Release Notes for Cisco UCS Software, Release 2.0

First Published: September 19, 2011
Last Updated: January 08, 2016
Part Number: OL-25363-01

This document describes system requirements, new features, catalog and bundle images information, resolved caveats, known caveats and workarounds for Cisco UCS Manager Release 2.0(1m), Release 2.0(1q), Release 2.0(1s), Release 2.0(1t), Release 2.0(1w), Release 2.0(1x), 2.0(2m), 2.0(2q), 2.0(2r), 2.0(3a), 2.0(3b), 2.0(3c), 2.0(4a), 2.0(4b), 2.0(4d), 2.0(5a), 2.0(5b), 2.0(5c), 2.0(5d), 2.0(5e), 2.0(5f), 2.0(5g). This document also includes the following:

- Current information that became available after the technical documentation was published
- Related firmware and BIOS versions on blade and rack servers and other Cisco Unified Computing System (UCS) components associated with the releases

Use this release notes as a supplement with the other documents listed in documentation roadmap http://www.cisco.com/go/unifiedcomputing/b-series-doc.

Make sure to review other available documentation on Cisco.com to obtain current information on Cisco UCS Manager.

Separate release notes for the VIC card drivers (which may be released out of sync with other software) are available at http://www.cisco.com/en/US/products/ps10281/prod_release_notes_list.html

Contents

This document includes the following sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Revision History

Table 1 shows the revision history for this document.

Table 1 Online History Change

Part Number	Revision	Date	Description
OL-25363-01	A0	September 19, 2011	Created release notes for Release 2.0(1m). [1]
	B0	October 14, 2011	Updated release notes for Release 2.0(1q).
	C0	November 8, 2011	Updated release notes for Release 2.0(1s).
	D0	November 29, 2011	Updated release notes for Release 2.0(1t).
	E0	December 15, 2011	Updated release notes for Catalog Release 2.0.1o.T.
	F0	February 9, 2012	Updated release notes for Release 2.0(1w).
	G0	March 16, 2012	Updated release notes for Release 2.0(1x).
	H0	March 22, 2012	Updated release notes for Release 2.0(2m).
	I0	April 9, 2012	Updated release notes for Release 2.0(2q).
	J0	May 25, 2012	Updated release notes for Release 2.0(2r).
	K0	June 21, 2012	Updated release notes for Release 2.0(3a).
	L0	June 28, 2012	Updated release notes for Catalog Release 2.0.3e.T.
	M0	July 10, 2012	Updated release notes for Catalog Release 2.0.3f.T.
	N0	July 26, 2012	Updated release notes for Release 2.0(3a).
	P0	August 01, 2012	Updated release notes for Release 2.0(3b).
	Q0	August 29, 2012	Updated release notes for Release 2.0(3c).
	R0	September 18, 2012	Updated release notes for Release 2.0(4a).
	S0	October 5, 2012	Added ‘The following caveats are common across Release 2.0’ section under Open Caveats.
	T0	October 25, 2012	Updated release notes for Release 2.0(4b).
	U0	December 6, 2012	Updated release notes for Catalog Release 2.0.4f.T.
	V0	December 14, 2012	Updated release notes for Release 2.0(4d).
	W0	February 7, 2013	Updated release notes for Release 2.0(5a).
	X0	May 8, 2013	Updated release notes for Catalog Release 2.0.5d.T.
	Y0	May 14, 2013	Updated release notes for Release 2.0(5b).
	Z0	June 18, 2013	Updated release notes for Release 2.0(5c).
	A1	August 22, 2013	Updated release notes for Release 2.0(5d).

Table 1 Online History Change (continued)

Part Number	Revision	Date	Description
OL-25363-01	B1	August 30, 2013	Added CSCue08620 in Open Caveats for 2.0(5d).
	C1	September 17, 2013	Updated release notes for Release 2.0(5e).
	D1	September 19, 2013	Updated release notes for Catalog Release 2.0.5g.T.
	E1	December 9, 2013	Updated release notes for Release 2.0(5f).
	F1	February 19, 2014	Updated release notes for Catalog Release 2.0.5i.T.
	G1	April 2, 2014	Updated release notes for Catalog Release 2.0.5j.T.
	H1	May 16, 2014	Added CSCuo78883 in Open Caveats for 2.0(5f).
	I1	May 30, 2014	Removed CSCua02797 from Resolved Caveats; applies only to VIC Driver release notes.
	J1	June 13, 2014	Updated release notes for Catalog Release 2.0.5l.T and removed a PID for ucs-catalog.2.0.1m.T.bin.
	K1	June 18, 2014	Removed a PID from catalog Release 2.0.5l.T that is already listed for a previous release.
	L1	July 28, 2014	Added CSCuh61202 to Open Caveats across 2.0 Releases table.
	M1	August 19, 2014	Updated release notes for Catalog Release 2.0.5n.T.
	N1	October 31, 2014	Updated release notes for Release 2.0(5g).
	O1	December 4, 2014	Updated release notes for Catalog Release 2.0.5o.T.
	P1	June 30, 2015	Updated release notes for Catalog Release 2.0.5p.T.
	Q1	January 08, 2016	Updated release notes for Catalog Release 2.0.5q.T.

1. This release was removed from the download area due to CSCts96949 and CSCts86890. See the software deferral notice.

Introduction

Cisco UCS™ Manager provides unified, embedded management of all software and hardware components of the Cisco Unified Computing System™ (Cisco UCS) across multiple chassis, rack-mount servers, and thousands of virtual machines. Cisco UCS Manager manages Cisco UCS as a single entity through an intuitive GUI, a command-line interface (CLI), or an XML API for comprehensive access to all Cisco UCS Manager functions.

System Requirements

To install Cisco UCS Manager your computer must meet or exceed the following system requirements:

- The Cisco UCS Manager GUI is a Java-based application. Starting with Release 2.0(3a), Cisco UCS Manager supports both Sun JRE 1.6 and JRE 1.7. Versions earlier than Cisco UCS Manager Release 2.0(3a) require Sun JRE 1.6. (Sun JRE must be 32-bit version due to the lack of 64-bit native libraries for the KVM/VMedia; the 32-bit JRE can be executed in both Win32 and Win64, as well as Linux 32 and 64).
- Cisco UCS Manager uses web start and supports the following web browsers:
  - Microsoft Internet Explorer 6.0 or higher

  - Mozilla Firefox 3.0 or higher

  Adobe Flash Player 10 or higher is required for some features

- Cisco UCS Manager is supported on the following operating systems:
  - Microsoft Windows XP
  - Microsoft Windows Vista
  - Microsoft Windows 7
  - Red Hat Enterprise Linux 5.0 or higher

Hardware and Software Interoperability

For a complete list of hardware and software interdependencies, see the *Hardware and Software Interoperability for UCSM Managed Servers* for a specific Cisco UCS Manager release, here*:*

http://www.cisco.com/c/en/us/support/servers-unified-computing/unified-computing-system/products-technical-reference-list.html

Note VMware ESX and ESXi 4.0 are not compatible with Intel 56xx processors. 55xx processors are not affected by this limitation. See the interoperability matrix for this release for OS and other support questions.

Updating Cisco UCS Versions

To update the Cisco UCS software and firmware, see the appropriate Upgrading Cisco UCS document for your installation. All A, B, and C bundles must be at the exact same version and patch level.

Use the **scope firmware** and **show package** *filename* **expand** CLI commands to view the contents of a given release package. For information about the contents of the Cisco UCS bundle images for each Cisco UCS 2.0 release, see *Release Bundle Contents for Cisco UCS Software, Release 2.0*.

Internal Dependencies

Table 2 shows interdependencies between the hardware and versions of Cisco UCS Manager. Server FRU items such as DIMMs are dependent on their server type, and chassis items such as fans and power supplies work with all versions of Cisco UCS Manager.

Caution You cannot mix component software versions (for example, you cannot have a B200 using the 1.0(1) BIOS with a UCS M81KR adapter running 1.0(2) firmware managed by Cisco UCS Manager 1.3(1)). Compare the minimum software version for all your components and use at least the latest of all the versions, or use the most current version of software for all components. Mixing M1 and M2 hardware versions is not an issue if they are running software at a version matching the other system components.

Table 2 Internal Dependencies

Component	Recommended Minimum Software Version	Recommended Software Version
Servers		
B22 M3	2.0(3a)	2.0(5g)
B200 M1	2.0(1m)	2.0(5g)
B200 M2	2.0(1m)	2.0(5g)
B200 M3	2.0(2m)	2.0(5g)
B230 M1	2.0(1m)	2.0(5g)
B230 M2	2.0(1m)	2.0(5g)
B250 M1	2.0(1m)	2.0(5g)
B250 M2	2.0(1m)	2.0(5g)
B420 M3	2.0(4b)	2.0(5g)
B440 M1	2.0(1m)	2.0(5g)
B440 M2	2.0(1m)	2.0(5g)
C22 M3	2.0(3a)	2.0(5g)
C24 M3	2.0(3a)	2.0(5g)
C200 M2	2.0(1m)	2.0(5g)
C200 M2 SFF	2.0(2m)	2.0(5g)
C210 M2	2.0(1m)	2.0(5g)
C220 M3[1]	2.0(4a)	2.0(5g)
C240 M3[1]	2.0(4a)	2.0(5g)
C260 M2	2.0(2m)	2.0(5g)
C250 M2	2.0(1m)	2.0(5g)
C460 M2	2.0(2m)	2.0(5g)
Adapters		
UCS 82598KR-CI UCS M71KR-E UCS M71KR-Q	2.0(1m)	2.0(5g)
UCS M81KR	2.0(1m)	2.0(5g)
UCS NIC M51KR-B UCS CNA M61KR-I [2] UCS CNA M72KR-Q UCS CNA M72KR-E	2.0(1m)	2.0(5g)
UCS-VIC-M82-8P UCSB-MLOM-40G-01 UCSB-MLOM-PT-01	2.0(2m)	2.0(5g)
Fabric Interconnect		
UCS 6120XP	2.0(5g)	2.0(5g)
UCS 6140XP	2.0(5g)	2.0(5g)

Table 2 Internal Dependencies (continued)

Component	Recommended Minimum Software Version	Recommended Software Version
UCS 6248UP	2.0(5g)	2.0(5g)
UCS 6296UP	2.0(5g)	2.0(5g)
Fabric Extender or I/OM		
UCS 2104	2.0(5g)	2.0(5g)
UCS 2208XP	2.0(1m)	2.0(5g)
UCS 2204XP	2.0(2m)	2.0(5g)
Cisco Nexus 2248[3]	2.0(1m)	2.0(1x)
Cisco Nexus 2232PP	2.0(2m)	2.0(5g)
Fabric Interconnect Expansion Modules		
N10-E0440 N10-E0600 N10-E0080	2.0(5g)	2.0(5g)
N10-E0060	2.0(5g)	2.0(5g)
UCS-FI-E16UP	2.0(5g)	2.0(5g)
10-GB Connections		
SFP-10G-SR, SFP-10G-LR SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M	2.0(5g)	2.0(5g)
SFP-H10GB-ACU7M SFP-H10GB-ACU10M	2.0(5g)	2.0(5g)
FET-10G	2.0(5g)	2.0(5g)
SFP-H10GB-ACU7M= SFP-H10GB-ACU10M=	2.0(5g)	2.0(5g)
8-GB Connections (FC Expansion Module N10-E0060)		
DS-SFP-FC8G-SW DS-SFP-FC8G-LW	2.0(5g)	2.0(5g)
4-GB Connections (FC Expansion Module N10-E0080)		
DS-SFP-FC4G-SW DS-SFP-FC4G-LW	2.0(5g)	2.0(5g)
1-GB Connections		
GLC-T (V03 or higher) GLC-SX-MM GLC-LH-SM	2.0(1m)	2.0(5g)

1. See the Software Advisory for the minimum firmware level required on the Cisco UCS C220 M3 and Cisco UCS C240 M3.
2. N20-AI0002, the Cisco UCS 82598KR-CI 10-Gb Ethernet Adapter, is not supported on the B440 server but is still available for other models. We suggest you use the Cisco UCS CNA M61KR-I Intel Converged Network Adapter in place of the Cisco UCS 82598KR-CI 10-Gb Ethernet Adapter.
3. The C-series integration using the Cisco Nexus 2248 Fabric Extender is no longer supported as of Release 2.0(2). See the UCS C-Series hardware documentation for details.

