Release Notes for Cisco UCS Invicta Scaling System, Version 5.0.1.3b

March 23, 2016

Contents

Introduction

This document describes changes to the Cisco UCS Invicta OS and the open and resolved caveats for the Cisco UCS Invicta Scaling System.

The ID numbers listed in the caveat tables in this document refer to a legacy system numbering scheme. Those numbers will not be found in the CDETS system, except where noted.

CiscoSystems,Inc.
www.cisco.com

System Requirements

This release supports the Cisco UCS Invicta Scaling System only.

Note Before an upgrade to the Cisco UCS Invicta OS 5.0.1.3b service pack can take place, the following prerequisites must be met:

- You must be logged in as the "admin" user.
- Ensure that the Cisco UCS Invicta OS 5.0.1.3 for the Cisco UCS Scaling System is installed.
- Ensure that all UCS C240 M3 Hardware is running BIOS/CIMC Release version 2.0(3i).
- I/O to the storage device must be quiesced prior to the upgrade installation.
- Make sure that all SSNs are reachable and in good state prior to the upgrade installation.
- SSRA and SSRB must have the eth2 port (P3) interface available. A second heartbeat cable must be connected to Ethernet Port 2 (P3) between the SSRs. Ensure that if P3 is otherwise occupied, the existing connection must be moved to Ethernet Port 3 (P4).
- Check the SDs' (boot devices) health on SSRs and SSNs using the Cisco Integrated Management Controller (CIMC) to ensure that there are no degraded RAID devices.
- Check the RAID device health using the Invicta GUI to make sure that there are no degraded RAID devices.
- Make sure that there are no degraded LUN mirrors.
- A system reboot is required after the update is completed.

Note HUU 2.0(3i) addresses a memory leak issue where the user was unable to access Cisco IMC using SSH or HTTP. However, pinging Cisco IMC was successful.

.

- Download the Cisco Host Upgrade Utility (HUU) 2.0(3i) (includes CIMC):
  https://software.cisco.com/download/release.html?mdfid=284296254&flowid=31743&softwareid=283850974&release=2.0%283i%29&relind=AVAILABLE&rellifecycle=&reltype=latest
- User guide for HUU (includes CIMC) upgrade:
  http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/lomug/2-0-x/b_huu_2_0_3/b_huu_2_0_3_chapter_011.html

Upgrade Installation Notes

For the addition of the Heartbeat Bond and for the Cisco UCS Invicta Scaling System installation, contact Cisco Technical Support.

Note If the Reserve logical volume (LV) was released prior to the upgrade to Cisco UCS Invicta OS 5.0.1.3b, then the Reserve LV will NOT be automatically created by the WSP package upon install. In this case, create the Reserve LV again manually after the WSP install by logging in as Super User.

⚠
Caution

A device reboot is required to complete this upgrade. I/O to the storage device must be quiesced prior to the upgrade installation. If traffic is present during shutdown, reboot time could increase d r a m a t i c a l l y .

