PlateSpin Forge 4.0

January, 2014

Version 4.0, a hardware and software release of Forge, provides new features, enhancements, and bug fixes.

For Release Notes documents that accompanied previous 3.*x* releases, visit the PlateSpin Forge 3 Documentation Web Site and go to *Previous Releases* in the Table of Contents at the bottom of the main page.

1 About This Release

1.1 New Features

- The bootstrap operating system used by the Failback ISO for Windows workloads has been transitioned from WinPE to SLES with Linux RAM disk. This change enables volume resizing during failback and replications running longer than 24 hours.
- Workloads running SUSE Linux Enterprise Server (SLES) 11 Support Pack 2 (SP2) and Novell Open Enterprise Server (OES) 11 SP1/SP2 are now supported.

  SLES 11 SP3 workloads are technically enabled (in preview of future product releases) but have not been formally tested.
- Microsoft Windows workloads can now be replicated using block-based transfers without requiring the installation (and associated reboot) of the Block Based Transfer (BBT) file system driver.
- A plug and play hardware ID translation feature is now included in the PlateSpin Driver Manager. The feature applies a standard transformation to the Linux plug and play ID to determine the Windows plug and play ID.

1.2 Discontinued Features

- **Documentation Localization:** Product documentation and the integrated WebHelp system accompanying this release is not localized to languages other than English. Future releases will be localized. Note that the English version of product documentation is located at the PlateSpin Forge 3.4 Documentation Web Site.
- **Upgrade:** Upgrading from previous versions has been disabled in this release. It will be re-enabled in future releases.
- **File-based replication:** File-based replication has been disabled in this release. It will be re-enabled in future releases.
- **Some Workload OS support:** Support for Microsoft Windows 2000, Windows XP and Windows Server 2003 SP0 workloads has been disabled in this release. Support for these workload operating systems might be re-enabled in future releases.

2 Bug Fixes

This release addresses the following bugs:

- **770964 (Windows) Problem running custom configuration script:** An issue with how the product handled batch files prevented certain custom configuration scripts from running properly.
- **753157 Replication reports by e-mail not functioning properly:** In some situations the removal of an email account that was listed as a recipient for PlateSpin Forge e-mail notifications might cause erratic behavior, such as 'flooding'.
- **753449 (Windows) Workload hostname failing to change as required:** In some cases the system might fail to assign a new hostname to the failover VM of a protected Windows Server 2008 workload when it was configured to join a domain.
- **770996 Wrong user in Events report:** In Events reports, all *Add Workload* jobs were erroneously shown as initiated by `system`, instead of the actual username.
- **762850 (Linux) Unable to use non-default shells:** PlateSpin Forge failed to protect Linux workloads that had a command line interpreter other than the Bash shell, which PlateSpin Protect Server uses by default. You can now override the default shell used by PlateSpin Forge Server to execute commands on a Linux workload.See KB Article 7010676.
- **756871 (Linux) Incorrect sequence of 2 NICs on target after failover:** In some cases an issue with target NIC mapping caused networking problems, such as the Novell eDirectory service binding to the wrong NIC.
- **773097 (Windows XP) Incorrect SCSI controller type on failover VM:** VM replicas of Windows XP workloads were being assigned `BusLogic` SCSI controllers (instead of `LSI` SCSI controllers), which negatively impacted failover functionality.
- **768137 (Windows) Registry hives not replicating correctly during incrementals:** In some cases an issue with how Windows Registry changes are handled in Windows Server 2003 and Windows XP might result in a mismatch between the Registries of a protected workload and its VM replica.
- **734525 (Linux) Unable to connect to port 3725:** An issue with how communication with a Linux workload with two NICs was being managed might occasionally cause problems in connectivity.
- **744867 Problem inventorying NLB cluster hosts:** In some cases an issue with the collection and processing of Windows Network Load Balancing (NLB) Cluster hosts might cause configuration problems on the VM replica.
- **722096 Failover VM info removed from inventory upon refreshing container:** Occasionally, when the PlateSpin Server was unable to properly retrieve information from its container, a Refresh Container operation might result in the removal of information about the failover VM, negatively impacting the protection contract and failover functionality.
- **697049 Protection contract broken after vNIC's MAC address change:** After setting up a protection contract, changing the MAC address of the failover VM's virtual network adapter (either manually or automatically by the hypervisor) impaired the contract.
- **672815 Unable to start initial full replication due to missing vNIC-to-vNetwork mapping:** In some situations during the Prepare Replication operation, a container refresh might interfere with the collection of inventory information about a newly created failover VM, impacting its network mapping and impairing the replication.
- **736280 Erroneous localhost.localdomain hostname in Linux failback:** On failback, if the target hostname was set to No Change, the workload was assigned a `localhost.localdomain` hostname.