Capability Catalog

The Cisco UCS Manager uses the catalog to update the display and configurability of server components such as newly qualified DIMMs and disk drives. The Cisco UCS Manager Capability Catalog is a single image, but it is also embedded in Cisco UCS Manager. Cisco UCS Manager 2.0 releases work with any 2.0 catalog file, but not the 1.0 catalog versions. If a server component is not dependent on a specific BIOS version, using it and having it recognized by Cisco UCS Manager is primarily a function of the catalog version. The catalog is released as a single image in some cases for convenience purposes in addition to being bundled with UCS infrastructure releases. See Table 3 for details on the mapping of versions to bundles.

Table 3 Version Mapping

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
2.0(1m)	ucs-catalog.2.0.1j.T.bin	—	
2.0(1q), 2.0(1s), and 2.0(1t)	ucs-catalog.2.0.1m.T.bin	UCS-CPU-X5687 on B200 M2 UCS-MR-2X082RX-C (Release 2.0(1s) and above) UCS-MR-2X324RX-C UCSB-5108-DC UCSB-PSU-2500ACPL	
—	ucs-catalog.2.0.1o.T.bin	A03-D146GC2 UCS-HDD900GI2F106 on C200 and C210 UCS-MR-2X164RX-C UCSB-PSU-2500DC48 on the DC UCS 5108 chassis (UCSB-5108-DC)	
2.0(1w) and 2.0(1x)	ucs-catalog.2.0.1p.T.bin	—	
2.0(2m) and 2.0(2q)	ucs-catalog.2.0(2f)T.bin	Cisco 2204 IO module Cisco C200 M2 SFF, C460 M2, C220 M3, C260 M3, and C240 M3 rack-mount servers Cisco UCS 6296 fabric interconnect Cisco UCS B200 M3 blade server Cisco VIC 1280 adapter card Nexus 2232 Fabric Extender UCS-CPU-E78837 UCSB-MLOM-40G-01 on the B200 M3 UCSB-MLOM-PT-01 on the B200 M3	
2.0(2r)	ucs-catalog.2.0.2g.T.bin	UCS-MR-2X164RX-D	
2.0(3a)	ucs-catalog.2.0.3e.T.bin	UCSB-B22-M3 UCSC-C22-M3L UCSC-C22-M3S UCSC-C24-M3L UCSC-C24-M3S	
2.0(3a), 2.0(3b), and 2.0(3c)	ucs-catalog.2.0.3f.T.bin	UCS-MR-1X162RY-A	

Table 3 Version Mapping (continued)

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
2.0(4a)	ucs-catalog.2.0.4a.T.bin	UCS-CPU-E5-2637 UCS-CPU-E5-2667 UCS-SD100G0KA2-G UCS-SD100G0KA2-S UCS-SD400G0KA2-G UCS-SD400G0KA2-S	
—	ucs-catalog.2.0.4f.T.bin	—	
2.0(4d)	ucs-catalog.2.0.4f.T.bin	—	
2.0(5a)	ucs-catalog.2.0.5a.T.bin	—	
2.0(5b)	ucs-catalog.2.0.5d.T.bin	UCS-CPU-E5-4617	
2.0(5c), 2.0(5d) and 2.0(5e)	ucs-catalog.2.0.5d.T.bin	—	
—	ucs-catalog.2.0.5g.T.bin	—	
2.0(5f)	ucs-catalog.2.0.5h.T.bin	UCS-SD200G0KS2-EP UCS-SD400G0KS2-EP UCS-SD800G0KS2-EP	
—	ucs-catalog.2.0.5i.T.bin	UCS-MR-1X041RY-A UCS-MR-1X082RY-A UCS-MR-1X082RZ-A UCS-MR-2X041RX-C UCS-MR-2X162RX-C	
—	ucs-catalog.2.0.5j.T.bin	UCS-HD12T10KS2-E UCS-ML-1X324RY-A UCS-MR-2X041RY-B UCS-MR-2X082RY-B	
—	ucs-catalog.2.0.5l.T.bin	UCS-SD120G0KS2-EV UCS-SD240G0KS2-EV UCS-SD480G0KS2-EV UCS-SD960G0KS2-EV	
—	ucs-catalog.2.0.5n.T.bin	UCS-HD450G15KS2-E	
2.0(5g)	—	—	
—	ucs-catalog.2.0.5o.T.bin	UCS-HDD300GI2F105	

Table 3 Version Mapping (continued)

UCS Release	Catalog File	Adds Support for PID	Additional Parts Qualified for PID
—	ucs-catalog-2.0.5p.T.bin	UCS-MR-1X162RY-A	
—	ucs-catalog.2.0.5q.T.bin	**Drives** • UCS-HD12TB10K12G • UCS-HD1T7K12G • UCS-HD2T7K12G • UCS-HD2T7KL12G • UCS-HD300G10K12G • UCS-HD300G15K12G • UCS-HD450G15K12G • UCS-HD4T7KL12G • UCS-HD600G10K12G • UCS-HD600G15K12G • UCS-HD6T7KL4K • UCS-HD900G10K12G • UCS-SD120GBKS4-EV • UCS-SD16TBKS4-EV • UCS-SD240GBKS4-EV • UCS-SD400G12S4-EP • UCS-SD480GBKS4-EV • UCS-SD800G12S4-EP • UCS-SD960GBKS4-EV **Memory** • UCS-ML-1X324RZ-A	**Memory** • UCS-ML-1X324RY-A • UCS-MR-1X162RY-A • UCS-MR-2X162RX-C

New Hardware Features in Release 2.0

Release 2.0(5b) adds support for the following:

- Cisco UCS B200 M3 blade server configurations with a single CPU

  This patch release provides support for UCS B200 M3 blade server configurations with a single CPU, in addition to the previously supported dual CPU configurations.

Release 2.0(4b) adds support for the following:

- B420M3

Release 2.0(3a) adds support for the following:

- B22M3, C22M3, C24M3, C220M3L, C240M3L, and C220M3S2
- QLogic QLE8242 CNA PCIe Adapter (UCSC-PCIE-QSFP) and Emulex OCe11102-F CNA PCIe Adapter (UCSC-PCIE-ESFP)

Release 2.0(2m) adds support for the following:

- Integration of Cisco C200 M2 SFF, C460 M2, C220 M3, C260 M2, and C240 M3 rack-mount servers
- Nexus 2232 Fabric Extender (replaces Nexus 2248 in this and following releases, see the Cisco UCS C-Series hardware documentation for details)
- Cisco UCS B200 M3 blade server
- Cisco VIC 1240 mLOM
- Port Expander Card for VIC 1240
- Cisco UCS 6296 fabric interconnect
- Cisco 2204 IO module
- Cisco VIC 1280 adapter card

Release 2.0(1w) adds support for the following:

- Version 2 of UCS B440 M1 and M2 Blade Servers. This new hardware version is part of a proactive replacement program. See Field Notice 63430 for further details.

Release 2.0(1s) adds support for the following:

- Intel Xeon x5687 CPU on B200 M2

Release 2.0(1m) adds support for the following:

- Cisco UCS 6248 Fabric interconnect
- Cisco 2208 IO Module
- 2500 Watt DC Power Supply for the Cisco UCS 5108 Blade Server Chassis

New Software Features in Release 2.0

Release 2.0(5d) adds support for the following:

- A new BIOS image containing the latest microcode updates for all Cisco UCS B-Series Servers.

Note The changes are documented in the Intel public Specification Updates for August 2013.

Release 2.0(5a) adds support for the following:

- BIOS Policy Settings—Provides the ability to select refresh interval rate for internal memory.

- Memory Speed—Enables 1333 MHz memory speed for 8GB/16GB 1600-MHz RDIMMs populated with 3 DIMMs Per Channel/1.5v on the Cisco UCS B200 M3 blade server and Cisco UCS C240 M3 rack server.
- Call Home—Enables you to configure call home for CMOS battery voltage low alert.

Release 2.0(1m) adds support for the following:

- Licensing—Updated information for new UCS hardware.
- Firmware Bundle Option—Enables you to select a bundle instead of a version when updating firmware using the Cisco UCS Manager GUI.
- Disk Drive Monitoring Support—Support for disk drive monitoring on certain blade servers and a specific LSI storage controller firmware level.
- iSCSI Boot—iSCSI boot enables a server to boot its operating system from an iSCSI target machine located remotely over a network.
- Pre-login Banner—Displays user-defined banner text prior to login when a user logs into Cisco UCS Manager using the GUI or CLI.
- Unified Ports—Unified ports are ports on the 6200 series fabric interconnect that can be configured to carry either Ethernet or Fibre Channel traffic.
- Upstream Disjoint Layer-2 Networks—Enables you to configure Cisco UCS to communicate with upstream disjoint layer-2 networks.
- Virtual Interfaces—The number of vNICs and vHBAs configurable for a service profile is determined by adapter capability and the amount of virtual interface (VIF) namespace available on the adapter.
- VM-FEX Integration for VMware—Cisco Virtual Machine Fabric Extender (VM-FEX) for VMware provides management integration and network communication between Cisco UCS Manager and VMware vCenter. In previous releases, this functionality was known as VN-Link in Hardware.
- VM-FEX Integration for KVM (Red Hat Linux)—Cisco Virtual Machine Fabric Extender (VM-FEX) for KVM provides external switching for virtual machines running on a KVM Linux-based hypervisor in a Cisco UCS instance.

