PlateSpin® Forge 4.0

User Guide

April 11, 2014

Legal Notice

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

893 Windows Vista Enhanced Cryptographic Provider (RSAENH)

894 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

989 Windows XP Enhanced Cryptographic Provider (RSAENH)

990 Windows XP Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

997 Microsoft Windows XP Kernel Mode Cryptographic Module (FIPS.SYS)

1000 Microsoft Windows Vista Kernel Mode Security Support Provider Interface (ksecdd.sys)

1001 Microsoft Windows Vista Cryptographic Primitives Library (bcrypt.dll)

1002 Windows Vista Enhanced Cryptographic Provider (RSAENH)

1003 Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1006 Windows Server 2008 Code Integrity (ci.dll)

1007 Microsoft Windows Server 2008 Kernel Mode Security Support Provider Interface (ksecdd.sys)

1008 Microsoft Windows Server 2008

1009 Windows Server 2008 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

1010 Windows Server 2008 Enhanced Cryptographic Provider

1012 Windows Server 2003 Enhanced Cryptographic Provider (RSAENH)

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

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

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

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

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

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

License Grant

Licenses for PlateSpin Forge 3.4 or later cannot be used for versions of PlateSpin Forge prior to 3.4.

Third-Party Software

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

Contents

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@platespin.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support
Technical Support Guide:	https://www.netiq.com/Support/process.asp#_Maintenance_Programs_and
Product Specific Information:	https://www.netiq.com/support/kb/product.php?id=SG_XPLATESPINFORGE_1_2

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

About This Guide

This *User Guide* provides information about using PlateSpin Forge. provides conceptual information about the PlateSpin Forge product. It also defines terminology and includes troubleshooting information.

Intended Audience

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

Other Information in the Library

The library provides the following information resources:

Getting Started Guide

Provides information about the basic steps required for setting up your PlateSpin Forge appliance.

Help

Provides embedded guidance to assist users with common tasks as they access the user interface.

Documentation Updates

The most recent version of this guide can be found at PlateSpin Forge 4 Online Documentation Web Site (https://www.netiq.com/documentation/platespin_forge_4/).

1 Product Overview

This section includes the following information:

1.1 About PlateSpin Forge

PlateSpin Forge is a consolidated recovery hardware appliance that protects physical and virtual workloads (operating systems, middleware, and data) 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 enables you to:

- Quickly recover workloads upon failure
- Simultaneously protect multiple workloads (10 to 25, depending on the model)
- Test the failover workload without interfering with your production environment
- Fail back failover workloads to either their original or to completely new infrastructures, physical or virtual
- Take advantage of existing external storage solutions, such as SANs

With internal, prepackaged storage, Forge has a total storage capacity of 3.5 terabytes, although the capacity is almost unlimited when external storage configurations are used by adding iSCSI or Fibre Channel cards.

1.2 Supported Configurations

1.2.1 Supported Windows Workloads

PlateSpin Forge supports most Windows-based workloads.

Both file-level and block-level replication are supported, with certain restrictions. See Section 6.3, “Data Transfer,” on page 78.

Table 1-1 *Supported Windows Workloads*

Operating System	Remarks
Server Class workloads	
Windows Server 2008 R2 (64-bit) Windows Server 2008 (64-bit)	Including domain controllers (DC) and Small Business Server (SBS) editions
Windows Server 2003 latest SP (64-bit) Windows Server 2003 latest SP (32-bit) Windows Server 2003 R2 (64-bit) Windows Server 2003 R2 (32-bit)	Including domain controllers (DC) and Small Business Server (SBS) editions
Windows Server 2000 SP4 (32-bit)	
Workstation Class workloads	
Windows 7	Professional, Enterprise, and Ultimate editions only
Windows Vista	
Windows XP	

The following are examples of Forge behavior when protecting and failing back between UEFI and BIOS-based systems:

- When transferring a UEFI-based workload to a VMware vSphere 4.*x* container (which does not support UEFI), Forge transitions the workload's UEFI firmware at failover time to BIOS firmware. Then, when failback is selected on a UEFI-based physical machine, Forge reverses the firmware transition from BIOS to UEFI.
- If you attempt to failback a protected Windows 2003 workload to a UEFI-based physical machine, Forge analyzes the choice and notifies you that it is not valid (that is, the firmware transition from BIOS to UEFI is not supported – Windows 2003 does not support the UEFI boot mode).
- When protecting a UEFI-based source on a BIOS-based target, Forge migrates the UEFI system's boot disks, which were GPT, to MBR disks. Failing back this BIOS workload to a UEFI-based physical machine converts the boot disks back to GPT.

1.2.2 Supported Linux Workloads

PlateSpin Forge supports a number of Linux distributions.

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

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

Table 1-2 *Supported Linux Workloads*

Operating System	Remarks
Linux Server class workloads	
Red Hat Enterprise Linux (RHEL) 5.0-5.5, 6.0-6.2	

Operating System	Remarks
RHEL 5.6-5.8, 6.3	You must compile the PlateSpin `blkwatch` module before inventorying these workloads. See KB Article 7005873 (https://www.netiq.com/support/kb/doc.php?id=7005873).
SUSE Linux Enterprise Server (SLES) 9, 10, 11 (SP1, SP2, SP3)	**NOTE:** Kernel version `3.0.13-0.27-pae` of SLES 11 SP2 is not supported. Please upgrade to kernel version `3.0.51-0.7.9-pae` or later before inventorying the workload.
◆ Novell Open Enterprise Server (OES) 11 SP1 and SP2 ◆ OES 2 (SP2, SP3)	
Oracle Enterprise Linux (OEL)	◆ Same level of support as that for workloads running RHEL. ◆ Workloads using the Unbreakable Enterprise Kernel are not supported.

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

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

1.2.3 Supported VM Containers

PlateSpin Forge ships with a VMware ESX 4.1, the appliance host serving as the hypervisor component of the product.

1.3 Security and Privacy

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

- Section 1.3.1, “Security of Workload Data in Transmission,” on page 15
- Section 1.3.2, “Security of Credentials,” on page 16
- Section 1.3.3, “User Authorization and Authentication,” on page 16

1.3.1 Security of Workload Data in Transmission

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

You can enable or disable encryption individually for each workload. See “Workload Protection Details” on page 66.

1.3.2 Security of Credentials

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

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

1.3.3 User Authorization and Authentication

PlateSpin Forge provides a comprehensive and secure user authorization and authentication mechanism based on user roles, and controls application access and operations that users can perform. See Section 2.2, "Setting Up User Authorization and Authentication," on page 20.

1.4 Performance

1.4.1 About Product Performance Characteristics

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

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

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

1.4.2 Data Compression

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

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

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

Data Compression can be configured individually for each workload or in a Protection Tier. See "Protection Tiers" on page 79.

1.4.3 Bandwidth Throttling

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

Bandwidth throttling can be configured individual for each workload or in a Protection Tier. See "Protection Tiers" on page 79.

1.4.4 RPO, RTO, and TTO Specifications

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

  The RTO for failing a workload over to its virtual replica is affected by the time it takes to configure and execute the failover operation (10 to 45 minutes). See "Failover" on page 70.
- **Test Time Objective (TTO):** Describes the time required for testing disaster recovery with some confidence of service restoration.

  Use the *Test Failover* feature to run through different scenarios and generate benchmark data. See "Using the Test Failover Feature" on page 71.

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

You should determine average failover times for workloads in your environment by doing test failovers at various times, then use them as benchmark data in your overall data recovery plans. See "Generating Workload and Workload Protection Reports" on page 61.

2 PlateSpin Forge Application Configuration

This section includes the following information:

2.1 Product Licensing

This section provides information about activating your PlateSpin Forge software.

2.1.1 Obtaining a License Activation Code

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

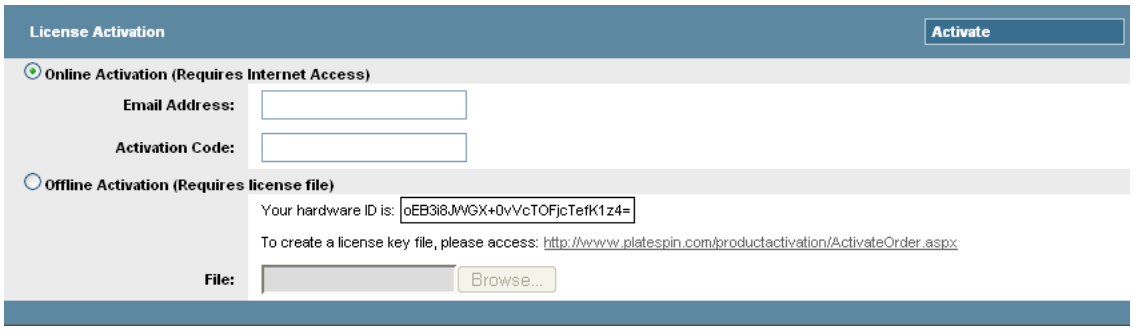
The first time you log into PlateSpin Forge, the browser is automatically redirected to the License Activation page. You have two options for activating your product license: Online License Activation or Offline License Activation.

2.1.2 Online License Activation

For online activation, PlateSpin Forge must have Internet access.

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

1 In the PlateSpin Forge Web Interface, click *Settings* > *Licenses* > *Add License*. The License Activation page is displayed.



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

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

2.1.3 Offline License Activation

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

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

---

1 Click *Settings* > *License*, then click *Add license*. The License Activation page is displayed.

2 Select *Offline Activation* and copy the hardware ID shown.

3 Use a Web browser on a computer that has internet access to navigate to the PlateSpin Product Activation Web Site (http://www.platespin.com/productactivation/ActivateOrder.aspx). Log in with your Novell username.

4 Enter in the appropriate fields:

- the activation code that you received
- the email address that you provided when placing your order
- the hardware ID that you copied in Step 2

5 Click *Activate*.

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

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

2.2 Setting Up User Authorization and Authentication

2.2.1 About PlateSpin Forge User Authorization and Authentication

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

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

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

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

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

When a user attempts to connect to PlateSpin Forge, the credentials provided through the browser are validated by IIS. If the user is not a member of one of the Workload Protection roles, connection is refused.

Table 2-1 *Workload Protection Roles and Permission Details*

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

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

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

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

1. Adding users to the required user groups detailed in Table 2-1 (see your Windows documentation).
2. Creating application-level security groups that associate these users with specified workloads (see "Managing PlateSpin Forge Security Groups and Workload Permissions" on page 24).

2.2.2 Managing PlateSpin Forge Access and Permissions

Accessing the PlateSpin Forge Server Administration Interface

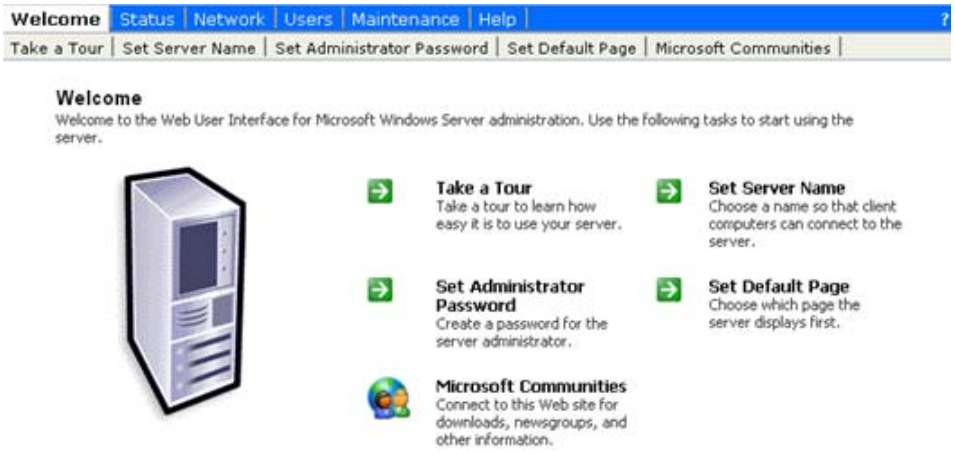
To access the Web User Interface for Microsoft Windows Server administration:

1 Open a Web browser and go to `https://IP_address:8098`

Replace *IP_address* with the IP address of the Forge VM.

Your browser connects to the server and displays the default Welcome page.

Figure 2-1 *Web User Interface for Microsoft Windows Server Administration*



Adding PlateSpin Forge Users

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

If you want to grant specific role permissions to an existing user on the Forge VM, see "Assigning a Workload Protection Role to a PlateSpin Forge User" on page 23.

1. Access your Forge VM's Server Administration Web User Interface.

   See "Accessing the PlateSpin Forge Server Administration Interface" on page 22.
2. Click *Users* > *Local Users*.

   The Local Users on Server page opens.
3. Under *Tasks*, click *New*, then type a username, a password, and other optional information.
4. Click *OK*.

   The Local Users on Server page reloads.

You can now assign a workload protection role to the newly created user. See "Assigning a Workload Protection Role to a PlateSpin Forge User" on page 23.

Assigning a Workload Protection Role to a PlateSpin Forge User

Before assigning a role to a user, determine the collection of permissions that best suits that user. See Table 2-1, "Workload Protection Roles and Permission Details," on page 21.

1. Access your Forge VM's Server Administration Web User Interface. See "Accessing the PlateSpin Forge Server Administration Interface" on page 22.
2. Click *Users* > *Local Groups*.

   The Local Groups on Server page opens.
3. In the list of groups, select the required workload protection group, then click *Properties* under *Tasks*.

   The corresponding group property page opens.
4. Click *Members*, select the required user from the list, and then click *Add*.

   The selected user is added to the *Members* list.
5. Click *OK*.

You can now add this user to a PlateSpin Forge security group and associate a specified collection of workloads. See "Managing PlateSpin Forge Security Groups and Workload Permissions" on page 24.

Changing the PlateSpin Forge Administrator Password

To change the password of the Forge VM's Administrator account:

1. Access your Forge VM's Server Administration Web User Interface. See "Accessing the PlateSpin Forge Server Administration Interface" on page 22.
2. Click *Set Administrator Password*, type the new password, confirm it, then click *OK*.

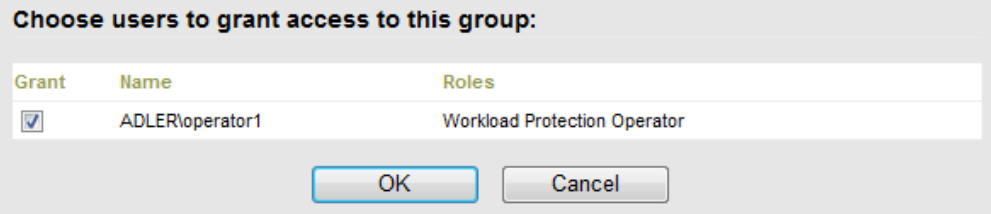
2.2.3 Managing PlateSpin Forge Security Groups and Workload Permissions

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

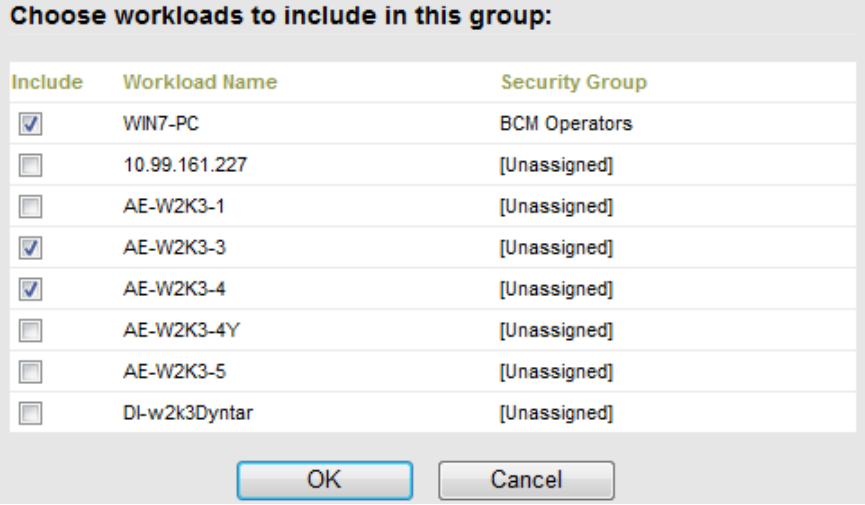
1. Assign a PlateSpin Forge user a Workload Protection Role whose permissions best suit that role in your organization. See "Assigning a Workload Protection Role to a PlateSpin Forge User" on page 23.
2. Access PlateSpin Forge as an administrator by using the PlateSpin Forge Web Interface, then click *Settings* > *Permissions*.

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

   If you want to add a PlateSpin Forge user that was recently added to the Forge VM, it might not be immediately available in the user interface. In this case, first click *Refresh User Accounts*.



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



   Only users in this security group will have access to the selected workloads.
7. Click *Create*.

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

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

2.3 Access and Communication Requirements across your Protection Network

2.3.1 Access and Communication Requirements for Workloads

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

Table 2-2 *Access and Communication Requirements for Workloads*

Workload Type	Prerequisites	Required Ports (Defaults)
All workloads	Ping (ICMP echo request and response) support	
All Windows workloads	Microsoft .NET Framework version 2.0 or 3.5 SP1	

Windows 7;
Windows Server 2008;
Windows Vista
	• Built-in `Administrator` or domain administrator account credentials (membership only in the local Administrators group is insufficient). On Vista, the account must be enabled (it is disabled by default).
	• The Windows Firewall configured to allow *File and Printer Sharing*. Use one of these options:
	  ◆ **Option 1, using Windows Firewall:** Use the basic *Windows Firewall* Control Panel item (`firewall.cpl`) and select *File and printer Sharing* in the list of exceptions.
	  - OR -
	  ◆ **Option 2, using Firewall with Advanced Security:** Use the *Windows Firewall with Advanced Security* utility (`wf.msc`) with the following *Inbound Rules* enabled and set to `Allow`:
	  ◆ *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)*
		TCP 3725
		NetBIOS 137 - 139
		SMB (TCP 139, 445 and UDP 137, 138)
		TCP 135/445

Workload Type	Prerequisites	Required Ports (Defaults)
Windows Server 2003 (including SP1 Standard, SP2 Enterprise, and R2 SP2 Enterprise)	**NOTE:** After enabling the required ports, run the following command at the server prompt to enable PlateSpin remote administration: `netsh firewall set service RemoteAdmin enable` For more information about netsh, see the Microsoft TechNet article, http://technet.microsoft.com/en-us/library/cc785383%28v=ws.10%29.aspx. (http://technet.microsoft.com/en-us/library/cc785383%28v=ws.10%29.aspx).	◆ **TCP:** 3725, 135, 139, 445 ◆ **UDP:** 137, 138, 139
Windows Server 2000; Windows XP	◆ Windows Management Instrumentation (WMI) installed WMI (RPC/DCOM) can use TCP ports 135 and 445 as well as random or dynamically assigned ports above 1024. If problems occur when adding the workload, consider temporarily placing the workload in a DMZ or temporarily opening the firewalled ports while adding the workload to PlateSpin Forge. For additional information, such as guidance in limiting the port range for DCOM and RPC, see the following Microsoft technical articles. ◆ Using DCOM with Firewalls (http://msdn.microsoft.com/en-us/library/ms809327.aspx) ◆ Configuring RPC dynamic port allocation to work with firewalls (http://support.microsoft.com/default.aspx?scid=kb;en-us;154596) ◆ Configuring DCOM to work over a NAT-based firewall (http://support.microsoft.com/kb/248809)	TCP 3725 NetBIOS 137 - 139 SMB (TCP 139, 445 and UDP 137, 138) RPC (TCP 135)
All Linux workloads	Secure Shell (SSH) server	TCP 22, 3725

2.3.2 Protection Across Public and Private Networks Through NAT

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

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

- **PlateSpin Server:** In your server's *PlateSpin Server Configuration* tool, record the additional IP addresses assigned to that host. See "Configuring the Application to Function through NAT" on page 27.
- **Workload:** When you are attempting to add a workload, specify the public (external) IP address of that workload in the discovery parameters.
- **Failed-over VM:** During failback, you can specify an alternative IP address for the failed-over workload in Failback Details (Workload to VM) (page 74).
- **Failback Target:** During an attempt to register a failback target, when prompted to provide the IP address of the PlateSpin Server, provide either the local address of the Protect Server host or one of its public (external) addresses recorded in the server's *PlateSpin Server Configuration* tool (see *PlateSpin Server* above).

Configuring the Application to Function through NAT

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

For information on the update procedure, see "Configuring PlateSpin Server Behavior through XML Configuration Parameters" on page 31.

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

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

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

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

2.4 Configuring PlateSpin Forge Default Options

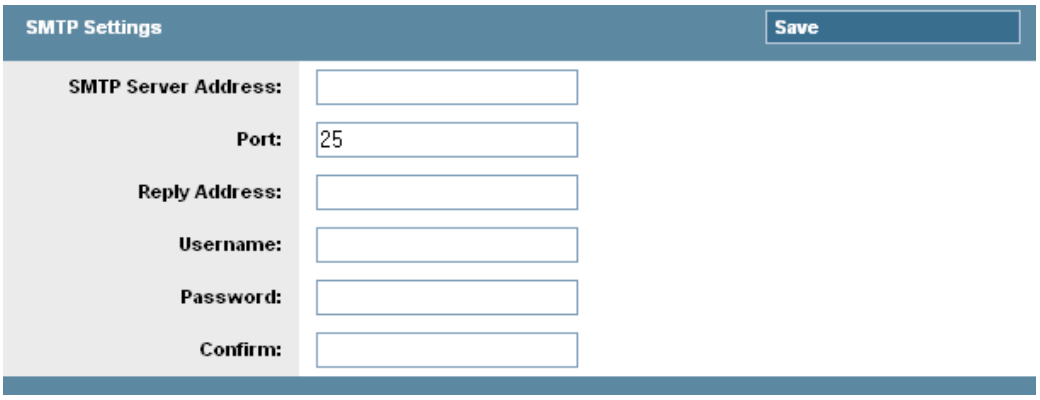
2.4.1 Setting Up Automatic Email Notifications of Events and Reports

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

SMTP Configuration

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

Figure 2-2 *Simple Mail Transfer Protocol Settings*

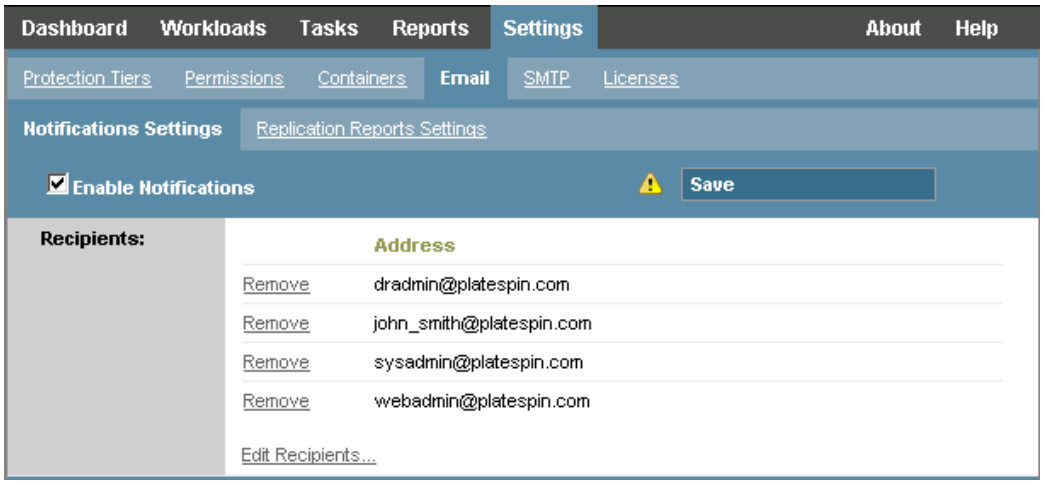


To configure SMTP settings:

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

Setting Up Automatic Event Notifications by Email

1. Set up an SMTP server for PlateSpin Forge to use. See "SMTP Configuration" on page 27.
2. In your PlateSpin Forge Web Interface, click *Settings* > *Email* > *Notification Settings*.
3. Select the *Enable Notifications* option.
4. Click *Edit Recipients*, type the required email addresses separated by commas, then click *OK*.



