

PlateSpin Migrate 9.3 Release Notes

July 31, 2013



Version 9.3 provides a number of new features, enhancements, and bug fixes.

For documentation that accompanied earlier 9.x releases, visit the [PlateSpin Migrate 9 Documentation Web Site](#).

- ♦ [Section 1, "New Features in This Release," on page 1](#)
- ♦ [Section 2, "Discontinued Features," on page 1](#)
- ♦ [Section 3, "Bug Fixes," on page 2](#)
- ♦ [Section 4, "Known Issues," on page 2](#)
- ♦ [Section 5, "Legal Notice," on page 4](#)

1 New Features in This Release

- ❑ **New workload types:** This release introduces support for migrating workloads that run the following operating systems:
 - ♦ Windows 8
 - ♦ Windows Server 2012

See the ["Supported Source Workloads and Target Platforms"](#) section in your *User Guide*.

- ❑ **Linux RAM disk:** The PlateSpin boot ISO now uses Linux RAM disk for the temporary pre-execution environment for the migration of all workload types.
- ❑ **New hypervisor (virtualization platform) support:** This release introduces support for two new virtualization platforms:
 - ♦ Microsoft Windows Server 2012 with Hyper-V
 - ♦ Citrix XenServer 6.1

Both of these platforms use semi-automated workload virtualization. See the ["Supported Target Virtualization Platforms"](#) section of the *User Guide*.

- ❑ **PnP ID Translation:** As part of the replacement of Windows PE, a PnP hardware ID translation feature is now included in the PlateSpin Driver Manager. The feature applies a standard transformation to the Linux PnP ID to determine the Windows PnP ID.

2 Discontinued Features

- ♦ **Discontinued:** The following features have been discontinued in this release:
 - ♦ Support for Microsoft Windows Server 2008 R2 with Hyper-V (semi-automated) and Citrix XenServer 5.5 as target virtualization platforms (fully automated).
 - ♦ Support for Windows Clusters workloads.
 - ♦ Microsoft WinPE as the temporary pre-execution environment for migration.

- ♦ **Temporarily Discontinued:** The following features have been temporarily discontinued in this release.
 - ♦ Support for imaging (X2I and I2X scenarios).
 - ♦ File-based transfer on Windows workloads.
 - ♦ Support for offline Windows workload migration.
 - ♦ Microsoft Windows workload conversions (Windows 2000, Windows XP, Windows 2003 SP0)
 - ♦ Support for Windows workloads with FAT volumes.
 - ♦ Upgrading from previous versions has been disabled in this release. It will be re-enabled in future releases.

3 Bug Fixes

The following is a list of bugs that were fixed for this release:

- ♦ **698884 Virtual CD-ROM drive is unavailable after V2V migration or failover.** VMware Tools are now uninstalled from the target VM upon configuration.
- ♦ **548208 ESX servers (managed by vCenter) without datastores are not discovered.** Although the discovery occurs normally now, the validation prevents these servers from being used as targets. A message displays stating that there are no datastores configured. Users can refresh and use the ESX server successfully.

4 Known Issues

- ♦ **No software RAID support for Linux workloads:** PlateSpin Migrate does not support Linux workloads with volumes on software RAID.
- ♦ **Requirements for VMware DRS Cluster support:** PlateSpin Migrate supports VMware Clusters with and without DRS enabled, and with any level of DRS (*Manual*, *Partially Automated*, or *Fully Automated*). However, to be a valid migration target, your VMware Cluster must be discovered via vCenter and not by directly inventorying individual ESX servers. See [“Discovery Guidelines for Machine Types and Credentials”](#) in your *User Guide*.
- ♦ **Support for the GUID Partition Table (GPT) standard:** PlateSpin Migrate supports the migration 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 the volumes of a migration source restricted to 2.19 a workload’s terabytes, the maximum for a partition allowed by MBR.
 - **X2P targets must boot from BIOS:** Most hardware vendors provide support for both disk partitioning standards; for information on how to configure an X2P 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](#).
- ♦ **Workloads cannot be migrated to Extensible Firmware Interface (EFI)-enabled hardware:** This issue is currently under investigation.