Resolved Caveats

This section contains resolved caveats for the following releases:

Release 2.0(5)

The following caveats are resolved in the 2.0(5g) release:

Table 4 Resolved Caveats in Release 2.0(5g)

Defect ID	Description
CSCuo78883	Cisco UCS Manager and KVM users or admins using JRE version 1.7 update >= 40 no longer encounter a pop-up window with the ' Application Blocked by Security Settings' dialog.
CSCur01379	The security vulnerabilities identified by Common Vulnerability and Exposures (CVE) CVE-2014-7169, CVE-2014-6271, CVE-2014-6277, CVE-2014-7186, CVE-2014-7187, and CVE-2014-6278 are addressed.

The following caveats are resolved in the 2.0(5f) release:

Table 5 Resolved Caveats in Release 2.0(5f)

Defect ID	Description
CSCuj84421	After updating to Java 7 update 45, you can now login to Cisco UCS Manager without any issues.
CSCuj32124	The IOM hot swap controller LTC4215 register is now configured to set GPIO as default IO.
CSCul21224	The Cisco UCS fabric interconnects (FI) are no longer reset due to *vlan_mgr* hap reset.

Table 5 Resolved Caveats in Release 2.0(5f) (continued)

Defect ID	Description
CSCui41165	After upgrading to Release 2.0.(5f) on a two chassis setup, sporadic *error accessing shared-storage* or transient callhome fan alerts are no longer seen.
CSCuh85553	When the IPMI feature is enabled from the Cisco UCS Management platform, the default cipher suite is no longer enabled on the IPMI and you cannot execute the commands without a valid password.

The following caveats are resolved in the 2.0(5e) release:

Table 6 Resolved Caveats in Release 2.0(5e)

Defect ID	Description
CSCug14669	When the Fibre Channel Forwarder (FCF) MAC is learned dynamically the Fibre Channel (FC) path loss no longer occurs.
CSCuh28239	During frequent MAC address changes between FIs, you no longer see a delay in learning MAC addresses, and if the MAC address changes between server ports on the same FI, the MAC address no longer points to an incorrect destination.
CSCuh35570	The fabric interconnect (FI) no longer reboots with a Kernel panic svr_sam_statsAG process error.
CSCue08620	You will no longer see the following issues: • Intermittent RHEL 6.3 boot hangs with certain DIMMS on B200 and B250 servers. • STREAM test score drops about 25%.
CSCuf55019	The vim hap reset no longer happens due to SYSMGR_DEATH_REASON_FAILURE_HEARTBEAT from vim.

The following caveats are resolved in the 2.0(5d) release:

Table 7 Resolved Caveats in Release 2.0(5d)

Defect ID	Description
CSCud89583	Cisco UCS B440 Blade servers running Citrix XenServer 6.0.2 with E7-4830 and all C states disabled no longer freeze with a "CATERR_N" error.
CSCuf34701	IOM process bmcd no longer fails to discover blades after reboot.
CSCuf61116	IOMs no longer crash due to a memory leak in the baseboard management controller (BMC).
CSCuf78224	On a Cisco UCS B440-M2 server with Cisco UCS CNA M72KR-Q adapter card, VMware Auto Deploy 5.1 no longer hangs during system boot.
CSCuh39242	The current severity level of Upper Non-critical and Upper Critical CPU thermal faults are no longer incorrectly classified as minor faults.
CSCuc79507	On a scale setup with 20 chassis, when stress tests like port flaps and simultaneous SNMP walks, process stats_AG no longer cores due to a memory leak.

Table 7 Resolved Caveats in Release 2.0(5d) (continued)

Defect ID	Description
CSCuh49786	The following new microcode was added to Release 2.0(5d): • M6D206D7_00000710
CSCuh49825	The following new microcodes were added to Release 2.0(5d): • M04206E6_0000000A • M05206F2_00000037
CSCuh49817	The following new microcodes were added to Release 2.0(5d): • M03106A5_00000019 • M03206C2_0000001A

The following caveats are resolved in the 2.0(5c) release:

Table 8 Resolved Caveats in Release 2.0(5c)

Defect ID	Description
CSCug93076 CSCug93221 CSCug98662	The Cisco UCS B200 M3, B22 M3, and B420 M3 blade servers no longer experience non-correctable memory errors during booting. This patch provides a CIMC update for the voltage regulator. To ensure the voltage regulator is updated successfully, perform the following steps: 1. Update the CIMC image to 2.0(5c). 2. Power off the host. **Caution** This step is disruptive. 3. Activate the CIMC. 4. Power on the host.
CSCuf60988	Virtual fibre channel ports are no longer error disabled on one FI when the server is rebooted.
CSCue46382	Chassis discovery process issues, such as ports on FI-B displaying no object statistics or Cisco UCS Manager reporting incorrect state for ports on both FIs, no longer occur during Cisco UCS Manager upgrade.
CSCuf03602	Power supply VID data can be obtained by connecting to the IOM and running the **`show platform software cmcctrl fru psu`** command.

CSCug20103	The FIs will no longer reset with the following error message:
	`%SYSMGR-2-SERVICE_CRASHED: Service "monitor" (PID XXXX) hasn't caught signal 6 (core will be saved).`
	`%KERN-0-SYSTEM_MSG: writing reset reason 16, monitor hap reset - kernel`

The following caveats are resolved in the 2.0(5b) release:

Table 9 Resolved Caveats in Release 2.0(5b)

Defect ID	Description
CSCue38650	After IOMs reboot, the IOMs and UCSM PSU Policy will no longer be out of sync.
CSCuc77602	Kernel will no longer run out of memory due to high memory usage.
CSCud22791	After deploying VMs, MAC address learning will no longer be an issue.
CSCue46600	When a blade with newer version of VID is inserted in the chassis, UCS Manager will no longer report old VID.
CSCue09506	Upgrade to UCS Manager release 2.0(x) will no longer cause a brief network outage.
CSCue49366	You will no longer see transient faults related to UCS Manager Chassis SEEPROM usage and power capping.
CSCue29352	When you change a boot policy with “local storage change” and “Reboot on Boot Order Change” option un checked, you will no longer see the server in pending activities list.
CSCud01598	Fabric port channel will no longer be deleted after you re-acknowledge the chassis.
CSCuc49414	When you upgrade UCS Manager from release 2.0(2q) to any later 2.0(x) release, servers with dynamic vNIC policy will no longer be rebooted.
CSCuc87547	UCS Manager will no longer report PSU failures in the Nexus 2232 fabric extenders configured for UCSM managed C-Series servers.
CSCue99255	UCS B200 M2 RAID rebuilds will no longer fail after replacing one of the two HDDs.
CSCuc57709	Intermittent loss of network connectivity no longer occurs when TCP Segmentation Offload (TSO) is enabled on a vNIC, and the configured value of the vNIC MTU is larger than the TCP Maximum Segment Size (MSS) value configured on the host.
CSCue09763	The Cisco UCS M71KR-Q adapter Option ROM no longer hangs during SAN boot at “Checking Adapter 0 Loop ID 1” if the primary target is unavailable.

The following caveats are resolved in the 2.0(5a) release:

Table 10 Resolved Caveats in Release 2.0(5a)

Defect ID	Description
CSCub48862	B420-M3 no longer stops working with bad FRU issues.
CSCtz56593	After a FEX reboot all backplane interfaces on the FEX will no longer remain administrative down.
CSCuc46614	The "`show pinning border-interfaces`" command will no longer cause ENM HAP Reset.
CSCua91672	The fcoe_mgr hap reset will no longer cause FI reboot.
CSCuc58676	VNIC hosted on VIC 1280 or VIC 1240 will no longer fail to obtain an IP address via DHCP when multiple servers are rebooted at the same time.

Table 10 Resolved Caveats in Release 2.0(5a) (continued)

Defect ID	Description
CSCuc61267	Blade servers using VIC 1240 and VIC 1280 will no longer stop IP traffic between the following: • blade servers (same VLAN/IP address range) with single NIC to same FI • blade servers and upstream switch
CSCud74915	You will no longer see a duplicate VIF after creating a new service profile using VM-FEX and will no longer prevent you from connecting to the original blade server.
CSCua34036	Power management setting for ESX 5 will no longer change after a BIOS upgrade.
CSCub60934	BMC SEL decoder will no longer decode incorrect CPU ID.
CSCub65434	HA cluster command will no longer hang FI's DME and other services.
CSCub90535	On the Cisco UCS Manager GUI, the Ethernet Uplink port status box will no longer stay off. It will display green.
CSCuc16494	You will no longer have any issues with modifying VNICs with Service Profile Network role, from the Network tab.
CSCud10237	The eight default port licenses for flexible GEM on the FI, will be available for use.
CSCuc47237	NPV process will no longer crash generating identical cores.
CSCud56660	Duplicate license ID will no longer cause LicenseAG process to core.
CSCud60153	LLDP process will no longer crash on the FI and cause FI reboot.
CSCts50187	CMOS low battery voltage will trigger a Call home email.
CSCuc59752	“snmptable” command will retrieve the table.
CSCub51516	DHCP will no longer fail when multiple servers are restarted at the same time. Some vNICs do not get an IP address when using DHCP.
CSCub29699	Windows system event log will no longer display a fatal hardware and shows the error source as Boot.
CSCud27494	Traffic to a blade server will no longer be dropped and forwarded to another working link when an uplink is shutdown either on the fabric interconnect or from the upstream switch.
CSCud36129	Intel Enhanced Speedstep option when configured as disabled, will no longer show as enabled in the BIOS settings.
CSCuc96677	Cluster state will no longer get stuck in admin failover.
CSCub78207	You can manage internal memory refresh rate from the BIOS policy settings.
CSCuc58056	You will no longer see “Inventory is not complete” errors after displaying FI inventory.

Release 2.0(4)

- “Resolved Caveats in Release 2.0(4d)” on page 17
- “Resolved Caveats in Release 2.0(4b)” on page 17
- “Resolved Caveats in Release 2.0(4a)” on page 18

The following caveats are resolved in the 2.0(4d) release:

Table 11 Resolved Caveats in Release 2.0(4d)

Defect ID	Description
CSCuc59306	Disabling the members in a fabric port channel and leaving only one link no longer causes traffic drop.
CSCuc00368	With this resolution, both B230 and B440 blade behavior is as follows with RAID1 configuration between two (or more) disks: 1. When a disk is removed and reinserted back, while RAID1 rebuild is in progress, Operational status of that disk will be shown as 'Inoperable'. 2. One RAID rebuild is complete, Operational status of that reinserted disk will get updated to 'Operable' state. 3. Other disk(s) will continue to be in 'Operable' state.
CSCuc24817	Veth no longer goes down after fabric interconnect failover or reboot even though fabric interconnect is showing up.
CSCuc52899	Peer IOM communication failure no longer causes inability to set power policy.
CSCuc76238	User Authorization is no longer broken for certain scenarios.
CSCuc92523	An IOM that is having a hardware issue no longer causes an AIPC timeout and triggers other IOMs to go offline.
CSCuc44700	Upon upgrading to 2.0(x), a server pool that is defined using CPU, Adapter or Server qualifications with PID (model) pattern match will no longer incorrectly get all servers in the pool.
CSCua82214	After the server reboots, a VNIC hosted on a VIC 1240 or VIC 1280 adapter will no longer fail to obtain an IP address via DHCP.