5. Click *Save*.

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

The following events trigger email notifications:

Event	Remarks
`Workload Online Detected`	Generated when the system detects that a previously offline workload is now online. Applies to workloads whose protection contract's state is not *Paused*.
`Workload Offline Detected`	Generated when the system detects that a previously online workload is now offline. Applies to workloads whose protection contract's state is not *Paused*.
`Full Replication Successfully Completed`	
`Full Replication Failed`	
`Full Replication Missed`	Similar to the `Incremental Replication Missed` event.
`Incremental Replication Successfully Completed`	
`Incremental Replication Failed`	
`Incremental Replication Missed`	Generated when any of the following applies: ◆ A replication is manually paused while a scheduled incremental replication is due. ◆ The system attempts to carry out a scheduled incremental replication while a manually-triggered replication is underway. ◆ The system determines that the target has insufficient free disk space.
`Test Failover Completed`	Generated upon manually marking a Test Failover operation a success or a failure.
`Prepare Failover Completed`	
`Prepare Failover Failed`	
`Failover Completed`	
`Failover Failed`	

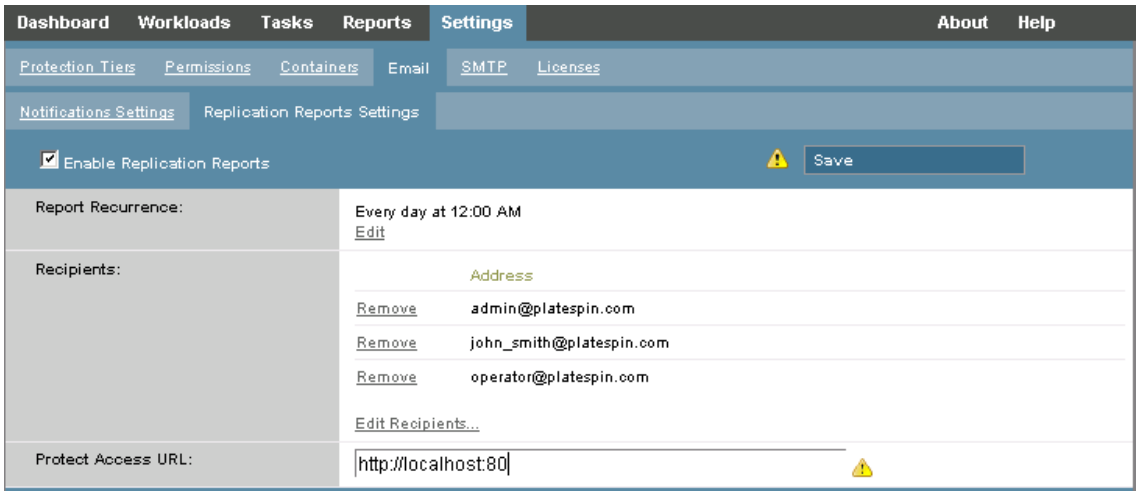
Setting Up Automatic Replication Reports by Email

To set up PlateSpin Forge to automatically send out replication reports by email, follow these steps:

1. Set up an SMTP server for PlateSpin Forge to use. See SMTP Configuration (page 27).
2. In your PlateSpin Forge Web Interface, click *Settings* > *Email* > *Replication Reports Settings*.
3. Select the *Enable Replication Reports* option.

4 In the *Report Recurrence* section, click *Configure* and specify the required recurrence pattern for the reports.

5 In the *Recipients* section, click *Edit Recipients*, type the required email addresses separated by commas, then click *OK*.



6 (Optional) In the *Protect Access URL* section, specify a non-default URL for your PlateSpin Server (for example, when your Forge VM has more than one NIC or if it is located behind a NAT server). This URL affects the title of the report and the functionality of accessing relevant content on the server through hyperlinks within emailed reports.

7 Click *Save*.

For information on other types of reports that you can generate and view on demand, see "Generating Workload and Workload Protection Reports" on page 61.

2.4.2 Language Setup for International Versions of PlateSpin Forge

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

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

1 Access the Languages setting in your Web browser:

- **Internet Explorer:** Click *Tools* > *Internet Options* > *General* tab > *Languages*.
- **Firefox:** Click *Tools* > *Options* > *Content* tab > *Languages*.

2 Add the required language and move it up the top of the list.

3 Save the settings, then start the client application by connecting to your PlateSpin Forge Server. See "Launching the PlateSpin Forge Web Interface" on page 53.

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

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

1. Access your Forge VM.

   See Section 3.4.1, "Accessing and Working with the Forge Management VM in the Appliance Host," on page 42.
2. Start the Regional and Language Options applet (click *Start* > *Run*, type `intl.cpl`, and press Enter), then click the *Languages* (Windows Server 2003) or *Keyboards and Languages* (Windows Server 2008) tab, as applicable.
3. If it is not already installed, install the required language pack. You might need access to your OS installation media.
4. Select the required language as the interface language of the operating system. When you are prompted, log out or restart the system.

2.4.3 Configuring PlateSpin Server Behavior through XML Configuration Parameters

Some aspects of your PlateSpin Server's behavior are controlled by configuration parameters that you set on a configuration Web page residing on your Forge VM (`https://Your_Forge_VM/platespinconfiguration/`).

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

Use the following procedure for changing and applying any configuration parameters:

1. On your Forge VM, go to the indicated directory.
2. Locate the required server parameter and change its value.
3. Save and your settings and exit the page.

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

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

- "Optimizing Data Transfer over WAN Connections" on page 31
- "Setting up Support for SRM" on page 32

Optimizing Data Transfer over WAN Connections

You can optimize data transfer performance and fine tune it for WAN connections. You do this by modifying configuration parameters that the system reads from settings you make in a configuration tool residing on your Forge VM. For the generic procedure, see "Configuring PlateSpin Server Behavior through XML Configuration Parameters" on page 31.

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

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

Table 2-3 lists the configuration parameters with the defaults and with the values recommended for optimum operation in a high-latency WAN environment.

Table 2-3 *Default and Optimized Configuration Parameters in* `https://Your_Forge_VM/platespinconfiguration/`

Parameter	Default Value	Optimized Value
`fileTransferMinCompressionLimit` Specifies the packet-level compression threshold in bytes.	0 (disabled)	max 65536 (64 KB)
`fileTransferCompressionThreadsCount` Controls the number of threads used for packet-level data compression. This is ignored if compression is disabled. Because the compression is CPU-bound, this setting might have a performance impact.	2	N/A

`fileTransferSendReceiveBufferSize`
 	
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:
 	
((LINK_SPEED(Mbps)/8)*DELAY(sec))*1000*1000
 	
For example, for a 100 Mbps link with 10 ms latency, the proper buffer size would be:
 	
`(100/8)*0.01*1000*1000 = 125000 bytes`
	0 (8192 bytes)	max 5242880 (5 MB)

Setting up Support for SRM

Workloads replicated by PlateSpin Forge and managed on VMware vCenter Site Recovery Manager (SRM) can behave seamlessly if you configure the product to support SRM. Some of the configuration requires a change to the XML configuration parameters of the PlateSpin Server. For information about these configuration changes, see the complete section: Section 2.4.4, “Configuring Support for VMware vCenter Site Recovery Manager,” on page 33

2.4.4 Configuring Support for VMware vCenter Site Recovery Manager

You might use PlateSpin Forge to protect your workloads locally and then use some additional method to replicate those workloads to a remote location, such as a SAN. For example, you might choose to use VMware vCenter Site Recovery Manager (SRM) to replicate an entire datastore of replicated target VMs to a remote site. In this case, specific configuration steps are needed to ensure that the target VMs can be replicated and behave correctly when powered on at the remote site.

Configuration for Forge SRM support consists of the following adjustments:

- Configure a setting to keep the PlateSpin Forge ISO and floppies on the same datastore as the VMware `.vmx` and `.vmdk` files.
- Prepare the PlateSpin Forge environment to copy VMware Tools to the failover target. This involves some manual file creation and copying in addition to making some configuration settings that expedite the VMware Tools installation process.

Use the following steps to make sure the workload files are kept on the same datastore:

1. From any Web browser, open `https://`*`Your_PlateSpin_Server`*`/platespinconfiguration/` to display the configuration Web page.
2. On the configuration Web page, locate the `CreatePSFilesInVmDatastore` server parameter and change its value to `true`.

   NOTE: The person configuring the replication contract is responsible to ensure that the same datastore is specified for all target VM disk files.

3. Save your settings and exit the page.

VMware Tools setup packages can be copied to the failover target during replication so that they can be installed by the configuration service when the VM is booted. This happens automatically when the failover target is able to contact the PlateSpin Forge Server. In cases where this cannot happen, you need to prepare your environment prior to replication by following these steps:

1. Retrieve the VMware Tools packages from an ESX host:
   - **1a** Secure copy (`scp`) the `windows.iso` image from the `/usr/lib/vmware/isoimages` directory on an accessible VMware host to a local temporary folder.
   - **1b** Open the ISO and extract its setup packages, saving them to an accessible location:
     - **VMware 5.0 and 5.1:** The setup packages are `setup.exe` and `setup64.exe`.
     - **VMware 4.0 and 4.1:** The setup packages are `VMware Tools.msi` and `VMware Tools64.msi`.
2. Create OFX packages from the setup packages you extracted from the VMware Server:
   - **2a** Zip the package you want, making sure that the setup installer file is at the root of the `.zip` archive.
   - **2b** Rename the `.zip` archive to `1.package` so that it can be used as an OFX package.

     NOTE: If you want to create an OFX package for more than one of the setup packages, remember that each setup package must have its own unique `.zip` archive.

     Because each package must have the same name (`1.package`), if you want to save multiple `.zip` archives as OFX packages, you need to save each in its own unique subdirectory.
3. Copy the appropriate OFX package (`1.package`) to `%ProgramFiles(x86)%\PlateSpin\Packages\%`*`GUID`*`%` on the PlateSpin Server. The value of `%`*`GUID`*`%` depends on the version of your VMware Server and its VMware Tools architecture.

The following table lists the server versions, VMware Tools architecture and the GUID identifier you need to copy the package to the correct directory:

VMware Server Version	VMware Tools Architecture	GUID
4.0	x86	D052CBAC-0A98-4880-8BCC-FE0608F0930F
4.0	x64	80B50267-B30C-4001-ABDF-EA288D1FD09C
4.1	x86	F2957064-65D7-4bda-A52B-3F5859624602
4.1	x64	80B1C53C-6B43-4843-9D63-E9911E9A15D5
5.0	x86	AD4FDE1D-DE86-4d05-B147-071F4E1D0326
5.0	x64	F7C9BC91-7733-4790-B7AF-62E074B73882
5.1	x86	34DD2CBE-183E-492f-9B36-7A8326080755
5.1	x64	AD4FDE1D-DE86-4d05-B147-071F4E1D0326

Expediting the Configuration Process

After the failover target boots, the configuration service launches to prepare the VM for use, but sits inactive for several minutes, waiting for data from the PlateSpin Server or looking for VMware Tools on the CD ROM. To shorten this wait time,

1. On the configuration Web page, locate the `ConfigurationServiceValues` configuration setting, and then change the value of its `WaitForFloppyTimeoutInSecs` subsetting to zero (0).
2. On the configuration Web page, locate the `ForceInstallVMToolsCustomPackage` and change the value to `true`.

With these settings in place, the configuration process takes less than 15 minutes: the target machine reboots (up to two times), the VMware tools are installed, and SRM accesses the tools to help it configure networking at the remote site.

3 Appliance Setup and Maintenance

This section provides information about appliance setup and maintenance tasks that you might need to complete on a regular basis.

3.1 Setting up Appliance Networking

This section provides information about customizing the networking settings of your appliance host.

3.1.1 Setting up Appliance Host Networking

Your PlateSpin Forge appliance has six physical network interfaces configured for external access:

- **External Test Network:** To isolate network traffic when testing a failover workload with the Test Failover feature.
- **Internal Test Network:** For testing a failover workload in complete isolation from the production network.
- **Replication Network:** To provide the system with networking designated for ongoing traffic between your production workload and its replica in the Management VM.
- **Production Network:** For real-life business continuity networking when performing a failover or a failback.
- **Management Network:** The Forge Management VM network.
- **Appliance Host Network:** Hypervisor management network. This network is unavailable for selection in the PlateSpin Forge Web Client.

By default, PlateSpin Forge ships with all 6 physical network interfaces mapped to one vSwitch in the hypervisor. You can customize the mapping to better suit your environment. For example, you can protect a workload that has two NICs, one of which is used for production connectivity, and the other strictly for replications. For additional information, see KB Article 7921062 (https://www.netiq.com/support/kb/doc.php?id=7921062).

In addition, to further fine-tune the control of your network traffic, consider assigning a different VLAN ID to each of these individual port groups. This ensures that your production network is not interfered with by traffic from workload protection and recovery operations. See KB Article 21057 (https://www.netiq.com/support/kb/doc.php?id=7921057).

3.2 Relocating PlateSpin Forge and Reassigning Its IP Addresses

Relocating your PlateSpin Forge appliance involves changing the IP addresses of its components to reflect the new environment. These are the IP addresses you specified during the initial setup of the appliance (see your *Forge Getting Started Guide*).

The procedure varies depending on the *appliance version* (1 or 2). For information on how to determine the appliance version of your unit, see "*Determining your Unit's Appliance Version*" in your *Forge Getting Started Guide*.

- Section 3.2.1, "Forge Relocation Procedure for Appliance Version 2," on page 36
- Section 3.2.2, "Forge Relocation Procedure for Appliance Version 1," on page 40

3.2.1 Forge Relocation Procedure for Appliance Version 2

Before starting the relocation procedure:

1 Pause all replication schedules, ensuring that at least one incremental has run for each workload:

   1a In your PlateSpin Forge Web Client, select all workloads, click *Pause*, then click *Execute*.

   1b Ensure that the status *Paused* is displayed for all the workloads.

The specifics of the relocation process vary depending on whether the new IP address of the appliance at the target site is known (scenario 1) or unknown (scenario 2).

- "Scenario 1 - Relocating Forge (New IP Address Known)" on page 36
- "Scenario 2 - Relocating Forge (New IP Address Unknown)" on page 38

Scenario 1 - Relocating Forge (New IP Address Known)

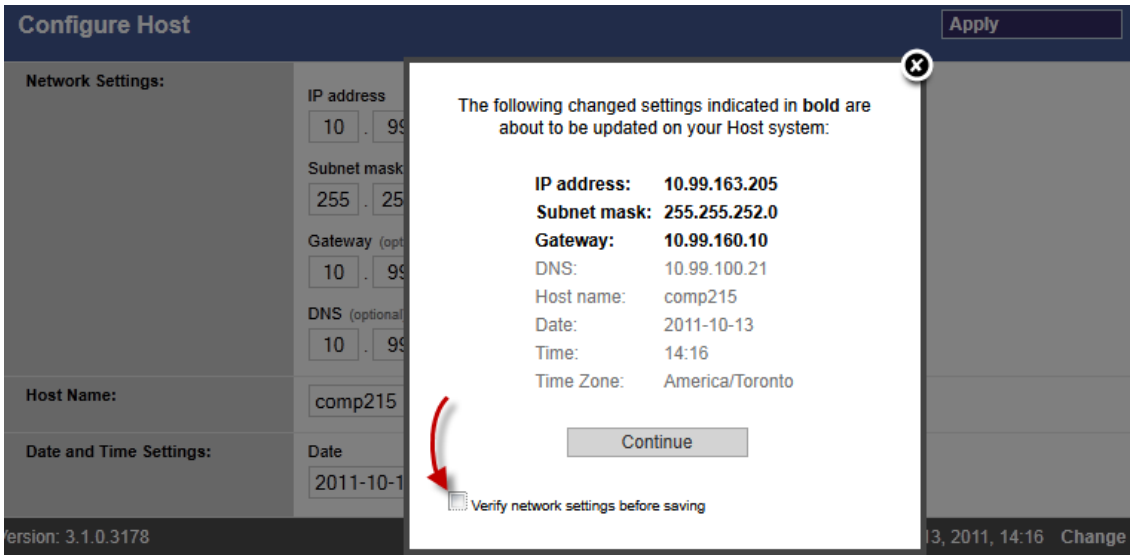
1 Pause all replications. See Step 1a and Step 1b above.

2 Launch the Forge Appliance Configuration Console (ACC): open a browser and go to `http://<Forge_IP_address>:10000`.

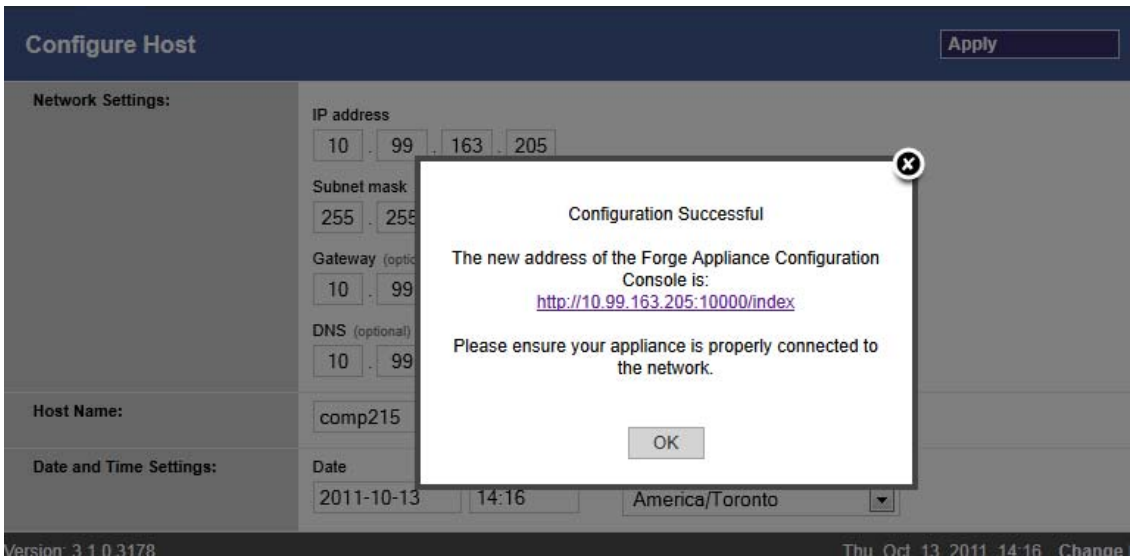
3 Log in using the `forgeuser` account and click *Configure Host*.

4 Enter the new network parameters and click *Apply*.

5 In the confirmation popup window, ensure that the new settings are correct, deselect the *Verify network settings before saving*, then click *Continue*.



6 Wait for the configuration process to complete and for the browser window to display the Configuration Successful popup window.



NOTE: The link in the popup window for the new ACC address will not work until you now physically disconnect your appliance and connect it to the new subnet.

7 Shut down the appliance:

7a Shut down the Forge Management VM. See "Starting and Shutting Down the Forge Management VM" on page 44.

7b Shut down the Appliance Host:

7b1 At the Forge Console, switch to the ESX Server console by pressing Alt-F2.

7b2 Log in as the superuser (user `root` with the associated password).

7b3 Type the following command and press Enter:

```
shutdown -h now
```

7c Power the appliance down.

8 Disconnect your appliance, move it to the new site, attach it to the new subnet, and power it on.

The new IP address should now be valid.

9 Launch the ACC and log in using the `forgeuser` account, click *Configure Forge VM*, specify the required parameters, then click *Apply*.

10 Verify that the setting are correct, click *Continue*, and wait for the process to complete.

NOTE: If you configured the Forge VM to use DHCP, do the following after the relocation:

1. Determine the Forge VM's new IP address (use the VMware client program to access the Forge VM and look it up in the VM's Windows interface. See "Launching the VMware Client and Accessing the Forge Management VM" on page 43).

2. Use the new IP address to launch the PlateSpin Forge Web Interface and refresh the container (click *Settings* > *Containers* > *then click* ↻).

---

11 Resume the paused replications.

Scenario 2 - Relocating Forge (New IP Address Unknown)

1 Pause all replications. See Step 1 on page 36.

2 Shut down the appliance:

- **2a** Shut down the Forge Management VM. See "Starting and Shutting Down the Forge Management VM" on page 44.
- **2b** Shut down the Appliance Host:
  - **2b1** At the Forge Console, switch to the ESX Server console by pressing Alt-F2.
  - **2b2** Log in as the superuser (user `root` with the associated password).
  - **2b3** Type the following command and press Enter:

    ```
    shutdown -h now
    ```
- **2c** Power the appliance off.

3 Disconnect your appliance, move it, attach to the new network, then power it on.

4 Set up a computer (notebook computer recommended) so that it is able to communicate with Forge at its current IP address (the IP address at the old site), then connect it to the appliance.

