bit
Windows 2000 Server SP4	X	
Windows 2000 Advanced Server SP4	X	
Windows 2000 Professional SP4	X	
Windows Server* 2003	X	X
Windows Server 2003 R2	X	X
Windows XP Professional SP2	X	X
Windows Server 2008	X	X

1.1.5 Browser Support

Forge currently supports these Windows-based browsers:

- ◆ Microsoft Internet Explorer 7
- ◆ Microsoft Internet Explorer 8 (compatibility mode)
- ◆ Mozilla Firefox 2.x, 3.x

1.2 Using This Guide

The purpose of this guide is to introduce you to the PlateSpin Forge 2.5 hardware appliance and walk you through the initial setup and configuration of all of its components. After completing the steps in this guide, you will be ready to protect and manage workloads.

For more information on setting up the PlateSpin Forge 2.5 hardware appliance, see [Chapter 5, “SAN Storage,”](#) on page 63.

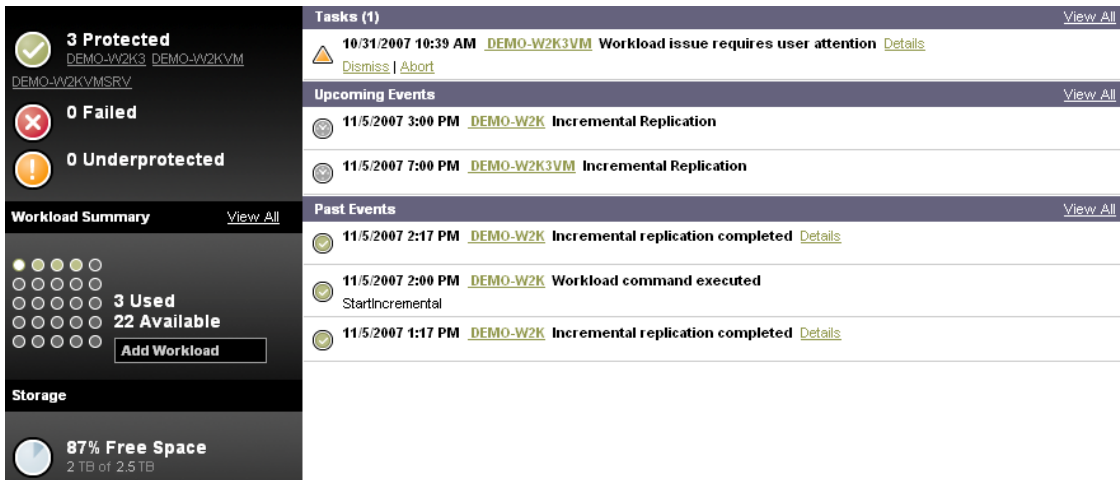
1.3 How Do I Interact with PlateSpin Forge?

Users interact with PlateSpin Forge through the Web-based client.

PlateSpin Forge supports both HTTPS and HTTP as the protocol used between server and client. It also supports both Microsoft* Internet Explorer* 7 and Mozilla* Firefox* 2.0.

To access the Dashboard page of the client, enter the IP address or hostname assigned to the Management VM during configuration in a browser, and log in in with your username and password. From here you can see current and past events, look at tasks requiring user attention, and you can access all features of the appliance by using the menus and display.

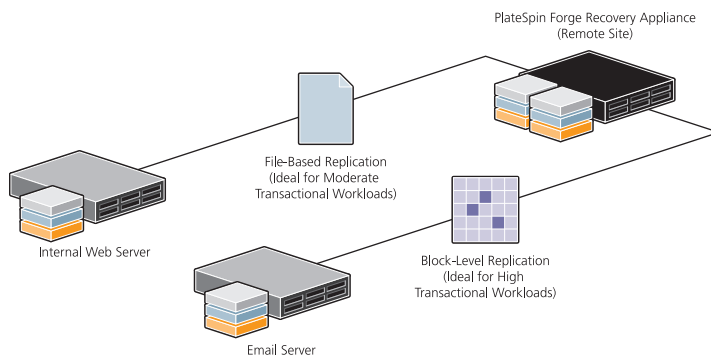
Figure 1-1 PlateSpin Forge Dashboard Page



1.4 How Servers Work with PlateSpin Forge

The PlateSpin Forge Recovery Appliance installs in the data center, and uses configured replication schedules to protect up to 25 workloads by using file-based, VSS, or block-level replication. Virtual machines of each protected workload are created on the Forge appliance and are updated based on the customizable replication schedules. You can also use recovery points to avoid loss of data because of a corrupted workload.

Figure 1-2 PlateSpin Forge Server Interaction



If an outage or system failure occurs on a protected workload, preconfigured notifications are sent by e-mail and are accessible by a mobile device. Administrators can then perform a failover simply by clicking a link in the notification or in the Forge UI, and the associated virtual machine on the Forge appliance is powered on.

Understanding Basic Functionality

2

This section includes basic information about PlateSpin Forge[®] and acquaints you with the appliance's interface and basic functionality.

- ◆ [Section 2.1, “Basic PlateSpin Forge Terms and Concepts,” on page 15](#)
- ◆ [Section 2.2, “Web Interface,” on page 26](#)
- ◆ [Section 2.3, “Product Expectations,” on page 41](#)

2.1 Basic PlateSpin Forge Terms and Concepts

To help you understand the PlateSpin Forge functionality, the following section describes terms and concepts you will see while using the appliance.

- ◆ [Section 2.1.1, “Role-Based Access,” on page 15](#)
- ◆ [Section 2.1.2, “Protection Tiers,” on page 16](#)
- ◆ [Section 2.1.3, “Failover,” on page 16](#)
- ◆ [Section 2.1.4, “Test Failover,” on page 17](#)
- ◆ [Section 2.1.5, “Prepare for Failover,” on page 17](#)
- ◆ [Section 2.1.6, “Failback,” on page 18](#)
- ◆ [Section 2.1.7, “Recovery Points,” on page 18](#)
- ◆ [Section 2.1.8, “Consolidated Workload Protection and Recovery,” on page 18](#)
- ◆ [Section 2.1.9, “Disaster Recovery,” on page 19](#)
- ◆ [Section 2.1.10, “Supported Transfer Methods,” on page 19](#)
- ◆ [Section 2.1.11, “Fine-Tuning Data Transfer Performance,” on page 21](#)
- ◆ [Section 2.1.12, “Terminology,” on page 24](#)
- ◆ [Section 2.1.13, “Events and Tasks,” on page 25](#)

2.1.1 Role-Based Access

Role-based access in Forge allows you to create security groups, assign workloads to those groups and then use one of three types of roles to determine who can do what. You first add users to the Host Appliance and designate them as a Workload Protection Administrator, Workload Protection Power User or Workload Protection Operator, each with varying levels of access. Then, in the Forge Management VM, you create the Security Groups, add workloads to those groups and then add the users you want to have access to those workloads, in whatever capacity, to those groups.

Host Appliance Local Administrators and users you specifically add to the Workload Protection Administrators group are automatically added to every security group.

For more information see [“Managing Role-Based Access” on page 43](#).

Table 2-1 Role-Based Access Matrix

	Administrator	PowerUser	Operator
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
Run Reports/ Diagnostics	Allowed	Allowed	Allowed
Failback	Allowed	Denied	Denied
Reprotect	Allowed	Allowed	Denied

2.1.2 Protection Tiers

Workloads belong to Protection Tiers, which define when and how often replications occur. Protection Tiers also determine how often a protected workload is checked for failure, how many detection attempts to try before triggering intervention, and how many recovery points to keep. Protection Tiers enable a user to create defined plans or templates that are appropriate to multiple workloads instead of configuring each workload's individual plan.

Schedule full and incremental replications as required by business needs—hourly, daily, weekly, or monthly. Select from predefined Protection Tiers, or create a user-defined Protection Tier.

For more information, see [“Creating a Protection Tier” on page 46](#).

2.1.3 Failover

PlateSpin Forge constantly monitors protected workloads. If no response is detected within a specified period of time, the user is notified that the workload has failed. If this happens, the user can choose to have the recovery workload that is running on the PlateSpin Forge appliance rapidly take its place, resulting in minimal interruption in uptime. The workload can then be restored to either the same or a different host by using the built-in failback function.

Failover is the process of bringing the recovery workload online to replace the failed protected workload. After the first full replication runs, the recovery workload can run on the PlateSpin Forge Appliance Host. This is a temporary solution until Failback can be performed. Recovery points can also be selected during Failover, avoiding corrupted replications.

NOTE: Workloads that have failed over and are running on Forge use as much RAM as the protected workloads they replace. Because PlateSpin Forge has a finite amount of RAM (16 or 32 GB, depending on the model), you might need to temporarily suspend other appliance operations to accommodate the workloads. This could include scheduled replications.

For more information, see [“Recovery Points” on page 18](#) and [“Planning for Failure” on page 50](#).

2.1.4 Test Failover

One of the major advantages of PlateSpin Forge is the availability of safe and quick disaster recovery testing. Forge’s unique Test Failover process allows users to test a recovery workload in a safe and isolated configuration that does not conflict with the protected workload or production servers.

The Test Failover process is also unique because it is quick and conducive to frequent testing. Unlike some disaster recovery testing, which can take days to complete, Test Failover provides a clear picture of success or failure in a fraction of that time. PlateSpin Forge reports can be consulted to find out exactly how long a particular test took. Recovery points can also be selected during Test Failover, avoiding corrupted replications.

Use Test Failover to make sure that the recovery workload runs smoothly and fulfills all requirements. When the virtual machine containing the recovery workload is shut down after the test, no changes persist.

In addition to being a safe method of testing, Test Failover is also quick, with a typical test taking less than an hour.

For more information, see [“Recovery Points” on page 18](#) and [“Planning for Failure” on page 50](#).

2.1.5 Prepare for Failover

In most cases, you use Prepare for Failover immediately upon receiving notification that a protected workload has failed. The recovery workload starts running on the PlateSpin Forge Appliance Host, but with its network cards mapped to an internal network to keep it isolated from the main (external) network. Aside from this, Prepare for Failover does all the work of a failover. Recovery points can also be selected during Prepare for Failover, avoiding corrupted replications.

After running Prepare for Failover, check that the problem with the protected workload is not trivial, such as the accidental disconnection of a power cord or network cable, or a temporary network outage. If the problem with the protected workload is not easily rectified, perform a Failover to quickly bring the recovery workload onto the main network, thereby replacing the protected workload. If it is determined that the protected workload can be easily brought back online, select *Cancel Failover*.

This method allows the failover process to start, thus saving valuable time if a failover turns out to be necessary. It also avoids the inconveniences with re-protecting a workload after a premature, unnecessary failover.

For more information, see [“Recovery Points” on page 18](#) and [“Planning for Failure” on page 50](#).

2.1.6 Failback

Failover is a temporary solution. The PlateSpin Forge Appliance Host has limited resources and is not intended to host failed-over workloads indefinitely. The recovery workload runs on the PlateSpin Forge Appliance Host to maintain the workload’s function until new server infrastructure is available.

When new hardware is acquired to permanently host the recovery workload, use the PlateSpin Forge failback feature to perform a V2P or V2V conversion. This transfers the recovery workload from the PlateSpin Forge Appliance Host to the new server.

For more information, see [“Preparing the Failback” on page 54](#).

2.1.7 Recovery Points

Recovery points are snapshots of protected workloads, providing even more protection and data integrity than synchronized workloads alone. When recovery points are enabled, a snapshot is taken during every replication. You can keep up to 32 recovery points for each workload. When the maximum is reached, the oldest point is replaced by the newest one, providing a pool of recovery opportunities.

During a Failover, Test Failover, or even a Prepare for Failover, a saved recovery point can be used to restore a failed workload. If a virus or other source corruption is replicated from the source, you can move back in time through the replications to easily find an unaffected workload. Under normal circumstances, the workload would be unrecoverable.

For more information, see [“Planning for Failure” on page 50](#).

2.1.8 Consolidated Workload Protection and Recovery

Protect data center workloads: You can recover multiple physical and virtual protected workloads by using a single PlateSpin Forge appliance. Workloads can be protected across geographically dispersed sites and then rapidly recovered after server downtime or a site disaster. With PlateSpin Forge, you can consolidate recovery platforms to protect workloads without investing in costly duplicate hardware or redundant operating system licenses. In addition to standard file-based or VSS-based replication, high-speed block-level replication options let you protect high transactional workloads, such as e-mail and database servers. Incremental transfers ensure that only changes to source data files are replicated to the PlateSpin Forge remote recovery environment, thereby minimizing WAN usage while meeting recovery point objectives (RPO) with minimal data loss.

Test the integrity of disaster recovery plans and processes: You need to ensure that recovery plans are sound before a disaster occurs, including testing them at least every six to twelve months. Test Time Objective (TTO), or the speed and ease with which a recovery plan can be tested, is emerging as a key measure of recovery effectiveness. One-click test recovery lets users test the integrity of the replication and recovery plan. To perform a test failover, PlateSpin Forge takes a snapshot of the recovery workload and powers it on within an isolated private internal network. This

lets users validate the recovery plan, and related business services, without disrupting the production workload. After validation, PlateSpin Forge drops changes that have occurred on the recovery workload snapshot during the testing process and then it resumes workload replication.

Monitor and report on workload replication and recovery functions: Forge’s Web-based interface provides a dashboard that lets you view the status of protection plans as well as manage, monitor, and report on workload protection. If there is production server downtime or a disaster, administrators are automatically alerted via e-mail. They can then take appropriate action simply by clicking a link within the notification e-mail from a PC or a mobile device. Administrators can use Forge’s reporting features to determine actual versus target recovery time, as well as visualize recovery point objectives (RTO and RPO), replication windows, and data transfer rates. Protection logs demonstrate successful replication and recovery tests, providing the audit capabilities required to meet defined service level agreements or regulatory compliance.

Recover workloads using failover and flexible restore options: PlateSpin Forge allows you to power on recovery workloads with a single click and restore to the same or different hardware. In the event of a production server outage or disaster, Administrators can recover protected workloads with a single-click failover that reconnects sessions and then allows PlateSpin Forge to take over the workload. The workload can continue to run as normal on the appliance while the production environment is restored. When the production environment is brought back online, flexible options allow for restoring workloads. If the original production server is repaired and the hardware is intact, users can move the workload from the virtual recovery environment back to the original platform by performing a virtual-to-physical (V2P) workload transfer. If the original hardware cannot be repaired, users can restore the workload with a V2P transfer to new hardware. Workloads can also be easily moved to a production virtual environment (V2V).

2.1.9 Disaster Recovery

PlateSpin Forge consists of a hypervisor Server that hosts the PlateSpin Forge virtual machine. PlateSpin Forge provides disaster recovery by replicating workloads targeted for protection, and storing a virtual machine copy. Initially, PlateSpin Forge performs a full replication of everything in the workload. Subsequent incremental replications copy to the stored virtual machine any files or blocks that have changed since the last replication. These incremental replications keep the copy synchronized with the current state of the protected workload. Users can specify how often and when to perform each type of replication.

2.1.10 Supported Transfer Methods

Forge enables you to select different methods for transferring workload data from the protected source to the Forge appliance.

For a list of workload types and conversions arranged by supported transfer mode, see [Knowledge Base Article Q20002 \(http://support.platespin.com/kb2/article.aspx?id=20002\)](http://support.platespin.com/kb2/article.aspx?id=20002).

