PlateSpin Protect 10.4 Release Notes

July 31, 2013

Version 10.4 provides new features and enhancements.

For Release Notes documents that accompanied previous 10.*x* releases, visit the PlateSpin Protect 10 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 in This Release

- The PlateSpin boot ISO now uses Linux RAM disk instead of Microsoft WinPE.
- 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.
- PlateSpin Protect can now use non-root accounts to manage VMware containers (that is, it supports VMware multi-tenancy)
- 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 Protect 10.4 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 Known Issues

- **No software RAID support for Linux workloads:** PlateSpin Protect does not support Linux workloads with volumes on software RAID.
- **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*).
- **590635 Inconsistent failover results after upgrading:** Following an upgrade to PlateSpin Protect, 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.
- **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.
- **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.
- **638392 ESX 4.1:** Direct host discovery results in missing VM port groups if dvSwitch port groups share the same name.

  Workaround: Ensure that port group names are unique.
- **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). Scroll down to the bulleted item `Poor TCP performance...`
- **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.
- **702152 Protection over a WAN takes a long time if VM container has a large number of datastores:** Under some circumstances the process of locating the appropriate ISO image required for booting the target might take longer than expected. This might happen when your PlateSpin Server is connected to the VM container over a WAN and your VM container has a large number of datastores. This issue is under investigation.

- **737715 Unable relocate failover VM using Storage vMotion:** In some circumstances, where your protection container is a VMware DRS Cluster in vSphere 5 and the initial replica of the workload is created incrementally, Storage vMotion might be unable to relocate the failover VM's disk files across shared storage locations.

  Workarounds: To work around the issue, use one of the following:

  - Use the VMware vSphere Client to unregister and re-register the failover VM, then attempt to relocate the VM using Storage vMotion.

    - OR -

  - Apply the VMware ESXi 5.0 Patch ESXi500-201109401-BG, which addresses an underlying issue. Reboot the host (required), then attempt to relocate the VM using Storage vMotion.

    For further technical information about the issue, see VMware Knowledge Base article 2005740 (http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2005740).

- **756454 (vSphere 5) Recovery points are stored in the same datastore as the target virtual machines' VMDK files:** When protecting a workload to a vSphere 5 DRS Cluster or ESXi Server container, indicating a *Configuration File Datastore* location only determines the storage location of the failover VMs' `.VMX` file, but not the storage location of Recovery Point snapshots. This might result in inaccurate free space calculation, impacting validation.

  For further information, see KB Article 7005494.

- **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 Protect 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.

3 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.