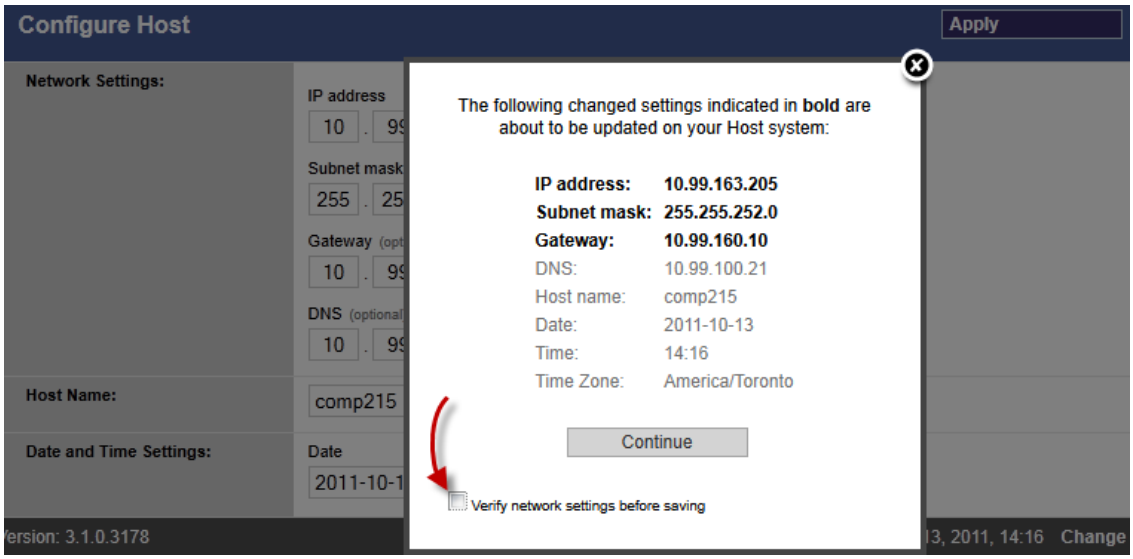
See Appliance v2 Configuration Procedure Using the Forge ACC in your *Getting Started Guide*.

5 Launch the Forge Appliance Configuration Console (ACC): open a browser and go to `http://<Forge_IP_address>:10000`.

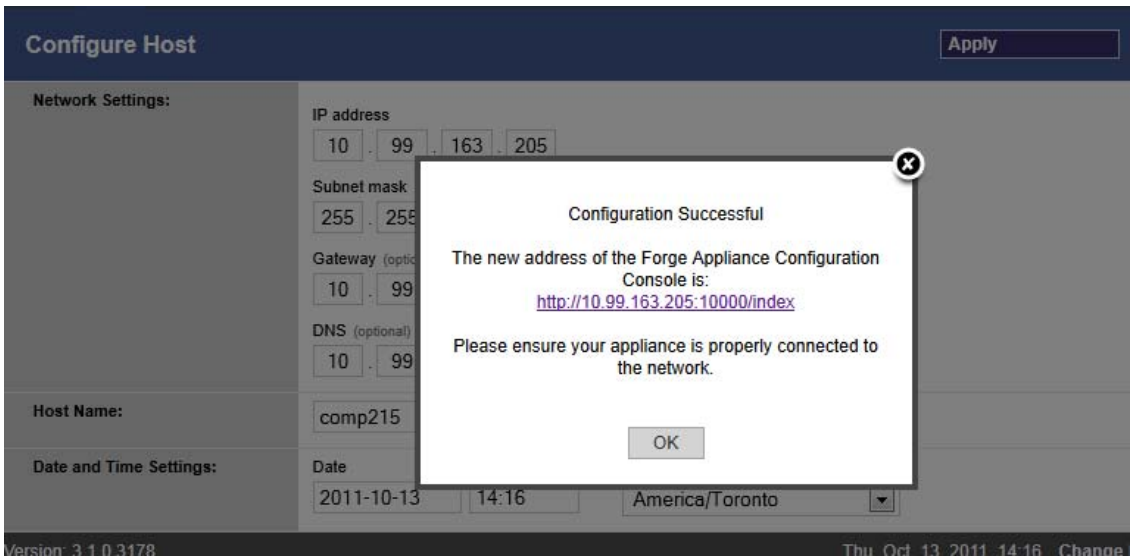
6 Log in using the `forgeuser` account and click *Configure Host*.

7 Enter the new network parameters and click *Apply*.

8 In the confirmation popup window, ensure that the new settings are correct, deselect the *Verify network settings before saving*, then click *Continue*.



9 Wait for the configuration process to complete and for the browser window to display the Configuration Successful popup window.



NOTE: The link in the popup window for the new ACC address will not work until you now physically disconnect your appliance and connect it to the new subnet.

10 Disconnect the computer from the appliance and connect the appliance to the new subnet.

The new IP address should now be valid.

11 Launch the ACC and log in using the `forgeuser` account, click *Configure Forge VM*, specify the required parameters, then click *Apply*.

12 Verify that the setting are correct, click *Continue*, and wait for the process to complete.

NOTE: If you configured the Forge VM to use DHCP, do the following after the relocation:

1. Determine the Forge VM's new IP address (use the VMware client program to access the Forge VM and look it up in the VM's Windows interface. See "Launching the VMware Client and Accessing the Forge Management VM" on page 43).

2. Use the new IP address to launch the PlateSpin Forge Web Interface and refresh the container (click *Settings* > *Containers* > *then click*).

13 Resume the paused replications.

3.2.2 Forge Relocation Procedure for Appliance Version 1

1 Pause all replication schedules, ensuring that at least one incremental has run for each workload:

- **1a** In your PlateSpin Forge Web Client, select all workloads, click *Pause*, then click *Execute*.
- **1b** Ensure that the status *Paused* is displayed for all the workloads.

2 Shut down the Forge Management VM. See "Starting and Shutting Down the Forge Management VM" on page 44.

3 Shut down the Appliance Host:

- **3a** At the Forge Console, switch to the ESX Server console by pressing Alt-F2 (to switch back to the Forge Console, press Alt-F1).
- **3b** Log in as the superuser (`root` and the associated password).
- **3c** Type the following command and press Enter:

  ```
  shutdown -h now
  ```

- **3d** Power the appliance off.

4 Move the appliance to the new location, set up the hardware, make the required cable connections, then power the appliance on.

5 Update the appliance network configuration:

- **5a** At the Forge console, log in as the superuser (`root` and the associated password).
- **5b** Update the *IP address, Netmask, and Gateway IP address* settings for the appliance host as required. You can use DHCP, but only if a static IP lease is enabled. For multiple appliance environments, assign unique hostnames to the appliances to avoid hostname conflicts.
- **5c** Update the *IP address, Netmask, Gateway IP address* and domain affiliation settings for the Forge Management VM as required.
- **5d** Select *OK*, review the updates, then select *OK* again.

6 Update the network settings for the paused replications; in your PlateSpin Forge Web Client, do the following for each paused workload:

- **6a** Access the Replication Settings section in the paused workload's protection details.
- **6b** Update the *Replication Network* value to reflect the network change.
- **6c** Save the settings.

7 Resume replications: in your PlateSpin Forge Web Client, select all workloads, click *Resume Schedule*, then click *Execute*.

3.3 Using External Storage Solutions with PlateSpin Forge

The following sections contain information to help you with the setup and configuration of external storage for PlateSpin Forge.

3.3.1 Using Forge with SAN Storage

PlateSpin Forge 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 workload data. 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 the Forge 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/).

- 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 (http://www.fujitsu.com)
- HP (http://www.hp.com)
- Hitachi (http://www.hitachi.com) and Hitachi Data Systems (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.xiotech.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/.

3.3.2 Adding a SAN LUN to Forge

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

1. Set up and configure your SAN system.
2. Access the appliance host (see "Downloading the VMware Client Program" on page 43).
3. In the VMware client interface, click the root (top-level) node in the Inventory panel, then click the *Configuration* tab.
4. Click the *Add Storage* hyperlink in the upper right.
5. In the Add Storage Wizard, click *Next* until you are prompted to specify datastore information.
6. Specify a datastore name and click *Next* in the subsequent wizard pages. When the wizard finishes, click *Finish*.
7. Click *Storage* under *Hardware* to see the Forge datastores. The newly added SAN LUN should appear in the window.
8. Quit the VMware client program.

In the PlateSpin Forge Web Client, the new datastore doesn't appear until the next replication runs and the Application Host is refreshed. You can force a refresh by selecting *Settings* > *Containers* and clicking  near the appliance hostname.

3.4 PlateSpin Forge Appliance Maintenance

Topics in this section provide information about tasks that deal with PlateSpin Forge appliance maintenance.

- Section 3.4.1, "Accessing and Working with the Forge Management VM in the Appliance Host," on page 42

3.4.1 Accessing and Working with the Forge Management VM in the Appliance Host

Occasionally you might need to access the Forge Management VM and perform maintenance tasks as described here or when you are advised to do so by PlateSpin Support.

Use the VMware client software to access the Forge Management VM, including its OS interface and VM settings.

NOTE: The VMware client software differs between ESX version 3.5 (Forge appliance version 1 systems) and ESX version 4.1 (Forge appliance version 2 systems.

- ESX 3.5 requires the VMware Virtual Infrastructure Client (VIC)
- ESX 4.1 requires the VMware vSphere Client

For convenience and ease of reference, these programs are sometimes referred to as *VMware Client*. In addition, the terms *Virtual Infrastructure Client (VIC)* and *vSphere Client* might be used interchangeably.

- "Downloading the VMware Client Program" on page 43
- "Launching the VMware Client and Accessing the Forge Management VM" on page 43

Downloading the VMware Client Program

Download the client software from the appliance host and install it on a Windows workstation external to PlateSpin Forge.

1 Download the client software:

- (Conditional: for Forge appliance version 2 with VMware ESX 4.1) Download the VMware vSphere Client) program (http://vsphereclient.vmware.com/vsphereclient/3/4/5/0/4/3/VMware-viclient-all-4.1.0-345043.exe).

  OR

- (Conditional: for Forge appliance version 1 with VMwre ESX 3.5) Open a Web browser and go to the home page of the appliance host (VMware ESX), using the appliance host's IP address. Ignore the warning related to the security certificate. On the VMWare ESX Server's Welcome page, click the *Download Virtual Infrastructure Client* hyperlink, and dowload the installation program.

2 Launch the downloaded installation program and follow the instructions to install the software.

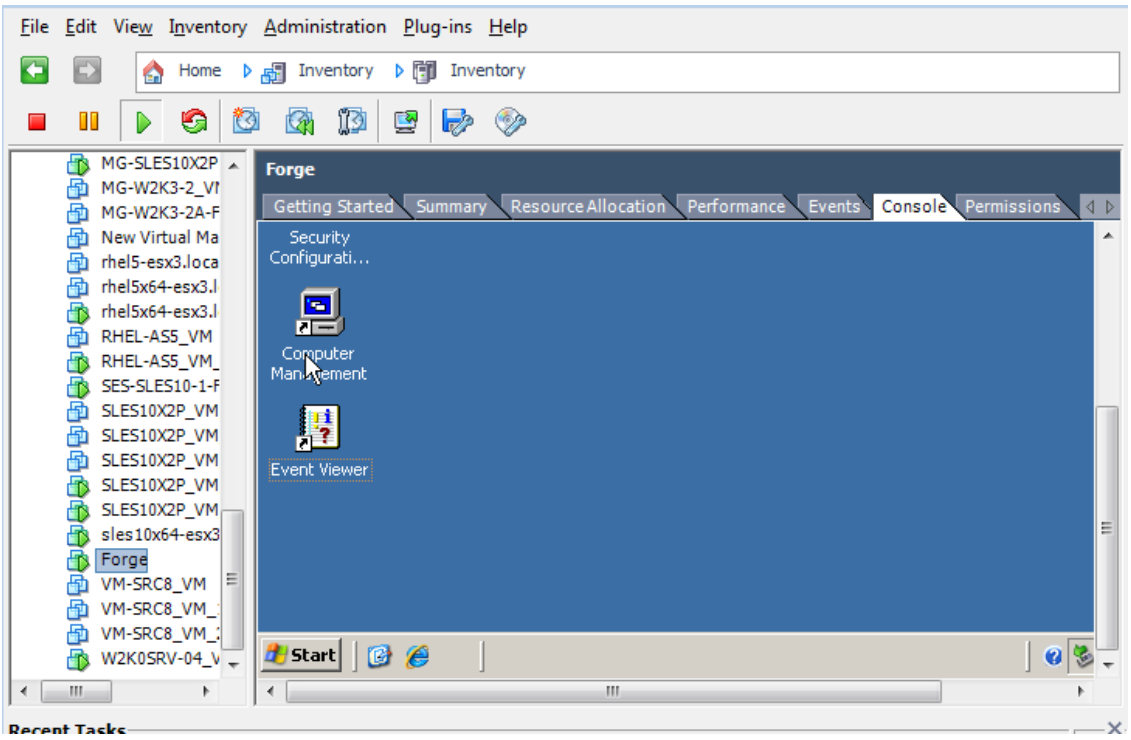
Launching the VMware Client and Accessing the Forge Management VM

1 Clicking *Start* > *Programs* > *VMWare* > *VMware vSphere* | *Virtual InfrastrucureClient*.

The VMware client login window is displayed.

2 Specify your administrator-level credentials and log in, ignoring any certificate warnings.

The VMware client program opens.



3 In the inventory panel at the left, locate and select the *PlateSpin Forge VM* item. At the top of the right panel, click the *Console* tab.

   The Client's console area displays the Forge Management VM's Windows interface.

Use the console to work with the Management VM the same way as you would work with Windows on a physical machine.

To unlock the Management VM, click inside the console and press Ctrl+Alt+Insert.

To release the cursor for working outside the VMware client program, press Ctrl+Alt.

Starting and Shutting Down the Forge Management VM

Occasionally you might need to shut down and then restart the Forge Management VM, such as when you relocate the appliance.

1 Use the VMware Client to access the Forge Management VM host. See "Downloading the VMware Client Program" on page 43.

2 Use the standard Windows procedure to shut down the VM (*Start* > *Shut Down*).

To restart the Management VM:

1. In the inventory panel at the left, right-click the *PlateSpin Forge Management VM* item and select *Power on*.

Managing Forge Snapshots on the Appliance Host

Occasionally you might need to take a point-in-time snapshot of your management VM, such as when you upgrade Forge software or when carry out troubleshooting tasks. You might also need to remove snapshots (recovery points) to free storage space.

1. Use the VMware Client to access the appliance host. See "Downloading the VMware Client Program" on page 43.
2. In the inventory panel at the left, right-click the *PlateSpin Forge Management VM* item and select *Snapshot* > *Take Snapshot*.
3. Type a name and a description for the snapshot, then click *OK*.

To revert the management VM to a previous state:

1. In the inventory panel at the left, right-click the *PlateSpin Forge Management VM* item and select *Snapshot* > *Snapshot Manager*.
2. In the tree representation of the VM states, select a snapshot, then click *Go to*.

To remove snapshots that represent recovery points:

1. In the inventory panel at the left, right-click the *PlateSpin Forge Management VM* item and select *Snapshot* > *Snapshot Manager*.
2. In the tree representation of the VM states, select a snapshot, then click *Remove*.

Manually Importing VMs into the Appliance Host's Datastore

Use this procedure to manually import a VM into the appliance host's datastore. You might want to consider this option when you want your failover workload to be created differentially (see "Initial Replication Method (Full and Incremental)" on page 81).

1. At the production site, create a VM (ESX 3.5 and later) from your production workload (for example, by using PlateSpin Migrate) and copy the VM files from the ESX host's datastore to portable media, such as a portable hard drive or a USB flash drive. Use the Datastore Browser of the client software to browse and locate the files.
2. At the disaster recovery site, attach the media to a workstation that has network access to Forge and has the VMware client program installed. See "Downloading the VMware Client Program" on page 43.
3. Use the VMware Client's Datastore Browser to access the Forge datastore (*Storage1*) and upload the VM files from the temporary media. Use the uploaded VM to register it with the appliance host (right-click > *Add to Inventory*).
4. Refresh the PlateSpin Forge inventory (in the PlateSpin Forge Web Client, click *Settings* > *Containers*, then click adjacent to the appliance host).

Guidelines for Applying Security Updates to the PlateSpin Forge Management VM

This section provides general guidelines for applying security patches to the Forge Management VM.

1. During a maintenance window, access the Forge Management VM by using the VMware VMware client program. See "Downloading the VMware Client Program" on page 43.
2. From within the Forge Management VM's Windows interface, check for security updates from Microsoft.
3. Use the PlateSpin Forge Web Client to put PlateSpin Forge into maintenance mode by pausing all replication schedules and ensuring that any incomplete replications are complete.
4. Take a snapshot of the Forge Management VM. See "Managing Forge Snapshots on the Appliance Host" on page 45.
5. Download and install the required security patches. When the installation finishes, reboot the Forge Management VM.
6. Use the PlateSpin Forge Web Client to resume replications paused in Step 3 and verify that replications are working properly.
7. Remove the snapshot of the Forge Management VM that you took in Step 4. See "Managing Forge Snapshots on the Appliance Host" on page 45.

3.5 Upgrading PlateSpin Forge

You can upgrade your Forge software from versions 3.3 and 3.4.

The rest of this section provides information about upgrading your PlateSpin Forge appliance.

3.5.1 Before Starting the Upgrade

Before starting the upgrade, make sure that you have the following prerequisites:

- The Forge setup installation executable.
- IP addresses and appropriate credentials for:
  - The Forge appliance (used for the Forge Web Client Interface and the Forge Management VM)
  - The Forge Appliance Host (VMware ESX server)
- The VMware client program. See "Downloading the VMware Client Program" on page 43.

3.5.2 Summary of Upgrade Tasks

To upgrade your Forge appliance, you need to perform the following tasks in order:

1. Ensure that no replications are currently running or are scheduled to run during the upgrade.
2. Save the current state of the management VM by taking a snapshot.

3. Update the Forge Management VM with the Microsoft .NET Framework software and any security patches.
4. Copy and run the required setup executable locally within the Forge Management VM.
5. Verify proper operation of the appliance after the upgrade.

3.5.3 Forge Upgrade Procedure

This phase involves pausing all scheduled replications of protected workloads and waiting for running replications to complete.

1. Use the PlateSpin Forge Web Client to pause all scheduled replications. Wait for any replications that are underway to complete. Ensure that the replication status of protected workloads is *idle* in the Replication Status column.

   See "Launching the PlateSpin Forge Web Interface" on page 53.
2. Power off the Forge Management VM. See "Starting and Shutting Down the Forge Management VM" on page 44.
3. Back up the Forge Management VM by creating a snapshot. See "Managing Forge Snapshots on the Appliance Host" on page 45.
4. Power on the Forge Management VM, access it with the VMware client program, and do the following:
   - **4a** Install the Microsoft .NET Framework software. Forge 4 requires Microsoft .NET Framework 3.5, SP1 and Microsoft .NET Framework 4.0.
   - **4b** Update Windows, applying any available security updates.
   - **4c** Reboot the Forge Management VM.
5. Run the Forge setup installation executable within the Forge Management VM and follow the on-screen instructions.
6. Use the PlateSpin Forge Web Client to resume all paused replications.
7. Use the VMware client program to remove the snapshot created in Step 3.

IMPORTANT: Drivers that were uploaded to the PlateSpin Forge driver database for failback are not preserved. Any such drivers need to be uploaded again after the upgrade.

3.6 Resetting Forge to Factory Defaults

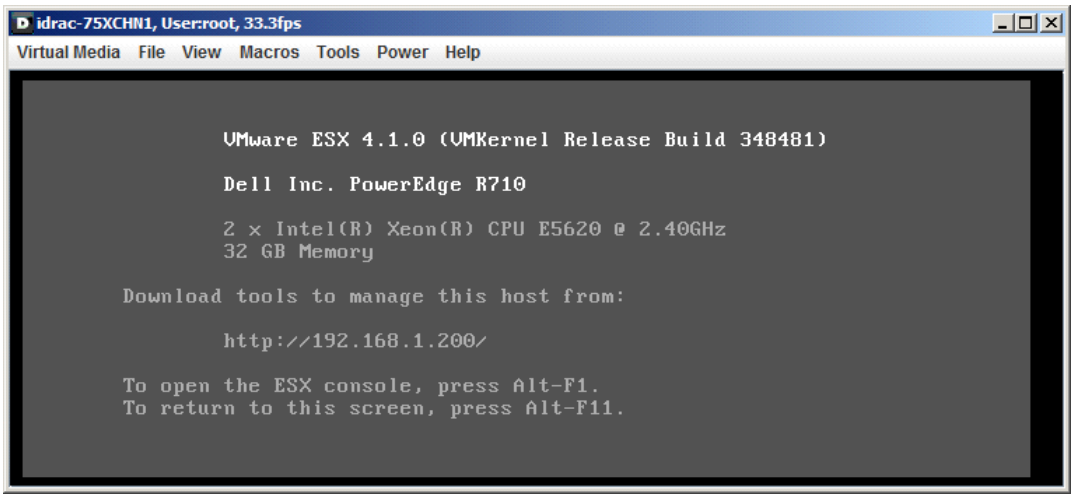
This section provides information on resetting your Forge 4, Appliance Version 2 unit to its factory default state.

Depending on your Forge model, this process might take 20 to 45 minutes or longer.

1. Disconnect all external/remote/shared storage systems from Forge (iSCSI, FiberChannel, NFS).
2. Disconnect all network cables from Forge.

   WARNING: If you are performing a factory reset on multiple Forge appliances connected to the same physical switch, skipping this step might cause IP address conflicts and result in failure.

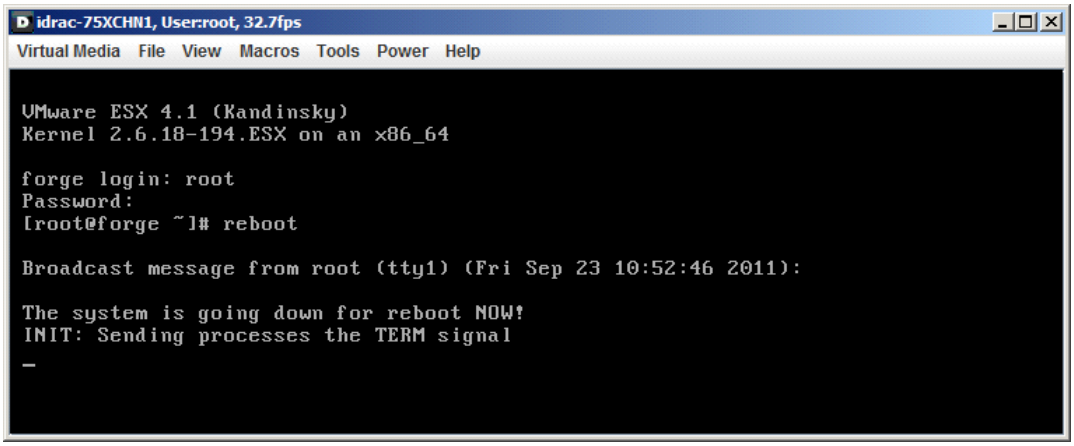
   ---
3. Reboot the appliance host:
   - **3a** Log in to the hypervisor (VMware ESX) either directly or by using DRAC.
   - **3b** Press Alt+F1 to open the ESX console.