- ◆ “File-Based” on page 20
- ◆ “VSS File-Based” on page 20
- ◆ “Block-Based” on page 20
- ◆ “VSS Block-Based” on page 21

File-Based

The File-Based Transfer method copies data and replicates changes at the file level. During File-Based Transfer, Forge transfers all files from the protected workloads while monitoring them for changes. When the transfer is complete, files that have changed during the transfer are resent. It is recommended, if present, that you stop Microsoft* SQL Server* or Microsoft Exchange Server* services.

You can configure the replication to stop these services when using the File-Based Transfer method (see “[Replication Settings](#)” on page 33). However, if there are other tools present that manage the back up of these databases, consider leaving services running during the transfer. When the transfer completes, verify that the copied database is current.

If file system changes are constant, data transfer is stopped after the tenth pass and a replication progress warning is displayed.

File-Based Transfer is appropriate for moderately active Windows-based workloads using NTFS.

VSS File-Based

This Transfer method transfers data at the file level and uses the Microsoft Volume Snapshot Service* (VSS) feature, also known as Shadow Copy, for Windows workloads (Windows 2003 SP1 and above) with applications and services that support VSS. The VSS File-Based Transfer method offers an exact point-in-time copy of the source workload.

During VSS File-Based Transfer, Forge takes a VSS snapshot of the protected workload and transfers the data file-by-file.

When the initial transfer is complete, the target is powered off. It is powered on again during the next scheduled incremental replication.

Use the VSS File-Based Transfer method to reduce service downtime during Windows workload relocations. Database servers, mail servers, and application servers that would otherwise require a temporary service stoppage can be protected by using this Transfer method. This method is also recommended for replications in networks with high latency. Because this is a point-in-time solution, data does not need to be retransmitted as it does with other methods.

WARNING: When using the file-based transfer method with VSS, encrypted files are not included in replications. Encrypted files show up as *skipped* in the job report, and the replication shows as “completed with warnings”. This is not an issue with block-based transfers.

Block-Based

The Block-Based Transfer method copies data and replicates changes at the block level instead of replicating an entire file.

During data transfer, changes on the protected volumes are monitored and continuously retransferred at the block level until full synchronization is achieved.

Because the Block-Based Transfer method transmits only changed blocks rather than entire files, it transfers significantly less data.

Use the Block-Based Transfer method when you want to reduce the service downtime during Windows workload replication. Using the Block-Based Transfer method, you can replicate critical database servers, mail servers, and application servers with large databases (more than 5 GB) and

with high disk activity. In addition, the Block-Based Transfer method is recommended for networks with high latency because the size of block-level changes is significantly smaller than an entire file (when file-level changes are detected during file-level data transfer, the changed files are transferred in their entirety).

If your protected workload is running Microsoft Exchange Server 2000 and 2003, and Microsoft SQL Server 2000, the Windows services of these applications are automatically detected. You can configure the replication to stop these services when using the Block-Based Transfer method (see [“Replication Settings” on page 33](#)). However, if there are other tools present that manage the backup of these databases, consider leaving services running during the transfer. When the transfer completes, verify that the copied database is current.

Block-Based Transfer is handled by the Block-Based Transfer Component, automatically installed on the protected workload. Because it operates in kernel mode, it requires the protected workload to reboot to initialize.

VSS Block-Based

This Transfer method transfers data at the block level and uses the Microsoft Volume Snapshot Service (VSS) feature, also known as Shadow Copy, for Windows workloads (Windows 2003 SP1 and above) with applications and services that support VSS. The VSS Block-Based Transfer method offers an exact point-in-time copy of the source workload.

During VSS Block-Based Transfer, Forge takes a VSS snapshot of the protected workloads and transfers the data block-by-block.

When the initial transfer is complete, the target is powered off. It is powered on again during the next scheduled incremental replication.

Use the VSS Block-Based Transfer method to eliminate service downtime during Windows workload relocations. Database servers, mail servers, and application servers that would otherwise require a temporary service stoppage can be protected by using this Transfer method. This method is also recommended for replications in networks with high latency. Because this is a point-in-time solution, data does not need to be retransmitted as it does with other methods.

2.1.11 Fine-Tuning Data Transfer Performance

You can fine-tune data transfer during replication for optimum performance over your network. The specifics of functionality and configuration procedures depend on the data transfer method selected for a particular job. See [“Supported Transfer Methods” on page 19](#).

- ♦ [“Fine-Tuning File-Level and VSS-Aware Block-Level Transfer Performance” on page 21](#)
- ♦ [“Fine-Tuning Block-Level Data Transfer Performance” on page 22](#)
- ♦ [“Fine-Tuning Block-Level Data Transfer Performance System-Wide” on page 23](#)
- ♦ [“Fine-Tuning Block-Level Data Transfer Performance on a Per-Workload Basis” on page 23](#)

Fine-Tuning File-Level and VSS-Aware Block-Level Transfer Performance

You can fine-tune your over-the-network data transfer for optimum performance in your specific environment. For example, you might need to control the number of your TCP connections or impose a packet-level compression threshold.

This functionality is supported for replications that use the following data transfer methods:

- ◆ File-level
- ◆ Block-level with the Microsoft Volume Shadow Copy Service (VSS) option selected

Fine-tuning is done by modifying the product's `productinternal.config` configuration file, located on your Forge host in the following directory:

```
..\PlateSpin Portability Suite Server\Web
```

Below is a list of the configuration parameters with two sets of values: the defaults and the values recommended for optimum operation in a high-latency WAN environment.

Table 2-2 Parameters for Fine-Tuning File-Level Data Transfer Performance

Parameter	Default Value	For High-Latency WANs
<code>fileTransferThreadcount</code> Controls the number of TCP connections opened for file-based data transfer.	2	4 to 6 (max)
<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. Ignored if compression is disabled. Because the compression is CPU-bound, this setting might have a performance impact during Live Transfer.	2	n/a
<code>fileTransferSendReceiveBufferSize</code> TCP/IP window size setting for file transfer connections; controls the number of bytes sent without TCP acknowledgement, in bytes. When the value is set to 0, the default TCP window size is used (8 KB). For custom sizes, specify the size in bytes. Use the following formula to determine the proper value: $((\text{LINK_SPEED (Mbps)} / 8) * \text{DELAY (sec)}) * 1024 * 1024$ For example, for a 100 Mbps link with 10 ms latency, the proper buffer size would be: $(100/8) * 0.01 * 1024 * 1024 = 131072 \text{ bytes}$	0 (8192 bytes)	max 5242880 (5 MB)

Fine-Tuning Block-Level Data Transfer Performance

You can fine-tune over-the-network block-level data transfer for optimum performance in your specific environment by implementing bandwidth throttling and compression.

This functionality is supported for replications that use the block-level data transfer method without the Microsoft Volume Shadow Copy Service (VSS) option.

The system's default settings for block-level data transfers impose no limitations on bandwidth consumption and do not compress data being transferred. Forge provides two methods for enabling bandwidth throttling and data compression:

- ♦ **System-wide:** By editing the Forge server's `web.config` file. Bandwidth throttling and data compression specified this way apply to all block-level migration jobs, including transfers of complete volume data, as well as incremental synchronizations.
- ♦ **Per-workload:** By importing a custom Windows Registration (*.reg) file into the source Windows machine's registry. This enables you to define customized bandwidth throttling and data compression settings for specific workloads to use during replications.

Both methods control bandwidth throttling and data compression on a per-volume basis. Settings specified through the Windows registry override those in the `web.config` file. Neither method requires a reboot or other intervention for the changes to take effect.

Before using either method to fine tune block-level data transfer performance, determine appropriate compression and bandwidth values that balance CPU usage and network efficiency for your particular system, network, and workload.

Fine-Tuning Block-Level Data Transfer Performance System-Wide

- 1 Make sure there are no workload replications underway.
- 2 Use a text editor to open the `web.config` file located on your Forge server host in the following directory:

```
..\PlateSpin Portability Suite Server\Web
```

- 3 Find the following lines:

```
<add key="BlockBasedTransferCompressionLevel" value="0" />  
<add key="BlockBasedTransferBandwidthThrottlingInKB" value="0" />
```

- 4 Edit the lines:

4a In the first line, change the compression level value in quotes to a number from 0-9 (with 0 for no compression and 9 for maximum compression).

4b In the second line, change the bandwidth throttling value in quotes to a number representing kilobytes per second.

For example, for a required compression level of 3 and bandwidth cap of 512 KB/sec per volume being transferred, the appropriate lines in `web.config` look like this:

```
<add key="BlockBasedTransferCompressionLevel" value="3" />  
<add key="BlockBasedTransferBandwidthThrottlingInKB" value="512" />
```

- 5 Save the `web.config` file.
- 6 For the changes to take effect, restart the following services on the Forge server, in the specified order:
 - 6a World Wide Web Publishing Service.
 - 6b Portability Suite Service.
 - 6c PlateSpin Operations Framework Controller.