The following caveats are resolved in the 2.0(4b) release:

Table 12 Resolved Caveats in Release 2.0(4b)

Defect ID	Description
CSCub08343	During reboot, Samsung 32GB LRDIMM will no longer display voltage errors on B200 M3.
CSCtz65329	You will no longer see a mismatch between UCSM Part number and mctools.
CSCub32324	The fabric interconnect will no longer reboot due to 'cdp hap reset'.
CSCub32386	FCoE VLANID Change will no longer drop all Storage Paths.
CSCua96703	You will no longer see random errors such as thermal-problem, performance-problem, and equipment-degraded false alarm.
CSCub94755	The Cisco UCS Manager GUI no longer displays "Unable to authenticate this site certificate" messages.
CSCuc35326	The Cisco UCS B200 M3, B22 M3, and B420 M3 Blade Servers no longer experience 'Server Hardware Not Supported' or discovery errors when you are upgrading from Release 2.0(2) to Release 2.0(3) or 2.0(4) and the blades are inserted into a Cisco UCS DC chassis.

Table 12 Resolved Caveats in Release 2.0(4b) (continued)

Defect ID	Description
CSCuc26360	The KVM Java client will no longer display an error/warning message stating that the KVM certificate to the blade has expired.
CSCuc15009	The IOM upgrade no longer fails and gets into a continuous reboot after the IOM is activated by the fabric interconnect.
CSCuc32555	Cisco UCS Manager is no longer truncating the last digit of the license file id from the license.

The following caveats are resolved in the 2.0(4a) release:

Table 13 Resolved Caveats in Release 2.0(4a)

Defect ID	Description
CSCub62959	The httpd.sh process no longer crashes after a Cisco UCS 6248UP Fabric Interconnect reloads.
CSCub53747	The Power Consumed column on the Power Groups tab in UCSM no longer displays “0” for the chassis or blades in the default power group.
CSCub59614	Adding a global VLAN to UCSM no longer causes some VIFs to fail.
CSCtz97031	Blade discovery no longer fails with a “Compute Failed” error after upgrading the firmware.
CSCua68423	ENM no longer crashes when port channels are created or removed.
CSCub34427	When adding VLAN to vNIC, the blade no longer reboots without warning.
CSCub36000	SNMP polling on eth_port_security objects no longer causes an eth_port_sec hap reset.
CSCub40588	“Waiting for FLOGI” error no longer persists after FLOGI succeeds.
CSCub48467	vNICs no longer intermittently show as “down” after an iSCSI boot on ESXi 5.0.
CSCub51662	The Intelligent Platform Management Interface (IPMI) on the blade is no longer unresponsive due to the LAN channel being disabled.
CSCub59458	Appliance ports in Layer 2 disjoint networks no longer get pinned to border ports configured with incorrect VLANs.
CSCua59404	You will no longer see a critical fault while deleting the Fibre Channel traffic monitoring session from the configuration.
CSCub16754	Discovery, association, and disassociation no longer fails after a BMC firmware update with a misleading message about the Cisco UCS M81KR adapter.

Release 2.0(3)

- "Resolved Caveats in Release 2.0(3a)" on page 20

The following caveats are resolved in the 2.0(3c) release:

Table 14 Resolved Caveats in Release 2.0(3c)

Defect ID	Description
CSCub08343	During reboot, the Samsung 32GB LRDIMM will no longer display voltage errors on the B200 M3 Blade Server.
CSCtz65329	You will no longer see a mismatch between the Cisco UCS Manager part number and mctools.
CSCub32324	The fabric interconnect will no longer reboot due to a 'cdp hap reset'.
CSCub32386	An FCoE VLAN ID change will no longer drop all storage paths.
CSCua96703	You will no longer see random errors such as thermal-problem, performance-problem, and equipment-degraded false alarms.
CSCtx52556	You will no longer see any transient thermal or fan problems.

The following caveats are resolved in the 2.0(3f).T catalog:

Table 15 Resolved Caveats in the 2.0(3f).T catalog

Defect ID	Description
CSCua71178	The Cisco UCS B230 M2 and B440 M2 servers now recognize the UCS-MR-2X164RX-D DIMMs.

The following caveats are resolved in the 2.0(3e).T catalog:

Table 16 Resolved Caveats in the 2.0(3e).T catalog

Defect ID	Description
CSCua61817	The 2.0(3d) catalog cannot be enabled on older release versions. The 2.0(2g) catalog (ucs-catalog.2.0.2g.T.bin) should be used for Release 2.0(2) and Release 2.0(1). ()

The following caveats are resolved in the 2.0(3b) release:

Table 17 Resolved Caveats in Release 2.0(3b)

Defect ID	Description
CSCua54788	User with server-profile role and locale access, will be able to reset, boot, and shut down a server from a KVM window.
CSCua66628	The Virtual Interface Manager (VIM) Daemon will no longer crash and cause the fabric interconnect to go down.

Table 17 Resolved Caveats in Release 2.0(3b) (continued)

Defect ID	Description
CSCua82545	You will no longer see stale mac addresses on VMotion for vswitch with dual path A and B.
CSCua65963	When you upgrade from Cisco UCS Manager 1.4 to 2.0(3b), Server Pool Policy Qualifications configuration involving PID property will no longer result in undesired changes to server pool content.

The following caveats are resolved in the 2.0(3a) release:

Table 18 Resolved Caveats in Release 2.0(3a)

Defect ID	Description
CSCub16642	Cisco UCS Manager 2.0(3a) supports Sun JRE 1.7.
CSCtz15271	There will no longer be a mismatch between the BIOS defaults policy and the actual BIOS settings on the server.
CSCty83359	After upgrading the Board Controller and CIMC firmware images using the host firmware package and the management firmware package, the blades will no longer reboot silently after performing any configuration change on the service profile.
CSCtx96556	The fabric interconnect to I/O module link comes up, or the packet CRC errors are no longer observed when using gen-2 10 or 7 meter twinax active cable and the 2204XP or 2208XP I/O module.
CSCua12013	When trust COS is enabled on an FCoE VNIC for a server running Red Hat Enterprise Linux 5.5, loss of access to configured remote LUN(s) will no longer occur.
CSCua59401	This issue applies Cisco UCS 2.0(3) and future releases. Prior to Cisco UCS 2.0(3), the BIOS setting *OS Boot Watchdog Timer Timeout* was incorrectly defined as *vpOSBootWatchdogTimerPolicy*. It has been changed to *vpOSBootWatchdogTimerTimeout*. The name of the managed object has been changed from *biosVfOSBootWatchdogTimerTimeOut* to *biosVfOSBootWatchdogTimerTimeout*. Any access to the older *biosVfOSBootWatchdogTimerTimeOut* managed object in Cisco UCS 2.0(3) or later releases will result in a XML API failure.
CSCty83542	The IOM cores will no longer occur after verifying the mac-sync functionality.
CSCty90643	The DME process on one fabric interconnect will no longer crash.
CSCty91471	A fabric interconnect will no longer reboot with an error during the firmware upgrade to current release.
CSCua36791	The s**how tech support** command no longer fails from the Cisco UCS Manager CLI or the Cisco UCS Manager GUI and the technical support files are generated from the CLI or GUI.
CSCua21324	The SAN connectivity to the blades on fabric interconnect B is lost after rebooting fabric interconnect A.
CSCtz01783	Under some rare circumstances, issuing the NX-OS CLI **show fex detail** command after an I/O module goes offline and online may cause a fabric interconnect to reload.
CSCtz48466	While upgrading from Cisco UCS Release 2.0(1t) to 2.0(2q), one of the internal process crashes and you cannot create service profiles from a template.

Table 18 Resolved Caveats in Release 2.0(3a) (continued)

Defect ID	Description
CSCtz87024	The Fibre Channel firmware issue will no longer disrupt SAN connectivity for the server.
CSCua07619	Read-only users can no longer create any log files at the /var/home/ directory and the operation performed by read-only users will no longer fill the "/" partition using the CLI show command. There will no longer be any remote authentication failure on Cisco UCS Manager.
CSCtx49686	If two fan enclosures are reseated on the same Cisco UCS 5108 chassis, the chassis will no longer be in a safe mode. The fan faults have been fixed and the functionality is not affected.
CSCtw67182	A blade with a Cisco UCS M81KR adapter will no longer display the error "initialize error 1" during an iSCSI boot.
CSCtz03288	Hard drives from one manufacturer were two to three times slower than the hard drives from another manufacturer even though both are sold under the same product ID. The issue with 300 GB SAS 10K RPM SFF drives is now resolved.
CSCty02218	While upgrading from Cisco UCS Release 2.0(1.180) to 2.1(1.185), the switch firmware activation will no longer fail.

Release 2.0(2)

The following caveats are resolved in the 2.0(2r) release:

Table 19 Resolved Caveats in Release 2.0(2r)

Defect ID	Description
CSCty85611	On the Cisco UCS B230 and B440 servers, the temperature sensors for the memory buffer will no longer return a false value that is higher than the upper non-recoverable value.
CSCtx90410	Cisco UCS Manager will no longer display a transient power supply unit input voltage error.
CSCtz39059	A BIOS change from Cisco UCS 1.4(1) to a Cisco USCS 2.0(1) or 2.0(2) release on the Cisco UCS B440 blade servers will no longer cause a Windows OS to re-enumerate the network interfaces that may cause a loss of network access.

The following caveats are resolved in the 2.0(2q) release:

Table 20 Resolved Caveats in Release 2.0(2q)

Defect ID	Description
CSCtz15569	The Cisco UCS Manager Turbo Boost now displays the correct state when EIST is disabled.
CSCty32929	A blade server will no longer have some of the POST LEDs on during operation when no faults or warnings were logged in Cisco UCS Manager.
CSCtz01009	Blades running Intel Westmere-EP processors such as the B200 M2 running the BIOS associated with Cisco UCS 2.0(2q) code no longer fail and display the message: “vMotion can fail with similar messages: Host CPU is incompatible with the virtual machine's requirements at CPUID level 0x1 register 'ecx'.
CSCty94457	A Windows Server 2008 bare metal host no longer loses network configuration and sees a NIC numbering shift after upgrading the Cisco UCS blade adapter card firmware from Cisco UCS Release 2.0(1w) to 2.0(2m).

The following caveats are resolved in the 2.0(2m) release:

Table 21 Resolved Caveats in Release 2.0(2m)

Defect ID	Description
CSCtt94543	While accessing a fabric interconnect via SSH, the SSHD process will no longer crash during the steady state.
CSCtw96111	Virtual machines using VM-FEX (Dynamic vNIC) port-profiles will no longer lose network connectivity unexpectedly.
CSCtq84985	An Intel Westmere-EP CPU on a B200-M2 or B250-M2 blade will no longer incorrectly initialize a value during boot up which keeps the CPU at P1 even when P0 is requested by an OS.
CSCtu16375	It is no longer necessary to disable Google analytics to download core files from the Cisco UCS Manager GUI.
CSCty10870	Any actions on a service profile that involve change impact evaluation no longer trigger a reboot even if it is not necessary.
CSCtr61016	The Cisco UCS Manager GUI no longer hangs while retrieving data for the performance statistics table.
CSCtx23541	After specifying an attribute setting in either the “General” LDAP setting or under the LDAP Provider setting, LDAPD no longer crashes when testing LDAP.
CSCtr07696	The LicenseAG process no longer crashes during Cisco UCS Manager restart after downloading license files.
CSCtx90742	If a VM’s vNIC is marked as masked in the VIF list it will still be able to receive traffic.
CSCty27581	An action on a trunked port-channel made from the Cisco UCS Manager GUI is quickly reflected in the Cisco UCS Manager CLI. Once ports are up, they show as trunking, however VSANs are no longer stuck in initializing.
CSCtx35808	The E2E diagnostic test now uses as much memory as possible when run.
CSCty26754	Blades no longer power off unexpectedly.