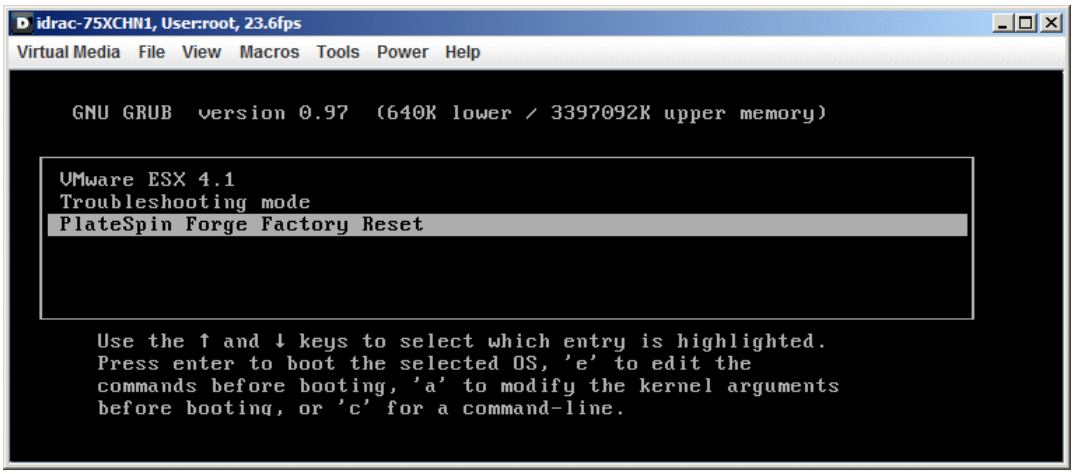
IMPORTANT: You need to remember the factory reset IP address of the appliance. You will need this address to log in to the ACC and "relocate" the container to a known, valid IP address. Use the procedure documented in Section 3.2.1, "Forge Relocation Procedure for Appliance Version 2," on page 36 to reset the IP properly.

3c Log in with your administrator-level credentials.

3d Type `reboot` and press Enter:

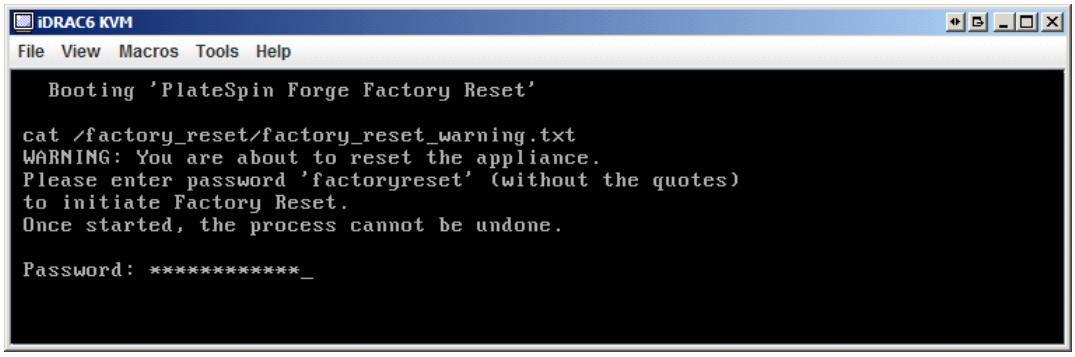


3e Wait until the reboot process is complete and the GRUB menu is displayed:



4 Select the *PlateSpin Forge Factory Reset* option and press Enter. Make sure that you do this before the default configuration is automatically applied. (about 25 seconds).

5 Follow the on-screen instructions, type the reset password (`factoryreset`) when prompted, and press Enter.

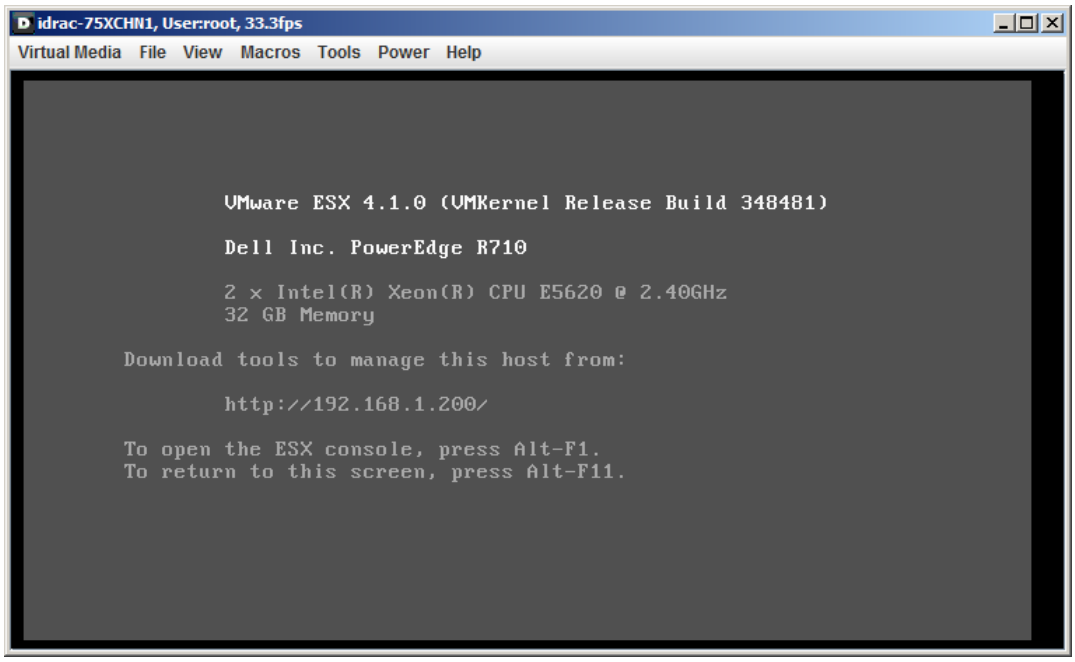


The system starts the reset process.

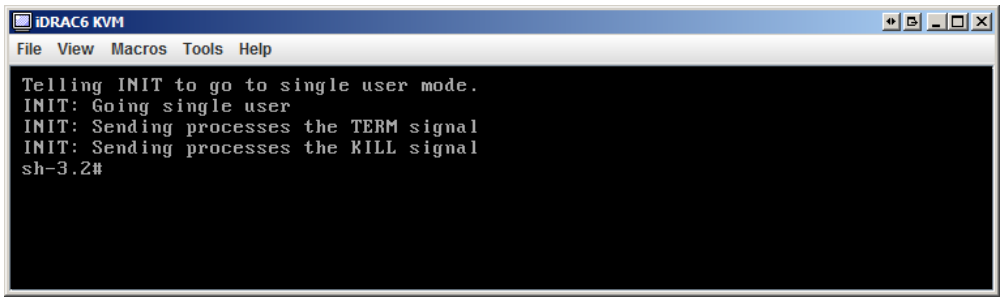
6 Wait for the Factory Reset process to complete.

NOTE: During the Factory Reset process, the appliance reboots twice. Allow the appliance to boot by itself using the default boot configuration (`VMware ESX 4.1`). Don't select the `PlateSpin Forge Factory Reset` option a second time.

If the reset process is successful, the command prompt window should look similar to the one below:



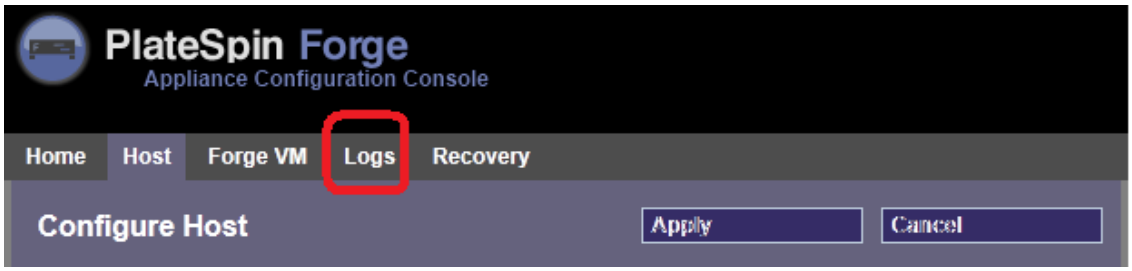
If the reset process is unsuccessful, the screen might look like the following:



In case of failure:

- Call PlateSpin Support and be prepared to provide the log files. Log files required for troubleshooting the reset process are:
  - `/var/log/forge/forge-recovery.log`
  - `/var/log/forge/INSTALL_LOG.log`
  - `/var/log/weasel.log`

  The contents of these log files should also be available through the Forge Appliance Configuration Console (ACC) interface.



- Consider rebuilding Forge using a Field Rebuild Kit that you can obtain from PlateSpin Support.

4 Up and Running

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

4.1 Launching the PlateSpin Forge Web Interface

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

The supported browsers are:

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

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

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

To launch the PlateSpin Forge Web Interface:

1 Open a Web browser and go to:

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

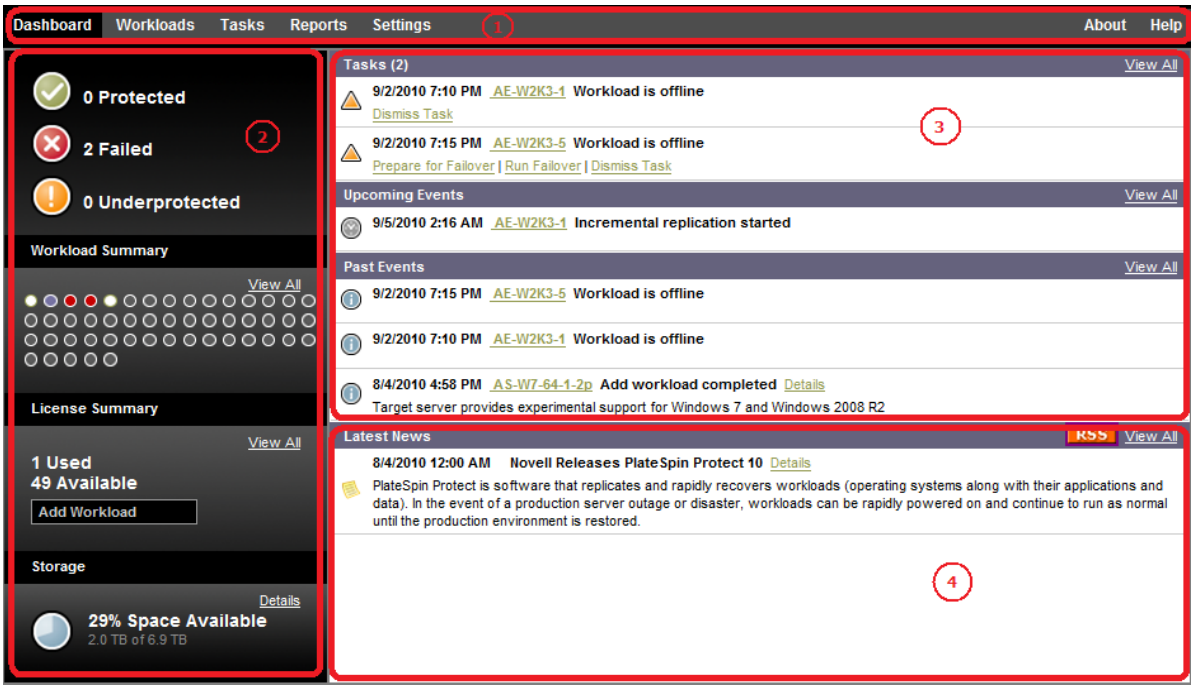
Replace <*hostname | IP_address*> with the hostname or the IP address of your Forge VM.

If SSL is not enabled, use `http` in the URL.

4.2 Elements of the PlateSpin Forge Web Interface

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

Figure 4-1 *The Default Dashboard Page of the PlateSpin Forge Web Interface*



The Dashboard page consists of the following elements:

1. **Navigation bar:** Found on most pages of the PlateSpin Forge Web Interface.
2. **Visual Summary panel:** Provides a high-level view of the overall state of the PlateSpin Forge workload inventory,
3. **Tasks and Events panel:** Provides information about events and tasks requiring user attention.

The following topics provide more details:

- Section 4.2.1, “Navigation Bar,” on page 55
- Section 4.2.2, “Visual Summary Panel,” on page 55
- Section 4.2.3, “Tasks and Events Panel,” on page 56

4.2.1 Navigation Bar

The Navigation bar provides the following links:

- **Dashboard:** Displays the default Dashboard page.
- **Workloads:** Displays the Workloads page. See "Workloads and Workload Commands" on page 56.
- **Tasks:** Displays the Tasks page, which lists items requiring user intervention.
- **Reports:** Displays the Reports page. See "Generating Workload and Workload Protection Reports" on page 61.
- **Settings:** Displays the Settings page, which provides access to the following configuration options:
  - **Protection Tiers:** See "Protection Tiers" on page 79.
  - **Permissions:** See "Setting Up User Authorization and Authentication" on page 20.
  - **Email/SMTP:** See "Setting Up Automatic Email Notifications of Events and Reports" on page 27.
  - **Licenses/License Designations:** See "Product Licensing" on page 19.

4.2.2 Visual Summary Panel

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

Inventoried workloads are represented by three categories:

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

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

Table 4-1 *Dot Icon Workload Representation*

Unprotected	*Underprotected*
Unprotected – Error	*Failed*
Protected	*Expired*
Unused	

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

Storage provides information about container storage space available to PlateSpin Forge.

4.2.3 Tasks and Events Panel

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

Events are logged whenever something relevant to the system or to the workload occurs. For example, an event could be the addition of a new protected workload, the replication of a workload starting or failing, or the detection of the failure of a protected workload. Some events generate automatic notifications by email if SMTP is configured. See "Setting Up Automatic Email Notifications of Events and Reports" on page 27.

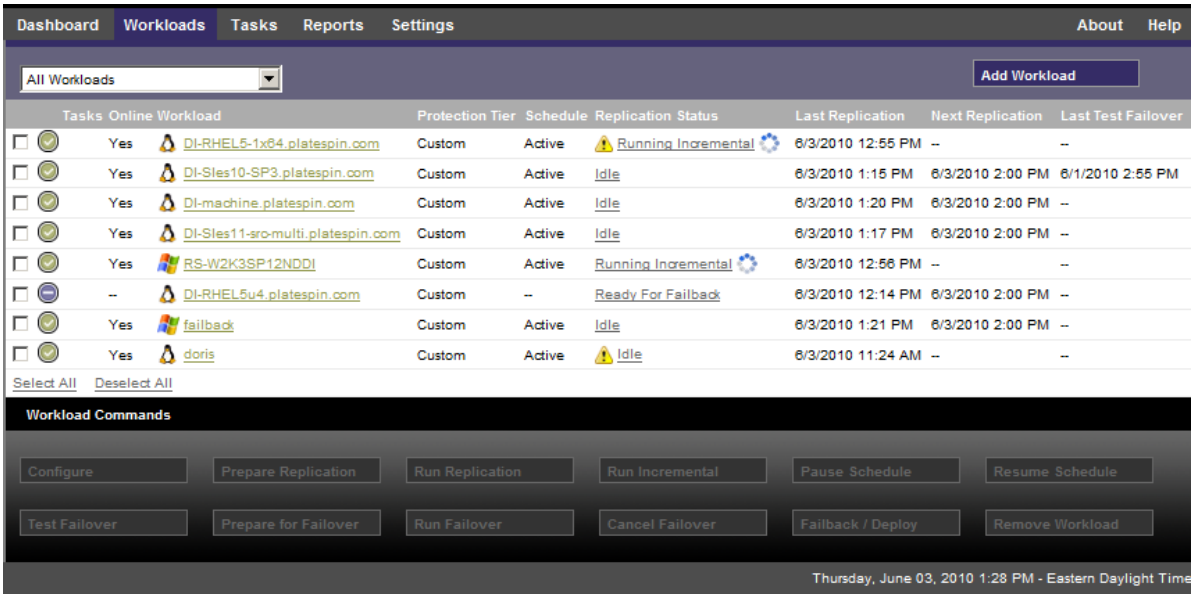
Tasks are special commands that are tied to events that require user intervention. For example, upon completion of a Test Failover command, the system generates an event associated with two tasks: `Mark Test as Success` and `Mark Test as Failure`. Clicking either task results in the Test Failover operation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

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

4.3 Workloads and Workload Commands

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

Figure 4-2 *The Workloads Page*

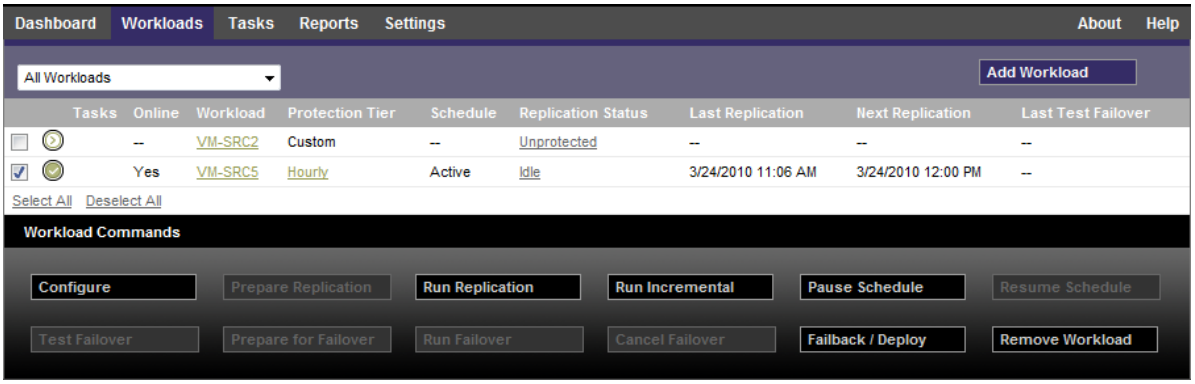


NOTE: All time stamps reflect the time zone of the Forge VM. This might be different from the time zone of the protected workload or the time zone of the host on which you are running the PlateSpin Forge Web Interface. A display of the server date and time appears at the bottom right of the client window.

4.3.1 Workload Protection and Recovery Commands

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

Figure 4-3 *Workload Commands*



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

Table 4-2 *Workload Protection and Recovery Commands*

Workload Command	Description
Configure	Starts the workload protection configuration with parameters applicable to an inventoried workload.
Prepare Replication	Installs required data transfer software on the source and creates a failover workload (a virtual machine) on the target container in preparation for workload replication.
Run Replication	Starts replicating the workload according to specified parameters (full replication).
Run Incremental	Performs an incremental transfer of changed data from the source to the target outside the workload protection contract.
Pause Schedule	Suspends the protection; all scheduled replications are skipped until the schedule is resumed.
Resume Schedule	Resumes the protection according to saved protection settings.
Test Failover	Boots and configures the failover workload in an isolated environment within the container for testing purposes.
Prepare for Failover	Boots the failover workload in preparation for a failover operation.
Run Failover	Boots and configures the failover workload, which takes over the business services of a failed workload.
Cancel Failover	Aborts the failover process.
Failback	Following a failover operation, fails the failover workload back to its original infrastructure or to a new infrastructure (virtual or physical).
Remove Workload	Removes a workload from the inventory.

4.4 Managing Multiple Instances of PlateSpin Protect and PlateSpin Forge

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

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

4.4.1 Using the PlateSpin Forge Management Console

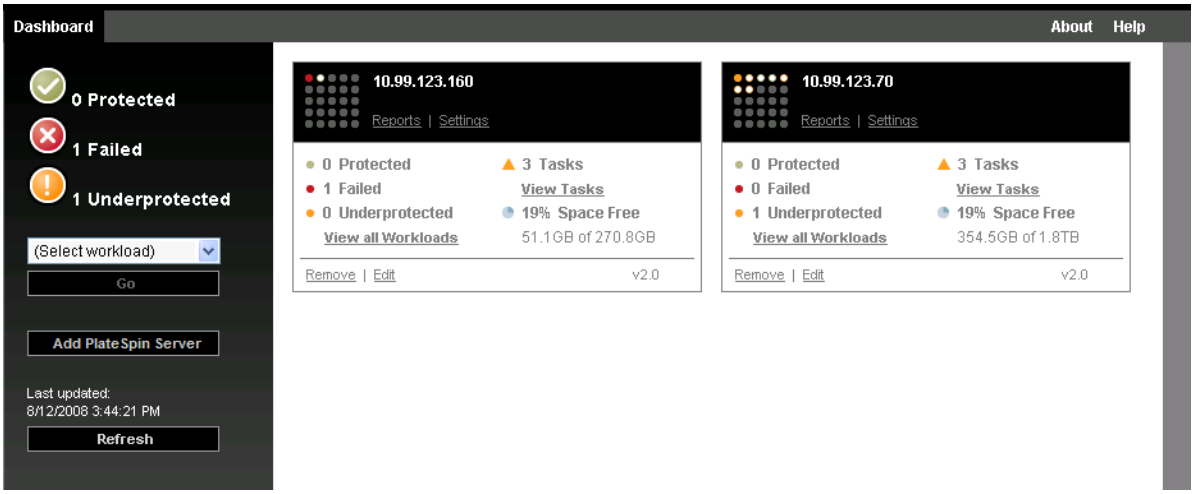
1. Open a Web browser on a machine that has access to your PlateSpin Forge instances and navigate to:

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

   Replace *<IP_address | hostname>* with either the IP address or the hostname of the Forge VM that is designated as the Manager.
2. Log in with your username and password.

   The console's default Dashboard page is displayed.

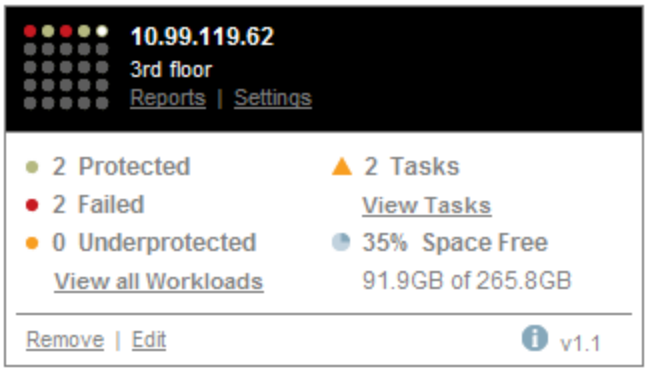
Figure 4-4 *The Management Console's Default Dashboard Page*



4.4.2 About PlateSpin Forge Management Console Cards

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

Figure 4-5 *PlateSpin Forge Instance Card*



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

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

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

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

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

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

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

1. On the console's main dashboard, click *Add PlateSpin Server*.

   The *Add/Edit* page is displayed.
2. Specify the URL of the PlateSpin Server host or Forge VM. Use HTTPS if SSL is enabled.
3. (Optional) Enable the *Use Management Console Credentials* check box to use the same credentials as those used by the console. When it is selected, the console automatically populates the *Domain\Username* field.
4. In the *Domain\Username* field, type a domain name and a username valid for the instance of PlateSpin Protect or PlateSpin Forge that you are adding. In the *Password* field, type the corresponding password.