3 Known Issues

- **Support for the GUID Partition Table (GPT) standard:** PlateSpin Forge supports the protection of workloads that use the GPT disk partition layout standard. However, targets are always configured to boot from BIOS using an MBR (Master Boot Record). This limitation has the following implications:
  - **Max 2 TB per volume:** The maximum size of a protected workload's volumes is restricted to 2.19 terabytes, the maximum for a partition allowed by MBR.
  - **Physical targets for failback must boot from BIOS:** Most hardware vendors provide support for multiple disk partitioning standards; for information on how to configure a physical target to boot from BIOS, or to reconfigure GPT hardware to operate in "legacy mode" (with support for BIOS), see your hardware vendor documentation.

  See also KB Article 7005452.
- **781217 (SLES 9) Issue with volumes mounted using UUIDs:** An issue with how mount points on SLES 9 workloads are looked up and how PlateSpin Forge handles Linux volumes might negatively impact the protection of SLES 9 workloads with volumes that are mounted by UUIDs. This issue is being investigated.

  Workaround: Modify the workload's `/etc/fstab` configuration file to use device names instead of UUIDs for storage devices and partitions. See KB Article 7010812.
- **686911 Problems with file downloads from or uploads to datastore:** Under certain conditions, where the protection target is a VMware DRS Cluster, the system might fail to upload or download a file, such as a boot ISO image. This negatively impacts a protection contract.

  See KB Article 7008306.
- **595490 Preserving boot partition on failback causes failback to stall:** In some failback scenarios, the system improperly allows you to preserve an active (or boot) partition on the target, preventing the target from booting properly. This issue is under investigation.

  Workaround: In Failback Details, do not opt to preserve any boot partitions on the target.
- **698611 Full cluster replication failure under certain circumstances:** If a Windows 2008 R2 Cluster protection contract is set up through the *sync to an existing VM* method, and if the active cluster node flips prior to the full replication, the full replication job fails.

  See KB Article 7008771.
- **655828 Failure to mount NSS volumes:** Upon failover or test failover, NSS volumes with snapshots enabled are not automatically mounted as expected.

  See KB Article 7008773.
- **680259 (VMware 4.1) Poor networking performance by traffic-forwarding VMs:** In some scenarios, the replica of a workload that is forwarding network traffic (for example, if the workload's purpose is to serve as a network bridge for NAT, VPN, or a firewall) might show significant network performance degradation. This is related to a problem with VMXNET 2 and VMXNET 3 adapters that have LRO (large receive offload) enabled.

  Workaround: Disable LRO on the virtual network adapter. For details, see the VMware vSphere 4.1 Release Notes (http://www.vmware.com/support/vsphere4/doc/vsp_esxi41_vc41_rel_notes.html). Sscroll down to the bulleted item `Poor TCP performance...`.
- **No software RAID support for Linux workloads:** PlateSpin Forge does not support Linux workloads with volumes on software RAID.
- **590635 Inconsistent failover results after upgrading:** Following an upgrade to PlateSpin Forge, a failover operation might fail to complete or might not apply the correct failover parameters, such as the proper hostname and workgroup settings.

  Workaround: Before performing a failover, run a replication.

- **581860 Browser exception in the Chinese edition of the product:** 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.
- **610918 Unresponsive Expand and Collapse icons in integrated help:** On some systems with enhanced browser security settings (such as Internet Explorer 8 on Windows Server 2008), the Expand and Collapse icons (+ and -) in the Table of Contents might fail to work. To fix the issue, enable JavaScript in your browser:
  - **Internet Explorer:** Click *Tools* > *Internet Options* > *Security* tab > *Internet* zone > *Custom level*, then select the *Enable* option for the *Active Scripting* feature.
  - **Firefox:** Click *Tools* > *Options* > *Content* tab, then select the *Enable JavaScript* option.
- **558937 Failure of block-level replications that use VSS (Windows):** If you are using third-party VSS-based backup software, block-level replications might occasionally fail.

  Workaround: Use blackout windows (see "Protection Tiers" in your *User Guide*).
- **611105 Missing protection contracts after upgrade:** After upgrading your Forge appliance to version 3, protection contracts with workloads in a *Ready for Failback* or a *Ready for Reprotect* state might be missing from the user interface. This issue is under consideration for an upcoming fix.

4 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.