Caveats

Resolved Caveats

Table 1 Resolved Caveats

Legacy Defect ID	Summary
4371 [CSCuo12271 / CSCup15888]	Added NTP functionality to sync ntp time, restart ntp service, get ntp status, and configure NTP.
4562 [CSCup70591]	"Test Autosupport" feature to provide a clear successful message to user when a successful test has been executed as well as adding a log entry to the user accessible log.
4625 [CSCup90385]	Include DMESG date timestamp in Autosupport.
5362 [CSCur31568]	Administration and Installation guides should open in new window.
6030 [CSCus31532, CSCus42989, CSCut45897]	OpenSSL Vulnerabilities: CVE-2014-3513, CVE-2014-3567, CVE-2014-3568, CVE-2014-3569, CVE-2014-3570, CVE-2014-3571, CVE-2014-3572, CVE-2014-8275, CVE-2015-0204, CVE-2015-0205, CVE-2015-0206, CVE-2015-0291, CVE-2015-0204, CVE-2015-0290, CVE-2015-0207, CVE-2015-0286, CVE-2015-0208, CVE-2015-0287, CVE-2015-0289, CVE-2015-0292, CVE-2015-0293, CVE-2015-1787, CVE-2015-0285, CVE-2015-0288
6049 [CSCut43553]	LEAP SECOND 2015 Vulnerability.
6056 [CSCuu02575]	PHP vulnerabilities: CVE-2013-6420 and CVE-2014-3515
[CSCuw84706]	NTP 2015 Vulnerabilities: CVE-2015-7691; CVE-2015-7692; CVE-2015-7701; CVE-2015-7702; CVE-2015-7703; CVE-2015-7704; CVE-2015-7705; CVE-2015-7848; CVE-2015-7849; CVE-2015-7850; CVE-2015-7851; CVE-2015-7852; CVE-2015-7853; CVE-2015-7854; CVE-2015-7855; CVE-2015-7871
[CSCut43965]	factoryReset.sh script has been relocated.
[CSCut91884]	Administration & installation guides from GUI was not reflecting correct document versions
[CSCuy03138]	Provision of reboot requirement after uninstalling the 5.0.1.3b WSP.
[CSCuy27109]	LUN delete error outs while peer SSR is coming online
[CSCuu37404]	Adding a new NTP server corrupts ntp.conf

Open Caveats

Table 2 Open Caveats

Legacy Defect ID	Knowledge Issue	Summary	Workarounds
5689	Asynchronous Replication	Asynchronous Replication job performance will be affected under heavy load conditions.	Reduce the heavy load to allow the asynchronous replication jobs start/complete.
4960/4947 [CSCur07226]	Database	Disabling FC ports manually is not recommended during operations	Refrain from disabling FC ports on SSR nodes.
5858 [CSCus64952]	Fibre Channel	Occasionally, in the event of multiple servers rebooting at the same time or switch/UCS-FI reboot, Multipath SAN booted Linux based servers (Red Hat 7.0, SLES 12Especially) may show some (not all) paths missing. Sometimes, in the case of an Invicta SSR reboot, similar symptoms may be seen, as well.	Use the utility 'issue_lip' and/or 'scan' to recover from a host reboot path loss. For an SSR reboot path loss issue, try performing a host reboot individually.
5771	LUN	If a target SSN becomes inaccessible while a LUN was in progress of being mirrored to, then the mirror operation will fail and the destination LUN would not be automatically deleted.	Please contact Cisco Technical Support.
5946	LUN	MSCS operations (online/offline of CSV) can potentially get blocked while large sized LUNs are being deleted simultaneously.	Perform large size LUN deletion operations on off peak hours.
4429	LUN Mirror	Possible data mismatch when rebooting both SSRs simultaneously after writing to an out-of-sync mirror.	Check LUN mirror status and make sure that all mirrors are in sync before performing a reboot. Perform a reboot on one
5885	Network	Upon Downgrade, heartbeat bondhb does not get removed.	Do not edit or delete the bondhb from any of the SSRs after the WSP has been uninstalled. Please contact Cisco Technical Support.

3264	Snapshots	Performance on LUNs with Snapshots will be 3-to-5 times slower than those without.	Remove unnecessary Snapshots to improve
5233 [CSCur08935]	System	When multiple users issue concurrent configuration changes to snapshots or Async replication, configuration or operation of these features can become unresponsive.	Avoid concurrent configuration changes with multiple users.
5910 [CSCus27263]	System	NTPd.org vulnerability CVE-2014-9293 CVE-2014-9294 CVE-2014-9295 CVE-2014-9296	No workaround is available at this time.
[CSCux84861]	System	ASync Repl-Win Installer download does NOT install CYGWIN Package	User need to install latest Cygwin setup-x86.exe to resolve the issue
[CSCuy78853]	GUI	LUNs which gets created after dlm recovery turns red on SSR's GUI	Make sure when peer SSR is in maintenance mode or unreachable, all the LUN related operations performed on GUI must be completed before peer comes online. Or refrain LUN operations if the peer is in the process of joining the cluster.
[CSCuy23884]	System	Re-installation failed for 5103b rel018 WSP	Delete old installation/uninstallation log files from /var/log/waspinstall

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

---

purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.