5. (Optional) Specify a descriptive or identifying *Display Name* (15 characters max), a *Location* (20 characters max), and any *Notes* you might require (400 characters max).
6. Click *Add*/*Save*.

   A new card is added to the dashboard.

4.4.4 Managing Cards on the Management Console

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

1. Click the *Edit* hyperlink on the card that you want to edit.

   The console's *Add*/*Edit* page is displayed.
2. Make any desired changes, then click *Add*/*Save*.

   The updated console dashboard is displayed.

To remove a card from the Management Console:

1. Click the *Remove* hyperlink on the card you want to remove.

   A confirmation prompt is displayed.
2. Click *OK*.

   The individual card is removed from the dashboard.

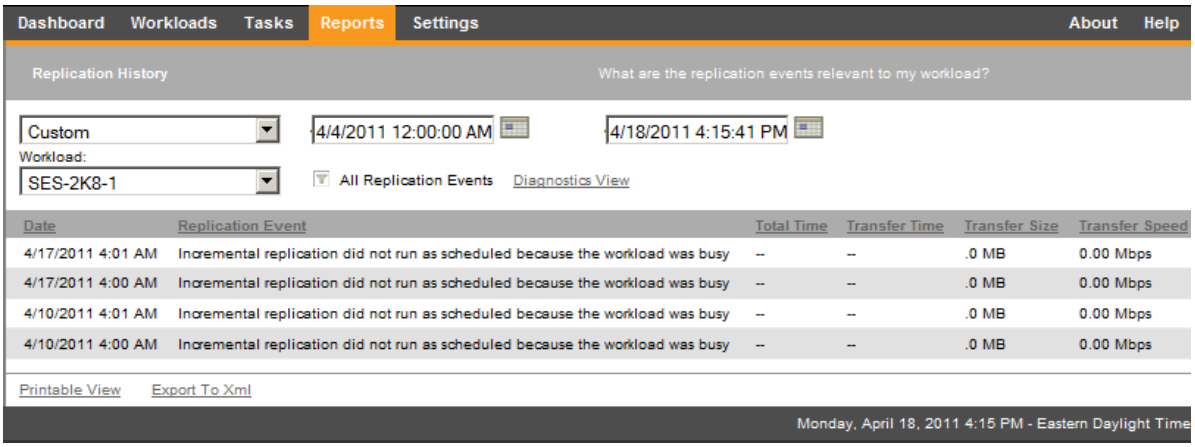
4.5 Generating Workload and Workload Protection Reports

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

The following report types are supported:

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

Figure 4-6 *Options for a Replication History Report*



To generate a report:

1. In your PlateSpin Forge Web Interface, click *Reports*.

   A list of the report types is displayed.
2. Click the name of the required report type.

5 Workload Protection

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

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

5.1 Basic Workflow for Workload Protection and Recovery

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

1 **Preparation:** This step involves preparatory steps to ensure that your workloads, containers, and environment meet the required criteria.

1a Make sure that PlateSpin Forge supports your workload.

See “Supported Configurations” on page 13.

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

See “Access and Communication Requirements across your Protection Network” on page 25.

1c (Linux only)

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

  See KB Article 7005873 (https://www.netiq.com/support/kb/doc.php?id=7005873).

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

  See KB Article 7005872 (https://www.netiq.com/support/kb/doc.php?id=7005872).

- (Optional) Prepare your `freeze` and `thaw` scripts to execute on your source workload upon each replication.

  See "Using Freeze and Thaw Scripts for Every Replication (Linux)" on page 82.

2. **Inventory:** This step involves adding workloads to the PlateSpin Server database.

   See "Adding Workloads for Protection" on page 64.

3. **Definition of the protection contract:** In this step, you define the details and specifications of a protection contract and prepare the replication.

   See "Configuring Protection Details and Preparing the Replication" on page 66.

4. **Initiating the Protection:** This step commences the protection contract according to your requirements.

   See "Starting the Workload Protection" on page 68.

5. **Optional Steps in the Protection Lifecycle:** These steps are outside the automated replication schedule but are often useful in different situations or might be dictated by your business continuity strategy.

   - *Manual incremental*. You can run an incremental replication manually, outside the workload protection contract, by clicking *Run Incremental*.
   - *Testing*. You can test failover functionality in a controlled manner and environment. See Using the Test Failover Feature.

6. **Failover:** This step carries out a failover of your protected workload to its replica running in your appliance host. See "Failover" on page 70.

7. **Failback:** This step corresponds to the business resumption phase after you have addressed any problems with your production workload. See "Failback" on page 72.

8. **Reprotection:** This step enables you to redefine the original protection contract for your workload. See "Reprotecting a Workload" on page 76

Most of these steps are represented by workload commands on the Workloads page. See "Workloads and Workload Commands" on page 56.

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

5.2 Adding Workloads for Protection

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

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

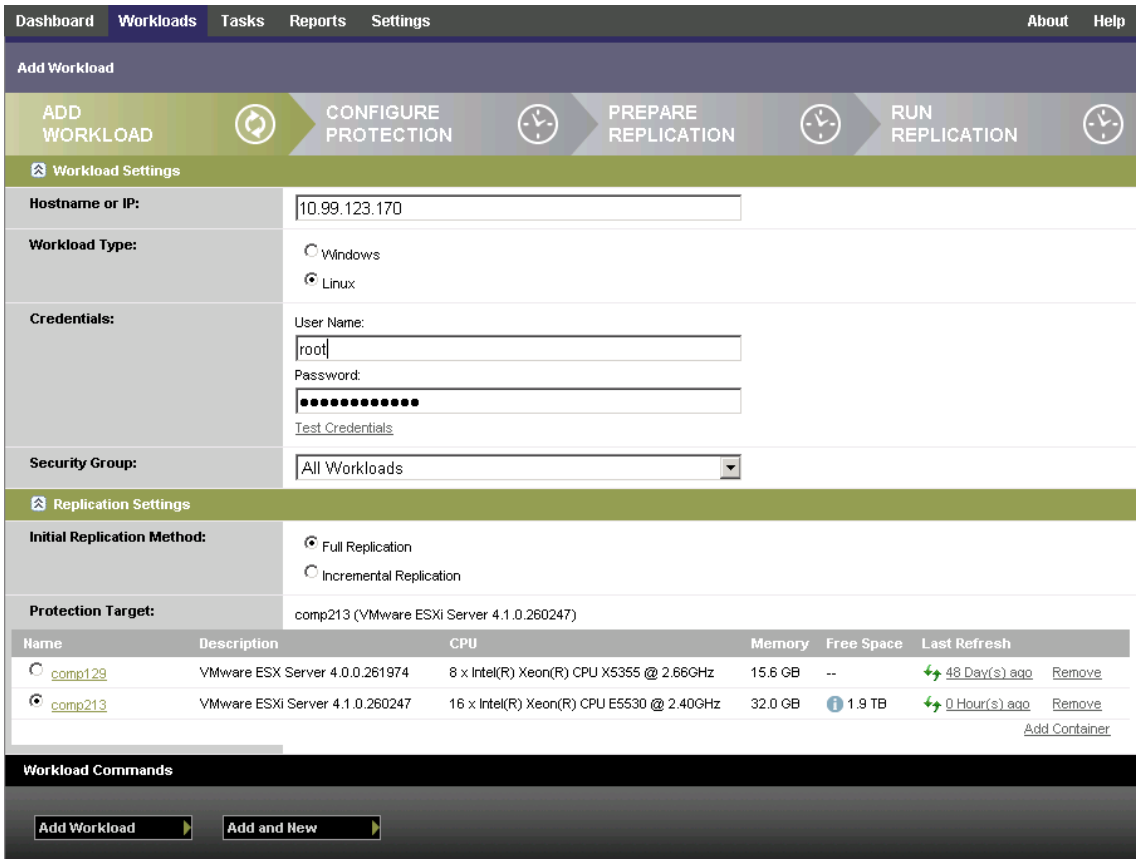
To add a workload:

1. Follow the required preparatory steps.

   See Step 1 in "Basic Workflow for Workload Protection and Recovery" on page 63.

2. On the Dashboard or Workloads page, click *Add Workload*.

   The PlateSpin Forge Web Interface displays the Add Workload page.



3 Specify the required workload details:

- **Workload Settings:** Specify your workload's hostname or IP address, the operating system, administrator-level credentials.

  Use the required credential format. See "Guidelines for Workload Credentials" on page 78.

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

4 Click *Add Workload*.

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

If you haven't added a container yet, add one to prepare for protecting the workload, otherwise, skip to "Configuring Protection Details and Preparing the Replication" on page 66

5.3 Configuring Protection Details and Preparing the Replication

Protection details control the workload protection and recovery settings and behavior over the entire life cycle of a workload under protection. At each phase of the protection and recovery workflow (see "Basic Workflow for Workload Protection and Recovery" on page 63), relevant settings are read from the protection details.

To configure your workload's protection details:

1. Add a workload. See "Adding Workloads for Protection" on page 64.
2. On the Workloads page, select the required workload and click *Configure*.

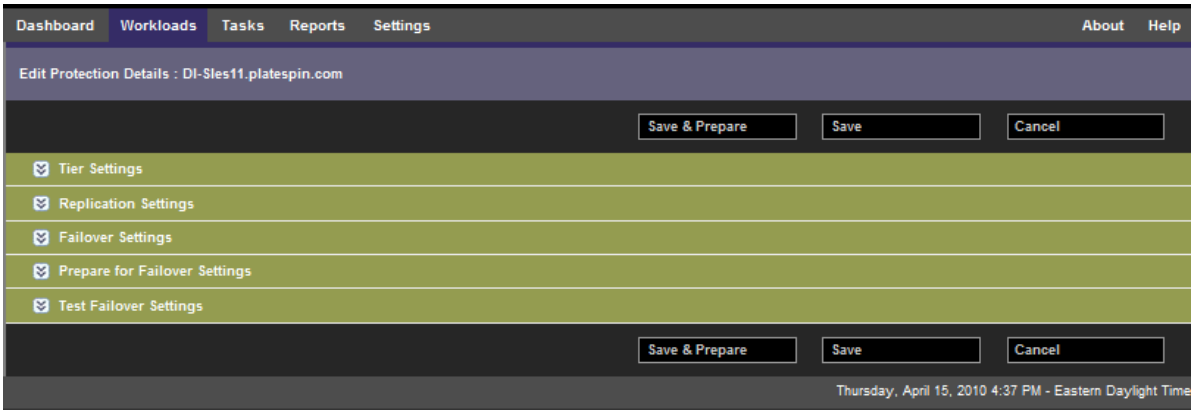
   Alternatively, you can click the name of the workload.
3. Select an *Initial Replication Method*. This indicates whether you want volume data transferred entirely from your workload to the failover VM or synchronized with volumes on an existing VM. See "Initial Replication Method (Full and Incremental)" on page 81.
4. Configure the protection details in each set of settings as dictated by your business continuity needs. See "Workload Protection Details" on page 66.
5. Correct any validation errors, if displayed by the PlateSpin Forge Web Interface.
6. Click *Save*.

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

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

5.3.1 Workload Protection Details

Workload protection details are represented by five sets of parameters:



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

The following are the details of the five parameter sets:

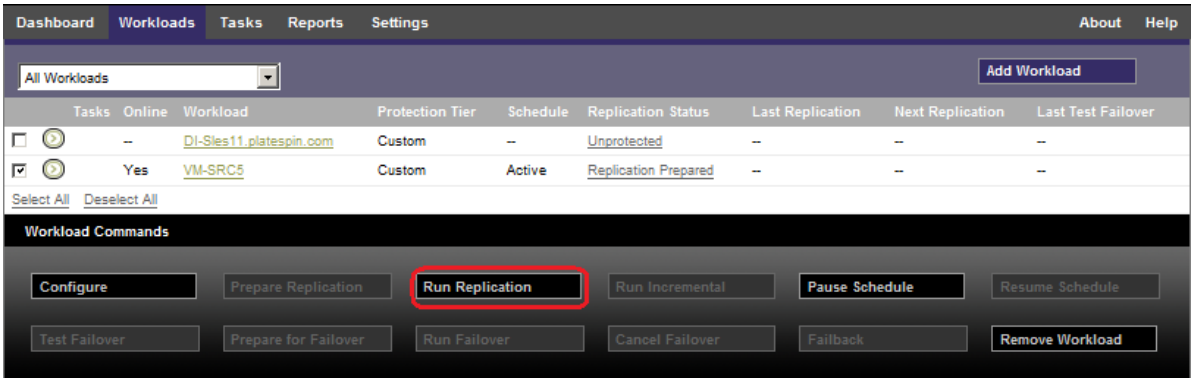
Table 5-1 *Workload Protection Details*

Parameter Set (Settings)	Details
Tier	Indicates the Protection Tier that the current protection uses. See “Protection Tiers” on page 79.
Replication	**Transfer Method:** (Windows) Enables you to select a data transfer mechanism and security through encryption. See “Data Transfer” on page 78.
	Transfer Encryption: To enable encryption, select the *Encrypt Data Transfer* option. See “Security and Privacy” on page 15.
	Source Credentials: Required for accessing the workload. See “Guidelines for Workload Credentials” on page 78.
	Number of CPUs: Enables you to specify the required number of vCPUs assigned to the failover workload (applicable only when the selected method of initial replication is *Full*).
	Replication Network: Enables you to separate replication traffic based on virtual networks defined on your appliance host. See “Networking” on page 85.
	Configuration File Datastore: Enables you to select a datastore associated with your appliance host for storing VM configuration files. See “Recovery Points” on page 80.
	Protected Volumes: Use these options to select volumes for protection and to assign their replicas to specific datastores on your appliance host.
	Thin Disk option: Enables the thin-provisioned virtual disk feature, whereby a virtual disk appears to the VM to have a set size, but only consumes the amount of disk space that is actually required by data on that disk.
	Services/Daemons to Stop During Replication: Enables you to select Windows services or Linux Daemons that are automatically stopped during the replication. See “Service and Daemon Control” on page 82.
Failover	**VM Memory:** Enables you to specify the amount of memory allocated to the failover workload.
	Hostname and Domain/Workgroup affiliation: Use these options to control the identity and domain/workgroup affiliation of the failover workload when it is live. For domain affiliation, domain administrator credentials are required.
	Network Connections: Use these options to control the LAN settings of the failover workload. See “Networking” on page 85.
	Service/Daemon States to Change: Enables you to control the startup state of specific application services (Windows) or daemons (Linux). See “Service and Daemon Control” on page 82.
Prepare for Failover	Enables you to control the temporary network settings of the failover workload during the optional Prepare for Failover operation. See “Networking” on page 85.

Parameter Set (Settings)	Details
Test Failover	**VM Memory:** Enables you to assign the required RAM to the temporary workload. **Hostname:** Enables you to assign a hostname to the temporary workload. **Domain/Workgroup:** Enables you to affiliate the temporary workload with a domain or a workgroup. For domain affiliation, domain administrator credentials are required. **Network Connections:** Controls the LAN settings of the temporary workload. See "Networking" on page 85. **Service/Daemon States to Change:** Enables you to control the startup state of specific application services (Windows) or daemons (Linux). See "Service and Daemon Control" on page 82.

5.4 Starting the Workload Protection

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



You can execute the Run Replication command after:

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

When you are ready to proceed:

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

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

NOTE: After a workload has been protected:

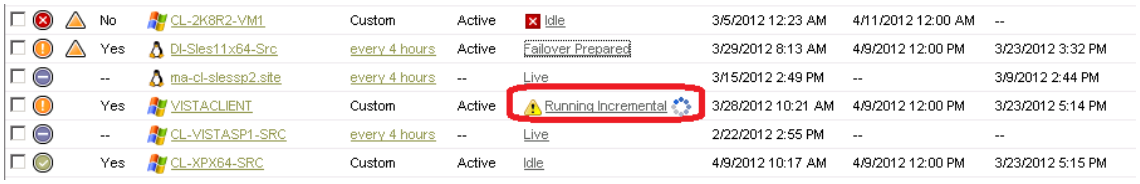
- Changing the size of a volume that is under block-level protection invalidates the protection. The appropriate procedure is to 1. remove the workload from protection, 2. resize the volumes as required. 3. re-establish the protection by re-adding the workload, configuring its protection details, and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

5.5 Aborting Commands

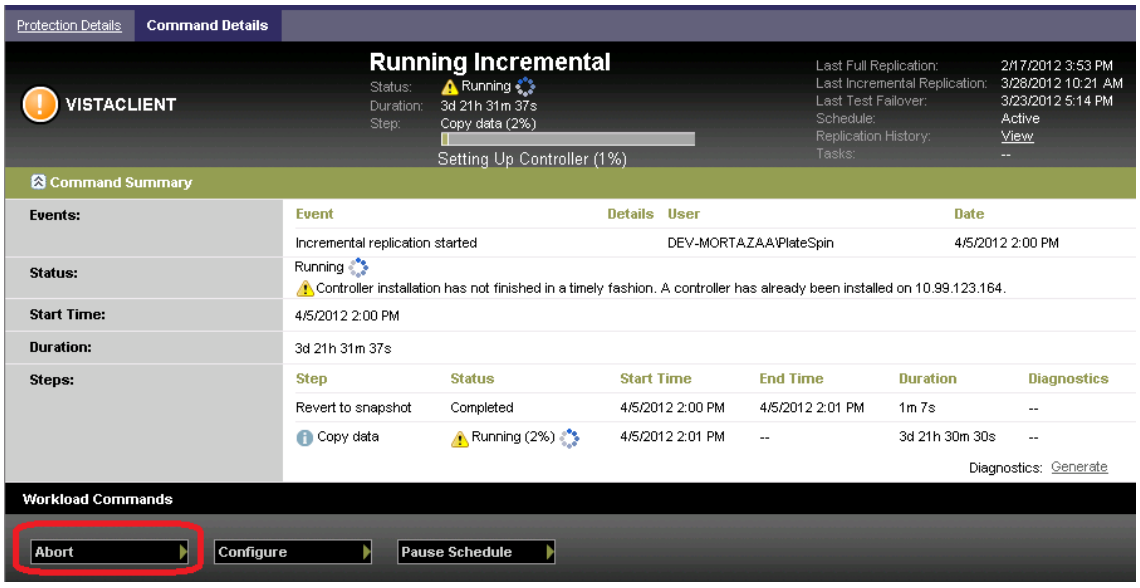
You can abort a command after executing it and while it is underway, on the Command Details page of that particular command.

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

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



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



3. Click *Abort*.

5.6 Failover

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

- Section 5.6.1, "Detecting Offline Workloads," on page 70
- Section 5.6.2, "Performing a Failover," on page 71
- Section 5.6.3, "Using the Test Failover Feature," on page 71

5.6.1 Detecting Offline Workloads

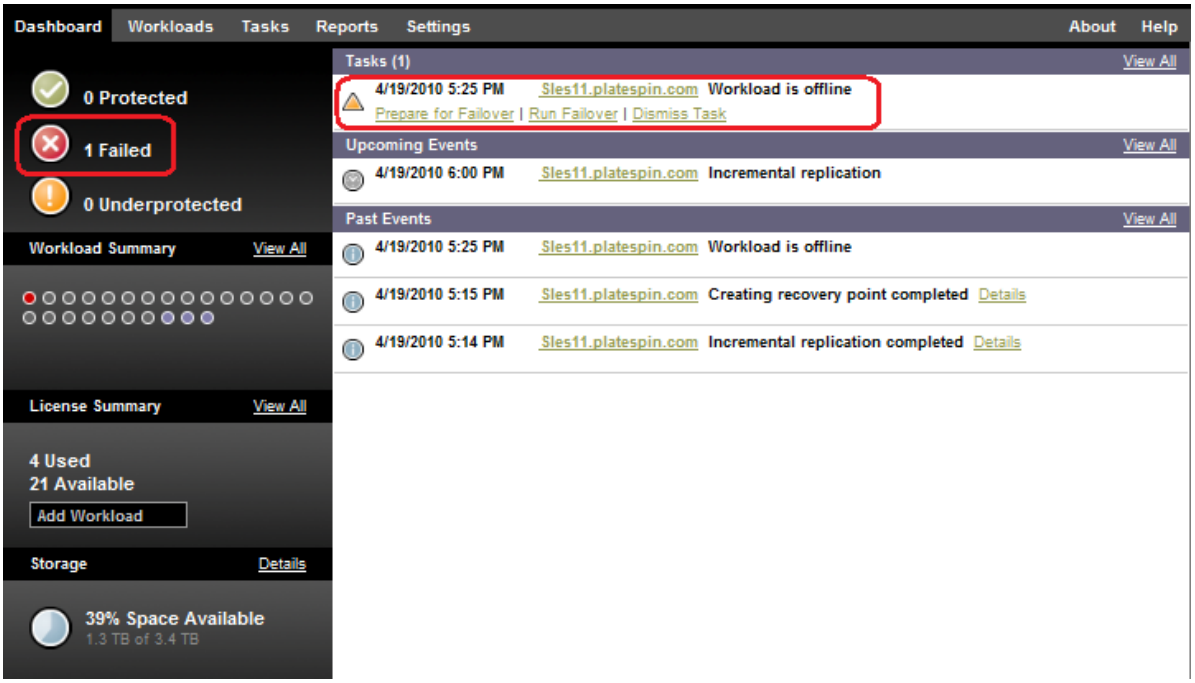
PlateSpin Forge constantly monitors your protected workloads. If an attempt to monitor a workload fails for a predefined number of times, PlateSpin Forge generates a *Workload is offline* event. Criteria that determine and log a workload failure are part of a workload protection's Tier settings (see the Tier row in "Workload Protection Details" on page 66).

If notifications are configured along with SMTP settings, PlateSpin Forge simultaneously sends a notification email to the specified recipients. See "Setting Up Automatic Email Notifications of Events and Reports" on page 27.

If a workload failure is detected while the status of the replication is *Idle*, you can proceed to the *Run Failover* command. If a workload fails while an incremental is underway, the job stalls. In this case, abort the command (see "Aborting Commands" on page 69), and then proceed to the *Run Failover* command. See "Performing a Failover" on page 71.

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

Figure 5-1 *The Dashboard Page upon Workload Failure Detection ('Workload Offline')*



5.6.2 Performing a Failover

Failover settings, including the failover workload's network identity and LAN settings, are saved together with the workload's protection details at configuration time. See the Failover row in "Workload Protection Details" on page 66.

You can use the following methods to perform a failover:

- Select the required workload on the Workloads page and click *Run Failover*.
- Click the corresponding command hyperlink of the *Workload is offline* event in the Tasks and Events pane. See Figure 5-1.
- Run a *Prepare for Failover* command to boot the failover VM ahead of time You still have the option to cancel the failover (useful in staged failovers).