Table 21 Resolved Caveats in Release 2.0(2m) (continued)

Defect ID	Description
CSCtx95937	When you create a vNIC template under the LAN tab, a VM-FEX port-profile is no longer automatically created under the VM tab.
CSCtx41463	A fabric interconnect no longer reboots unexpectedly.
CSCtu11613	When an IOM reboots after a software update on a full width blade, the HIF ports on the second adapter are successfully brought up by the IOM.
CSCtr91923	Thermal faults now have more meaningful details.
CSCtu22052	A BladeAg crash no longer occurs if a request bios_recovery_ctrl message is sent to a blade, but the response came back too late and is ignored by mcclient.
CSCts48719	A KVM application will now take keyboard inputs in windowed mode.
CSCtu10771	When using a UCS 2208 I/O module you will no longer see a linkState fault for the virtual interface corresponding to the CIMC management port (port 33 on the IO module).
CSCtu41480	After a service profile configuration change, the changes list no longer shows "Networking" changes to be deployed even if there's no configuration change done in the networking area.
CSCtw59783	LEDs for ports 1 and 2 on a UCS 6296 fabric interconnect behave as expected.
Cisco UCS Manager	
CSCti86217	In Cisco UCS Manager there is now an option to change the port speed of the SPAN destination port.
CSCts56107	On a service profile configuration change, a server will not reboot before the maintenance window if you make some configuration change on the service profile which does not require a reboot then immediately make another change which does requires a blade reboot.
CSCtx12353	After a VLAN mapping change, vNIC pinning no longer fails.
CSCto59775	If the Secondary iSCSI vNIC comes up earlier than the Primary iSCSI vNIC (due to its overlay vNIC having a lower PCI order than that of the overlay vNIC for the Primary) and LUN discovery fails on the Primary, the iBFT will still post and the host will still boot.
CSCtt42482	When an FC port channel member is deleted, an unconfigured FC uplink port is no longer automatically created for the same slot ID and port ID.
CSCty71770	The Maintenance dialog box, from Server and Rack properties, now shows the option "Remove."
CSCtr62641	Cisco UCS Manager can now automatically auto-generate IQN identifiers for iSCSI, and validate the IQN format.
CSCtt38889	Upon bringup or if you manually restart the standby vNIC, the misleading error message "Virtual interface 872 link state is down" no longer appears.
BMC	
CSCtw62347	The chassis beaconing LED now works as expected in a chassis with a UCS-IOM-2208XP.
BIOS	
CSCto23446	When memory mirroring is configured, the redundant memory size is now correctly reported in Cisco UCS Manager.

Table 21 Resolved Caveats in Release 2.0(2m) (continued)

Defect ID	Description
Fabric Interconnect	
CSCtu14851	If port profiles are configured for VM-FEX, the fabric interconnect will no longer crash during upgrade due to a heartbeat failure.
CSCtx27555	Unknown multicast frames are no longer dropped at ingress into the fabric interconnect.
CSCtx45591	Cisco UCS fabric interconnects discover via DCNM as expected. (x)

Release 2.0(1)

The following caveats are resolved in the 2.0(1x) release:

Table 22 Resolved Caveats in Release 2.0(1x)

Defect ID	Description
CSCty40485	In Cisco UCS End Host Mode forwarding, when there are multiple uplinks, the ratio of server interfaces pinned to one uplink versus another uplink remains even.
CSCty35860	When the first port-channel member that comes up goes down and a fabric interconnect is in End Host Mode, and if the border ports are configured in port-channel, the fabric interconnect will no longer reflect IGMP queries received from the upstream switch back to the upstream.
CSCty46946	When a fabric interconnect is in End Host Mode, and if there are multiple border ports used by VM-FEX interfaces, server interfaces will be pinned to the border ports as expected.s
CSCtx96515	A board controller firmware upgrade of a B230 or B440 blade will no longer get stuck in "Activate-Status: Activating" when updating it after a system upgrade.
Upgrade	
CSCtw97157	When following the steps in the Cisco UCS upgrade guide and activating the subordinate fabric interconnect, guest virtual machines no longer experience a high CPU load.

The following caveats are resolved in the 2.0(1w) release:

Table 23 Resolved Caveats in Release 2.0(1w)

Defect ID	Description
CSCtw73436	When activating a firmware image for a blade controller, only PLD images appropriate for that blade are available as menu selections in the Cisco UCS Manager GUI.
CSCtw99501	The latest Board Controller version now shows up in the Cisco UCS Manager GUI drop down list for the B250 server.
CSCts98411	Generating a show tech-support output from the Cisco UCS Manager CLI or Cisco UCS Manager GUI no longer causes a stuck object in the Cisco UCS Manager GUI that reads as a timeout in the Cisco UCS Manager CLI.
CSCtw70911	Upgrading the Board Controller image on B250 M1/M2 blades is now supported.
CSCts60501	The software no longer experiences a connectivity flap after a shallow association, which can be caused by a process restart or an I/O Module link flap.
CSCtw65162	A vNIC with its active path set to fabric interconnect B will no longer go to a non-participating state.
CSCtu22407	Multiple Chassis decommission or recommission operations no longer result in incorrect computation of the access port VLAN count.
CSCtx06311	The VIM no longer crashes unexpectedly.
CSCtv21887	SAN connectivity is no longer lost during a Cisco UCS software upgrade.

The following caveats are resolved in the 2.0(1t) release:

Table 24 Resolved Caveats in Release 2.0(1t)

Defect ID	Description
CSCtt99770	The fabric interconnect no longer reboots unexpectedly with an SNMP error message.
CSCtu22633	A Guest VM running RHEL no longer loses all inbound network traffic after the guest VM is migrated from one host to another host.
CSCts86550	An HIF port seen on a fabric interconnect will no longer go down for few seconds and then comes back up. This is primarily due to an adapter firmware crash and restart.
CSCtu30346	After enabling Microsoft Hyper-V in Windows 2008 R2 SP1 then rebooting, the server no longer shows a black KVM screen and a failure of windows startup and login.
CSCtr30372	In the Cisco UCS Manager GUI, a power cycle with graceful operating system shutdown behaves as expected.

The following caveats are resolved in the 2.0(1s) release:

Table 25 Resolved Caveats in Release 2.0(1s)

Defect ID	Description
CSCtt27260	IOM backplane port 1 of a 5108 chassis will not be falsely reported as administratively down when a blade is present in slot-1 of the chassis.
CSCtv21855	When connecting a Cisco UCS server running Release 2.0 to a Nexus 5000 Series platform running Release 4.0(1a)N1(1), the uplinks will no longer get disabled after being operationally up.
CSCtt18526	After upgrade to Cisco UCS 2.0(1s), blades with Cisco UCS M81KR adapters will not show the error “initialize error 4” during FC boot.
CSCtt41541	While upgrading to Cisco UCS 2.0 with QoS policies defined, QoS policies will not generate error messages and VIFs with QoS policies defined on them will remain up after upgrading the subordinate interconnect but before upgrading the primary interconnect. During the upgrade there is no longer a period of downtime between when the primary restarts and when the secondary becomes primary and brings up its VIFs, and there is no longer lost connectivity to both LAN and SAN.

The following caveats are resolved in the 2.0(1q) release:

Table 26 Resolved Caveats in Release 2.0(1q)

Defect ID	Description
Cisco UCS Manager	
CSCty05262	PAA for a SPAN session now works with 8Gb transceivers and Fibre Channel expansion modules on the fabric interconnect.
CSCts95454	Using the Cisco UCS Manager GUI, you are now able to disassociate a service profile that is currently bound to a template.
CSCts60863	When you assign an organization to a locale in the Cisco UCS Manager GUI, the operation sometimes fails due to an internal error. This error is now corrected.
CSCts96949	The PCI Device address of a vNIC will not change after an upgrade of Cisco UCS Manager from Release 1.x to Release 2.0(1q).
CSCts86689	When the DHCP server is using an option 67 (RFC 2132) to report the bootfile name to the gPXE client, gPXE will receive the boot parameters and the boot will function normally.
BIOS	
CSCts86890	When the BIOS is upgraded on a B230-M1 blade from Cisco UCS Release 1.x to Release 2.0, the PCI address is preserved. **Note** In the New Hardware Features in Release 2.0, page 9, see the BIOS section for issues when upgrading the B230-M1 BIOS from Release 2.0(1m) to Release 2.0(1q) or later.
CSCtj54470	A B230-M1 blade discovered while running a Cisco UCS 1.4 BIOS Release image and now running a Cisco UCS 2.0 Release BIOS image will associate and disassociate normally.

Table 26 Resolved Caveats in Release 2.0(1q) (continued)

Defect ID	Description
CSCtt12615	The **show mac address-table aging-time vlan** *x* command or running an SNMP agent querying this SNMP object will no longer cause an unexpected reboot.
CSCtt18508	If the hostname is configured for the vCenter in Cisco UCS Manager and the DNS server does not reply with the hostname to IP mapping within 30 seconds, the VMS process will no longer crash unexpectedly.
CSCtt13313	A Blade with a service profile with a 22 character or longer name will boot as expected from the local disk after upgrading the BIOS from a 1.x release to the BIOS in the 2.0(1q) release.