Fine-Tuning Block-Level Data Transfer Performance on a Per-Workload Basis

- 1 Make sure the Block-based Transfer Component is already installed on the source machine.
- 2 Use the text below to create a Windows Registration (*.reg) file:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\PlateSpin\BlockBasedTransfer]
"CompressionLevel"=dword:00000000
"BandwidthThrottling"=dword:00000000
```

Replace the last digit of the dword value for "CompressionLevel" with a number from 0-9 (with 0 for no compression and 9 for maximum compression), and replace the dword value for "BandwidthThrottling" with a number representing bits per second (for example, 512 kilobytes per second would be 00512000).

These values override any settings made in the Forge server's `web.config` file.

- 3 Use your Windows Registry Editor to import the *.reg file into the Windows Registry.

2.1.12 Terminology

The following are key PlateSpin Forge terms.

Term	Definition
PlateSpin Forge Appliance Host	PlateSpin Forge ships with VMware ESX v3 Server, which hosts the PlateSpin Forge Management virtual machine, as well as the recovery workloads.
PlateSpin Forge Management VM	The management virtual machine containing the PlateSpin Forge software. The IP address of the virtual machine is configured during the initial step; this IP address is used when connecting to the appliance management page by means of a browser.
Workload	The operating system, application, and data stack. All the software components that are necessary for the workload to run and provide its business value.
Protected workload	The workload under protection. Any changes made to the protected workload are reflected in the recovery workload.
Recovery workload	The receiving end of a replication. The recovery workload acts as a bootable backup for the protected workload. It is a virtual machine copy that is stored on, and runs on the PlateSpin Forge appliance.
Recovery point	A point-in-time snapshot, allowing a replicated workload to be restored to a previously good state. See "Recovery Points" on page 42 for more information.
Replication	Copying a protected workload so that it can be restored (failover, failback) at a later date.
Server Sync	The incremental replication of a protected workload to an existing or imported virtual machine. Instead of transferring a source server's entire workload, only the changes are transferred to the protected workload, saving time and bandwidth.
Replication schedule	The schedule that is set up to control the replication of a workload. A replication schedule can include full and incremental replications.
Recovery Time Objective (RTO)	A measure of how long a workload can remain offline in the event of disaster. For PlateSpin Forge, this is the time required to fail over (that is, how long it takes to configure and start the recovery workload). See "RTO" on page 41 for more information.

Term	Definition
Recovery Point Objective (RPO)	A measure of how long a business can tolerate losing or not having access to data. If a business can tolerate a loss of 10 minutes of data, then its RPO is 10 minutes. If a business cannot tolerate any loss of data, then its RPO is zero. For PlateSpin Forge, this is the interval between incremental replications. See "RPO" on page 42 for more information.
Test Time Objective (TTO)	A measure of the ease with which a disaster recovery plan can be tested. It is similar to RTO, but includes the time needed for a user to test the recovery workload.

2.1.13 Events and Tasks

Events can occur during the process of protecting workloads. When an event occurs, a record is added to the event list, which is accessible from the Dashboard or through the Events report.

Tasks are related to events and require user action. An entry on the Task page shows the current state of a workload; allowable actions enable the user to choose the workload's next state. These actions vary according to the task

The following table describes key events, whether or not a task is generated, possible actions, and whether or not an e-mail notification is issued.

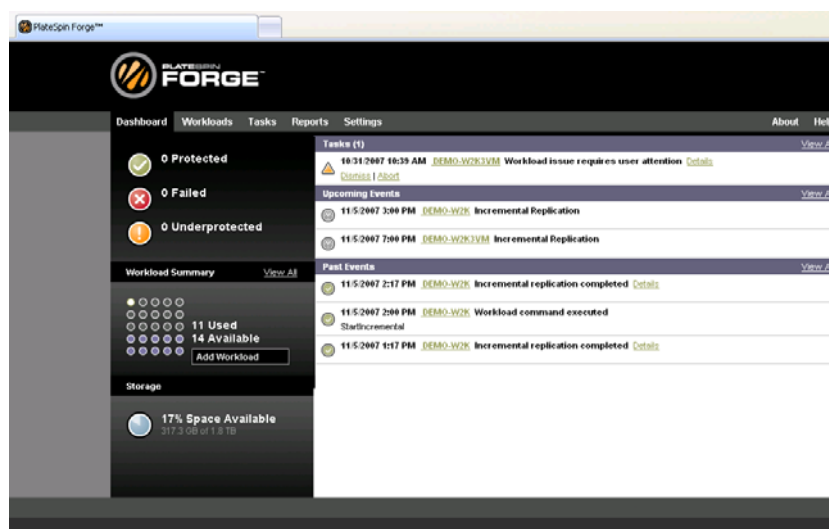
Event	Description	Task?	Action	e-mail?
Workload task requires user attention	Generated when a current operation state is changing to "require user activity." This happens during a Test Restore operation, when the recovery workload is ready for examination.	Yes	<ul style="list-style-type: none"> ◆ Dismiss ◆ Mark Test Failover as successful ◆ Mark Test Failover as failed 	Yes
Workload task resolved	Generated when a current operation state is changing from "require user activity." This happens during a Test Restore operation, after the recovery workload is shut down.	No	<ul style="list-style-type: none"> ◆ Dismiss 	No
Workload issue resolved	Generated when a current operation state is changing from "require user intervention" to "running."	No	<ul style="list-style-type: none"> ◆ Dismiss 	Yes
Workload issue requires user attention	Generated when a current operation state is changing to "require user intervention."	Yes		
Workload is offline	Generated when PlateSpin Forge detects that a workload is offline.	Yes	<ul style="list-style-type: none"> ◆ Failover ◆ Prepare for Failover ◆ Dismiss 	Yes
Workload is online	Generated when PlateSpin Forge detects that a workload is online.	No	<ul style="list-style-type: none"> ◆ Dismiss 	

Event	Description	Task?	Action	e-mail?
Incremental replication did not run at scheduled time	Generated when a scheduled incremental replication is missed because of error conditions	No		Yes
Full replication did not run at scheduled time	Generated when a scheduled full replication is missed because of error conditions	No		Yes

2.2 Web Interface

PlateSpin Forge is accessed through the appliance's Web Interface. Using a browser locally or remotely, you enter the IP address of the Forge appliance. When you are logged on, the main Dashboard page is displayed.

Figure 2-1 Main Dashboard Page



Navigation

Figure 2-2 Navigation Bar



Each PlateSpin Forge Web page contains a navigation bar that allows you to navigate the Web interface's pages, including viewing the help file and the About page.

- ◆ Section 2.2.1, “The Dashboard Page,” on page 27
- ◆ Section 2.2.2, “The Workloads Page,” on page 29
- ◆ Section 2.2.3, “Workload Commands,” on page 30
- ◆ Section 2.2.4, “Add Workload,” on page 31
- ◆ Section 2.2.5, “Remove Workload,” on page 32
- ◆ Section 2.2.6, “Workload Details,” on page 33
- ◆ Section 2.2.7, “The Tasks Page,” on page 36

- ◆ Section 2.2.8, “The Reports Page,” on page 36
- ◆ Section 2.2.9, “Workload Protection,” on page 37
- ◆ Section 2.2.10, “Replication History,” on page 37
- ◆ Section 2.2.11, “Replication Window,” on page 37
- ◆ Section 2.2.12, “Current Protection Status,” on page 38
- ◆ Section 2.2.13, “Events and Upcoming Events,” on page 38
- ◆ Section 2.2.14, “The Settings Page,” on page 38

2.2.1 The Dashboard Page

The Dashboard page is the appliance’s home page. From the Dashboard page you can see an overview of the PlateSpin Forge appliance’s workload status, activity, and availability.

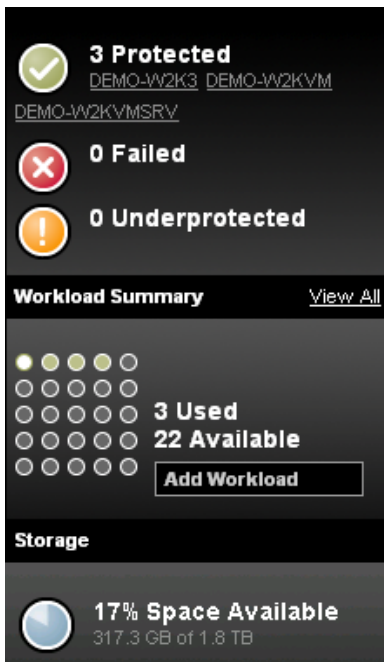
- ◆ “Workload Summary” on page 28
- ◆ “Storage” on page 28
- ◆ “Tasks and Events” on page 28

Visual Summary

The left panel displays information such as a visual workload summary of all licensed workloads and the amount of available storage on the appliance.

On the upper left, a panel displays icons representing protection states:

Figure 2-3 Left Hand Panel










The upper panel icons group the workloads into three categories: Protected, Failed and Underprotected. For definitions of these terms, see [Table 2-4 on page 29](#).

Click an icon to navigate to the Workloads page and see a list of workloads with that state of protection. Click a workload to view detailed information on the Workload Details page, or to edit the configuration for an unconfigured workload.

Workload Summary

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

Table 2-3 *Dot icon workload representation*

	<i>Unprotected</i>		<i>Underprotected</i>
	<i>Unprotected – Error</i>		<i>Failed</i>
	<i>Protected</i>		<i>Expired</i>
	<i>Unused</i>		

The icons are shown in alphabetical order according to workload name. Hover Mouse over a workload summary icon to display the workload name, or click it to display its Workload Details page. Click *View All* to display the Workloads page and see a list of all workloads along with their status and current information.

This area also includes a description of how many workload licenses have been used, and how many are available. Used and expired workload licenses are presented along the bottom of the grouping of icons, and read *Used* when you mouse over them . Click *Add Workload* to discover a new workload and add it to the PlateSpin Forge appliance.

Storage

The *Storage* area shows a graphic depicting what percentage of PlateSpin Forge disk space is available. It also displays the total storage space in terabytes.

Tasks and Events

The right side of the Dashboard shows the next *Tasks*, the most recent *Past Events*, and the next *Upcoming Events*. 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. For more information, see [“Events and Tasks” on page 25](#).

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.

2.2.2 The Workloads Page

The Workloads page displays a table with a row for each workload currently on the PlateSpin Forge appliance. Use the drop-down list to filter on all workloads, protected workloads, failed workloads, or unprotected workloads. Each row shows the workload’s name and the name of the associated Protection Tier. Click a workload name to display a Workload Details page for viewing or editing configuration relevant to the workload. See [“Workload Details” on page 33](#) for more information.

Figure 2-4 Workload details page

All Workloads		Add Workload							
Tasks	Online	Workload	Protection Tier	Schedule	Replication Status	Last Replication	Next Replication	Last Test Failover	
<input type="checkbox"/>		Yes DEMO-WORKS	Custom	Active	Idle	11/8/2007 4:26 PM	--	--	
<input type="checkbox"/>		Yes DEMO-WORKMSRV	--	--	Unprotected	--	--	--	

In addition, each row shows the schedule and workload replication status. An *Active* status in the *Schedule* column can refer to either a full or incremental replication. A *Paused* status in this column means the replication schedule is on hold and the next replication will not run. A “—” status means that the schedule has not yet been set up.

NOTE: All times, including dates and times for the last and next replication and the last test failover, are based on the time zone where the PlateSpin Forge Management VM is located. This might be different from the time zone of the protected workload or of the browser running the PlateSpin Forge Web Interface. A display of the server date and time appears at the bottom right of the PlateSpin Forge UI.

Table 2-4 Workload states

	Unprotected	An unprotected workload. The workload was added and is in the process of being protected.
	Unprotected – Error	An unprotected workload. It might not be possible to protect the workload; it might be necessary to remove the workload. One of three possible errors is preventing the workload from being protected: <ul style="list-style-type: none"> ◆ Error during discovery. For example, there is an unsupported server that cannot be inventoried. ◆ Pre-validation error. For example, a platform is unsupported. ◆ Error during Prepare Replication. For example, there is an incorrect configuration.
	Protected	The protected workload is online and there were no errors executing the most recent replication.
	Underprotected	The workload is protected, but not optimally. There might be a problem with the replication schedule, or the protected workload is offline but failed over to a recovery workload.



Failed

The protected workload is offline and the recovery workload is not in a failover state.



Expired

The workload has either failed over or it was deleted.

2.2.3 Workload Commands

At the bottom of the Workloads page are command buttons. When a workload is selected on the top part of the page, the commands available for that workload in its current state are enabled. If more than one workload is selected, only commands commonly available to the selected workloads are enabled. This allows users to select multiple workloads when the same command is to be applied to several workloads.

Figure 2-5 *Workload commands*

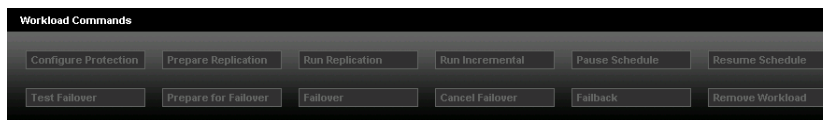


Table 2-5 *Workload commands*

Configure Protection	Displays the workload details page for editing configuration details.
Prepare Replication	When a workload is discovered, PlateSpin Forge creates the recovery workload copy of the protected workload. This command is only available after a protection schedule is assigned to the workload.
Run Replication	Copies the entire protected workload to the recovery workload stored on the PlateSpin Forge Appliance Host. Click <i>Execute</i> to run the replication immediately, or click <i>Edit</i> to adjust the workload's configuration. This command is also known as Full Replication.
Run Incremental	Copies any changes made on the workload since the last replication. Also known as Incremental Replication.
Pause Schedule	Pauses the workload's replication schedule and prevents any scheduled replications from running. This command is useful for scheduled maintenance windows when the workload is offline, but e-mail notifications and event logs are not necessary. It can also be used to reduce the load on the PlateSpin Forge Appliance during a large-scale failover.
Resume Schedule	Restarts all scheduled replications after a Pause Schedule command.
Test Failover	Starts running the recovery workload in a PlateSpin Forge virtual machine, but when the virtual machine is shut off, changes do not persist. During Test Failover, replications do not run.
Prepare for Failover	Starts running the recovery workload in a PlateSpin Forge virtual machine, but optionally maps network cards to an internal network to keep the workload isolated from the production network.

Failover	Starts running the recovery workload in a PlateSpin Forge virtual machine. The recovery workload takes over the protected workload's function on the network.
Cancel Failover	Cancels a Failover after a Prepare for Failover and returns the recovery workload to its regular replication schedule.
Failback	Initiates Failback.
Remove Workload	Undiscoveres the workload and removes it from PlateSpin Forge. This command offers the option to also remove the replicated workload (virtual machine) or to leave it on the PlateSpin Forge server.

2.2.4 Add Workload

The *Add Workload* button at the top of the Workloads page opens a Web page where you can discover a workload and add it to the list on the Workloads page. The *Add Workload* button on the Dashboard page can also be used.

Figure 2-6 Add workload

You have the option of adding a workload that uses full replication or adding an existing or imported workload and running incremental replications to save time and bandwidth. When incremental replication is selected, the *Add Workload* and *Prepare Replication* steps of the Add Workload Wizard at the top of the Add Workload page are combined so that there are only three steps to the procedure.

NOTE: Regardless of which replication type you select, the workload to be protected still needs to be discovered. The difference is that once you discover a workload with an existing/imported recovery workload on the Forge appliance, you synchronize the discovered workload to the existing/imported recovery workload.

Figure 2-7 Add workload wizard

The screenshot shows the 'Add Workload' wizard interface. At the top, there are three main steps: 'ADD WORKLOAD PREPARE REPLICATION', 'CONFIGURE PROTECTION', and 'RUN REPLICATION'. The current step is '1) Enter Workload Details', which includes fields for 'Hostname or IP', 'Domain\Username', and 'Password'. Below these fields is an 'Add' button. The next step is '2) Choose Initial Replication Method', which offers three options: 'Full Replication', 'Incremental Replication (to an existing or imported workload)', and 'DHCP Static (0.0.0.0) Configure...'. The 'Incremental Replication' option is selected, and it shows a dropdown menu with 'SDSFORGE14_VM (Windows2003)' and another dropdown for 'Workload Inventory Network' set to 'External Test Network'.

2.2.5 Remove Workload

Workloads can be removed either by selecting the workload on the Workloads page and then clicking the Remove Workload command button or by clicking the Remove Workload button at the bottom of the Protection Details page for the workload. When you remove a workload, you can choose whether or not to also remove the virtual machine for that workload from Forge. Leaving the VM behind allows you to import the VM at a later time, should you decide to re-add the workload to Forge. This would allow you to only need incremental replications to update the workload instead of having to do a full replication from scratch.

To free up the license associated with the removed workload, see [“License Designations Tab” on page 41](#). For information on importing a workload, see [“Importing a Workload into Forge” on page 56](#).

To remove a workload:

- 1 Click *Workloads* on the Forge dashboard.
The Workloads page is displayed.
- 2 Select the workload you want to remove.
- 3 (Optional) To retain the virtual machine for the workload on Forge, clear the *Delete VM* check box.
- 4 Click *Execute*.
The Workloads page is displayed, showing that the workload is being removed.

If the workload was protected using block-based tools, a few more steps are required to clean up and uninstall the block-based tools.

- 1 Click *Start > Run* on the source workload.
- 2 Type in `appwiz.cpl` and hit Enter.
The Add/Remove Programs window is displayed.
- 3 Find *SteelEye DataKeeper for Windows* in the list of programs and uninstall it.
- 4 Reboot the source workload.

2.2.6 Workload Details

The Workload Details page displays all the configuration details relevant to protecting and replicating the workload.

- ◆ [“Tier Settings” on page 33](#)
- ◆ [“Replication Settings” on page 33](#)
- ◆ [“Failover Settings” on page 34](#)
- ◆ [“Prepare for Failover Settings” on page 34](#)
- ◆ [“Test Failover Settings” on page 35](#)