Use one of these methods to start the failover process and select a recovery point to apply to the failover workload (see "Recovery Points" on page 80). Click *Execute* and monitor the progress. Upon completion, the replication status of the workload should indicate *Live*.

For testing the failover workload or testing the failover process as part of a planned disaster recovery exercise, see "Using the Test Failover Feature" on page 71.

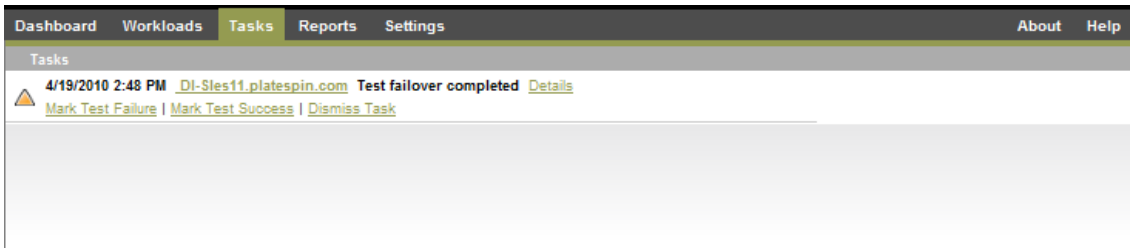
5.6.3 Using the Test Failover Feature

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

When you execute the command, PlateSpin Forge applies the Test Failover Settings, as saved in the workload protection details, to the failover workload (see the Test Failover row in "Workload Protection Details" on page 66.

1. Define an appropriate time window for testing and make sure that there are no replications underway. The replication status of the workload must be *Idle*.
2. On the Workloads page, select the required workload, click *Test Failover*, select a recovery point (see "Recovery Points" on page 80), and the click *Execute*.

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



3. Verify the integrity and business functionality of the failover workload. Use the VMware vSphere Client to access the failover workload in the appliance host.

   See "Downloading the VMware Client Program" on page 43.

4 Mark the test as a *failure* or a *success*. Use the corresponding commands in the task (*Mark Test Failure*, *Mark Test Success*). The selected action is saved in the history of events associated with the workload and is retrievable by reports. *Dismiss Task* discards the task and the event.

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

5.7 Failback

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

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

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

The following topics provide more information:

- Section 5.7.1, "Automated Failback to a VM Platform," on page 72
- Section 5.7.2, "Semi-Automated Failback to a Physical Machine," on page 75
- Section 5.7.3, "Semi-Automated Failback to a Virtual Machine," on page 76

5.7.1 Automated Failback to a VM Platform

The following containers are supported as automated failback targets:

Target	Notes
VMware DRS Cluster in vSphere 5.1	◆ The DRS configuration must be either **Partially Automated** or **Fully Automated** (it must not be set to **Manual**) ◆ As a VM Container, the DRS Cluster must consist of ESXi 5.1 servers only, and can be managed by vCenter 5.1 only.
VMware DRS Cluster in vSphere 5.0	◆ The DRS configuration must be either **Partially Automated** or **Fully Automated** (it must not be set to **Manual**) ◆ As a VM Container, the DRS Cluster must consist of ESXi 5.0 servers only, and can be managed by vCenter 5.0 only.
VMware DRS Cluster in vSphere 4.1	◆ The DRS configuration must be either **Partially Automated** or **Fully Automated** (it must not be set to **Manual**) ◆ As a VM Container, the Cluster, as a container, can use a combination of ESX 4.1 and ESX**i** 4.1 servers, and can be managed by vCenter 4.1 only
VMware ESX**i** 4.1, 5.0, 5.1	ESX**i** versions must have a paid license; protection is unsupported with these systems if they are operating with a free license.
VMware ESX 4.1	

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

1. Following a failover, select the workload on the Workloads page and click *Failback*.

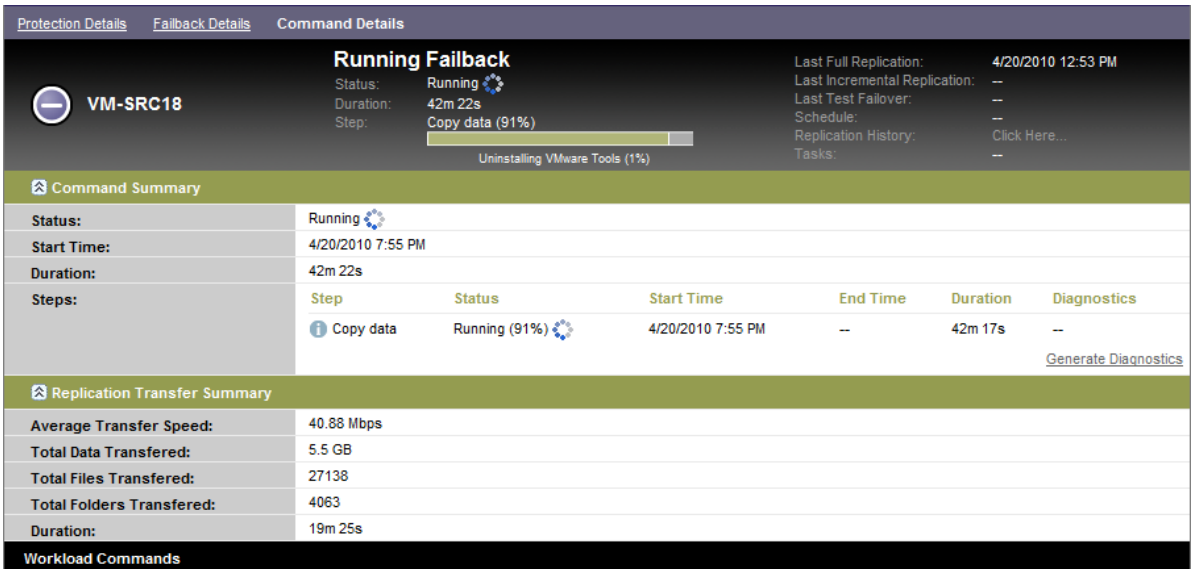
   The system prompts you to make the following selections

2. Specify the following sets of parameters:
   - **Workload Settings:** Specify the failover workload's hostname or IP address and provide administrator-level credentials. Use the required credential format (see "Guidelines for Workload Credentials" on page 78).
   - **Failback Target Settings:** Specify the following parameters:
     - **Replication Method:** Select the scope of data replication. If you select *Incremental*, you must *Prepare* a target. See "Initial Replication Method (Full and Incremental)" on page 81.
     - **Target Type:** Select *Virtual Target*. If you don't yet have a failback container, click *Add Container* and inventory a supported container.
3. Click *Save and Prepare* and monitor the progress on the Command Details screen.

   Upon successful completion, PlateSpin Forge loads the Ready for Failback screen, prompting you to specify the details of the failback operation.
4. Configure the failback details. See "Failback Details (Workload to VM)" on page 74.
5. Click *Save and Failback* and monitor the progress on the Command Details page. See Figure 5-2.

   PlateSpin Forge executes the command. If you selected *Reprotect after Failback* in the Post-Failback parameter set, a *Reprotect* command is shown in the PlateSpin Forge Web Interface.

Figure 5-2 *Failback Command Details*



Failback Details (Workload to VM)

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

Table 5-2 *Failback Details (VM)*

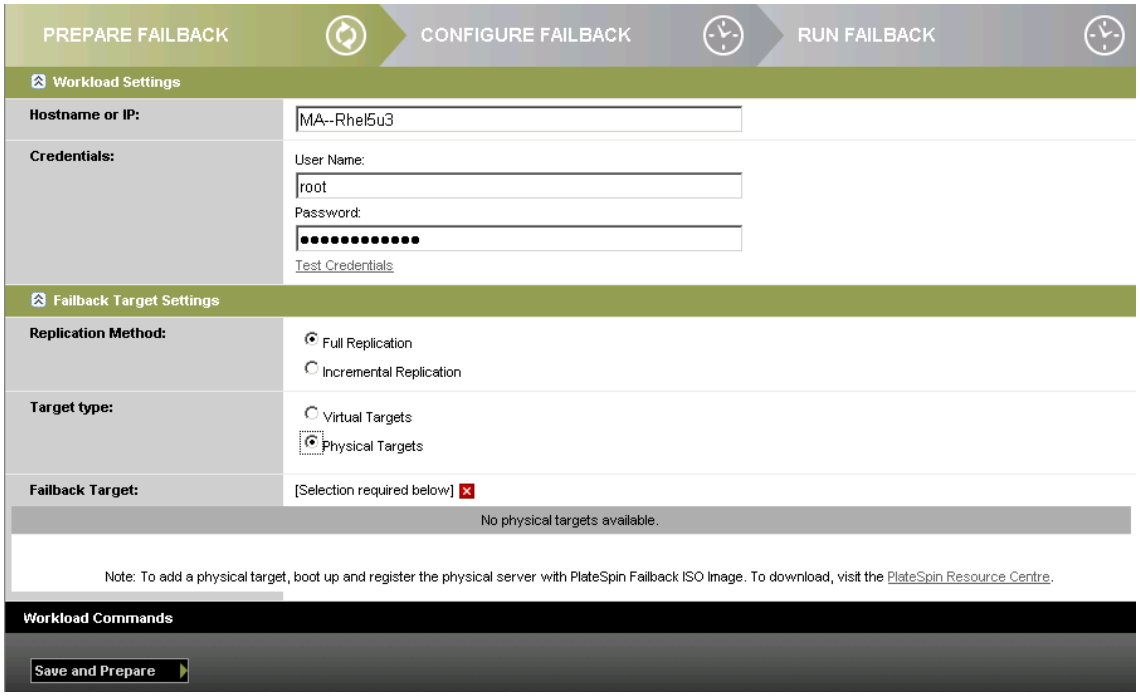
Parameter Set (Settings)	Details
Failback	**Transfer Method:** Enables you to select a data transfer mechanism and security through encryption. See "Data Transfer" on page 78.
	Failback Network: Enables you to direct failback traffic over a dedicated network based on virtual networks defined on your appliance host. See "Networking" on page 85.
	VM Datastore: Enables you to select a datastore associated with your failback container for the target workload.
	Volume Mapping: When the initial replication method is specified as "incremental", enables you to select source volumes and map to volumes on the failback target for synchronization.
	Services/Daemons to stop: Enables you to select Windows services or Linux daemons that are automatically stopped during the failback. See "Service and Daemon Control" on page 82.
	Alternative Address for Source: Accepts input of an additional IP address for the failed-over VM if applicable. See "Protection Across Public and Private Networks Through NAT" on page 26.
Workload	***Number of CPUs:*** Enables you to specify the required number of vCPUs assigned to the target workload.
	VM Memory: Enables you to assign the required RAM to the target workload .
	Hostname, Domain/Workgroup: Use these options to control the identity and domain/workgroup affiliation of the target workload. For domain affiliation, domain administrator credentials are required.
	Network Connections: Use these options to specify the network mapping of the target workload based on the virtual networks of the underlying VM container.
	Service States to Change: Enables you to control the startup state of specific application services (Windows) or daemons (Linux). See "Service and Daemon Control" on page 82.
Post-Failback	**Reprotect Workload:** Use this option if you plan to re-create the protection contract for the target workload after deployment. This maintains a continuous event history for the workload and auto-assigns/designates a workload license. ◆ ***Reprotect after Failback:*** Select this option if you intend to re-create a protection contract for the target workload. When the failback is complete, a *Reprotect* command will be available in the PlateSpin Forge Web Interface for the failed-back workload. ◆ ***No reprotect*****:** Select this option if you don't intend to re-create a protection contract for the target workload. To protect the failed-back workload upon completion, you will have to re-inventory that workload and reconfigure its protection details.

5.7.2 Semi-Automated Failback to a Physical Machine

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

1. Register the required physical machine with your PlateSpin Server. See "Failback to Physical Machines" on page 85.
2. If the drivers are missing or incompatible, upload the required drivers to the PlateSpin Forge device driver database. See "Managing Device Drivers" on page 89.
3. Following a failover, select the workload on the Workloads page and click *Failback*.
4. Specify the following sets of parameters:
   - **Workload Settings:** Specify the failover workload's hostname or IP address and provide administrator-level credentials. Use the required credential format (see "Guidelines for Workload Credentials" on page 78.
   - **Failback Target Settings:** Specify the following parameters:
     - ***Replication Method:*** Select the scope of data replication.

       See "Initial Replication Method (Full and Incremental)" on page 81.
     - ***Target Type:*** Select the *Physical Target* option and then select the physical machine you registered in Step 1.



5. Click *Save and Prepare* and monitor the progress on the Command Details screen.

   Upon successful completion, PlateSpin Forge loads the Ready for Failback screen, prompting you to specify the details of the failback operation.
6. Configure the failback details, then click *Save and Failback*.

   Monitor the progress on the Command Details screen.

5.7.3 Semi-Automated Failback to a Virtual Machine

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

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

- Xen on SLES 10 SP2
- Microsoft Hyper-V Server 2008 (*not* R2)

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

5.8 Reprotecting a Workload

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

NOTE: The *Reprotect* command becomes availble only if you selected the *Reprotect* option in the Failback details. See "Failback" on page 72.

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

6 Essentials of Workload Protection

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

6.1 Workload License Consumption

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

For information about product licensing and license activation, see “Product Licensing” on page 19.

6.2 Guidelines for Workload Credentials

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

Table 6-1 *Workload Credentials*

To Discover	Credentials	Remarks
All Windows workloads	Local or domain administrator credentials.	For the username, use this format: ◆ For domain member machines: *authority\principal* ◆ For workgroup member machines: *hostname\principal*
All Linux workloads	Root-level username and password	Non-root accounts must be properly configured to use `sudo`. See KB Article 7920711.

6.3 Data Transfer

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

- Section 6.3.1, "Transfer Methods," on page 78
- Section 6.3.2, "Data Encryption," on page 79

6.3.1 Transfer Methods

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

- "Transfer Methods Supported for Windows Workloads" on page 78
- "Transfer Methods Supported for Linux Workloads" on page 79

Transfer Methods Supported for Windows Workloads

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

❒ **Windows Block-level Replication:** Data is replicated at a volume's block level. For this transfer method, PlateSpin Forge provides two mechanisms that differ by their continuity impact and performance. You can toggle between these mechanisms as required.

- **Replication using the Block-Based Component:** This option uses a dedicated software component for block-level data transfer and leverages the Microsoft Volume Snapshot Service (VSS) with applications and services that support VSS. The installation of the component on your protected workload is automatic.

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

- **Replication without the Block-Based Component:** This option uses an internal 'hashing' mechanism in combination with Microsoft VSS to track changes on the protected volumes.

  This option requires no reboot, but its performance is inferior to that of the block-based component.

❒ **Windows File-level Replication:** Data is replicated on a file-by-file basis (Windows only).

Transfer Methods Supported for Linux Workloads

For Linux workloads, PlateSpin Forge provides a mechanism to transfer workload volume data at block level only. Data transfer is powered by a block-level data transfer component that leverages LVM snapshots if available (this is the default and recommended option). See KB Article 7005872 (https://www.netiq.com/support/kb/doc.php?id=7005872).

The Linux block-based component included in your PlateSpin Forge distribution is precompiled for the standard, non-debug kernels of the supported Linux distributions. If you have a non-standard, customized, or newer kernel, you can rebuild the block-based component for your specific kernel. See KB Article 7005873 (https://www.netiq.com/support/kb/doc.php?id=7005873).

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

6.3.2 Data Encryption

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

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

6.4 Protection Tiers

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

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

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

You can also create custom Protection Tiers in advance:

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

Name	Type the name you want to use for the tier.
Incremental Recurrence	Specify the frequency of incremental replications and the incremental recurrence pattern. You can type directly in the *Start of recurrence* field, or click the calendar icon to select a date. Select *None* as the Recurrence Pattern to never use incremental replication.
Full Recurrence	Specify the frequency of full replications and the full recurrence pattern.
Blackout Window	Use these settings to force a replication blackout (for suspending scheduled replications during peak utilization hours or to prevent conflicts between VSS-aware software and the PlateSpin VSS block-level data transfer component). To specify a blackout window, click *Edit*, then select a blackout recurrence pattern (daily, weekly, etc.), and the blackout period's start and end times. **NOTE:** The blackout start and end times are based on the system clock on your PlateSpin Server.
Compression Level	These settings control whether and how workload data is compressed before transmission. See "Data Compression" on page 17. Select one of the available options. *Fast* consumes the least CPU resources on the source but yields a lower compression ratio, *Maximum* consumes the most, but yields a higher compression ratio. *Optimal*, the middle ground, is the recommended option.
Bandwidth Throttling	These settings control bandwidth throttling. See "Bandwidth Throttling" on page 17. To throttle replications to a specified rate, specify the required throughput value in Mbps and indicate the time pattern.
Recovery Points to Keep	Specify the number of recovery points to keep for workloads that use this Protection Tier. See "Recovery Points" on page 80.
Workload Failure	Specify the number of workload detection attempts before it is considered failed.
Workload Detection	Specify the time interval (in seconds) between workload detection attempts.

6.5 Recovery Points

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

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

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

To remove recovery points from your appliance, see "Managing Forge Snapshots on the Appliance Host" on page 45.

6.6 Initial Replication Method (Full and Incremental)

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

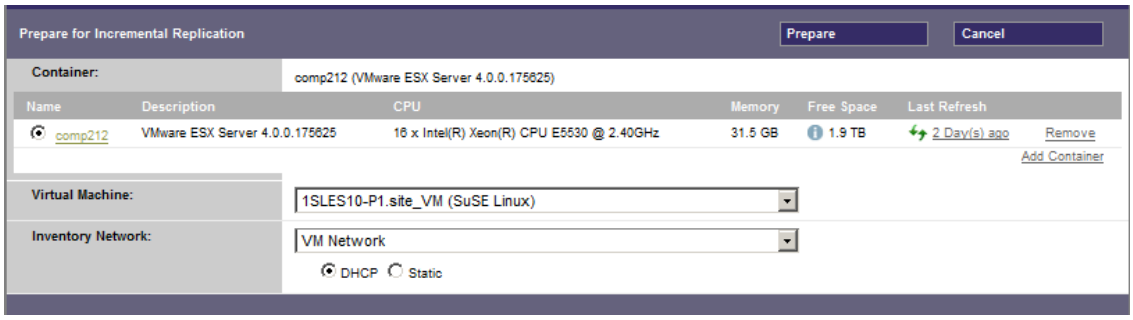
- **Full:** A full volume transfer takes place from a production workload to its replica (the failover workload), or from a failover workload to its original virtual or physical infrastructure.
- **Incremental:** Only differences are transferred from a source to its target, provided that they have similar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

      See "Manually Importing VMs into the Appliance Host's Datastore" on page 45.
  - During failback to a virtual machine: The failover workload is compared with an existing VM in a failback container.
  - During failback to a physical machine: The failover workload is compared with a workload on the target physical machine, if the physical machine is registered with PlateSpin Forge (see "Semi-Automated Failback to a Physical Machine" on page 75).

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

1. Proceed with the required workload command, such as *Configure (Protection Details)* or *Failback.*
2. For the *Initial Replication Method* option, select *Incremental Replication*.
3. Click *Prepare Workload*.

   The PlateSpin Forge Web Interface displays the Prepare for Incremental Replication page.



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

5 Click *Prepare*.

Wait for the process to complete and for the user interface to return to the original command, then select the prepared workload.

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

6.7 Service and Daemon Control

PlateSpin Forge enables you to control services and daemons:

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

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

  For additional control of Linux sources during replication, consider the capability to run custom scripts on your Linux workloads during each replication. See "Using Freeze and Thaw Scripts for Every Replication (Linux)" on page 82.
- **Target startup sate/run level control:** You can select the startup state (Windows) or the run level (Linux) of services/daemons on the failover VM. When you perform a Failover or Test Failover operation, you can specify which services or daemons you want to be running or stopped when the failover workload has gone live.

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

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

For Linux systems, PlateSpin Forge provides you with the capability to automatically execute custom scripts, `freeze` and `thaw`, that complement the automatic daemon control feature.

The `freeze` script is executed at the beginning of a replication, and `thaw` is executed at the end of a replication.

Consider using this capability to complement the automated daemon control feature provided through the user interface (see "Source service/daemon control:" on page 82. For example, you might want to use this feature to temporarily freeze certain daemons instead of shutting them down during replications.

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

1 Create the following files:
   - `platespin.freeze.sh`: A shell script to execute at the beginning of the replication
   - `platespin.thaw.sh`: A shell script to execute at the end of the replication

- `platespin.conf`: A text file defining any required arguments, along with a timeout value.

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

  ```
  [ServiceControl]

  FreezeArguments=<arguments>

  ThawArguments=<arguments>

  TimeOut=<timeout>
  ```

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

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

   `/etc/platespin`

6.9 Volumes

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

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

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

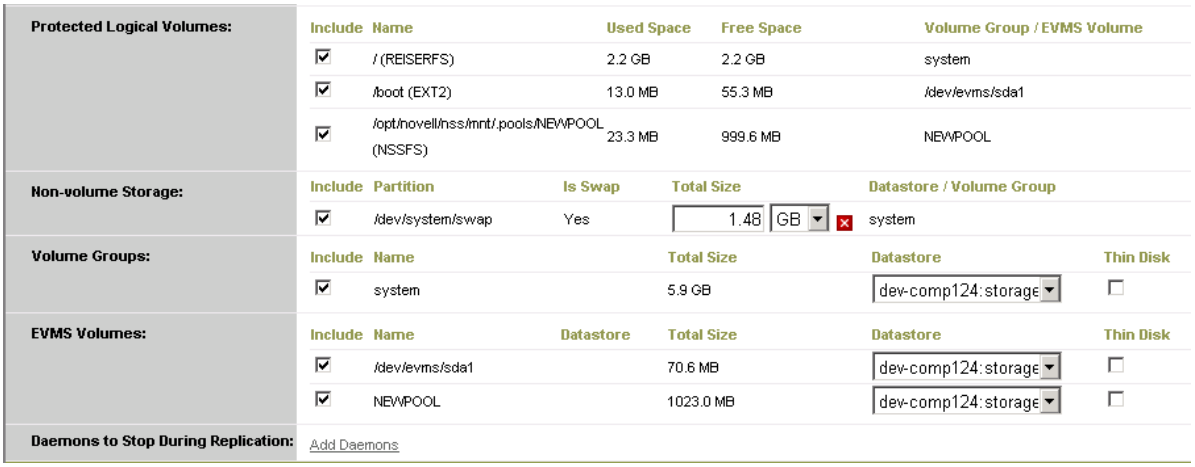
- Non-volume storage, such as a swap partition that is associated with the source workload, is recreated in the failover workload.
- The layout of volume groups and logical volumes is preserved so that you can re-create it during failback.
- (OES 2 workloads) EVMS layouts of source workloads are preserved and re-created in the appliance host. NSS pools are copied from the source to the recovery VM.