The following caveats are resolved in the 2.0(1m) release:

Table 27 Resolved Caveats in Release 2.0(1m)

Defect ID	Description
Cisco UCS Manager	
CSCtk55618	Blade and rack-mount servers that include unequal sized HDDs or SSDs no longer see intermittent failures.
CSCts36501	100 GB SSD Cache Size is correctly reported as 256 KB in Cisco UCS Manager.
CSCtj96263	When a DIMM is detected by the CIMC as present but SMBIOS table 203 shows it as either failed or ignored, the DIMM will show up with location information with the correct value for the speed.
CSCtl05696	The MAC sync feature introduced in Cisco UCS Release 1.4.1 keeps the VNIC MAC address in sync between the fabric interconnects. This feature is now automatically enabled for service profiles that were associated and active before upgrade to the Cisco UCS Release 2.0 version of Cisco UCS Manager and fabric interconnect software.
CSCta56527	The Cisco UCS Manager GUI will no longer mistakenly show all DIMMs to be in array 1 on a B200.
CSCtj17237	Dynamic vNIC creation no longer fails with a message saying the port profile is not available in NPPM.
CSCtg94770	SNMP authentication no longer fails when using user details configured from a third-party authentication server such as RADIUS.
CSCto55519	After upgrading to Cisco UCS Release 2.0, VLAN 4048 is not mis-configured for a FCoE vSAN mapping and reset to VLAN 1.
CSCto85358	When an earlier version of a management extension did not support a BIOS token, but a newer version of the management extensions supports that BIOS token, new tokens will now be displayed in the BIOS Defaults in the Cisco UCS Manager GUI and are deployed to the blade server.
CSCtq98495	100 GB SSD discovery works as expected in the blade and rack-mount servers. Upgrade to Cisco UCS 2.0 before using these drives.
CSCtn87981	Cisco UCS B230 and B440 blade servers with Cisco UCS M81KR and 82598KR-CI adapters no longer fail with an "illegal fru" error.
Fabric Interconnect	

Table 27 Resolved Caveats in Release 2.0(1m) (continued)

Defect ID	Description
CSCtn84605	Associated or discovered rack-mount servers will come up after downgrading only Cisco UCS Manager from Cisco UCS Release 2.0 release to earlier releases, then returning to Cisco UCS Release 2.0 from the earlier release.
Rack Integration	
CSCtl91937	Nexus 2248 Fabric Extenders no longer show up as a chassis after a downgrade from a Cisco UCS 2.0 release, they are automatically decommissioned.
CSCti94883	Behavior of rack-mount servers is now stable when using mixed adapter vendor types.
CIMC	
CSCti68905	For a B200-M2 when a blade is configured in Low Voltage mode, and a LPC reset is asserted, the 1.5V DDR3 sensors no longer cause threshold crossing SEL events.
CSCtl43716	Fans no longer erroneously show as inoperable when operating at 100%.
Adapter Cards	
CSCtg91013	VMs are updated correctly under the VM tab after a power cycle.
VMware	
CSCtj63157	ESXi installation no longer fails on RAID clusters with two SSDs on the B230 server.
CSCtj98207	There is no longer a problem with installing ESXi 4.x on systems with Intel M61KR-I, Emulex M72KR-E, Broadcom M51KR-B or Qlogic M72KR-Q CNA Adapters.
RAID Controller	
CSCtr66115	If a hot spare drive is added in a B200 or B250 server when replacing a bad disk in the RAID array the Auto Rebuild functions as expected.
BIOS	
CSCsy97698	When a faulty DIMM is detected in early BIOS POST (e.g. the blade was powered on with a faulty DIMM), only one SEL entry will be sent to the CIMC.
CSCtk63908	Network connection to CIMC is no longer lost intermittently after 400 host reboots or power-ons.

Open Caveats

This section contains open caveats for the following releases:

Common Across Release 2.0

The following caveats are common across Release 2.0:

Table 28 Open Caveats that are Common across Release 2.0

Defect ID	Symptom	Workaround
CSCuc15009	Under some conditions, the IOM upgrade fails and gets into a continuous reboot after the IOM is activated by the fabric interconnect. Rebooting the fabric interconnect on a failed IOM update does not fix this issue.	Resolved in Cisco UCS, Release 2.0(4b). Upgrade to Release 2.0(4b). Contact Cisco technical support if you have any issues upgrading to this release.
CSCuh61202	FC storage traffic through an IOM stops when the IOM is reset or reinserted, or the cable between the IOM and FI is removed or reinserted.	To avoid being impacted when upgrading from a release prior to 2.1(3a) or 2.2(1b), upgrade the server firmware **before** performing an infrastructure upgrade. This caveat affects FC traffic on the Cisco 1240, Cisco 1280, and Cisco M81KR adapters and is an exception to the normal upgrade procedures found in Cisco UCS Manager upgrade guides. For more details, please refer to CSCuh61202.

Release 2.0(5)

The following caveats were found in Release 2.0(5g)

Table 29 Open Caveats in Release 2.0(5g)

Defect ID	Symptom	Workaround
CSCuo50049	In some rare cases after upgrading from release 1.4 to a higher version of UCS Manager, you may see issues such as cluster command timeout or switchover command not working.	There is no known workaround to avoid this issue. To recover from this issue, you can reload the FIs after the software is upgraded. If you need further assistance, contact Cisco TAC.

The following caveats were found in Release 2.0(5f)

Table 30 Open Caveats in Release 2.0(5f)

Defect ID	Symptom	Workaround
CSCuo40713	The serial number is not displayed correctly when the following disks are used on Cisco UCS M3 servers: • MZ6ER200HAGM/003DM0B (PID: UCS-SD200G0KS2-EP) • MZ6ER400HAGL/003DM0B (PID: UCS-SD400G0KS2-EP) • MZ6ER800HAGL/003DM0B (PID: UCS-SD800G0KS2-EP)	This issue has no known workaround. When these disks are used, all information is displayed correctly except serial numbers. There is no impact to functionality.

Table 30 Open Caveats in Release 2.0(5f) (continued)

Defect ID	Symptom	Workaround

CSCuo78883	'Application Blocked by Security Settings' error when starting the Cisco UCS Manager GUI or KVM Console application.
	
	Because the Java Code Signing Certificate expired, users on Java 7 update 40 or higher might see the following message:
	
	`Application Blocked by Security Settings`
	`Your security settings have blocked an application signed with an expired or not-yet-valid certificate from running.`
	
	Resolved in 2.0(5g).
		To fix this issue, you can either temporarily lower your Java security settings to add Cisco UCS Manager as an exception, or if you are using Java 7 update 51 or higher, you can add the Cisco UCS Manager host IP address to the Exception Site list.
		
		To temporarily lower your security settings:
		
		1. Start your Java Control Panel. The location may vary depending on your operating system and browser preferences.
		2. Lower the Security level to Medium.
		3. Start Cisco UCS Manager.
		4. At the warning message, check the "I accept the risk and want to run this application'" checkbox and click **Run**.
		5. Return to the Java Control Panel and reset your security level.
		
		To add the IP address to the exception site list (for Java 7 version 51 and higher):
		
		1. Start your Java Control Panel. The location may vary depending on your operating system and browser preferences.
		2. In the Security area, click the Edit Site button to add the IP address to the list.
		
		If you use HTTPS to access Cisco UCS Manager, ensure that you have the correct prefix.
		
		3. Click **OK**.

The following caveats were found in Release 2.0(5e)

Table 31 Open Caveats in Release 2.0(5e)

Defect ID	Symptom	Workaround
CSCui87195	FLS cores, with the following message: `130820-19:06:33.645547 fls.fc vnic 15: Local port down for lif 4.130820-19:06:33.646164 fls.sa_log ERROR: ASSERT FAILED ((ep->ex_e_stat & ESB_ST_COMPLETE) == 0) @ fc/fc_exch.c:1116`	This issue has no known workaround.

The following caveats were found in Release 2.0(5d)

Table 32 Open Caveats in Release 2.0(5d)

Defect ID	Symptom	Workaround
CSCue08620	You might have one of the following two symptoms: 1. Under some conditions the RHEL 6.3 boot hangs intermittently with certain DIMMS on B200 and B250 servers. 2. STREAM test score drops about 25%.	This issue has no known workaround.

The following caveats were found in Release 2.0(5c)

Table 33 Open Caveats in Release 2.0(5c)

Defect ID	Symptom	Workaround
CSCuh28239	During frequent MAC address changes between FIs, you may see a delay in learning MAC addresses, and if the MAC address changes between server ports on the same FI, the MAC address may point to an incorrect destination.	This issue has no known workaround.
CSCuh35570	The fabric interconnect (FI) reboots with a Kernel panic svr_sam_statsAG process error.	This issue has no known workaround.

The following caveats were found in Release 2.0(5a)

Table 34 Open Caveats in Release 2.0(5a)

Defect ID	Symptom	Workaround
CSCug88824	When ten chassis are connected to two FIs, and one FI is manually brought down, some of the virtual interfaces failed to display a fault on Cisco UCS Manager.	This issue has no known workaround.
CSCug62535	BMC continuously prints the following message: multicast_solshell.c:86:SOL Connection Attempted with SOL disabled	This issue has no known workaround.
CSCud77420	Cisco UCS Manager sends Call Home alert emails with information on a fan failure and immediately follows-up with another email that the failure is recovered.	This issue has no known workaround.
CSCud86528	Blades Power off during firmware update.	Use the "Boot Server" option from the service profile to keep the power states between the service profile and associated physical server in sync. Do not use the “Reset” option as displayed in Cisco UCS Manager’s warning message.
CSCue04360	After you boot, the B200 M3 servers hang after few days, with PECI errors.	Reboot the server.
CSCue29184	The servers are stuck in discovery mode with no progress on the FSM screen.	Perform cluster lead in the other FI.
CSCue29352	When you try to change the boot order without checking the options “local storage change" and "Reboot on Boot Order Change", the server is listed in pending activities list.	Check mark the "Reboot on Boot Order Change" to trigger server reboot.
CSCue38335	Failure to recreate a deleted team due to Windows BSOD.	Re-install Windows.
CSCud71227	FWM crashes causing the switches to reboot.	Acknowledge the chassis. **Note**: This might cause the traffic to stop.
CSCue11936	UCS cluster lead results in VIF or vEth flap, because the FI and IOM links are reset by Cisco UCS Manager.	This issue has no known workaround.

Table 34 Open Caveats in Release 2.0(5a) (continued)

Defect ID	Symptom	Workaround
CSCuc49414	Servers with dynamic vNIC policy will be rebooted when Cisco UCS Manager is upgraded from release 2.0(2q) to any later 2.0(x) releases.	Do not deploy vHBAs along with static and dynamic vNICs configuration. Subsequent upgrades to later Capitola releases would not result in server reboots.
CSCuc66914	A global VLAN goes missing on an FI after rectifying a conflicting FCoE VLAN condition after upgrade from 1.4.1 to 2.0(4a) or later.	There are two options based on whether you want to retain the existing VSAN-VLAN assignment or retain the VLAN as global VLAN. 1) If the intent is to retain the VLAN as a global VLAN then after changing FCoE VLAN assignment, delete and re-create the missing VLAN. The VLAN will get correctly reconfigured on NXOS. Or 2) If you want to retain the VLAN as an FCoE VLAN, then assign a different VLAN for the veths using it.