- ◆ [“Recovery Points” on page 35](#)
- ◆ [“Workload Details” on page 35](#)
- ◆ [“Workload Commands” on page 35](#)

Tier Settings

These settings define when and how often a workload’s replications occur. You can select one of the built-in Protection Tiers or one that you have previously created from the Protection Tier drop-down list. You can also select *Custom*, which allows you to customize the settings just for this workload. Custom settings are not accessible by other workloads and it is recommended that you create the Protection Tier beforehand to save time and effort. See [“Protection Tiers” on page 16](#) and [“Creating a Protection Tier” on page 46](#) for more information.

Figure 2-8 Tier settings

Tier Settings	
Protection Tier:	Nightly
Workload Failure:	5 failed detection attempts
Workload Detection Every:	60 seconds
Incremental Recurrence:	Every day at 9:00 PM Configure...
Full Recurrence:	No recurrences defined Configure...
Recovery Points To Keep:	7

Replication Settings

These settings define how the replication occurs. They provide any necessary network specifications and credentials so the replication can run unattended. These settings also allow you to specify which volumes to replicate and which services to stop on the protected workloads during replication. For more information on transfer methods, see [“Supported Transfer Methods” on page 19](#).

Figure 2-9 Replication settings

Replication Settings

Transfer Method: File Based
 Snapshot (using Volume Shadow Copy Service)
 Block Based
 Install Block Based tools during: Prepare Replication First Replication

Source Credentials: User Name: demo\administrator
 Password: [REDACTED]
[Test Credentials](#)
 Credentials have not been tested...

Replication Network: External Test Network
 DHCP Static (0.0.0.0) Configure...

Volume	Used Space	Total Size	Map To
C: (NTFS - System)	139.2 GB	195.3 GB	(Don't sync)
D: (NTFS - Boot)	31.4 GB	37.5 GB	C: (NTFS - System)

Services to Stop During Replication:

Service Name
MSSQLRECON
MSSQLSERVER

[Delete](#) [Delete](#) [Add Service](#)

Failover Settings

These settings are used when the recovery workload is brought online to replace a failed protected workload. For more information on failovers, see [“Failover” on page 16](#).

Figure 2-10 Failover settings

Failover Settings

VM Memory: 1.64 GB

Hostname: demosvr

Domain / Workgroup: Workgroup WORKGROUP
 Domain

Domain Credentials: Username: [REDACTED]
 Password: [REDACTED]
 Confirm Password: [REDACTED]

Guest NIC 1: Production Network
 DHCP Static (0.0.0.0) Configure...

Guest NIC 2: Production Network
 DHCP Static (192.168.43.1) Configure...

Target Services: [Add Service](#)

Prepare for Failover Settings

This setting allows you to define which network to use for the Prepare for Failover commands. During Prepare for Failover, the recovery workload runs with its network cards mapped to this network.

Figure 2-11 Prepare for failover settings

Prepare For Failover Settings

Temporary Failover Network: Internal Test Network

Test Failover Settings

These settings are used when the recovery workload is brought online as a test. These settings are similar to the Failover settings.

Figure 2-12 Test failover settings

Test Failover Settings	
Hostname:	demosvr2
Domain / Workgroup:	<input checked="" type="radio"/> Workgroup WORKGROUP <input type="radio"/> Domain
Domain Credentials:	Username: Password: Confirm Password:
Guest NIC 1	Internal Test Network <input checked="" type="radio"/> DHCP <input type="radio"/> Static (0.0.0.0) Configure...
Guest NIC 2	Internal Test Network <input checked="" type="radio"/> DHCP <input type="radio"/> Static (192.168.43.1) Configure...
Target Services:	Add Service

Recovery Points

These settings show the recovery points that currently exist for the protected workload, including when they were created.

Figure 2-13 Recovery points

Recovery Points	
Recovery Points:	
Name	Created
PlateSpin Forge Recovery Point:1344395c-6d26-417a-9e70-87899adca6b0	8/13/2008 8:17 PM
PlateSpin Forge Recovery Point:178a17e2-4eab-4801-bd17-a6c92492dc3c	8/13/2008 7:15 PM
PlateSpin Forge Recovery Point:ad09bf25-76ce-4463-bac3-50aebf1717e0	8/13/2008 6:17 PM
PlateSpin Forge Recovery Point:8d3169e3-2390-47b0-a764-a682b21c16d3	8/13/2008 5:13 PM
PlateSpin Forge Recovery Point:815f9950-449a-46c4-99fe-d9dad155b20e	8/13/2008 4:52 PM

Workload Details

This section shows the operating system and hostname of the protected workload.

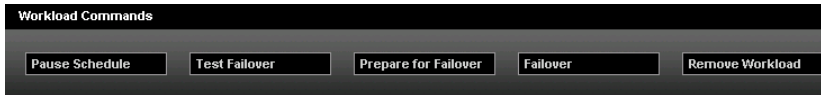
Figure 2-14 Workload details

Workload Details	
Operating System:	Windows2003
Hostname:	SDSFORGE34

Workload Commands

At the bottom of the Workload Details page is a limited list of workload commands. For an explanation of each command, see [“Workload Commands” on page 30](#).

Figure 2-15 Limited set of workload commands



2.2.7 The Tasks Page

The Tasks page lists individual tasks, each with the following commands representing allowable actions:

Table 2-6 Allowable actions

Command	Description
Remove Workload	Removes the workload's inventory information from PlateSpin Forge.
Do Full	Does a full replication of the workload.
Dismiss	Deletes the task from the task list without performing any action.
Mark Test Success	Labels the Test Failover as a success. The system logs an event that can be retrieved as part of an Events Report.
Mark Test Failure	Labels the Test Failover as unsuccessful. The system logs an event that can be retrieved as part of an Events Report.
Prepare for Failover	Starts running the workload's virtual machine copy on PlateSpin Forge, but maps network cards to an internal network.
Failover	Starts running the recovery workload on the PlateSpin Forge Appliance Host.
Retry	Retries the workload's failed discovery or replication.
Abort	Cancels the task in progress.

For more information, see [“Events and Tasks” on page 25](#).

2.2.8 The Reports Page

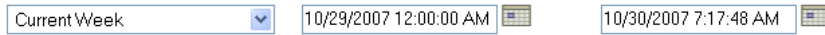
PlateSpin Forge includes reports that provide information about workload protection and events. These enable users to gain a clear picture into resources being used, save costs by identifying unnecessary data replication, and demonstrate policy compliance.

Click *Reports* on the navigation bar to display a list of available reports. Click a link to display a particular report page.

To toggle the sort order of column information in a report, click the column header. Reports containing a large amount of information can span multiple pages.

Click *Printable View* to display a print-friendly page. Click *Export to XML* to display an XML page. Alternatively, right-click *Export to XML*, then click *Save Link As* or *Save Target As* (depending on the browser) to save the report as an XML file.

Figure 2-16 Report filters



Except for *Current Protection Status*, report pages include date/time and report-specific filters to assist with refining the information displayed. The first box has a drop-down list of time range filters, including current and last day, week, and year filters, as well as a custom filter. The second and third boxes display the start and end date/times of the selected filter. For a custom time range, specify the start and end date/times of the desired period in these boxes, or select from the pop-up calendars.

Use report-specific filters to further refine the information. Click the adjacent button to display a list box of criteria. Use check boxes to select items individually, or use *Select/Deselect All*, then click *Apply*. At least one item must be selected when you click *Apply*, or the filter defaults to the previously selected items. These filters are detailed in subsequent report topics.

2.2.9 Workload Protection

Workload Protection reports show how well workloads are protected over time by displaying all events that have happened to a particular workload, when they occurred, the user who initiated the event, the Job ID of the job that triggered the event, and any details associated with the event.

In addition to date/time filters, Workload Protection reports feature these filters:

- ♦ **Workloads:** Click *Select All* or *Deselect All*, or use the check boxes to select the particular workloads to include in the report. Click *Apply*.
- ♦ **Protections Tiers:** Click *Select All* or *Deselect All*, or use the check boxes to select the particular protection tiers to include in the report. Click *Apply*.

2.2.10 Replication History

Replication History reports show a record of all protection events that have occurred for a particular workload. Protection events include:

- ♦ Incremental replication completed
- ♦ Incremental replication did not run at scheduled time
- ♦ Incremental replication failed
- ♦ Full replication completed
- ♦ Full replication did not run at scheduled time
- ♦ Full replication failed

The columns for Replication History reports are the same as those for Event reports (for more information, see “[Events and Upcoming Events](#)” on page 38). Use the drop-down list box to select the workload on which to report.

2.2.11 Replication Window

Replication Window reports show how much data PlateSpin Forge is transferring over the network and how long replications take.

For each workload, the report displays the size, speed, and amount of time taken for a Full and an Incremental transfer. The time shown is the amount of time that PlateSpin Forge takes to do the actual copying of the workload from the protected workload to the recovery workload and does not include preparatory steps taken by PlateSpin Forge prior to this transfer.

Use the drop-down box to select the most recent full and incremental replications, the sum of all replications within the specified time period, the peak value for each column in the chart within the specified time period, or the average value for each column in the chart within the specified time period.

2.2.12 Current Protection Status

Current Protection Status reports show how well workloads are protected. For each workload, the report shows the following values:

- ♦ **Target Recovery Point Objective (RPO):** The largest amount of time during which changes to a workload are not protected. This is the longest interval between replications because any changes since the last replication are not protected in case of failure.
- ♦ **Actual RPO:** The amount of time that has elapsed since the last full or incremental replication.
- ♦ **Actual Recovery Time Objective (RTO):** The amount of time it takes from the time the user initiates a test failover until the recovery workload is up and running, ready to be tested.
- ♦ **Actual Test Time Objective (TTO):** The time it takes to test the recovery workload, from the time the user initiates a test failover until after testing is complete and the recovery workload is powered off.
- ♦ **Last Test Restore:** The date and time of the last test restore performed on the workload.
- ♦ **Last Replication:** The date and time of the most recent full or incremental replication performed on the workload.

2.2.13 Events and Upcoming Events

Events reports show a historical record of everything that has occurred on the PlateSpin Forge appliance. Upcoming Events reports show events that are scheduled to occur in the future.

As with Workload Protection reports, Events and Upcoming Events reports allow filtering on workloads and Protection Tiers. In addition, Events reports allow filtering on event types. Click *Select All* or *Deselect All*, or use the check boxes to select which particular event types to include in the report. Use the scroll bar to view all the choices. Click *Apply*.

Events reports show each event that occurred (except for System events), the workload with which it is associated, and the protection tier to which it belongs. The report also shows the user who caused the event, as well as the date and time at which the event occurred. The *Details* column shows a message about a user-initiated event, an error message associated with a failed job, or information about a system event. The *Jobs* column contains a link to a job report associated with the event, if one is available.

2.2.14 The Settings Page

Click the *Settings* link in the navigation bar to configure the various settings.

Figure 2-17 Settings page

Protection Tiers					
Protection Tiers					
Name	Incremental Recurrence	Full Recurrence	Recovery Points To Keep	Workload Failure	Workload Detection
Hourly	Every hour	No recurrences defined	12	3 attempts	Every 20 seconds
Nightly	Every day at 9:00 PM	No recurrences defined	7	5 attempts	Every 60 seconds
Weekly	Friday every week at 10:00 PM	No recurrences defined	4	5 attempts	Every 60 seconds

- ◆ “Protection Tiers Tab” on page 39
- ◆ “Permissions Tab” on page 39
- ◆ “Appliance Host Tab” on page 39
- ◆ “Email Tab” on page 40
- ◆ “SMTP Tab” on page 40
- ◆ “License Tab” on page 40
- ◆ “License Designations Tab” on page 41
- ◆ “Events Tab” on page 41

Protection Tiers Tab

This is where you create custom protection tiers that can be used when configuring a workload’s replication details. For more information, see “Protection Tiers” on page 16, “Workload Details” on page 33 and “Tier Settings” on page 33.

Permissions Tab

This is where you manage role-based access in Forge, creating security groups, assigning workloads to those groups and then using one of the three types of roles (Administrator, Power User or Operator) to determine who can do what. See “Role-Based Access” on page 15 and “Managing Role-Based Access” on page 43 for more information.

Appliance Host Tab

This is where you enter credentials for the host running PlateSpin Forge, if the credentials have been changed since the initial configuration. Click *Save*.

Figure 2-18 Appliance host tab

Dashboard Workloads Tasks Reports Settings About Help

Protection Tiers Appliance Host Email SMTP License Events

Appliance Host Settings Refresh Host Save

Address: 10.99.122.130

Username:

Password:

When changing host credentials please note that any jobs running at the time will go into recoverable error and must be aborted.

For PlateSpin Forge™ Management VM Settings, please click [here](#) (requires Internet Explorer).

Refresh Host: The Application Host is refreshed every time a replication runs. If you don’t want to wait, you can click *Refresh Host* to force an immediate refresh.

Windows Administration Web UI: At the bottom of the Application Host page is a hyperlink that allows you to access the Windows Administration Web UI so you can perform administrative functions, such as adding users.

Email Tab

Select *Enable email notifications* to receive e-mail notification of important Protection Events related to protected workloads. See “[Events and Tasks](#)” on page 25 for a list of which events trigger e-mail notification.

Click *Add email addresses* to specify addresses to which to send the notifications. In the text box, type an e-mail address or multiple addresses separated by commas and click *Add*. To delete listed addresses, click *Delete* adjacent to the address to be removed.

SMTP Tab

The SMTP (Simple Mail Transfer Protocol) server is used to deliver e-mail notifications to administrators. Specify an SMTP server address, port, and reply address (to e-mail event and progress notifications. Specify valid e-mail account credentials. Click *Save Changes*.

License Tab

PlateSpin Forge includes a predefined number of workload licenses. Each workload license can be used to protect, fail over, and fail back one workload. When all workload licenses are used, no more workloads can be protected.

If a protected workload is on a machine that you plan to decommission, you can use the [PlateSpin License Entitlement Manager \(http://www.platespin.com/entitlementmgr/\)](#) to recover the used workload license and apply it to the replacement machine.

For more information about resetting workloads, see this PlateSpin Knowledge Base [article \(http://support.platespin.com/kb2/article.aspx?id=20876\)](#).

The License Settings page displays a list of all available licenses with associated information including what module is licensed, the license’s expiry date, and entitlements. To delete a license, click *Delete* adjacent to the license to be removed.

WARNING: Do not delete licenses unless instructed to do so by PlateSpin Customer Support.

To add a license, click *Add New License* and select one of the following activation methods:

- ◆ Online Activation
- ◆ Offline Activation

For either activation method, the e-mail address required is the address originally used to place your PlateSpin order. The user name, password, and activation code are provided by PlateSpin in response to the order.

For more information, see “[License Activation](#)” in the *PlateSpin Forge 2.5 Getting Started Guide*.

License Designations Tab

When workloads are removed from Forge, the licenses associated with them are not automatically released or transferred to the available license pool. This tab allows you to transfer freed up licenses back to the license pool so they are available for use with other workloads.

After a workload has been removed from Forge, the associated license is available for transfer. On the License Designation tab, licenses with the *Transfer License* hyperlink beside them are available for transfer back to the license pool.

- 1 On the License Designations tab, click *Transfer License* next to the license you want to transfer back to the license pool.
- 2 Follow the on screen instructions to transfer the license.

Events Tab

Type a date (*mm/dd/yyyy*), or click the calendar icon and select a date, to delete all events before that date. This is used to reduce the size of the database.

WARNING: This command cannot be undone.

2.3 Product Expectations

- ♦ [Section 2.3.1, “RTO,” on page 41](#)
- ♦ [Section 2.3.2, “RPO,” on page 42](#)
- ♦ [Section 2.3.3, “Failover,” on page 42](#)
- ♦ [Section 2.3.4, “Recovery Points,” on page 42](#)

2.3.1 RTO

RTO (Recovery Time Objective) is the time it takes to failover a workload in Forge and typically occurs in 10 to 30 minutes. This duration includes:

- ♦ booting up the workload
- ♦ configuring the failover

The boot up time is typically affected by the number of services running on the workload. The more services that need initialization, the longer it takes the workload to completely boot up. Certain failover configurations (e.g. joining the domain) may also require extra reboots.