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

Figure 6-1 *Volumes, Logical Volumes, and Volume Groups of a Protected Linux Workload*

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

Figure 6-2 *Replication Settings, Volume-Related Options (OES 2 Workload)*



6.10 Networking

PlateSpin Forge enables you to control your failover workload's network identity and LAN settings to prevent replication traffic from interfering with your main LAN or WAN traffic.

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

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

6.11 Failback to Physical Machines

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

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

- Section 6.11.1, "Downloading the PlateSpin Boot ISO Image," on page 85
- Section 6.11.2, "Injecting Additional Device Drivers into the Boot ISO Image," on page 85
- Section 6.11.3, "Registering Physical Machines as Failback Targets with PlateSpin Forge," on page 86

6.11.1 Downloading the PlateSpin Boot ISO Image

You can download the PlateSpin boot ISO image (`PlateSpinFailback.ISO`) from the PlateSpin Forge area of Novell Downloads (http://download.novell.com) by doing a search with the following parameters:

- *Product or Technology:* `PlateSpin Forge`
- *Select Version:* `PlateSpin Forge 4`
- *Date Range:* `All Dates`

6.11.2 Injecting Additional Device Drivers into the Boot ISO Image

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

1 Obtain or compile `*.ko` driver files appropriate for the target hardware manufacturer.

IMPORTANT: Make sure the drivers are valid for the kernel included with the ISO file (for x86 systems: `3.0.93-0.8-pae`, for x64 systems: `3.0.93-0.8-default`) and are appropriate for the target architecture. See also KB Article 7005990.

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

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

3 Copy the `rebuildiso.sh` script, located in the `/tools` subdirectory of the mounted ISO file, into a temporary working directory. When you have finished, unmount the ISO file (execute the command `unmount <mount_point>`).

4 Create another working directory for the required driver files and save them in that directory.

5 In the directory where you saved the `rebuildiso.sh` script, run the following command as `root` to copy SOURCE files into the ISO file:

```
./rebuildiso.sh <SOURCE> <-m32|-m64> <-i ISO file>
```

NOTE: SOURCE must be one or more of the following parameters:

`-d` path to the directory containing drivers (that is, *.ko files) to inject

`-c` Path to the `ConfigureTakeControl.xml` file

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

6.11.3 Registering Physical Machines as Failback Targets with PlateSpin Forge

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

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

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

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

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

5 Press Enter.

6 When you are prompted, enter the hostname or the IP address of your Forge VM.

7 Provide your administrator-level credentials for the Forge VM, specifying an authority. For the user account, use this format:

*domain**username* or *hostname**username*

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

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

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

10 When prompted to indicate whether to use HTTPS, enter `Y` if you have enabled SSL, and `N` if you have not.

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

6.12 Advanced Workload Protection Topics

6.12.1 Using Workload Protection Features through the PlateSpin Forge Web Services API

PlateSpin Forge exposes a REST-based API technology preview that developers can use as they build their own applications to work with the product. The API includes information about the following operations:

- discover containers
- discover workloads
- configure protection
- run replications, failover operations and failback
- query for status of workload and container status
- query for status of running operations
- query security groups and their protection ties

Forge administrators can leverage a Jscript sample (`https://localhost/protectionservices/Documentation/Samples/protect.js`) from the command line to access the product through the API. The sample can help you write scripts to help you work with the product. Using the command line utility, you can perform the following operations:

- add a single workload
- add a single container
- run the replication, failover, and failback operations
- add multiple workloads and containers at one time

  NOTE: For more information about this operation, see the API documentation at `https://localhost/protectionservices/Documentation/AddWorkloadsAndContainersFromCsvFile.htm`.

- remove all workloads at one time
- remove all container at one time

The PlateSpin Forge REST API home page (`https://localhost/protectionservices/` or `https://<server page>/protectionservices/`) includes links to the content that can be useful for developers and administrators.

This technology preview will be fully developed with more features in subsequent releases.

7 Auxiliary Tools for Working with Physical Machines

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

7.1 Managing Device Drivers

PlateSpin Forge ships with a library of device drivers and automatically installs the appropriate ones on target workloads. If some drivers are missing or incompatible, or if you require specific drivers for a target infrastructure, you might need to add (upload) drivers to the PlateSpin ProtectPlateSpin Forge driver database.

7.1.1 Packaging Device Drivers for Windows Systems

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

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

The drivers are now ready for upload. See “Uploading Drivers to the PlateSpin Forge Device Driver Database” on page 90.

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

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

7.1.2 Packaging Device Drivers for Linux Systems

To package your Linux device drivers for uploading to the PlateSpin Forge driver database, you can use a custom utility included in your PlateSpin boot ISO image.

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

   For example, assuming that the ISO has been copied under the `/root` directory, issue this command for BIOS firmware-based targets:

   ```
   # mkdir /mnt/ps # mount -o loop /root/bootofx.x2p.iso /mnt/ps
   ```

   or this command for UEFI firmware-based targets:

   ```
   # mkdir /mnt/ps # mount -o loop /root/bootofx.x2p.uefi.iso /mnt/ps
   ```
3. From the `/tools` subdirectory of the mounted ISO image, copy the `packageModules.tar.gz` archive into a another working directory and extract it.

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

   ```
   tar -xvzf packageModules.tar.gz
   ```
4. Enter the working directory and execute the following command:

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

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

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

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

The package is now ready for uploading. See "Uploading Drivers to the PlateSpin Forge Device Driver Database" on page 90.

7.1.3 Uploading Drivers to the PlateSpin Forge Device Driver Database

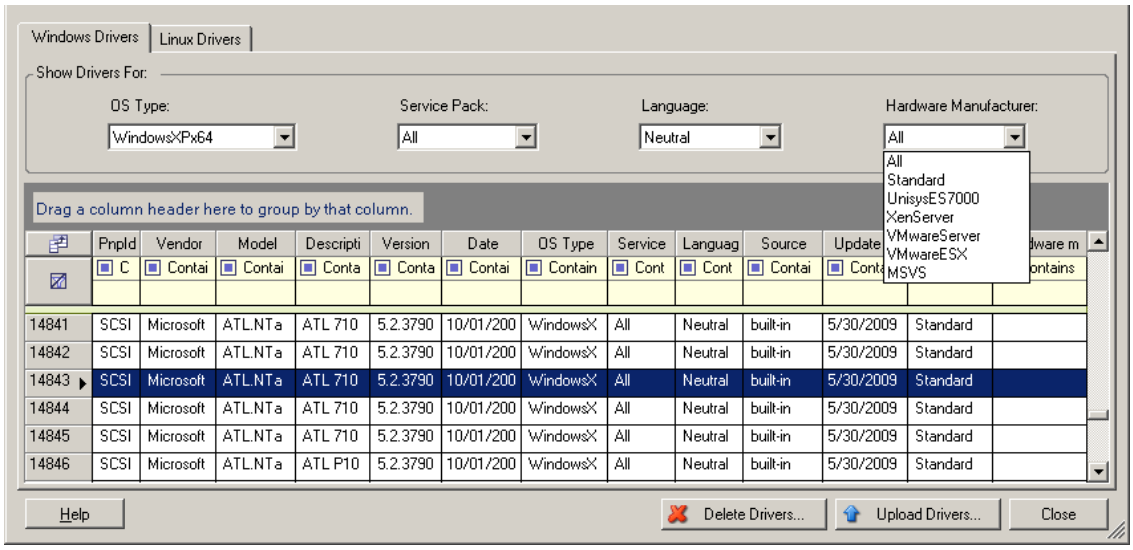
Use the PlateSpin Driver Manager to upload device drivers to the driver database.

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

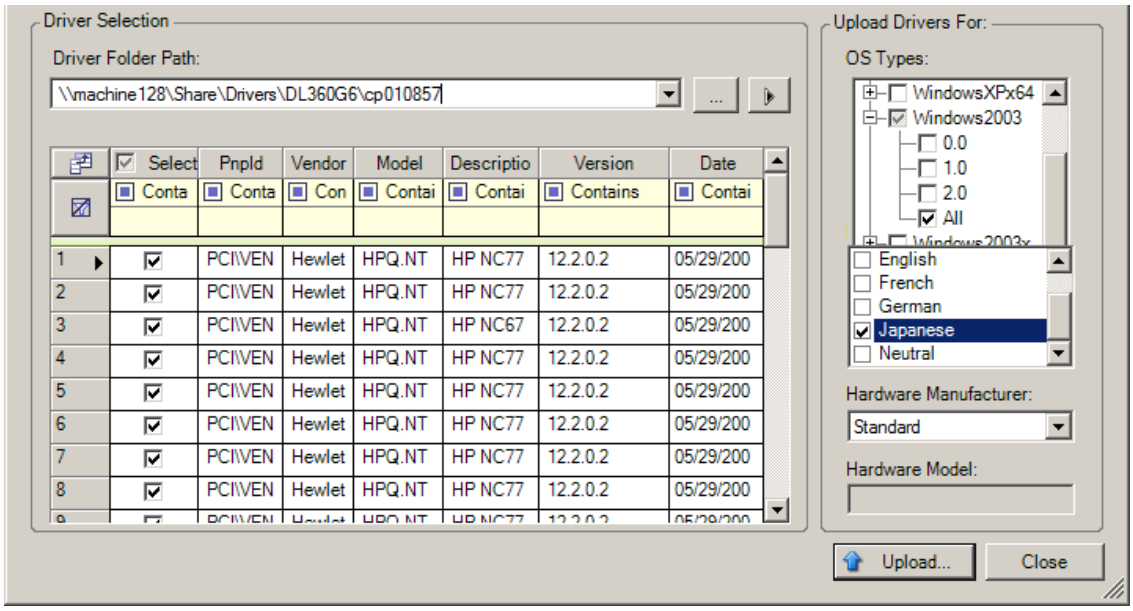
- "Device Driver Upload Procedure (Windows)" on page 90
- "Device Driver Upload Procedure (Linux)" on page 91

Device Driver Upload Procedure (Windows)

1. Obtain and prepare the required device drivers. See Packaging Device Drivers for Windows Systems.
2. On your Forge VM, under `Program Files\PlateSpin Forge Server\DriverManager`, start the `DriverManager.exe` program and select the *Windows Drivers* tab.



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



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

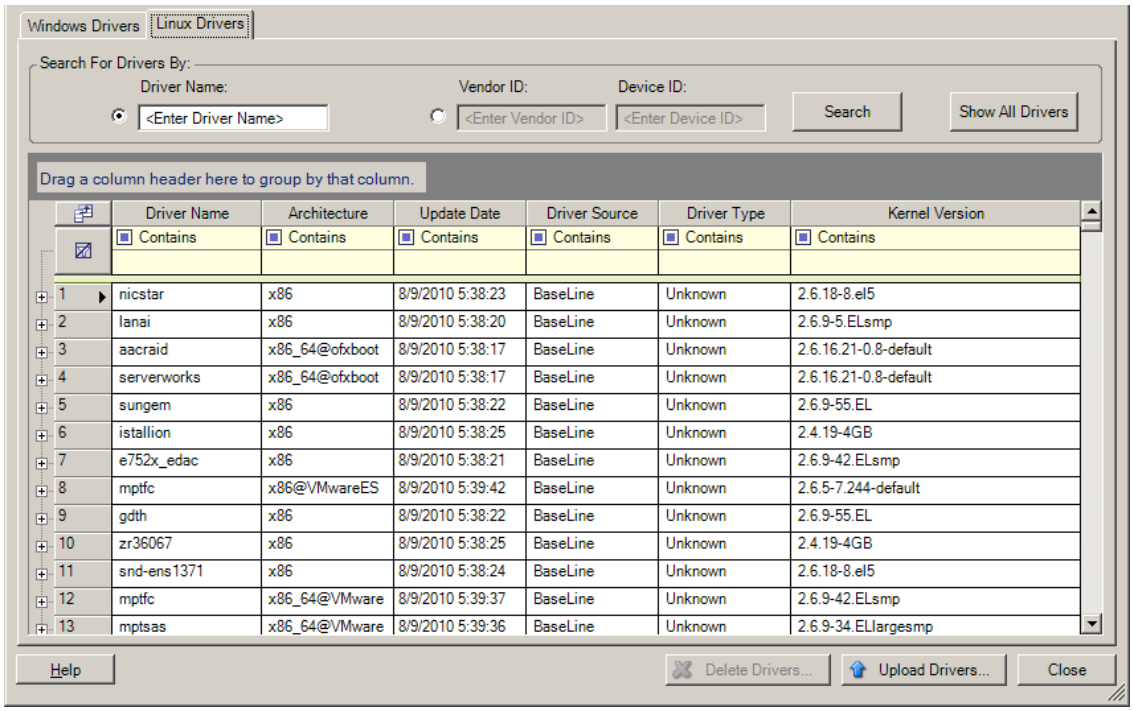
4 Click *Upload* and confirm your selections when prompted.

The system uploads the selected drivers to the driver database.

Device Driver Upload Procedure (Linux)

1 Obtain and prepare the required device drivers. See Packaging Device Drivers for Linux Systems.

2 Click *Tools* > *Manage Device Drivers* and select the *Linux Drivers* tab:



3 Click *Upload Drivers*, browse to the folder that contains the required driver package (`*.pkg`), and click *Upload All Drivers*.

The system uploads the selected drivers to the driver database.

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

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

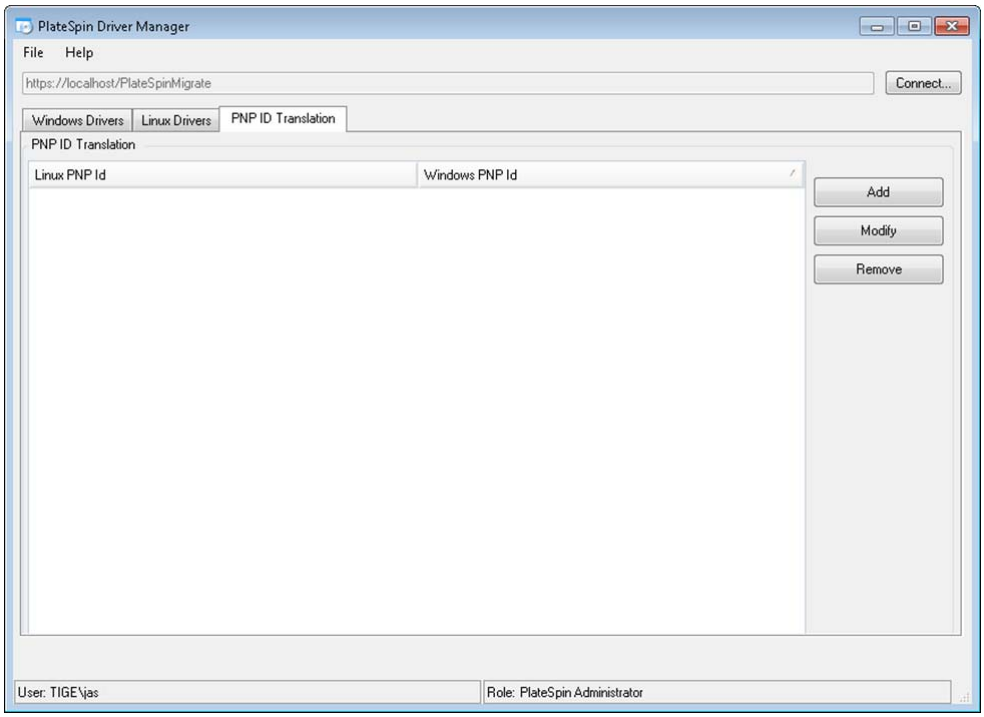
When the PlateSpin Server discovers workloads and their available hardware, the discovery includes these PnP IDs and the storage of that data as part of the workload's details. PlateSpin uses the IDs to determine which, if any, drivers need to be injected during a failover/failback operation. The PlateSpin Server maintains a database of PnP IDs for the associated drivers of each of the supported operating systems. Because Windows and Linux use different formats for PnP IDs, a Windows workload discovered by the Protect Linux RAM disk contains Linux-style PnP IDs.

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

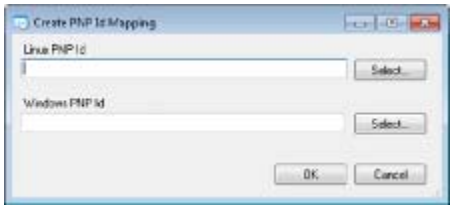
Follow these steps to use the PnP ID Translation feature:

1 Launch the PlateSpin Driver Manager tool and connect to the PlateSpin Server.

2 In the Driver Manager tool, select the PNP ID Translation tab to open the *PNP ID Translation* list, which includes the currently known custom PnP ID mappings.



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



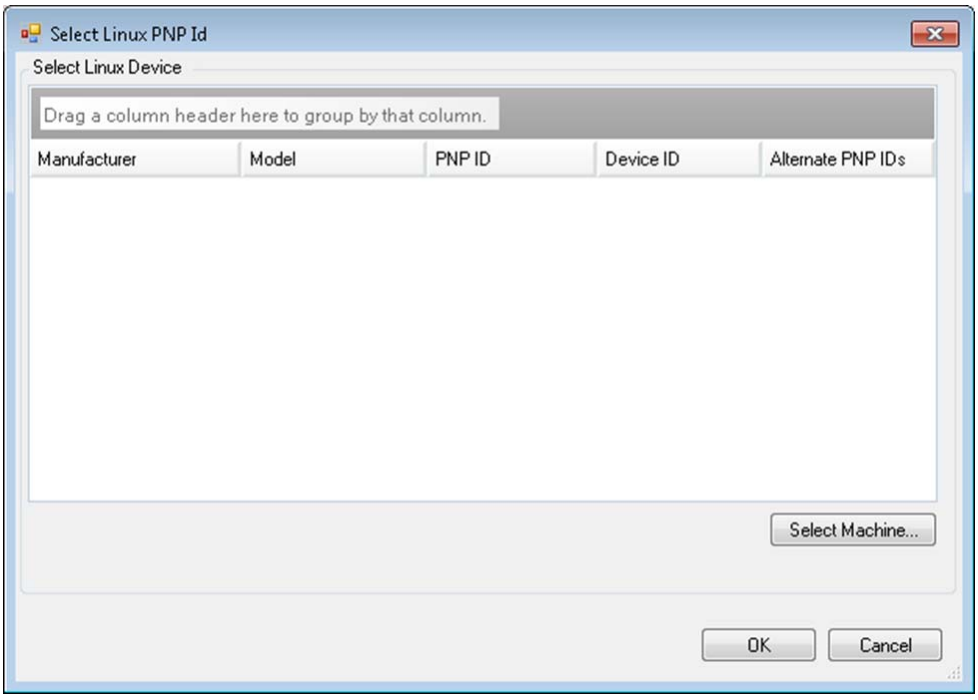
4 In the *Linux PNP ID* field, add a Linux PnP ID.

4a (Conditional) If you know it, type the Linux PnP ID you want to use.

or

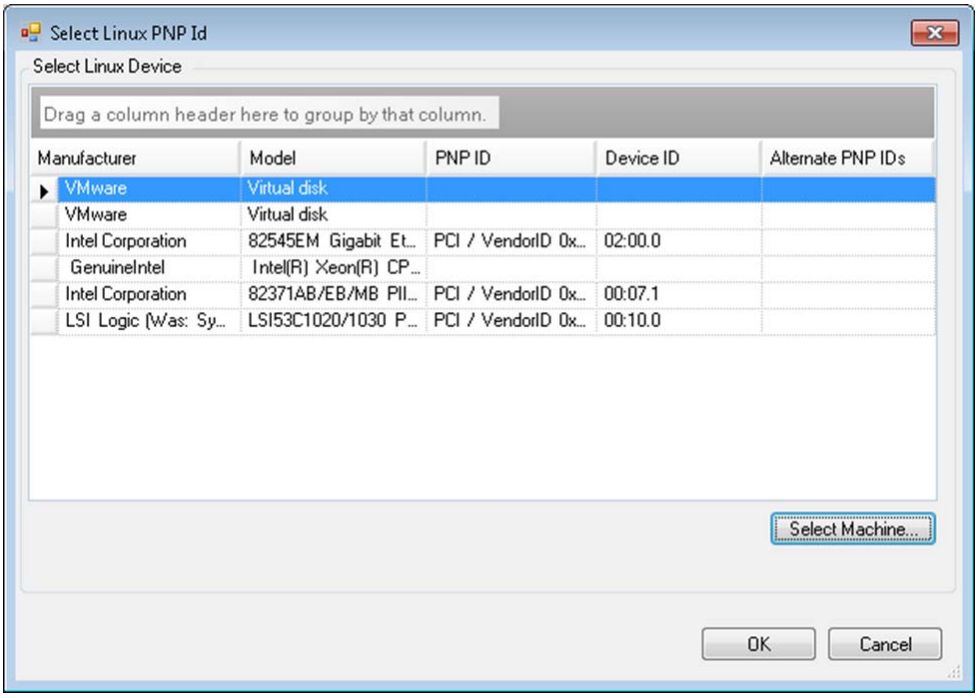
4b (Conditional) Select an ID from a previously discovered workload:

4b1 Adjacent to the *Linux PnP ID* field, click *Select* to open the Select Linux PnP ID dialog box.



4b2 On the dialog box, click *Select Machine* to display a list of the machines previously discovered by the PlateSpin Linux RAM disk.

4b3 Highlight one of the devices in the list, then click *Select* to populate the list in the Select Linux PnP ID dialog box.