- ◆ **493589 (Windows sources) Non-default per-volume VSS settings are not preserved after migration:** This issue is under consideration for an upcoming fix.
- ◆ **505426 (ESX4) No warning or error on wrong vCPU selection:** If the number of the requested vCPUs exceeds the number of physical CPUs on the ESX 4 host, the requested number is ignored and the target VM is created with a single vCPU without a warning. This issue is under consideration for an upcoming fix.
- ◆ **506154 Special character in datastore name causing migration problems:** Migration operations might fail when they are attempted on ESX datastores that have the “+” or other special characters in the datastore name.
See [KB Article 7009373](#).
- ◆ **595490 Preserving boot partition causes migration problems:** In some migration scenarios, the system improperly allows you to preserve your boot partition on the target, preventing the proper workload from booting. This issue is under investigation.
Workaround: Do not opt to preserve your boot partition on the target.
- ◆ **604320 (Linux to ESX 4) Problem completing migration if the source OS has autologin or CD automount features enabled:** The migration is also affected if you log in to the target during the job’s Configuration step.
Workaround: Disable the autologin and CD automount features on the source; avoid logging in to the target workload prior to the completion of the migration.
- ◆ **619942 Failure to execute a post-migration script with Unicode characters in the filename:** If you use Unicode characters in the filename of your post-migration script, the script fails to execute.
Workaround: Use only ASCII characters when naming a post-migration action.
- ◆ **655828 Failure to mount NSS volumes:** After a migration is completed, 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 guidance, 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...).
- ◆ **685509 Failure with ‘Access Denied’ error during replication to an image stored on a network share:** The Controller service on Image servers that use network shares for storage does not preserve the service Log On As credentials after an upgrade. Image operations fail with an Access Denied message until the controller service is updated with the correct Log On As credentials.
See [KB Article 7008772](#).
- ◆ **692680 VSS snapshots are not preserved:** VSS snapshots taken by third-party applications on the source workload are not replicated to the target upon migration.
- ◆ **702152 Migration over WAN taking a long time if target VM host has a high number of datastores:** Under some circumstances, when your Migrate server is connected to the VM host over WAN, and if your VM host has a high number of datastores, the process of locating the appropriate ISO image required for booting the target might take longer than expected. This issue is under investigation.

- ♦ **810460 VMware tools are not installed during a conversion of a Windows 2012 server core:**
VMware tools are not installed during a conversion of a Windows 2012 server core.
Workaround: Install the VMware tools manually after the conversion.
- ♦ **822601 Network card is not initialized on SLES 11 target VM hosted on Windows 2008 Hyper-V host:** If you perform a SLES 11 workload (cloned VM) migration using the semi-automated method to a target VM (faked physical) on a Windows 2008 Hyper-V host, the process freezes at the "Configuring OS" step.
Workaround: For information about working around this issue, see [KB 7012911](#).
- ♦ **824724 Target VM does not boot after migration from VMware ESX to Citrix Xen if boot files are located in second disk:** When a VM is converted from VMware ESX to Citrix Xen and its boot files are allocated in second disk, the VM does not boot and manual intervention is requested. This is because Citrix XEN VM tries to boot with disk 0 rather than with the bootfiles allocated to disk 2.
Workaround: To resolve this problem, rearrange the virtual-disk position in XenCenter so that the virtual machine boots from the virtual disk containing the operating system. [The knowledge article at the Citrix Web site \(http://support.citrix.com/servlet/KbServlet/download/32320-102-691310/xcm-10-guide.pdf\)](http://support.citrix.com/servlet/KbServlet/download/32320-102-691310/xcm-10-guide.pdf) includes information about how to change the position of the virtual disk containing the operating system.
See also [KB Article 7012906](#).
- ♦ **825016 XenServer tools are not being removed after conversion:** XenServer tools on a Windows VM in a Citrix XenServer hypervisor environment are not removed when the VM is converted to a VMware container or a physical container.
Workaround: The user must manually uninstall the XenServer tools after conversion.
- ♦ **825434 After migration, the primary partition (C:) is converted to a logical partition on the target:** *Scenario:* Moving or copying a Windows OS machine with more than three primary partitions to a physical machine where a Windows OS has been installed with minimum 3 primary partitions. At least one primary partition is preserved in the target machine.
Effect: After the migration, the Windows OS machine is unable to boot.
Example: The following error occurs when Windows 2003 machine is converted to Physical machine:


```
Windows could not start because the following file is missing or corrupt:  
<Windows root>\system32\ntoskrnl.exe.Please re-install a copy of the above  
file.
```


Workaround: For information about working around this issue, see [KB 7012913](#).
- ♦ **825841 Image Server Installation is available as an option, but Imaging is not available in the 9.3 release:** When you install PlateSpin Migrate and then discover any Windows computer, the option to install the PlateSpin Image Server is available. Although the installation option is available in the interface, the product does not support imaging capability in version 9.3.
- ♦ **826545 When Migrate undiscovers a machine, the machine node shown on the ESX host is not undiscovered:** When you undiscover a workload, it displays as such in the Migrate client, but the ESX host shows that the node is not undiscovered.
Workaround: Undiscover the workload on the ESX host, then refresh the ESX host.

5 Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE

AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

© 2013 NetIQ Corporation and its affiliates. All Rights Reserved.

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.