Forge use also plays a factor in the RTO. The more operations (i.e. replications or other failovers) running on Forge, the longer it takes to failover the workload. To get an average failover time for workloads in your environment, perform test failovers at various times and run the Forge reports.

NOTE: Domain controllers typically take longer to failover as they require more configuration and reboots. The duration may be as much as double the time it takes to perform a typical failover.

2.3.2 RPO

RPO (Recovery Point Objective) is the time between incremental replications. The minimum achievable RPO depends on the current utilization of Forge, the number and scope of changes on the workload and the network speed. Typically, the overhead time for a replication is between 10 and 20 minutes, depending on how many other operations are currently running on Forge. Therefore, the time it takes to complete a replication is 10 to 20 minutes plus the amount of time it takes to transfer the changes.

2.3.3 Failover

At the time of a disaster, if a single workload has to be failed over, typically there will be enough resources (memory and CPU) on Forge to allow it to perform as well as the production workload. In the case where multiple workloads have to be failed over concurrently, the resources will have to be shared among these workloads and the performance may not be on par with production workloads. This should be taken into consideration when designing the disaster recovery plan. You may run through different scenarios using the test failover functionality to be better prepared for such scenarios.

NOTE: You may suspend other operations, such as replications, to free up additional resources, as required. You can also adjust the amount of memory assigned to each workload in the failover settings.

2.3.4 Recovery Points

By enabling recovery points, Forge keeps track of changes between replications for the applicable workloads. In order to store this information, each recovery point requires extra disk space on Forge. The amount of required disk space is directly tied to the amount of changes on the workload. The more changes, the more disk space that is required. This should be taken into consideration when choosing the number of recovery points. You may consult the Forge reports to estimate the average amount of change for each workload.

This section includes information on how to use the Forge hardware appliance.

- ◆ [Section 3.1, “Managing Role-Based Access,” on page 43](#)
- ◆ [Section 3.2, “Protecting a Workload,” on page 46](#)
- ◆ [Section 3.3, “Planning for Failure,” on page 50](#)
- ◆ [Section 3.4, “Failback,” on page 54](#)
- ◆ [Section 3.5, “Importing a Workload into Forge,” on page 56](#)
- ◆ [Section 3.6, “Adding a SAN LUN to Forge,” on page 57](#)
- ◆ [Section 3.7, “Running Diagnostics,” on page 58](#)

3.1 Managing Role-Based Access

This section explains how to set up and use role-based access in Forge.

For more information see [Section 2.1.1, “Role-Based Access,” on page 15](#).

- ◆ [Section 3.1.1, “Creating Host Appliance Users,” on page 43](#)
- ◆ [Section 3.1.2, “Creating Security Groups,” on page 44](#)
- ◆ [Section 3.1.3, “Editing Security Groups,” on page 44](#)
- ◆ [Section 3.1.4, “Deleting Security Groups,” on page 45](#)
- ◆ [Section 3.1.5, “Removing Users from Security Groups,” on page 45](#)
- ◆ [Section 3.1.6, “Removing Workloads from Security Groups,” on page 45](#)

3.1.1 Creating Host Appliance Users

Before users can be added to security groups in Forge, you need to add them to the Host Appliance.

To add a user to the Host Appliance:

- 1 Log in to the Host Appliance either by using Remote Desktop or through the VMware Infrastructure Client (VIC).
- 2 Right-click on the My Computer icon and click *Manage*. If the My Computer icon is not displayed on the Host Appliance desktop, click *Start > Run*, type `compmgmt.msc` and hit Enter.
- 3 Expand *Local Users and Groups* in the left pane. You may need to expand *System Tools* first if you don't see *Local Users and Groups*.
- 4 Select *Users* and click *Action > New User*.
- 5 Enter desired informaton in the New User dialog and click *Create*.
- 6 Double-click the user name you just created.
- 7 Click the Member Of tab and click *Add*.
- 8 Type in the name of the group exactly to which you want to add the user and hit Enter.

There are three available group names: Workload Protection Administrators, Workload Protection Operators and Workload Protection Power Users. For more information on the rights for each group, see [Table 2-1 on page 16](#).

9 Click *OK*.

3.1.2 Creating Security Groups

Only Administrators can access the Forge Settings page and manage security groups. If no users or groups exist yet, then this is the default Forge Administrator.

To create a security group in Forge:

1 Log in to Forge as an administrator.

2 Click the Settings tab and then click *Permissions*.

The Security Groups page is displayed. Notice there is a default, undeletable security group called All Workloads. This group is used to set up appliance-wide permissions for users.

3 Click *Create Security Group*.

4 Change the supplied group name if desired. Notice that all administrators are automatically added to the group.

5 To add non-administrator users (power users or operators), click *Add Users*.

For information on creating users, see [“Creating Host Appliance Users” on page 43](#).

6 Select the *Grant* check box beside the users you want added to the new security group.

NOTE: Non-administrator users who are not granted access here are the only users who won't have access to the workloads in this security group.

7 Click *OK*.

8 To add workloads to the new group, click *Add Workloads*.

9 Select the *Grant* check box beside the workloads you want added to the new security group.

Notice that workloads already assigned to a security group do not have a check box to select beside them and show the name of the security group they are assigned to in the Security Group column. Workloads that can be selected display a check box and say Unassigned under the Security Group column.

NOTE: Workloads can belong to only one Security Group at a time.

10 Click *OK*.

11 Click *Create* to create the security group with your configurations.

3.1.3 Editing Security Groups

After a Security Group is set up, you can go in and change which users or workloads are a part of that Security Group or change the Security Group name.

To edit a Security Group:

1 Log in to Forge as an administrator.

2 Click the Settings tab and then click *Permissions*.

The Security Groups page is displayed.

- 3 Click the name of the Security Group you want to edit.
- 4 Make any changes desired and click *Save*.

3.1.4 Deleting Security Groups

Deleting Security Groups has no affect on the users and workloads in those Security Groups, except to change user access.

To delete a Security Group:

- 1 Log in to Forge as an administrator.
- 2 Click the Settings tab and then click *Permissions*.
The Security Groups page is displayed.
- 3 Click *Delete* beside the Security Group you want to delete. Notice that the All Workloads default Security Group has no *Delete* hyperlink beside it and cannot be deleted.
- 4 Click *OK*.

3.1.5 Removing Users from Security Groups

If you delete a user from the Application Host, you still need to remove the user from the Security Group, though when you view the Security Group after deleting the user from the Application Host, they are displayed with a line through their name.

The exception is for Administrators, either Local Administrators or members of the Workload Protection Administrators group, in which case deleting them from the Application Host also removes them from the Security Group. In fact, this is the only way to remove any type of administrator from a Security Group.

To remove a user from a Security Group:

- 1 Log in to Forge as an administrator.
- 2 Click the Settings tab and then click *Permissions*.
The Security Groups page is displayed.
- 3 Click the name of the Security Group from which you want to remove a user.
- 4 The *Remove* hyperlink is displayed next to any users capable of being removed. Click *Remove* to remove that user.
- 5 Click *Save*.

3.1.6 Removing Workloads from Security Groups

If you remove a workload from Forge, it is also removed from any Security Group to which it belongs. No further steps are required. If you want to remove a workload from a Security Group but keep the workload in Forge and protected, you can do so on the Security Groups page.

To remove a workload from a Security Group:

- 1 Log in to Forge as an administrator.

- 2 Click the Settings tab and then click *Permissions*.
The Security Groups page is displayed.
- 3 Click the name of the Security Group from which you want to remove a workload.
- 4 Click *Remove* next to any workload you want to remove.
- 5 Click *Save*.

3.2 Protecting a Workload

This section explains how to typically protect workloads.

- ♦ [Section 3.2.1, “Creating a Protection Tier,” on page 46](#)
- ♦ [Section 3.2.2, “Network Communication Prerequisites for Discovery,” on page 47](#)
- ♦ [Section 3.2.3, “Adding a Workload,” on page 49](#)
- ♦ [Section 3.2.4, “Configuring Protection and Preparing Replication,” on page 49](#)
- ♦ [Section 3.2.5, “Running Replication,” on page 50](#)

3.2.1 Creating a Protection Tier

If you are going to use one of the built-in Protection Tiers, or if you have created the necessary Protection Tier in the past, this step can be skipped. Protection Tiers determine when and how often a protected workload’s replication runs.

To create a Protection tier:

- 1 On the Settings page, click *Create Protection Tier*.
The Create Protection Tier page is displayed.
- 2 In the *Name* field, type the name you want to use for the tier .
- 3 In the *Workload Failure* field, specify the number of times Forge should try to detect the workload before giving up .
- 4 In the *Workload Detection Every* field, specify the time intervals (in seconds) that Forge should use between detection attempts.

For example, entering 60 means Forge attempts every 60 seconds to detect if the workload has gone offline . The value in the *Workload Failure* field indicates how many missed Workload Detection attempts occur before Forge sends out a Workload Offline notification.
- 5 In the *Recovery Points To Keep* field, specify the number of recovery points to keep for workloads that use this Protection Tier.

Entering 0 disables this feature. There is a limit of 32 recovery points that can be kept, but if there are many protected workloads on the Forge appliance and they are all keeping the maximum number of recovery points, storage space can become an issue.

Reducing the *Recovery Points to Keep* value when there are multiple existing recovery points already stored can result in a lengthy merge procedure.
- 6 In the *Incremental Recurrence* section, specify how often you want to run an incremental replication.

Specify the date to start using the incremental recurrence, as well as the incremental recurrence pattern. You can type directly in the *Start of recurrence* field, or click the calendar icon to graphically select a date. You can also select None as the Recurrence Pattern to never use incremental replication.

Depending on which recurrence pattern you select, different accompanying fields are displayed.

7 Specify how often you want to run a full replication in the *Full Recurrence* section.

Specify the date to start using the full recurrence, as well as the full recurrence pattern. You can type directly in the *Start of recurrence* field, or click the calendar icon to graphically select a date. You can also select None as the Recurrence Pattern to never use full replication.

Depending on which recurrence pattern you select, different accompanying fields are displayed.

8 Click *Save*.

The Protection Tier list is displayed again, now showing your new Protection Tier in the list.

To edit an existing Protection Tier, click its name in the list. To delete an existing Protection Tier, click *delete* next to the Protection Tier you want to delete. If a Protection Tier assigned to a protected workload is deleted, the settings are retained in the workload, but the Protection Tier is set to *Custom*. The built-in Protection Tiers (Hourly, Nightly, and Weekly) can neither be edited nor deleted.

If a workload's incremental and full recurrences coincide, the full recurrence takes precedence.

For more information on Protection Tiers, see [“Protection Tiers” on page 16](#).

3.2.2 Network Communication Prerequisites for Discovery

The following are software, network, and firewall requirements that systems in your environment must meet for the discovery process. For a full list of required ports, see [Table 7-1 on page 75](#).

Table 3-1 Network Communication Prerequisites for Discovery Operations

System	Prerequisites
Microsoft* Windows* Server 2008 and Windows Vista* sources	<ol style="list-style-type: none"> 1. Built-in Administrator or domain admin account credentials (mere membership in the local Administrators group is insufficient). On Vista, the account must be enabled (it is disabled by default). 2. The Remote Registry service enabled (disabled on Vista by default). 3. Firewall configured with these Inbound Rules enabled and set to Allow: <ul style="list-style-type: none"> ◆ File and Printer Sharing (Echo Request - ICMPv4In) ◆ File and Printer Sharing (Echo Request - ICMPv6In) ◆ File and Printer Sharing (NB-Datagram-In) ◆ File and Printer Sharing (NB-Name-In) ◆ File and Printer Sharing (NB-Session-In) ◆ File and Printer Sharing (SMB-In) ◆ File and Printer Sharing (Spooler Service - RPC) ◆ File and Printer Sharing (Spooler Service - RPC-EPMAP)
All supported Windows sources prior to Windows Server 2008 and Windows Vista	<ul style="list-style-type: none"> ◆ Windows Management Instrumentation (WMI) installed ◆ Open ports 135/445 (TCP) for DCOM/RPC <p>Windows NT* Server does not include WMI as part of the default installation. Obtain the WMI Core from the Microsoft Web site. If WMI is not installed, discovery of the workload fails.</p> <p>WMI (RPC/DCOM) can use TCP ports 135 and 445 as well as random or dynamically assigned ports above 1024. If problems occur during the discovery process, consider temporarily placing the workload in a DMZ or temporarily opening the firewalled ports for the discovery process only.</p> <p>For additional information, such as guidance in limiting the port range for DCOM and RPC, see the following Microsoft technical articles.</p> <ul style="list-style-type: none"> ◆ Using DCOM with Firewalls (http://msdn.microsoft.com/en-us/library/ms809327.aspx) ◆ Configuring RPC dynamic port allocation to work with firewalls (http://support.microsoft.com/default.aspx?scid=kb;en-us;154596) ◆ Configuring DCOM to work over a NAT-based firewall (http://support.microsoft.com/kb/248809)

3.2.3 Adding a Workload

Before a workload can have protection applied to it, PlateSpin Forge needs to add or discover it by using details you enter.

- 1 Click *Add Workload* on the Dashboard page or on the Workloads page.
The Add Workload page is displayed.
- 2 In the *Hostname or IP* field, specify the IP address or hostname of the workload to be protected .
- 3 In the *Domain\Username* and *Password* fields, specify the credentials for the workload.
The username must have Administrative privileges on the workload being added.
- 4 Select a replication method.
 - ♦ Select *Full Replication* and click *Add* for workloads that will use a full replication to Forge.
 - ♦ Select *Incremental Replication* to add a workload that already exists on Forge (for example, a contract that needs to be re-established after a failover) or that has been previously imported to Forge. Select the existing/imported workload from the drop-down list and select the desired network options. Click *Add*.

PlateSpin Forge attempts to discover the workload using the details you entered.

The Block-level transfer method is not supported for incremental workload synchronizations.

For more information on adding a workload imported to Forge, see [Section 3.5, “Importing a Workload into Forge,” on page 56](#).

When the workload is added (discovery is successful), it appears in the Workload list on the Workloads page with a Replication Status of *Unprotected*.

3.2.4 Configuring Protection and Preparing Replication

When a workload has been added to PlateSpin Forge, it needs to have its protection configured before any replications can be run.

- 1 On the Workloads page, click the name of the workload for which you want to configure protection.
The Workload Details page is displayed.
- 2 Select a Protection Tier from the *Protection Tier* drop-down box.
The parameters in the Protection Tier section are set to the values in the selected Protection Tier and are read-only. You can also select *Custom* as the Protection Tier so all the fields are editable.
- 3 Select a transfer method.
For more information on transfer methods, see [“Supported Transfer Methods” on page 19](#).
- 4 Select a Recovery Point Datastore. This is the location where the recovery point file will be stored.
- 5 Deselect any detected volumes that you do not want protected.
- 6 Specify any services you want stopped during replication.

- 7 In the *VM Memory* field, set the recovery workload memory allocation . The default value is the size of the protected workload memory size.
- 8 Specify the hostname and domain/workgroup and any necessary credentials. The default values are those set in the protected workload.
- 9 In the *Guest NIC* section, specify the network to use for the recovery workload during failover .
- 10 If desired, change the run state of any Windows services in the *Target Services* section.
- 11 Select the network the recovery workload should use by clicking the *Temporary Failover Network* drop-down.
- 12 Click *Save & Prepare*.
- 13 Click *Execute*.

When the workload is prepared (the recovery workload virtual machine is created and ready to receive data), its entry in the Workload list on the Workloads page displays a Replication Status of *Replication Prepared*.

3.2.5 Running Replication