Release 2.0(4)

The following caveats were found in Release 2.0(4d)

Table 35 Open Caveats in Release 2.0(4d)

Defect ID	Symptom	Workaround
CSCue41489	When a server is associated to a service profile with a Maintenance Policy that requires user acknowledgement, under some conditions, on upgrade, the server might reboot without triggering the user acknowledgement.	This issue has no known workaround.
CSCuc82212	VMware ESX cold migration is slow. The issue has been reproduced on various Cisco servers, including the B230M1 and B200M3), as well as on other server vendors' hardware. This issue does not occur on the Cisco B200M2 server.	This issue has no known workaround.
CSCuc82601	All IOMs connected to a fabric interconnect disconnect, but the peer IOMs do not go down. This causes complete path failure on the side of the failure.	Graceful recovery occurs after about 15 seconds. Reboot any servers which were affected to restore Fibre Channel connectivity.
CSCuc87547	PSU failures of a Cisco Nexus 2232 FEX configured for a C-series server that is managed by Cisco UCS Manager may be continuously reported by Cisco UCS Manager.	This is a cosmetic issue with no known workaround. Reloading the FEXes may or may not correct this issue.
CSCuc88168	The fabric interconnect reboots upon SNMP crash.	If you are running a version of Cisco UCSM Manager lower than Cisco UCS 2.0(1t), see CSCtt99770. Disabling SNMP on the fabric interconnect may help prevent a recurrence of the issue.
CSCuc91844	A boot profile is configured with two iSCSI boot vNICs. However, iBFT is posted only for one of the boot vNICs. Therefore, the host boots up with only one path to the LUN. As a result, Microsoft MPIO will only see a single path and additional redundant paths cannot be added for fault tolerance.	This issue has no known workaround.
CSCuc94895	Cisco UCS 2104XP IOM reboots abruptly for unknown reason.	Contact Cisco TAC to have the IOM replaced.

Table 35 Open Caveats in Release 2.0(4d) (continued)

Defect ID	Symptom	Workaround
CSCud10901	A B420-M3 blade server with 48 x 32G DIMMs fails discovery and generates a fault.	This issue has no known workaround. However, it occurs very rarely and if it happens, discovery is triggered again and completes successfully. **Resolved**: This issue is resolved in Cisco UCS Manager Release 2.0(5a).
CSCud27494	Traffic to a blade server is dropped when an uplink is shutdown either on the fabric interconnect or from the upstream switch. The traffic is forwarded to the fabric interconnect on the other working link but the fabric interconnect does not forward the traffic to the vNIC.	Do one of the following: • Initiate a connection from the server or VM. • Clear the ARP entry on the gateway to force an ARP broadcast. The fabric interconnect will forward that broadcast. **Resolved**: This issue is resolved in Cisco UCS Manager Release 2.0(5a).
CSCud36129	Intel Enhanced Speedstep option is configured as disabled. However, when you verify the BIOS settings, the configuration did not take effect and the Intel Enhanced Speedstep option shows as enabled.	This issue has no known workaround. **Resolved**: This issue is resolved in Cisco UCS Manager Release 2.0(5a).
CSCud54919	On blade servers that are not associated with a service profile, CIMC could not respond from UCS Manager at the same time.	Do the following: 1. Decommission the server. 2. Remove the blade and then reinsert it. 3. Reacknowledge the server. **Resolved**: This issue is resolved in Cisco UCS Manager Release 2.0(5a).

The following caveats were found in Release 2.0(4c)

Table 36 Open Caveats in Release 2.0(4c)

Defect ID	Symptom	Workaround
CSCuf51475	M71KR DCE interface may form port channel with 22xxXP IOM and cause connectivity issues.	Reset DCE interfaces to stabilize connection.

The following caveats were found in Release 2.0(4b)

Table 37 Open Caveats in Release 2.0(4b)

Defect ID	Symptom	Workaround
CSCug14669	Fibre Channel (FC) path loss occurs when the Fibre Channel Forwarder (FCF) MAC is learned dynamically.	Flap the FC uplink, or pin the FC to a different uplink.
CSCue17295	The 6296 FI with pre-installed license displays license grace period warning.	There is no known workaround for this issue.
CSCud45832	In some cases, when you upgrade to release 2.0(4b), UCS Manager does not display LDAP Group Maps configuration.	From NX-OS, use “show ldap” CLI command to view the configured LDAP Group Maps.

CSCud21197	"CISCO-UNIFIED-COMPUTING-TC-MIB" fails to get compiled on Cisco Rosa NMS system.	Edit the CISCO-UNIFIED-COMPUTING-TC-MIB.my MIB. Remove all the platformRecommended and platformDefault entries for BIOS tokens and recompile the MIB.
		For example, if you see the following:
		`CucsBiosVfSriovConfigVpSriov ::= TEXTUAL-CONVENTION`
		`STATUS current`
		`DESCRIPTION ""`
		`SYNTAX Gauge32 { platformRecommended(0), disabled(258), enabled(259), platformDefault(4294967294) }`
		Delete this and make sure you have the following:
		`CucsBiosVfSriovConfigVpSriov ::= TEXTUAL-CONVENTION`
		`STATUS current`
		`DESCRIPTION ""`
		`SYNTAX Gauge32 { disabled(258), enabled(259), }`

CSCuc24817	After fabric interconnect reboot or fabric interconnect failover, vETH is shown as down in the Cisco UCS M81KR VIC logs, but shown as up in NX-OS.	Disable then enable (shut/no shut) the DCE interface for the vNIC in Cisco UCS Manager.

Table 37 Open Caveats in Release 2.0(4b) (continued)

Defect ID	Symptom	Workaround
CSCuc26566	The Cisco UCS 6200 Series fabric interconnect reboots without a final confirmation warning after configuration changes.	This issue has no known workaround.
CSCuc27213	After upgrading from Cisco UCS 2.0(1s) to 2.0(3a), the Cisco UCS B200 M3 blade server continuously reboots.	Change the quiet boot option in BIOS policy from disabled to enabled. **Resolved**: This issue is resolved in Cisco UCS Manager Release 2.0(5a).
CSCuc44209	Cisco UCS Manager displays the names for PSUs connected to a Cisco Nexus 2200 Series FEX in reverse order.	This issue has no known workaround.
CSCuc47311	When a Cisco UCS chassis using DC power supplies (PSU) abruptly loses power to the PSUs, the PSUs may exhibit a RED LED Fail status after power is restored.	Remove and reinsert the PSUs.
CSCuc52981	Downloading licence files for the Cisco UCS 6100 and 6200 Series fabric interconnects appears to complete successfully, but the license files are not visible.	Obtain a single license file with all licenses consolidated, and use that license file to license the fabric interconnects.
CSCuc58056	“Inventory is not complete” errors received after displaying FI inventory.	This issue has no known workaround. **Resolved**: This issue is resolved in Cisco UCS Manager Release 2.0(5a).
CSCuc59299	When downloading a firmware bundle, ethpm crashes with 'Out of Memory: Killed process' error and the fabric interconnect reboots.	This issue has no known workaround.
CSCuc59306	When members are disabled (simulating failure) leaving one link active from the port-channel between the Cisco UCS 6248UP FI and the Cisco UCS 2208XP FI, all I/O for both the A side and B side of the vFC interface pauses for approximately 45-60 seconds.	Switch the chassis discovery policy and connectivity policy from “port-channel” to “none”, then reacknowledge the chassis.
CSCuc59752	The **snmptable** command does not return any values.	This issue has no known workaround. **Resolved**: This issue is resolved in Cisco UCS Manager Release 2.0(5a).
CSCuc65457	The svc_sam_bladeAG service crashes and creates a core dump.	This issue has no known workaround.

Table 37 Open Caveats in Release 2.0(4b) (continued)

Defect ID	Symptom	Workaround
CSCuc68863	Newly installed 8 GM DIMM shows as “Equipped Identity Unestablishable” and “invalid FRU” in Cisco UCS Manager.	This issue has no known workaround.
CSCuc72049	When creating an access mode appliance port-channel in Cisco UCS Manager, the default VLAN is used instead of the specified VLAN. Changing the port-channel VLAN to the originally specified VLAN programs the port-channel correctly in NX-OS, but the individual members are not changed. This can result in communication issues where the port-channel and MAC addresses are discovered on the incorrect VLAN.	Configure the appliance port-channel in trunk mode with native vLAN specified instead of access mode.
CSCuc76238	Authenticated but unauthorized users are able to perform operations that should not be allowed. These operations include service profile instantiation from template and service profile cloning.	This issue has no known workaround.
CSCuc82601	All IOMs connected to a fabric interconnect experienced a link flap while the peer IOMs remained connected.	Recovery occurs automatically within 15 seconds. Reboot any servers that are still experiencing connection issues to resume FC connectivity.
CSCuc82895	When downgrading Cisco UCS Manager from Release 2.0(4b) to earlier releases, for example, Release 2.0(3c), Release 1.4.4, or Release 1.3.1, the license count displayed and available might incorrectly be greater than the licenses you have obtained.	This issue has no known workaround. **Resolved**: This issue is resolved in Cisco UCS Manager Release 2.0(5a).

The following caveats were found in Release 2.0(4a)

Table 38 Open Caveats in Release 2.0(4a)

Defect ID	Symptom	Workaround
CSCuh01579	When the server is rebooted, or the UCS reset option is used, the Cisco UCS B200 M2 displays a USB composite device mounted in Windows. The drive letter assigned to this device varies, which may cause the clustering service to fail.	Disable the USB mass storage controller to prevent the USB composite device from mounting. **Note** Disabling the USM mass storage controller also disables virtual CD/DVD ROM functionality.
CSCug25894	During boot and reack in Cisco 2100 Series IOM, sysmgr cores are seen.	The system resumes normal behavior after process restart. This should take approximately three minutes.
CSCug76389	6140 FIs connected to 2104 IOMs may sometimes crash and generate core files. When the IOM reboots, you will see the expected behaviour.	This issue has no known workaround.
CSCuf78247	When a blade server loses the SAN path, UCS Manager does not display any error messages.	Reboot the server.
CSCue72786	The B230 M2 servers with VIC M18KR do not update the vfc pinning consistently.	Reset the DCE interface or reboot the B230 M2 server.
CSCtq77181	The fNIC driver rate limit feature does not work for vHBA devices supported by the VIC 1280, VIC 1240, and VIC 1225 adapters.	This issue has no known workaround. Do not configure the rate limit on vHBA devices hosted by these adapters.
CSCua82214	After the server reboots, a VNIC hosted on a VIC 1240 or VIC 1280 adapter might fail to obtain an IP address via DHCP.	Disable and enable the host interface to initiate a DHCP retry. **Resolved**: his issue is resolved in Cisco UCS Manager Release 2.0(5a).
CSCub64209	FCoE packets are dropped when host-control is enabled in QOS policies assigned to vNICs.	For Redhat and other Linux-based operating systems, set the host-control to “none” in the QoS policies assigned to vNICs.

Table 38 Open Caveats in Release 2.0(4a) (continued)

Defect ID	Symptom	Workaround
CSCuc08556	A Cisco P81E CNA card installed in slot #2 on a Cisco UCS C240 might experience network disruptions with Cisco UCS Release 2.0(2), Release 2.0(3) or Release 2.0(4).	Try one of the following: • Move the P81E card to slot #5. • Leave the P81E card in slot #2, and install an additional PCIe card in slot #3.
CSCuc09958	Java 1.7 detected error occurs when downgrading from Cisco UCS Manager Release 2.0(3a) and later releases running JRE 1.7 to UCS Manager Release 2.0(2r) and earlier releases.	Downgrade your Java runtime environment to JRE 1.6 (minimum version is 1.6.0_10) and restart Cisco UCS Manager.