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

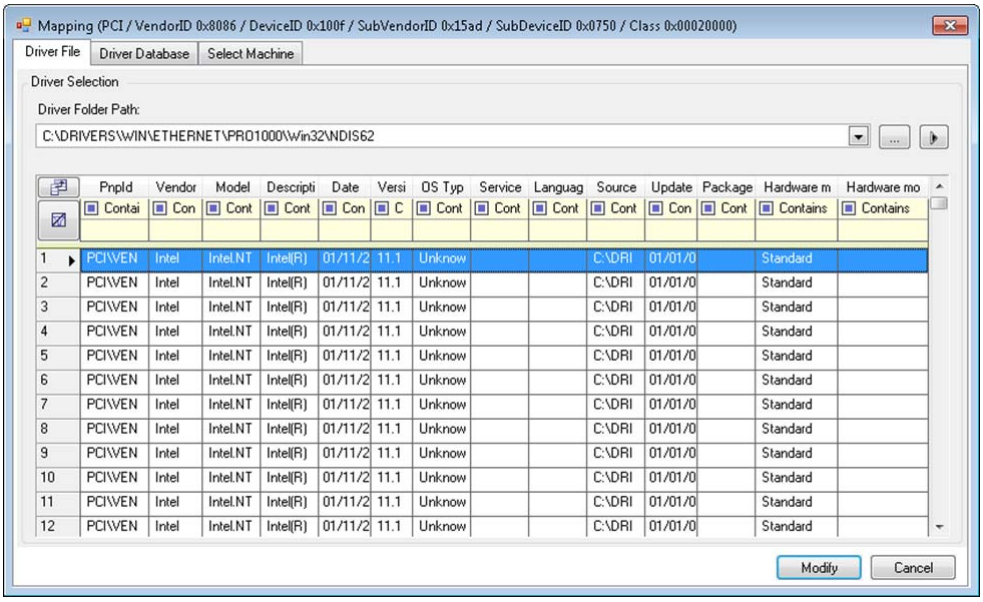
5 In the *Windows PNP ID* field, add a Windows PnP ID:

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

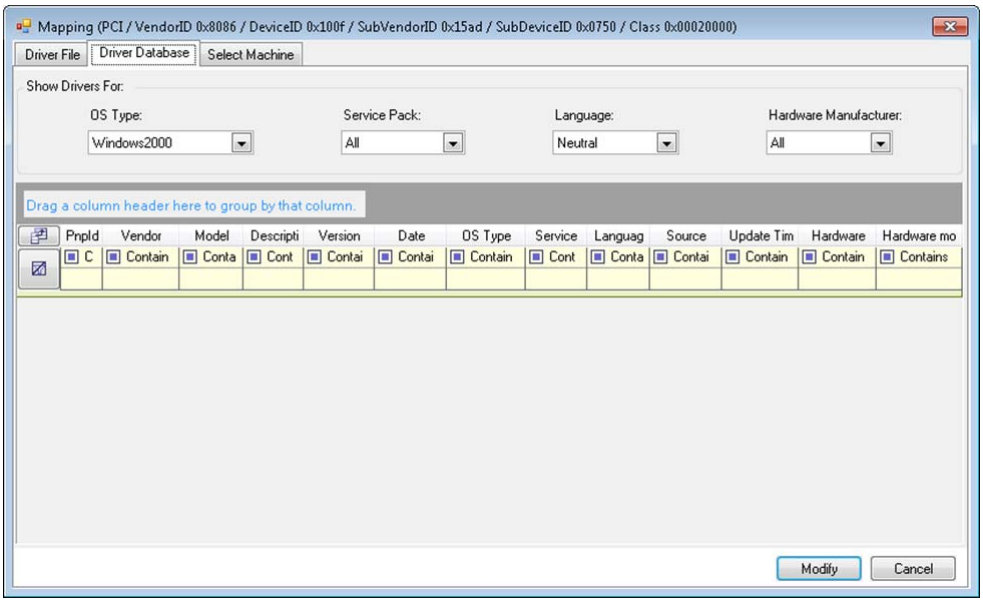
or

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

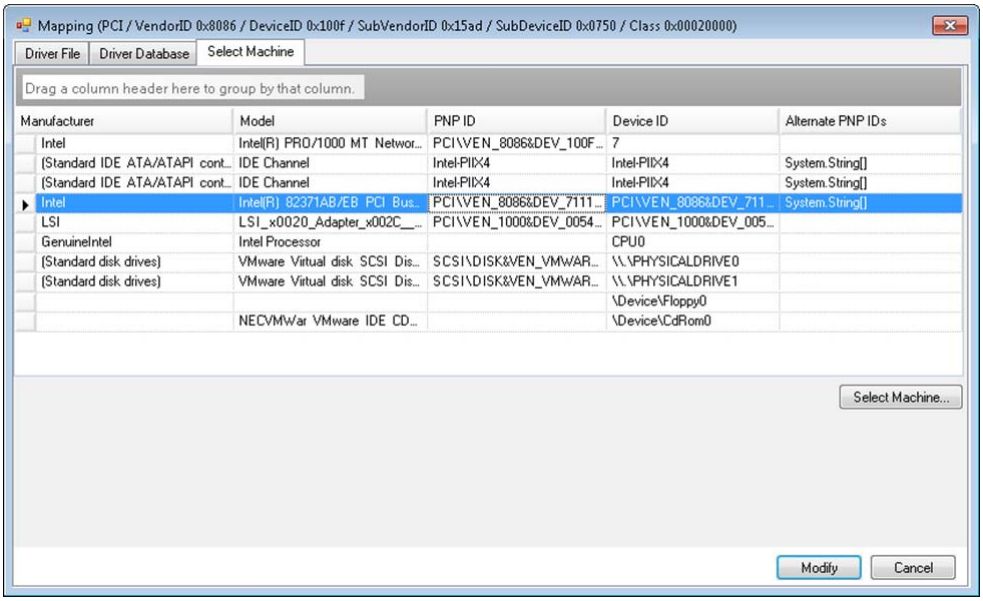
- Under the *Driver File* tab, browse to and select a Windows driver file (that is, a file with the *.`inf` extension), select the desired PnP ID, then click *Modify*.



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

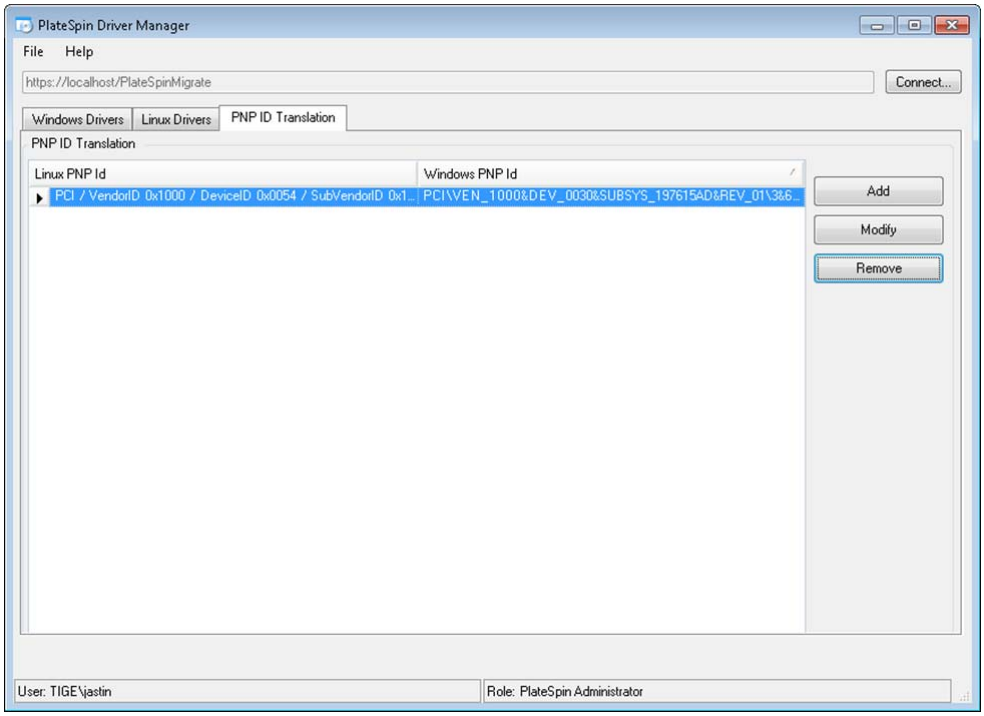


- Under the *Select Machine* tab, click *Select Machine*, then, from the list of Windows machines discovered using live discovery, select a machine, click *OK* to display its devices, select the desired PnP ID, then click *Modify*.



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

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



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

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

To modify,

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

7b Repeat Step 5 on page 95 to modify the Windows PnP ID.

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

---

8 Troubleshooting

8.1 Troubleshooting Workload Inventory (Windows)

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

Problems or Messages	Solutions
`The domain in the credentials is invalid or blank`	This error occurs when the Credential Format is incorrect. Try the discovery by using a local administrator account with the credential format `hostname\LocalAdmin` Or, try the discovery by using a domain administrator account with the credential format `domain\DomainAdmin`
`Unable to connect to Windows server...Access is denied`	A non-account was used when trying to add a workload. Use an administrator account or add the user to the administrators group and try again. This message might also indicate WMI connectivity failure. For each of the following possible resolutions, attempt the solution and then perform the “WMI Connectivity Test” on page 101 again. If the test succeeds, try adding the workload again. ◆ “Troubleshooting DCOM Connectivity” on page 101 ◆ “Troubleshooting RPC Service Connectivity” on page 101
`Unable to connect to Windows server...The network path was not found`	Network connectivity failure. Perform the tests in “Performing Connectivity Tests” on page 100. If a test fails, ensure that PlateSpin Forge and the workload are on the same network. Reconfigure the network and try again.

Problems or Messages	Solutions
`D"iscover Server Details {hostname}" Failed Progress: 0% Status: NotStarted`	This error can occur for several reasons and each has a unique solution: ◆ For environments using a local proxy with authentication, bypass the proxy or add the proper permissions. See KB Article 7920339 (https://www.netiq.com/support/kb/doc.php?id=7920339) for more details. ◆ If local or domain policies restrict required permissions, follow the steps outlined in KB Article 7920862 (https://www.netiq.com/support/kb/doc.php?id=7920862).

Workload Discovery fails with error message
`Could not find file output.xml`
or
`Network path not found`
	There are several possible reasons for the `Could not find file output.xml` error:
	◆ Antivirus software on the source could be interfering with the discovery. Disable the antivirus software to determine whether or not it is the cause of the problem. See "Disabling AntiVirus Software" on page 102.
	◆ File and Printer Sharing for Microsoft Networks might not be enabled. Enable it under the Network Interface Card properties.
	◆ The Admin$ shares on the source might not be accessible. Ensure that PlateSpin Forge can access those shares. See "Enabling File/Share Permissions and Access" on page 102.
	◆ The Server or the Workstation service might not be running. If this is the case, enable them and set the startup mode to `automatic`.
	◆ The Windows remote registry service is disabled. Start the service and set the startup type to automatic.

This section also contains the following information:

8.1.1 Performing Connectivity Tests

Network Connectivity Test

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

1 Go to your Forge VM.

See "Downloading the VMware Client Program" on page 43.

2 Open a command prompt and ping your workload:

`ping` *workload_ip*

WMI Connectivity Test

1 Go to your Forge VM.

See "Downloading the VMware Client Program" on page 43"Downloading the VMware Client Program" on page 43.

2 Click *Start* > *Run*, type `Wbemtest` and press `Enter`.

3 Click *Connect*.

4 In the *Namespace*, type the name of the workload you are trying to discover with `\root\cimv2` appended to it. For example, if the hostname is `win2k`, type:

`\\win2k\root\cimv2`

5 Enter the appropriate credentials, using either the `hostname\LocalAdmin` or `domain\DomainAdmin` format.

6 Click *Connect* to test the WMI connection.

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

Troubleshooting DCOM Connectivity

1 Log into the workload that you want to protect.

2 Click *Start* > *Run*.

3 Type `dcomcnfg` and press Enter.

4 Check connectivity:

- For Windows systems (XP/Vista/2003/2008/7), the Component Services window is displayed. In the *Computers* folder of the console tree of the Component Services administrative tool, right-click the computer that you want to check for DCOM connectivity, then click *Properties*. Click the *Default Properties* tab and ensure that *Enable Distributed COM on this computer* is selected.
- On a Windows 2000 Server machine, the DCOM Configuration dialog box is displayed. Click the *Default Properties* tab and ensure that *Enable Distributed COM on this computer* is selected.

5 If DCOM was not enabled, enable it and either reboot the server or restart the Windows Management Instrumentation Service. Then try adding the workload again.

Troubleshooting RPC Service Connectivity

There are three potential blockages for the RPC service:

- The Windows Service
- A Windows firewall
- A network firewall

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

- Putting PlateSpin Forge and the workload on the same side of the firewall
- Opening up specific ports between PlateSpin Forge and the workload (See "Access and Communication Requirements across your Protection Network" on page 25.

8.1.2 Disabling AntiVirus Software

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

8.1.3 Enabling File/Share Permissions and Access

To successfully protect a workload, PlateSpin Forge needs to successfully deploy and install software within the workload. Upon deployment of these components to a workload, as well as during the Add Workload process, PlateSpin Forge uses the workload's administrative shares. PlateSpin Forge needs administrative access to the shares, using either a local administrator account or a domain administrator account for this to work.

To ensure that the Administrative shares are enabled:

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

After confirming that the shares are enabled, ensure that they are accessible from within the Forge VM:

1. Go to your Forge VM.

   See "Downloading the VMware Client Program" on page 43.
2. Click *Start* > *Run*, type `\\<server_host>\Admin$`, then click *OK*.
3. If you are prompted, use the same credentials as those you will use to add the workload to the PlateSpin Forge workload inventory.

   The directory is opened and you should be able to browse and modify its contents.
4. Repeat the process for all shares with the exception of the IPC$ share.

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

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

8.2 Troubleshooting Workload Inventory (Linux)

Problems or Messages	Solutions
`Unable to connect neither to the SSH server running on <IP_address> nor to VMware Virtual Infrastructure web-services at <ip_address>/sdk`	This message has a number of possible causes: ◆ The workload is unreachable. ◆ The workload does not have SSH running. ◆ The firewall is on and the required ports have not been opened. ◆ The workload's specific operating system is not supported. For network and access requirements for a workload, see "Access and Communication Requirements across your Protection Network" on page 25.
`Access denied`	This authentication problem indicates either an invalid username or password. For information on proper workload access credentials, see "Guidelines for Workload Credentials" on page 78.

8.3 Troubleshooting Problems during the Prepare Replication Command (Windows)

Problems or Messages	Solutions
Authentication error when verifying the controller connection while setting up the controller on the source.	The account used to add a workload needs to be allowed by this policy. See "Group Policy and User Rights" on page 103.
Failure to determine whether .NET Framework is installed (with exception `The trust relationship between this workstation and the primarydomain failed`).	Check whether the Remote Registry service on the source is enabled and started. See also "Troubleshooting Workload Inventory (Windows)" on page 99.

8.3.1 Group Policy and User Rights

Because of the way that PlateSpin Forge interacts with the source workload's operating system, it requires the administrator account that is used to add a workload to have certain user rights on the source machine. In most instances, these settings are defaults of group policy; however, if the environment has been locked down, the following user rights assignments might have been removed:

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

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

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

8.4 Troubleshooting Workload Replication

Problems or Messages	Solutions
Recoverable error during replication either during *Scheduling Taking Snapshot of Virtual Machine* or *Scheduling Reverting Virtual Machine to Snapshot before Starting*.	This problem occurs when the server is under load and the process is taking longer than expected. Wait until the replication is complete.
Workload issue requires user intervention	Several types of issues might cause this message. In most cases the message should contain further specifics about the nature of the problem and the problem area (such as connectivity, credentials, . After troubleshooting, wait for a few minutes. If the message persists, contact PlateSpin Support.
All workloads go into recoverable errors because you are out of disk space.	Verify the free space. If more space is required, remove a workload.
Slow network speeds under 1 MB.	Confirm that the source machine's network interface card's duplex setting is on and the switch it is connected to has a matching setting. That is, if the switch is set to auto, the source can't be set to 100 MB.
Slow network speeds over 1 MB.	Measure the latency by running the following command from the source workload: `ping ip-t` (replace *ip* with the IP address of your Forge VM). Allow it to run for 50 iterations and the average indicates the latency. Also see "Optimizing Data Transfer over WAN Connections" on page 31.

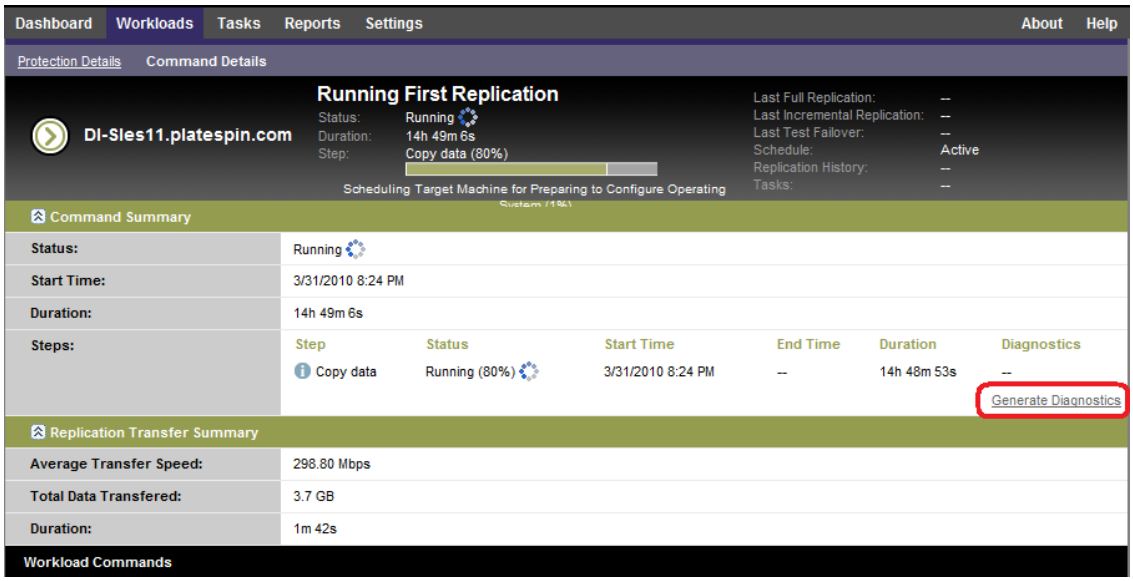
`The file transfer cannot begin - port 3725 is already in use`
or
`3725 unable to connect`
	Ensure that the port is open and listening:
	Run `netstat -ano` on the workload.
	Check the firewall.
	Retry the replication.

Problems or Messages	Solutions
`Controller connection not established` Replication fails at the *Take Control of Virtual Machine* step.	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 VM. Change the replication IP to a static IP or enable the DHCP server. Ensure that the virtual network selected for replication is routable to the Forge VM.
Replication job does not start (stuck at 0%)	This error can occur for different reasons and each has a unique solution: ◆ For environments using a local proxy with authentication, bypass the proxy or add proper permissions to resolve this problem. See KB Article 20339 (https://www.netiq.com/support/kb/doc.php?id=7920339) for more details. ◆ If local or domain policies restrict required permissions, follow the steps outlined in KB Article 7920862 (https://www.netiq.com/support/kb/doc.php?id=7920862). This is a common issue when Forge VM is affiliated with a domain and the domain policies are applied with restrictions. See “Group Policy and User Rights” on page 103.

8.5 Generating and Viewing Diagnostic Reports

In the PlateSpin Forge Web Interface, after you have executed a command, you can generate detailed diagnostic reports about the command’s details.

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



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

2 Click *View*.

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

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

8.6 Removing Workloads

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

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

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

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

2 On the Command Confirmation page, click *Confirm* to execute the command.

Wait for the process to complete.

8.7 Post-Protection Workload Cleanup

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

8.7.1 Cleaning Up Windows Workloads

Component	Removal Instructions
PlateSpin Block-Based Transfer Component	See KB Article 7005616 (https://www.netiq.com/support/kb/doc.php?id=7005616).
Third-party Block-based Transfer Component (discontinued)	1. Use the Windows Add/Remove Programs applet (run `appwiz.cpl`) and remove the component. Depending on the source, you might have either of the following versions: ◆ SteelEye Data Replication for Windows v6 Update2 ◆ SteelEye DataKeeper For Windows v7 2. Reboot the machine.
File-based Transfer Component	At root level for each volume under protection, remove all files named `PlateSpinCatalog*.dat`
Workload Inventory software	In the workload's `Windows` directory: ◆ Remove all files named `machinediscovery*`. ◆ Remove the subdirectory named `platespin`.
Controller software	1. Open a command prompt and change the current directory to: ◆ `\Program Files\platespin*` (32-bit systems) ◆ `\Program Files (x86)\platespin*` (64-bit systems) 2. Run the following command: `ofxcontroller.exe /uninstall` 3. Remove the `platespin*` directory

8.7.2 Cleaning Up Linux Workloads

Component	Removal Instructions
Controller software	◆ Kill these processes: ◆ `pkill -9 ofxcontrollerd` ◆ `pkill -9 ofxjobexec` ◆ remove the OFX controller rpm package: `rpm -e ofxcontrollerd` ◆ In the workload's file system, remove the `/usr/lib/ofx` directory with its contents.

Component	Removal Instructions

Block-level data transfer software	1. Check if the driver is active:
	`lsmod | grep blkwatch`
	If the driver is still loaded in memory, the result should contain a line, similar to the following:
	`blkwatch_7616 70924 0`
	2. (Conditional) If the driver is still loaded, remove it from memory:
	`rmmod blkwatch_7616`
	3. Remove the driver from the boot sequence:
	`blkconfig -u`
	4. Remove the driver files by deleting the following directory with its contents:
	`/lib/modules/`*`[Kernel_Version]`*`/Platespin`
	5. Delete the following file:
	`/etc/blkwatch.conf`

LVM snapshots	LVP snapshots used by ongoing replications are named according to a *`volume_name`*`-PS-snapshot` convention. For example, a snapshot of a `LogVol01` volume will be named `LogVol01-PS-snapshot`. To remove these LVM snapshots: 1. Generate a list of snapshot on the required workload by using one of the following ways: ◆ Use the PlateSpin Forge Web Interface to generate a Job Report for the failed job. The report should contain information about LVM snapshots and their names. - OR - ◆ On the required Linux workload, run the following command to display a list of all volumes and snapshots: `# lvdisplay -a` 2. Note the names and locations of the snapshots you want to remove. 3. Remove the snapshots by using the following command: `lvremove` *snapshot_name*
Bitmap files	For each volume under protection, at the root of the volume, remove the corresponding `.blocks_bitmap` file.
Tools	On the source workload, under `/sbin`, remove the following files: ◆ `bmaputil` ◆ `blkconfig`

8.8 Shrinking the PlateSpin Forge Databases

When the PlateSpin Forge databases (OFX, PortabilitySuite, and Protection) reach a predetermined capacity, cleanup on those databases occurs at regular intervals. If there is a need to further regulate the size or content of those databases, Forge provides a utility (`PlateSpin.DBCleanup.exe`) to further clean up and shrink those databases. KB Article 7006458 (https://www.netiq.com/support/kb/doc.php?id=7006458) explains the location of the tool and the options available for it, should you decide to use it for offline database operations.

Glossary

Appliance Host. *See* Container.

Container. The VM host that contains the failover workload (a protected workload's bootable virtual replica).

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

Failback. Restoration of the business function of a failed workload in its original environment when the business function of a temporary failover workload within PlateSpin Forge is no longer required.

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

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

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

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

Management VM. The management virtual machine containing the PlateSpin Forge software.

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

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

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

Recovery Point. A point-in-time snapshot, allowing a replicated workload to be restored to a previous state.

Recovery Point Objective (RPO). Tolerable data loss measured in time and defined by a configurable interval between incremental replications of a protected workload.

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

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

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

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

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

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

See also Target.

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

See also Source.

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

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

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