Before a workload is protected, a replication needs to be run so the replication workload is synchronized with it.

- 1 On the Workloads page, select the check box next to the workload you want to replicate.
- 2 Click *Run Replication* in the Workload Commands panel.
- 3 Click *Execute*.

The workload is transferred to Forge and incremental updates automatically occur, based on the created Protection Tier.

If Block-level is being used as the transfer method, the protected workload reboots.

3.3 Planning for Failure

After workloads are properly protected, it is necessary to periodically test the protection and be ready for catastrophic system failure. The following tasks show how to be ready and respond.

- ♦ [Section 3.3.1, “Workload Testing,” on page 50](#)
- ♦ [Section 3.3.2, “Preparing for Failover,” on page 51](#)
- ♦ [Section 3.3.3, “Running a Prepared Failover,” on page 52](#)
- ♦ [Section 3.3.4, “Running an Unprepared Failover,” on page 53](#)
- ♦ [Section 3.3.5, “Removing a Snapshot After Failover \(Optional\),” on page 53](#)

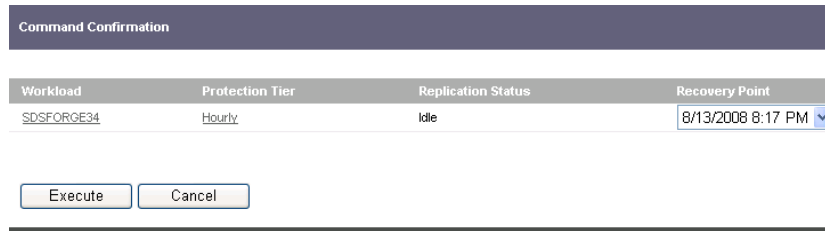
3.3.1 Workload Testing

Use Test Failover to confirm the integrity of a replicated workload. Typical Test Failovers take only an hour.

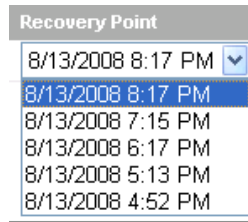
- 1 Click *Workloads* on the toolbar to navigate to the Workloads page.
- 2 Select the check box next to the workload you want to test.
Workload Commands are activated.

3 Click *Test Failover*.

The Command Confirmation page is displayed.



4 Select a *Recovery Point* to use for the test, if desired.



5 To run the Test Failover immediately, click *Execute*. To continue, see [Step 6](#). To cancel the Test Failover, click *Cancel*.

or

To view and optionally change any workload settings before running the Test Failover, click the workload name. Click *Test Failover* at the bottom of the Web page to restart the Test Failover, then click *Execute*.

- 6** Navigate to the Workloads page. When the workload's *Replication Status* changes to *Live*, the virtual machine is running.
- 7** Log in to the virtual machine by using Remote Desktop Connection or the VMware Virtual Infrastructure Client.
- 8** Inspect the virtual machine to verify that the recovery workload is functioning properly.
- 9** Shut down the virtual machine.
- 10** Navigate to the *Dashboard*. Select *Mark Test as Success* or *Mark Test as Failure* for the workload.

NOTE: PlateSpin Forge logs the success or failure of the test failover as an event. This event can later be retrieved as part of an Events report.

3.3.2 Preparing for Failover

When a protected workload fails, Preparing for Failover protects your workload, but gives you time to determine if the problem is trivial.

- 1** Click *Workloads* on the toolbar to navigate to the Workloads page.
- 2** Select the workload that requires a Failover.
- 3** Select *Prepare for Failover*.

The Command Confirmation page is displayed.

Workload	Protection Tier	Replication Status	Recovery Point
SDSFORGE34	Hourly	Idle	8/13/2008 8:17 PM

Execute Cancel

- 4 Select a *Recovery Point* to use for the test, if desired.

Recovery Point

8/13/2008 8:17 PM

8/13/2008 7:15 PM

8/13/2008 6:17 PM

8/13/2008 5:13 PM

8/13/2008 4:52 PM

- 5 To run the Prepare for Failover immediately, click *Execute*. To continue, see [Step 6](#). To cancel the Failover, click *Cancel*.

or

To view and optionally change any workload settings before running Prepare for Failover, click the workload name. Click *Test Failover* at the bottom of the Web page to restart the Test Failover, then click *Execute*.

- 6 Navigate to the Workloads page. The workload *Replication Status* changes to *Preparing Failover*.
- 7 When the recovery workload is running and ready to be joined to the main network, its *Replication Status* changes to *Failover Prepared*.

3.3.3 Running a Prepared Failover

After preparing for a failover, carefully investigate the situation to make sure a failover is required. If it is required, bring the recovered workload on to the main network by running Failover.

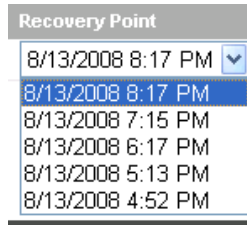
- 1 Click *Workloads* on the toolbar to navigate to the Workloads page.
- 2 Select the workload that requires a failover.
- 3 Select *Failover*.

The Command Confirmation page is displayed.

Workload	Protection Tier	Replication Status	Recovery Point
SDSFORGE34	Hourly	Idle	8/13/2008 8:17 PM

Execute Cancel

- 4 Select a *Recovery Point* to use for the test, if desired.



- 5 The workload *Replication Status* changes to *Going Live*.

When the operation is complete and the recovery workload has taken the primary workload's place on the network, the *Replication Status* changes to *Live*.

3.3.4 Running an Unprepared Failover

In the rare case, such as natural disaster, where it is immediately obvious that a primary workload is irreparably disabled, run *Failover* directly.

- 1 Click *Workloads* on the toolbar to navigate to the Workloads page.
- 2 Select the workload that requires a failover.
- 3 Select *Failover*.
- 4 To run the Failover immediately, click *Execute*. To continue, see [Step 5](#). To cancel the Failover, click *Cancel*.

or

To view and optionally change any workload settings before running the Failover, click the workload name. Click *Failover* at the bottom of the Web page to restart the Failover, then click *Execute*.

- 5 Navigate to the Workloads page. The workload *Replication Status* changes to *Running Failover*.

When the failover is complete, the *Replication Status* changes to *Live*. The workload is now running on the PlateSpin Forge Appliance Host.

3.3.5 Removing a Snapshot After Failover (Optional)

Forge leverages hypervisor snapshot technology to facilitate a rapid failover. Although it is not necessary, snapshots can be removed after the failover to improve performance and reclaim disk space.

NOTE: While the snapshot is being removed, the responsiveness of the workload is temporarily degraded. It is recommended that you perform this process during a scheduled down time.

- 1 Login to the VMware Infrastructure Client using the Host Appliance IP address. Ignore any warnings.
- 2 Expand the Virtual Machine list if necessary and locate the VM with the snapshot you want to remove.

NOTE: While it is not necessary, the removal is significantly faster when the host VM is powered off.

- 3 Right-click the VM and select *Snapshot > Snapshot Manager*.
- 4 Select the snapshot you would like to remove and click *Delete All*.
All changes are merged into the base.

3.4 Failback

This section assumes an original source server has failed, and a failover to a disaster recovery virtual machine has already taken place (see “[Planning for Failure](#)” on page 50). It also assumes that the target for the failback procedure does not already exist in Forge. The following instructions are a guide to deploying the virtual machine back onto physical hardware or to a virtual server (depending on whether the protected workload was a physical server or a virtual machine).

To failback a failed over workload you need to prepare the failback, configure the failback, run the failback and then optionally configure re-protection for the workload.

- ♦ [Section 3.4.1, “Preparing the Failback,”](#) on page 54
- ♦ [Section 3.4.2, “Configuring and Running Failback,”](#) on page 55
- ♦ [Section 3.4.3, “Configuring Reprotect,”](#) on page 55

3.4.1 Preparing the Failback

- 1 From the Forge dashboard, click *Workloads*.
- 2 Select the checkbox next to the failed over (live) workload for which you would like to configure failback.
Notice that some of the command buttons on the bottom of the screen become available in response to the type of workload selected. In this case, since the workload has been failed over, you can either configure failback or remove the workload.
- 3 Click *Configure Failback*.
The Failback Details page is displayed, prepopulated with the credentials for the workload you selected.

NOTE: The IP and/or password for the workload may have changed while the workload was failed over. If so, make any required adjustments to the credentials.

- 4 If you are failing back to brand new hardware or a new virtual machine, select *Full Replication*. If you are failing back to the same hardware or the same virtual machine that was previously protected, select *Incremental Replication*.
- 5 Select either *Virtual Targets* or *Physical Targets*, as appropriate for your task.
- 6 To failback to a physical target, see [Step 7](#). To failback to a virtual target, skip to [Step 8](#).
- 7 To failback to a physical target for either a full (new hardware) or incremental (existing hardware) replication, you need to boot up and register the target physical server using the WinPE* ISO image. You can get the image by clicking *Click to download* at the bottom of the page. Once the target is booted up and registered, it will appear in the list of physical targets you can select for the failback task. Skip to [Step 13](#).

- 8 To failback to a virtual machine, click *Add Target*.
For a full replication, see [Step 9](#). For an incremental replication, skip to [Step 11](#).
- 9 For full replications, enter the *Hostname/IP Address*, the *Username* and the *Password* for the failback target server (hypervisor where Forge will create the virtual machine to which you will failback).

NOTE: If both the failover and source workloads are online, use the IP address to identify them, since they will both have the same hostname.

- 10 Click *Add* to return to the Prepare Failback page. Skip to [Step 13](#).
- 11 For incremental replications, click *Add Target* to display the Add Target(Virtual Server) page.
Enter the *Hostname/IP Address*, the *Username* and the *Password* for the failback target server (hypervisor where the virtual machine to which you will failback resides) and click *Add*.
The Add Target(Virtual Machine) page is displayed where you can select the virtual machine and network to which you want to failback.

NOTE: Currently only ESX 3.x and 3i are supported as failback targets. When specifying a virtual failback target using incremental replication, you actually need to specify the hypervisor container as the target. In subsequent steps, you will specify the virtual machine in that container as the actual failback target.

- 12 Click *Add* to return to the Prepare Failback page.
- 13 Select the radio button next to the target you just added.
- 14 Click *Save and Prepare*.
Notice the green arrow in this button which indicates no confirmation message is displayed for this step. Proceed to [“Configuring and Running Failback” on page 55](#).

3.4.2 Configuring and Running Failback

- 1 Confirm the failback settings. Most of these setting typically are fine as is. For information on file transfer methods, see [“Supported Transfer Methods” on page 19](#).
- 2 (Optional) To stop any running services during the failback procedure, click *Add Services*, select services to stop and click *Apply*.
- 3 Make any desired changes to the workload settings, including changing the state of any existing services.
- 4 In the post-failback settings, specify whether you want to reprotect the workload after failback.
If you choose not to reprotect the workload, you can choose whether to leave the failed-back workload powered on or not.
- 5 Click *Save and Failback*.
Optionally, proceed to [“Configuring Reprotect” on page 55](#).

3.4.3 Configuring Reprotect

If you opted to reprotect the workload after failback, when the failback has completed running, you are presented with the Configure Reprotect page.

- 1 Confirm the workload hostname/IP and credentials supplied by Forge.

- 2 Specify whether you want the initial replication to be full or incremental. If you select incremental, confirm the Network and whether the IP assignment is DHCP or Static. If it is a static IP, fields are displayed for you to enter the configuration information.
- 3 Click *Save and Reprotect*.
To complete reprotect, see “[Configuring Protection and Preparing Replication](#)” on page 49.

3.5 Importing a Workload into Forge


When bandwidth or time is an issue, you can perform an incremental synchronization between the replicated workload and the protected workload instead of running a full workload replication. This means only the changes to the workload between replications need to be sent across your network.

But before this can happen, the initial fully replicated workload must exist on your Forge appliance, as a base.

Create a virtual machine of the source workload (for example, by using PlateSpin Portability Suite) at the production site. Copy the files to a portable media (such as a portable hard drive) and transport it to the disaster recovery site. At the site, attach the media to a workstation that has network access to Forge.

To import a workload VM:

NOTE: If the VMware Infrastructure Client is already installed, skip to [Step 3](#).

- 1 From a workstation other than your Forge appliance, open a Web browser and navigate to the ESX Server’s IP address (the first IP address you configured when you set up your Forge appliance).
- 2 Click the *Download VMware Infrastructure Client* link, then follow the instructions to download and install the software. Ignore any SSL warnings.
- 3 On your Forge appliance, select *Start > Programs > VMware > VMware Infrastructure Client*.
- 4 Log in, using the ESX Server’s IP address and the username/password you set up when the appliance was initially configured.
The VIC Inventory UI is displayed.
- 5 Click the *Forge* node in the Inventory panel.
- 6 Click the *Configuration* tab.
- 7 Click *Storage* under *Hardware*.
- 8 Right-click the Forge datastore (*Storage1*) and select *Browse Datastore* from the pop-up menu.
The *Datastore Browser* is displayed.
- 9 Click the *Datastore Upload* icon in the toolbar.

- 10 Select *Upload File* from the pop-up menu.
The Upload Items dialog box is displayed.
- 11 Browse to your image file and click *Open*.

- 12 Find your uploaded file in the Datastore window (you might need to scroll down to the bottom if there are many items).
- 13 Right-click the uploaded file and select *Add to Inventory* from the pop-up menu.
- 14 Specify a name for the uploaded VM if desired and click *Next*.
- 15 Click *Next* again and then click *Finish*.
- 16 Your image can now be found by Forge’s Application Host.
- 17 Quit the VIC.
From Forge, the uploaded image won’t show up until the next replication runs and the Application Host is refreshed. You can force a refresh by selecting *Settings > Application Host > Refresh Host*.

You can now add the workload to Forge. See [“Adding a Workload” on page 49](#).

3.6 Adding a SAN LUN to Forge

PlateSpin Forge supports the use of Storage Area Network (SAN) storage, as described in the [PlateSpin Forge 2.5 Getting Started Guide](#), but before Forge can access an existing SAN, a SAN Logical Unit (LUN) needs to be added to Forge’s ESX.

NOTE: If the VMware Infrastructure Client is already installed, skip to [Step 3](#).

- 1 From a workstation other than your Forge appliance, open a Web browser and navigate to the ESX Server’s IP address (the first IP address you configured when you set up your Forge appliance).
- 2 Click the *Download VMware Infrastructure Client* link, then follow the instructions to download and install the software. Ignore any SSL warnings.
- 3 On your Forge appliance, select *Start > Programs > VMware > VMware Infrastructure Client*.
- 4 Log in, using the ESX Server’s IP address and the username/password you set up when the appliance was initially configured.
The VIC Inventory UI is displayed.
- 5 Click the *Forge* node in the Inventory panel.
- 6 Click the *Configuration* tab.
- 7 Click the *Add Storage* hyperlink in the upper right.
- 8 In the Add Storage Wizard, click *Next*.
- 9 Click *Next*.
- 10 Click *Next*.
- 11 Specify a datastore name and click *Next*.
- 12 Click *Next*.
- 13 Click *Finish*.
- 14 Click *Storage* under *Hardware* to see the Forge’s datastores. The newly added SAN LUN should appear in the window.

15 Quit the VIC.

From Forge, the new datastore won't show up until the next replication runs and the Application Host is refreshed. You can force a refresh by selecting *Settings > Application Host > Refresh Host*.

You can now see the new datastore when adding and working with workloads.

3.7 Running Diagnostics

Users can run Diagnostics on any running or completed job. This provides information about a job's status, start time, and end time, as well as progress for running jobs. The report can be sent directly to PlateSpin Support for assistance in resolving user difficulties.

To run Diagnostics on a running job:

- 1 After clicking a command and starting a job, go to the Workloads page, then click the workload on which the job is running.
- 2 Click the *details* link near the top of the Workload Details page.
- 3 Click the *generate* link on the top of the page.
- 4 Click *View* to see a report.
- 5 Follow the instructions to send the report to PlateSpin Support.

To run Diagnostics on a completed job:

- 1 Run the Events report
- 2 Click the details link for the desired job.
- 3 Click the *generate* link on the top of the page.
- 4 Click *View* to see a report.
- 5 Follow the instructions to send the report to PlateSpin Support.

Forge Management Console

4

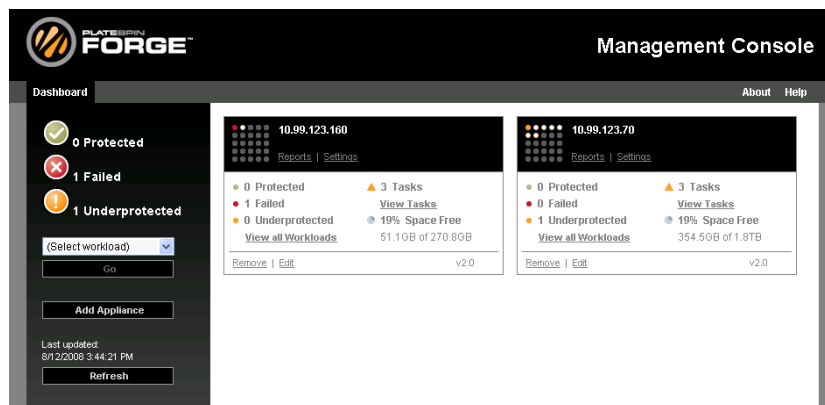
This section includes introductory and functional information about the Forge Management Console.

- ◆ [Section 4.1, “Overview,”](#) on page 59
- ◆ [Section 4.2, “Starting the Console,”](#) on page 59
- ◆ [Section 4.3, “Working with Appliances,”](#) on page 60

4.1 Overview

The PlateSpin Forge Management Console client is included with each PlateSpin Forge hardware appliance. The Console is a browser-based application providing centralized access to multiple PlateSpin Forge appliances. In a data center with more than one Forge appliance deployed, one of the appliances is the Manager and the Management Console is run from there. The other Forge appliances are added under the Manager, providing a single point of control and interaction.

Figure 4-1 Forge Management Console



4.2 Starting the Console

To start the PlateSpin Forge Management Console:

- 1 Open a Web browser with access to the Forge appliances on your network and navigate to the following URL:

```
http://<IP_address | console_host>/ForgeConsole
```

where *<IP_address | console_host>* is the IP address or hostname of the PlateSpin Forge Management VM on the Forge appliance you have chosen as the unit from which you want to manage multiple Forge appliances.

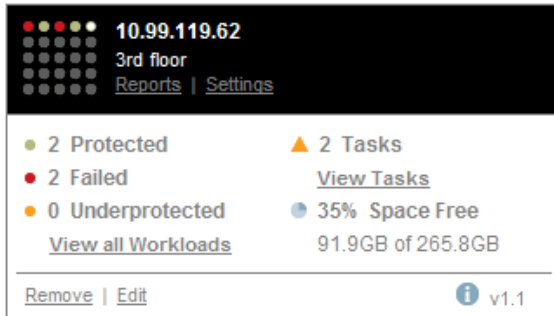
- 2 Log in with your username and password.

The console’s default Dashboard page is displayed.

4.3 Working with Appliances

Individual Forge appliances, when added to the PlateSpin Forge Management Console, are represented by cards.

Figure 4-2 Forge Appliance Card



A card displays basic information about the Forge appliance, such as:

- ◆ IP address/hostname
- ◆ Location
- ◆ Version number
- ◆ Workload count
- ◆ Workload status
- ◆ Appliance storage capacity
- ◆ Remaining free space

Hyperlinks on each card allow you to navigate to that particular appliance'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.

4.3.1 Adding Appliances

Adding an appliance results in a new appliance card on the PlateSpin Forge Management Console's dashboard.

NOTE: When you log in to the PlateSpin Forge Management Console on a Forge appliance, that appliance is not automatically added to the console. As with other Forge appliances in your network, the resident Forge appliance must also be manually added to the console.

To add an appliance to the console dashboard:

- 1 On the console's main dashboard, click *Add Appliance*.
The Forge Management Console - Add/Edit Appliance page is displayed.
- 2 Specify the URL of the Forge Management VM in the *Enter Forge URL* field.
You can use either http or https.

- 3** Optionally, enable the *Use Management Console Credentials* check box to use the same credentials as those used by the console. When selected, the console automatically populates the *Domain\Username* field.
- 4** In the *Domain\Username* field, specify a Domain and Username valid for the appliance you want to add to the console.
- 5** Specify a password in the *Password* field that is associated with the Username entered in **Step 4**.
- 6** (Optional) Specify an identifying name in the *Display Name* field.
There is a 15-character limit.
- 7** (Optional) In the *Location* field, specify where the Forge appliance is located.
There is a 20-character limit.
- 8** (Optional) In the *Notes* field, specify any additional information about the appliance. .
Information in the *Notes* field is not shown on the card. There is a 400-character limit.
- 9** Click *Add/Save*.
A new appliance card is added to the dashboard.

4.3.2 Editing Appliance Information

You can modify the details of a managed Forge appliance.

- 1** Click the *Edit* hyperlink on the card to be edited..
The Forge Management Console - Add/Edit Appliance page is displayed.
- 2** Make any desired changes, then click *Add/Save*.
The updated console dashboard is displayed.

4.3.3 Removing Appliances

You can remove a Forge appliance from the console dashboard.

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

The following sections contain information to help you with the setup and configuration of Storage Area Network implementations for your PlateSpin Forge[®] hardware appliance:

- ♦ [Section 5.1, “Using Forge with SAN Storage,” on page 63](#)
- ♦ [Section 5.2, “Adding a SAN LUN to Forge,” on page 64](#)

5.1 Using Forge with SAN Storage

PlateSpin Forge 2.5 supports existing external storage solutions, such as Storage Area Network (SAN) implementations. Both Fibre Channel and iSCSI solutions are supported. SAN support for Fibre Channel and iSCSI HBAs allows a Forge appliance to be connected to a SAN array. You can then use SAN-array LUNs (Logical Units) to store workloads and workload recovery points. Using Forge with a SAN improves flexibility, efficiency, and reliability.

Each SAN product has its own nuances and differences that do not migrate from one hardware manufacturer to the next. This is especially true when considering how these products connect and interact with a Management VM. As such, specific configuration steps for each possible environment and context are beyond the scope of this guide.

The best place to find this type of information is from your hardware vendor or your SAN product sales representative. Many hardware vendors have support guides available describing these tasks in detail. You can find a wealth of information at the following sites:

The [VMware Documentation Web site](http://www.vmware.com/support/pubs/) (<http://www.vmware.com/support/pubs/>).

- ♦ The *Fibre Channel SAN Configuration Guide* discusses the use of ESX Server with Fibre Channel storage area networks.
- ♦ The *iSCSI SAN Configuration Guide* discusses the use of ESX Server with iSCSI storage area networks.
- ♦ The *VMware I/O Compatibility Guide* lists the currently approved HBAs, HBA drivers, and driver versions.
- ♦ The *VMware Storage/SAN Compatibility Guide* lists currently approved storage arrays.
- ♦ The *VMware Release Notes* give information about known issues and workarounds.
- ♦ The *VMware Knowledge Bases* have information on common issues and workarounds.

The following vendors provide storage products that have all been tested by VMware:

- ♦ 3PAR*: <http://www.3par.com>
- ♦ Bull: <http://www.bull.com> (FC only)
- ♦ Compellent: <http://www.compellent.com>
- ♦ Dell*: <http://www.dell.com>
- ♦ EMC*: <http://www.emc.com>
- ♦ EqualLogic*: <http://www.equallogic.com> (iSCSI only)
- ♦ Fujitsu*/Fujitsu Siemens: <http://www.fujitsu.com> and <http://www.fujitsu-siemens.com>

- ♦ HP*: <http://www.hp.com>
- ♦ Hitachi*/Hitachi Data Systems (HDS): <http://www.hitachi.com> and <http://www.hds.com> (FC only)
- ♦ IBM*: <http://www.ibm.com>
- ♦ NEC*: <http://www.nec.com> (FC only)
- ♦ Network Appliance (NetApp*): <http://www.netapp.com>
- ♦ Nihon Unisys*: <http://www.unisys.com> (FC only)
- ♦ Pillar Data: <http://www.pillardata.com> (FC only)
- ♦ Sun Microsystems*: <http://www.sun.com>
- ♦ Xiotech*: <http://www.xiootech.com> (FC only)

You can also learn more about iSCSI by visiting the Storage Networking Industry Association Web site at http://www.snia.org/tech_activities/ip_storage/iscsi/.

5.2 Adding a SAN LUN to Forge

PlateSpin Forge supports the use of Storage Area Network (SAN) storage, as described above, but before Forge can access an existing SAN, a SAN Logical Unit (LUN) needs to be added to Forge's ESX.

To add a SAN LUN to Forge:

NOTE: If the VMware Infrastructure Client is already installed, skip to **Step 3**.

- 1** From a workstation other than your Forge appliance, open a Web browser and navigate to the ESX Server's IP address (the first IP address you configured when you set up your Forge appliance).
- 2** Click the *Download VMware Infrastructure Client* link, then follow the instructions to download and install the software. Ignore any SSL warnings.
- 3** On your Forge appliance, select *Start > Programs > VMware > VMware Infrastructure Client*.
- 4** Log in using the ESX Server's IP address and the username and password you set up when the Appliance was initially configured.
The VIC Inventory UI is displayed.
- 5** Click the *Forge* node in the Inventory panel.
- 6** Click the *Configuration* tab.
- 7** Click the *Add Storage* hyperlink in the upper right.
- 8** In the *Add Storage Wizard*, click *Next*.
- 9** Click *Next*.
- 10** Click *Next*.
- 11** Enter a datastore name and click *Next*.
- 12** Click *Next*.
- 13** Click *Finish*.
- 14** Click *Storage* under *Hardware* to see the Forgedatastores. The newly added SAN LUN should appear in the window.

- 15** Quit the VIC.
- 16** From Forge, the new datastore won't show up until the next replication runs and the Application Host is refreshed. You can force a refresh by selecting *Settings > Application Host > Refresh Host*.

You can now see the new datastore when adding and working with workloads.

Forge Relocation

6

This document provides information about upgrading your PlateSpin Forge appliance from version 1.1, 1.2.0 or 1.2.1. to version 2.5.

For information about functional enhancements and bug fixes included in this release, see the Release Notes document.

IMPORTANT: User-uploaded drivers for failback are not preserved during an upgrade. Any such drivers need to be uploaded again after the upgrade .

- ◆ [Section 6.1, “Forge IP Addresses,” on page 67](#)
- ◆ [Section 6.2, “Changing IP Addresses,” on page 67](#)

6.1 Forge IP Addresses

When the Forge appliance is first set up, several IP addresses are assigned to it, including the PlateSpin Forge Appliance Host (ESX) and the PlateSpin Forge Management VM.

The Appliance Host

The Appliance Host IP address is used to identify the Forge hardware to your network. It provides access to the various workloads you will want to protect.

The Management VM

The Management VM IP address is used to access the Forge web-based client. This is how you logon to Forge to setup protection schedules, perform failover tests and initiate failback activity, among other things. Anything you want to configure the Forge Appliance to do, you do through the client.

Replication IP Addresses

A temporary IP address is assigned to the recovery workload while Forge is replicating data into it.

6.2 Changing IP Addresses

In the event the Forge appliance needs to be moved after its initial configuration, the IP addresses originally assigned to it will need to be changed as well.

There are three things you need to do to change the Forge appliance IP addresses gracefully:

- ◆ Prepare any currently protected workloads for the change
- ◆ Make the change
- ◆ Reconfigure workloads to reflect the change

6.2.1 Preparing Currently Protected Workloads for the Change

Before you can change the IP addresses assigned to a PlateSpin Forge appliance, any currently protected workloads need to be paused.

NOTE: Ensure at least one incremental has been run for each workload prior to relocating it (changing its IP address).

To pause currently protected workloads:

- 1 Login to the PlateSpin Forge web client.
- 2 Click the *Workloads* tab.
- 3 Select all the workloads and click *Pause Schedule*.
- 4 Click *Execute*.

The status *Paused* is displayed in the *schedule* column for all the workloads.

NOTE: Wait for any running replications to complete before proceeding to “[Making the Change](#)” on page 69.

- 5 If you are changing IP address(es) because you want to physically move the Forge appliance, follow the steps in “[To shutdown the Forge Management VM](#)” on page 68 and “[To shutdown the Appliance Host](#)” on page 69. Otherwise, you can now proceed to the next part of the IP Change procedure: “[Making the Change](#)” on page 69.

To shutdown the Forge Management VM

There are three ways that you can shutdown the Forge Management VM:

- 1 Use a web browser:
 - 1a Logon to the Forge web client
 - 1b Click *Settings > Appliance Host*.
 - 1c Click the *here* link at the bottom of the page to open the Forge Management VM Settings page.
 - 1d Click *Maintenance*.
 - 1e Click *Shutdown*.
- 2 Use Remote Desktop:
 - 2a Connect to the Forge Management VM using Remote Desktop.
 - 2b Click *Start > Shutdown*.
- 3 Use the VMware Infrastructure Client:

NOTE: If the VMware Infrastructure Client is already installed, skip to [Step 3c](#).

- 3a From a workstation other than your Forge appliance, open a Web browser and navigate to the ESX Server’s IP address (the Appliance Host IP address).
- 3b Click the *Download VMware Infrastructure Client* link, and then follow the instructions to download and install the software. Ignore any SSL warnings.
- 3c On your Forge appliance, select *Start > Programs > VMware > VMware Infrastructure Client*.

- 3d** Login using the ESX Server (Appliance Host) IP address and the username/password you setup.
The VIC Inventory UI is displayed.
- 3e** Click on the Console tab.
- 3f** In Windows, select *Start > Shutdown*.

Once the Forge Management VM is shutdown, you need to shutdown the Appliance Host.

To shutdown the Appliance Host

- 1** At the Forge Console, press Alt-F2 to switch to the ESX Server console.

NOTE: To switchback to the Forge Console, press Alt-F1.

- 2** Login as the superuser using login ID `root` and the password you setup.
- 3** Type in `shutdown` and hit Enter.

Once the Forge Appliance Host is shutdown, power the appliance down and perform the physical move. When the appliance is in the new location, make all required connections and power it on.

You can now proceed to the next part of the IP Change procedure: “[Making the Change](#)” on page 69.

6.2.2 Making the Change

When all the currently protected workloads are paused, you can proceed with changing the IP addresses.

NOTE: If you want to change IP address(es) because you are physically moving the Forge appliance, move the appliance prior to proceeding.

To change the IP address:

- 1** At the Forge console, login as the superuser. This is `root` for the *Login* field and the password you setup during the initial configuration in the *Password* field. Click *OK*.
The PlateSpin Forge Appliance Configuration dialog is displayed.
- 2** If you only want to change the Management VM IP address, click *Skip* and proceed to [Step 4](#).
- 3** Change the *IP* address, *Netmask*, and *Gateway* IP address as desired for the Appliance Host. Optionally, you can change the *Hostname* as well. Click *OK*.

The PlateSpin Forge Appliance Host credentials dialog is displayed.

NOTE: You may also use DHCP, but only if static IP lease is enabled. It is also recommended that in multiple appliance environments you should assign unique hostnames to the appliances to avoid hostname conflicts.

- 4** Login using the PlateSpin Forge Appliance Host login and password setup during the initial configuration of the appliance. Click *OK*.
The PlateSpin Forge Management VM network settings dialog is displayed.
- 5** If you only want to change the Appliance Host IP address, click *Skip* and proceed to [Step 7](#).

- 6 Change the *IP* address, *Netmask*, and *Gateway* IP address as desired for the Management VM. Optionally, you can change the *Hostname* as well. Click *OK*.

NOTE: You may also use DHCP, but only if static IP lease is enabled. It is also recommended that in multiple appliance environments you should assign unique hostnames to the Management VMs to avoid hostname conflicts.

- 7 If aside from IP address changes, you also want to change the workgroup or domain assignment, click *Yes*. Otherwise, click *Skip* and proceed to **Step 9**.
- 8 Enter the domain *Name*, *User* and *Password* or specify the Workgroup to which you want to add the Forge Appliance. Click *OK*.
- 9 A configuration review dialog is displayed with a summary of the parameters you have changed. Use this information to verify your settings. Click *OK* to accept the changes. Your changes, if any, are applied to the Management VM.

NOTE: You can select *Cancel* at this point to abandon the changes or use *Back* to go and edit your changes.

You can now proceed to the third part of the IP Change procedure: **“Reconfiguring Workloads to Reflect the Change”** on page 70.

6.2.3 Reconfiguring Workloads to Reflect the Change

Once you have physically moved the Forge appliance (if necessary) and changed the IP address(es) of the Forge appliance, you might need to reconfigure the replication IP addresses of any currently protected (and paused) workloads so that they adhere to any new subnets or networks as a result of the move.

NOTE: If you cannot connect to the Forge web client after changing the Forge Appliance Host or Management VM IP addresses, verify that the Windows firewall has not been set to *On*. If it has, set it to *Off* and try connecting again.

To reconfigure workloads to reflect the change:

- 1 Login to the PlateSpin Forge web client.
- 2 Click the Workloads tab.
- 3 For each workload:
 - 3a Click the name of the workload in the Workload column.
The Workload Details page is displayed.
 - 3b Click *Edit*.
 - 3c In the Replication Settings section, change the Replication Network configuration to reflect the changes you made to the PlateSpin Forge appliance IP address.
 - 3d Click *Save* at the bottom of the Workload Details page.
 - 3e Click the Workloads tab to return to the Workloads page.
 - 3f Repeat **Step 3a** through **Step 3e** for all of the paused workloads.
- 4 Once all the paused workloads have been reconfigured, select all the workloads on the Workloads page and click *Resume Schedule*.

5 Click *Execute*.

The workloads return to their previous replication schedule.

NOTE: Changing the replication IP address for a workload using the Block-based Transfer Method will cause a warning to display in the Workload Details page notifying you that the production workload (source machine) will reboot after the next scheduled incremental replication runs. You can manually run the incremental replication instead of waiting for the schedule, forcing an immediate reboot of the production workload, if desired.

WARNING: The first incremental replication after a source reboot may fail if the source hasn't completely rebooted when the incremental runs. If this occurs, manually run the replication again or wait for the next scheduled replication.

To manually run a scheduled incremental replication:

1 Logon to the PlateSpin Forge web client.

2 Click *Workloads*.

The Workloads page is displayed.

3 Select the workload(s) for which you would like to manually run incremental replication(s).

4 Click *Run Incremental*.

Incremental replications using the Block-based transfer method that have had their Replication IP address(es) changed since their last scheduled replication will force the production workload(s) to reboot.

NOTE: Manual incremental replications do not remove the next scheduled incremental replication for that workload from the schedule, but in the above scenario they do remove the forced reboot.

Troubleshooting

7

This section provides information about troubleshooting the PlateSpin Forge[®] hardware appliance. For the most up-to-date troubleshooting information, see knowledgebase article [Q21176 \(http://support.platespin.com/kb2/article.aspx?id=21176\)](http://support.platespin.com/kb2/article.aspx?id=21176).

- ◆ [Section 7.1, “Add Workload - Configuration,” on page 73](#)
- ◆ [Section 7.2, “Add Workload - Discovery,” on page 76](#)
- ◆ [Section 7.3, “Prepare Replication,” on page 78](#)
- ◆ [Section 7.4, “Replication,” on page 79](#)

7.1 Add Workload - Configuration

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 using a local admin account with the user name syntax: <code>hostname\LocalAdmin</code></p> <p>Or try the discovery with a domain admin account with the user name syntax: <code>domain\DomainAdmin</code></p>
“Unable to connect to Windows server...Access is denied.”	<p>A Non-admin account is used when trying to add a workload—Use an admin account or add the user to the administrators group and try again.</p> <p>WMI connectivity failure. For each of the following possible resolutions, attempt the solution and then perform the “WMI Connectivity Test” on page 74 again. If the test succeeds, try adding the workload again. Possible resolutions are:</p> <ul style="list-style-type: none">◆ “Enabling DCOM” on page 75◆ “Ensuring RPC Service is Running” on page 75
“Unable to connect to Windows server...The network path was not found.”	<p>Network connectivity failure—perform the “Network Connectivity Test” on page 74. If it fails, ensure that Forge and the workload are on the same network. Reconfigure the network and try again.</p>

7.1.1 Network Connectivity Test

NOTE: If the VMware Infrastructure Client is already installed, skip to [Step 3](#).

- 1 From a workstation other than your Forge appliance, open a Web browser and navigate to the ESX Server's IP address (the first IP address you configured when you set up your Forge appliance).
- 2 Click the *Download VMware Infrastructure Client* link, then follow the instructions to download and install the software. Ignore any SSL warnings.
- 3 Login using the ESX Server (Appliance Host) IP address and the username/password you setup.
The VIC Inventory UI is displayed.
- 4 Select the Forge VM in the inventory list on the left.
- 5 Click on the Console tab.
- 6 Click *Start > Run*, type in `cmd` and press Enter.
A terminal window is displayed.
- 7 Type `ping server_ip` and press Enter to ping the workload.

7.1.2 WMI Connectivity Test

NOTE: If the VMware Infrastructure Client is already installed, skip to [Step 3](#).

- 1 From a workstation other than your Forge appliance, open a Web browser and navigate to the ESX Server's IP address (the first IP address you configured when you set up your Forge appliance).
- 2 Click the *Download VMware Infrastructure Client* link, then follow the instructions to download and install the software. Ignore any SSL warnings.
- 3 Login using the ESX Server (Appliance Host) IP address and the username/password you setup.
The VIC Inventory UI is displayed.
- 4 Select the Forge VM in the inventory list on the left.
- 5 Click on the Console tab.
- 6 From the Forge Management VM, click *Start > Run*, type `wbemtest` and press Enter.
- 7 In the *Namespace* type in the name of the machine you are trying to discover with `\root\cimv2` appended to it. For example, if your machine name is `win2k` type:
`\\win2k\root\cimv2`
- 8 Enter the appropriate credentials using either the `hostname\LocalAdmin` or `domain\DomainAdmin` format.
- 9 Click *Connect* to test the WMI connection. If an error message is returned a WMI connection cannot be established between Forge and the workload being added.

7.1.3 Enabling DCOM

- 1 Log into the workload that you would like to protect.
- 2 Click *Start > Run*.
- 3 Type `dcomcnfg` and press Enter.
- 4 On a Windows NT/2000 server machine, the DCOM Configuration dialog is displayed. Click the Default Properties tab and ensure that *Enable Distributed COM on this computer* is checked.

For Windows 2003, the Component Services window is displayed. In the *Computers* folder of the console tree of the Component Services administrative tool, right-click on the computer for which you want to check if DCOM is enabled and then click *Properties*. Click the Default Properties tab and ensure that *Enable Distributed COM on this computer* is checked.

- 5 If DCOM was not enabled, please enable it and restart the Windows Management Instrumentation Service (if rebooting the server is not possible) and try adding the workload again.

7.1.4 Ensuring RPC Service is Running

There are three potential blockages for the RPC service:

- ♦ Windows Service
- ♦ Windows Firewall
- ♦ Hardware Firewall

For the Windows Service, ensure that the RPC service is running on the workload. To access the services panel, run `services.msc` from a command prompt.

For a Windows firewall, add RPC exception.

For hardware firewalls, you can try:

- ♦ Putting Forge and the workload on the same side of the firewall
- ♦ Opening up specific ports between Forge and the workload (see [Table 7-1 on page 75](#))
- ♦ Opening up all the ports

Table 7-1 Required Source Ports

Port	Protocol	Description
135/445	TCP	DCOM\RPC ports used to add Windows workloads.
137-139/445	TCP	Ports used for Named Pipe communications and File and Printer Sharing between the protected workload and the corresponding target VM on the Forge appliance.
SMB (TCP 139, TCP 445, UDP 137, UDP 138)	TCP/UDP	Ports used during failback process.

Port	Protocol	Description
3725	TCP	Port used to transfer files for file-based and VSS based protection.
10000 and higher	TCP	After the initial handshake, another TCP connection from the source to the target is initiated. The source machine uses port 10000 + X (where X = drive letter 'A' to 'X'). For example, the port for drive C is 10002, D will use TCP port 10003, and so on. There is one TCP connection for every drive being mirrored.
Random port above 1024		WMI uses the DCOM and RPC ports, but also uses a randomly assigned port above 1024.
9999		Block-based component

7.2 Add Workload - Discovery

Problems or Messages	Solutions
<p>"Discover Server Details {hostname}" Failed</p> <p>Progress: 0%</p> <p>Status: NotStarted</p>	<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 knowledgebase article Q20339 (http://support.platespin.com/kb2/article.aspx?id=20339) for more details. ◆ If local or domain policies restrict required permissions, follow the steps outlined in knowledgebase article Q20862 (http://support.platespin.com/kb2/article.aspx?id=20862).

Problems or Messages	Solutions
Workload Discovery failed “Could not find file <code>output.xml</code> ” or “Network path not found”	There are several possible reasons for the “Could not find file <code>output.xml</code> ” error: <ul style="list-style-type: none"> ◆ Anti-virus software on the source could be interfering with the discovery. Disable the anti-virus software to determine whether or not it is the cause of the problem. See “Disabling Anti-Virus Software” on page 77. ◆ File and Printer Sharing for Microsoft Networks may not be enabled. Enable it under the Network Interface Card properties. ◆ The C\$ and/or Admin\$ shares on the source may not be accessible. Ensure the Forge VM can access those shares. See “Enabling File/Share Permissions and Access” on page 78. ◆ Change the flag <code>ForceMachineDiscoveryUsingService</code> to <code>true</code> in the <code>web.config</code> file in the <code>\Program Files\PlateSpin Portability Suite Server\Web</code> folder. ◆ The Server and/or the Workstation service may not be running. If this is the case, enable them and set their startup mode to <code>automatic</code>. ◆ The Windows remote registry service is disabled. Start the service and set the startup type to <code>automatic</code>.

7.2.1 Disabling Anti-Virus Software

When working with a source workload running anti-virus software, issues are sometimes encountered where the anti-virus software is blocking some of the Forge functionality. These problems primarily occur when adding the workload to be protected.

As part of the process of adding the workload, Forge gathers a profile of the source. The profile contains information on the disks, operating system, software and services installed, along with other components. To perform this data gathering, Forge leverages a combination of WMI and Remote Registry calls. Some of the calls made can sometimes be interpreted as intrusions by anti-virus software, and could restrict access to the necessary data.

In order to ensure functionality, it may be necessary to disable the anti-virus service prior to adding the workload.

Anti-virus software can sometimes also lock access to certain files, allowing only certain processes or executables to access them. This can sometimes prevent Forge from replicating some files when using file-based protection. In this case, when configuring the protection of the workload, you are able to select services to disable – such as services installed and used by anti-virus software. These services are only disabled for the duration of the file transfer, and are restarted once the process completes. This is not necessary when performing VSS or BBT protection tasks.

7.2.2 Enabling File/Share Permissions and Access

To successfully protect a workload, Forge needs to successfully deploy and install the OFX Controller and, if using BBT, the block-based agent. When deploying those components to the workload being protected, as well as when gathering information about the workload during the “add workload” process, Forge uses the source machine’s administrative shares. Forge needs administrative access to the shares using either a local administrator account or a domain admin account for this to work.

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` you should see `C$` and `Admin$`, among other shares.

Once you have confirmed that the shares are enabled you need to ensure that they are accessible from the Forge Management VM.

From the Forge Management VM:

- 1 Click `Start > Run`.
- 2 Type `server>\C$` and then click `OK`.
- 3 If prompted for credentials, use the same credentials that will be used to add the workload in Forge.

The directory is opened and you should be able to browse and modify the contents as desired.

- 4 Repeat the process for all shares with the exception of the `IPC$` share. The `IPC$` share is used for credential validation and authentication purposes by Windows. It is not mapped to a folder or file on the workload, so the test will always fail, however the share should still be visible in the above test.

Forge will not modify the existing content of the volume, however it will create its own directory, to which it requires access and permissions.

7.3 Prepare Replication

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 78.

7.3.1 Group Policy and User Rights

Refresh the policy immediately using `gpupdate /force` (for Windows 2003/XP) or `secedit /refreshpolicy machine_policy /enforce` (for Windows 2000). Due to the way that Forge interacts with the source workload’s operating system, it requires the administrator account used to

add a workload 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 below user rights assignments may have been removed:

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

In order to verify that the above Group Policy settings have been set, you can run `gpresult /v` from the command line on the source machine, or alternatively `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.

7.4 Replication

Problems or Messages	Solutions
Workload issue requires user intervention	This problem occurs when the server is under load and things are taking longer than expected.
Replication is in recoverable error during replication either during <i>Scheduling Taking Snapshot of Virtual Machine</i> or <i>Scheduling Reverting Virtual Machine to Snapshot before Starting</i> .	The solution is to wait until the replication is complete.
All workloads go into recoverable errors because you are out of disk space.	Verify the free space. If more space is required, remove a workload.
Slow network speeds under 1 MB.	Confirm that the source machine's Network Interface Card's duplex setting is on and the switch is connected to matches (i.e. if the switch is set to auto, the source can't be set to 100 MB. They need to match.)
Slow network speeds over 1 MB.	Measure the latency by running the following from the source to the Forge: <code>ping forge_ip -t</code> Allow it to run for 50 iterations and the average will indicate the latency. Also see "Optimizing File-based Transfers for WAN Connections" on page 80 .
: "The file transfer cannot begin - port 3725 is already in use"	Ensure that the port is open and listening:
or	Run <code>netstat -ano</code> on the workload.
"3725 unable to connect"	Check the firewall. Retry the replication.

Problems or Messages	Solutions
<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 Forge Management VM.</p> <p>Change the replication IP to a static IP or enable the DHCP server.</p> <p>Ensure the virtual network selected for replication is routable to the Forge Management VM.</p>
<p>Replication job does not start (stuck at 0%)</p> <p>“Controller connection not established.”</p>	<p>This error can occur for different reasons and each has a unique solution:</p> <ul style="list-style-type: none"> ◆ For environments using a local proxy with authentication, bypass the proxy or add proper permissions to resolve this problem. See knowledgebase article Q20339 (http://support.platespin.com/kb2/article.aspx?id=20339) for more details. ◆ If local or domain policies restrict required permissions, to resolve this problem follow the steps outlined in knowledgebase article Q20862 (http://support.platespin.com/kb2/article.aspx?id=20862). <p>This is a common issue when Forge has been added to a domain and domain policies are applied with restrictions. See “Group Policy and User Rights” on page 78.</p>

7.4.1 Optimizing File-based Transfers for WAN Connections

The following settings will optimize file-based transfers across a Wide Area Network. These settings are global and will affect all replications, including file-based and VSS replications.

To optimize over the network replications, you need to modify the `productinternal.config` file in the `\Program Files\PlateSpin Portability Suite Server\Web` folder.

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

Below is a list of the configuration parameters with two sets of values: the defaults and the values recommended for optimum operation in a high-latency WAN environment.

Table 7-2 *Default and Optimized Configuration Parameters*

Parameter	Default Value	Optimized Value
<code>fileTransferThreadcount</code>	2	4 to 6
Controls the number of TCP connections opened for file-based data transfer.		

Parameter	Default Value	Optimized Value
fileTransferMinCompressionLimit	0 (disabled)	max 65536 (64 KB)
Specifies the packet-level compression threshold in bytes.		
fileTransferCompressionThreadsCount	2	N/A
Controls the number of threads used for packet-level data compression. This is ignored if compression is disabled. Since the compression is CPU-bound, this setting might have a performance impact.		
fileTransferSendReceiveBufferSize	0 (8192 bytes)	max 5242880 (5 MB)
TCP/IP window size setting for file transfer connections. It controls the number of bytes sent without TCP acknowledgement, in bytes.		
When the value is set to 0, the default TCP window size is used (8 KB). For custom sizes, specify the size in bytes. Use the following formula to determine the proper value:		
$((\text{LINK_SPEED}(\text{Mbps})/8) * \text{DELAY}(\text{sec})) * 1024 * 1024$		
For example, for a 100 Mbps link with 10 ms latency, the proper buffer size would be:		
$(100/8) * 0.01 * 1024 * 1024 = 131072 \text{ bytes}$		