Release 2.0(3)

- "Open Caveats in Release 2.0(3c)" on page 41
- "Open Caveats in Release 2.0(3b)" on page 42
- "Open Caveats in Release 2.0(3a)" on page 43

The following caveats were found in Release 2.0(3c)

Table 39 Open Caveats in Release 2.0(3c)

Defect ID	Symptom	Workaround
CSCuh21841	Cisco UCS Manager might display that the server health is inoperable, even though all of the DIMMs are shown as operable, and all of the DIMMs are available to the OS.	This is a cosmetic issue. Reset the CIMC to clear the error.
CSCuf19514	If you use LDAP when SSL option is enabled, the LDAP daemon crashes and causes authentication failures.	Force UCS Manager for cluster failover to enable AD users to login.
CSCug40776	FI reboots while running the following commands: • connect nxos • show vlan • show run	This issue has no known workaround.

The following caveats were found in Release 2.0(3b)

Table 40 Open Caveats in Release 2.0(3b)

Defect ID	Symptom	Workaround

CSCub62959	The httpd.sh process crashes after a Cisco UCS 6248UP fabric interconnect reloads.	Run the following commands on the primary fabric interconnect to bring up the Cisco UCS Manager GUI, and on the secondary fabric interconnect to start the httpd.sh process:
		`UCS-A /security # create keyring default`
		`UCS-A /security/keyring* # set modulus mod1024`
		`UCS-A /security/keyring* # commit-buffer`
		`UCS-A /security/keyring #`
		
		`UCS# connect local-mgmt`
		`UCS-B(local-mgmt)# pmon stop`
		`UCS-B(local-mgmt)# pmon start`

CSCub19173	When adding multiple VLANs, MAC learning fails with resource exhaustion.	Reduce the number of VLANs.
CSCub20455	When testing the Twinax cables between IOMs and fabric interconnects or one of IOMs, blade discovery happens and displays B230M2v “Mismatch Identity Unestablishable”.	Try one of the following: • Reset CIMC • Change the server to a different slot.
CSCub32324	A fabric interconnect crashes and shows ‘cdp hap reset’ as the reason.	This issue has no known workaround.
CSCub34427	When adding a VLAN to a vNIC, the blade reboots without warning.	This issue has no known workaround.
CSCub34939	After upgrading Cisco UCS Manager, while activating, SNMP crash reboots both fabric interconnects.	This issue has no known workaround.

The following caveats were found in Release 2.0(3a)

Table 41 Open Caveats in Release 2.0(3a)

Defect ID	Symptom	Workaround
CSCud93569	When upgrading from Release 1.4, the FI firmware NX-OS code fails because the MTS queues run out of space due to SNMP messages.	Reload the FI, check the mts buffers summary, and once they are clean proceed with the upgrade again.
CSCtz15707	When the Cisco UCS C24 M3 server has more than 16 hard disk drives installed, creation of RAID 10 using a CISCO UCS Manager Service Profile fails for the server. Other supported RAID levels are not affected.	Use either one of following two options: • Reduce number of installed hard disk drives to less than 17. • Use LSI WebBIOS Configuration utility during server boot to manually create RAID 10 when more than 16 disk drives are required for RAID10 configuration. Press CTRL+H during server BIOS POST to launch LSI WebBIOS Configuration utility.
CSCtz15594	The IOM reboots unexpectedly while polling via SNMP.	This issue has no known workaround. This is a rare issue that occurs during polling via SNMP.
CSCtz30836 CSCty40501	Cisco UCS Manager reports incorrect errors for certain storage configurations or fails to reject the invalid configurations.	This issue has no known workaround.
CSCtz68194	When a 8G Fibre Channel port is configured as a SPNAN destination (SD mode) on 6-port 1/2/4/8G GEM card and the 6-port GEM card is not swapped with the 8-port 1/2/4 FC GEM card and the SPAN session is deleted, the Fibre Channel port does not come up.	Remove the Fibre Channel port as span destination before performing the hot swap. After hot swap, Configure the Fibre Channel port as a SPAN destination.
CSCtz79579	Cisco UCS Manager will report an incorrect status for the faulty disks that fail to power on or link up.	This issue has no known workaround. This is a rare issue.
CSCua17481	One of the blades on the fabric interconnect causes an issue due to an internal process.	This issue has no known workaround. This is a rare issue.
CSCua19893	Some of the Fibre Channel ports that are part of the san-port-channel on the fabric interconnect fail to come up after reboot of the fabric interconnect. This issue usually happens when there is a large number of member ports (for example. more than 8) in the san-port-channel.	Disable or enable the failed member ports on the fabric interconnect and the ports will be operationally up again.

Table 41 Open Caveats in Release 2.0(3a) (continued)

Defect ID	Symptom	Workaround
CSCua31847	While upgrading from Cisco UCS Release 1.4(3l) to 2.0(2q), the controller on IOM displays an error message during the upgrade process.	This issue has no known workaround. This is a firmware issue.
CSCua59404	A critical fault is observed while deleting a Fibre Channel traffic monitoring session from the configuration and the fault is not cleared later.	This issue has no known workaround. There is no functional impact since the FC SPAN destination port is correctly configured to its default role: FC uplink.
CSCua71178	The Cisco UCS B230 M2 and B440 M2 servers fail to recognize the UCS-MR-2X164RX-D DIMMs.	Upgrade to the Cisco UCS Release 2.0.3f.T catalog (ucs-catalog.2.0.3f.T.bin).
CSCub48467	VIC 1240 iSCSI boot causes the vNIC links status to show “down” intermittently.	This issue has no known workaround.
CSCub82338	The IPv6 neighbor discovery does not work with dynamic mac learning.	Set a network control policy to change the “mac register mode” to “all host vlans”. This will create static mac addresses for any learned devices learned and the neighbor discovery will work.
CSCub99354	Under some rare circumstances, blade discovery fails due to FRU corruption after upgrading from Cisco UCS Release 2.0(1s) to Release 2.0(3a).	Contact Cisco TAC to reprogram the FRU.
CSCuc35326	The Cisco UCS B200 M3, B22 M3, and B420 M3 Blade Servers experience ‘Server Hardware Not Supported’ or discovery errors when you are upgrading from Cisco UCS Release 2.0(2) to Release 2.0(3) or 2.0(4) and the blades are inserted into a Cisco UCS DC chassis.	Upgrade to Cisco UCS Release 2.0(4b).

Release 2.0(2)

- “Open Caveats in Release 2.0(2r)” on page 45
- “Open Caveats in Release 2.0(2q)” on page 47
- “Open Caveats in Release 2.0(2m)” on page 50

The following caveats were found in Release 2.0(2r)

Table 42 Open Caveats in Release 2.0(2r)

Defect ID	Symptom	Workaround
CSCud75506	The UUID is translated incorrectly when you upgrade ESXi from version 4.1 or 5.1 on the Cisco UCS B200 M3, B220 M3, or B440 M3 blade servers. This is a display issue only, and does not affect the service profiles associated with the blades.	This issue has no known workaround.
CSCtr45130	After upgrading Cisco UCS Manager from Release 1.4.(1j) to 1.4(2b), when you activate, it causes the blade server to reboot.	Before beginning the upgrade, change the maintenance policy to “user-ack”/“scheduled” to defer or control any blade reboot.
CSCtz03288	Hard drives from one manufacturer are two to three times slower than the hard drives from another manufacturer even though both are sold under the same product ID. This issue is observed with 300 GB SAS 10K RPM SFF drives.	Use the correct LSI driver.
CSCtz36973	After upgrading the Cisco UCS Manager from Cisco UCS Release 1.4(3m) to 2.0(2m) release, Cisco UCS Manager alerts a few warning messages to all the associated service profiles and the vNICs configured for these service profiles. Check if there are issues on the vNICs, the uplinks, and the VLANs. If there are no issues, these messages are not harmful to the network connectivity.	This issue has no known workaround.
CSCtz44130	After upgrading from Cisco UCS 2.0(2m) to 2.0(2q) release, a few false positive thermal alerts cause the chassis fans to spool up to full speed.	Reseat the I/O modules to clear the alerts.
CSCtz76897	While upgrading or discovering Cisco UCS Manager, when the chassis discovery policy is changed to the **set link-aggregation-pref port-channel** policy, it creates the port-channel and the FEX is offline for approximately 40 seconds.	After changing the chassis discovery policy, shut down the system and reacknowledge the chassis. Verify that the FEX port-channel has been created.

Table 42 Open Caveats in Release 2.0(2r) (continued)

Defect ID	Symptom	Workaround
CSCtz86513	After sending an inventory message from Cisco UCS Manager, no registration email is received from the SCH Portal. Devices are registered on the SCH portal but the new inventory messages are not logged and the cases do not get created. The Contact field in the Contact information section contains a < or > character.	Remove the > and < from the SCH configuration fields in Cisco UCS Manager.
CSCtz87024	Fibre Channel firmware issues disconnect the SAN and cause a server outage.	Reboot the SAN multiple times to restore the connectivity.
CSCtz87068	After upgrading from Cisco CUS Release 1.4(3i) to 2.0(1w), a false alert about a conflicting VLAN ID is observed on the VLAN. Deleting the conflicting VSAN does not clear the critical fault on the VLAN.	Change the VLAN ID on the conflicting VLAN to a different value and then reset it to the previous value.
CSCtz88815	The auto core transfer failure fault does not get cleared from the Cisco UCS Manager GUI.	This issue has no known workaround.
CSCtz88841	Cisco UCS Manager generates a false VIF Down alarm even though the VIF is active on the fabric interconnect.	Reset the DCE interface from Cisco UCS Manager for the VIF for which the false alarm is generated.
CSCtz93271	Some VFC interfaces are disabled with an error message after rebooting the fabric interconnect.	Reset the DCE interfaces on the affected adapters and ports.
CSCtz99909	When a new BIOS policy is created with the C1E state set to disabled from Cisco UCS Manager, the ESX displays the C1E state as enabled. The BIOS setup menu displays that the C1E is disabled as BIOS policy from Cisco UCS Manager.	Use it as a default policy.
CSCtz99795	When two Cisco UCS domains push the same VLAN profile, the port profile from one Cisco UCS domain disappears.	Modify the maximum port in the port profile of the first Cisco UCS domain and save the configuration. The port profiles are now displayed in both Cisco UCS domains.
CSCua63323	Under low resource conditions, poor performance of PALO Microsoft Exchange DAG causes RQ drop.	This issue has no known workaround.

Table 42 Open Caveats in Release 2.0(2r) (continued)

Defect ID	Symptom	Workaround
CSCub34427	When adding a VLAN to a vNIC, under certain circumstances the server reboots unexpectedly.	This issue has no known workaround.
CSCub51662	When upgrading the firmware to Cisco UCS Release 2.0, the IPMI commands/queries fail to get data from a B-series server.	Reboot CIMC. **Resolved**: This issue is resolved in Cisco UCS Manager Release 2.0(4a).
CSCub59614	Adding a global VLAN to Cisco UCS Manager causes some VIFs to fail.	This issue has no known workaround.

The following caveats were found in Release 2.0(2q)

Table 43 Open Caveats in Release 2.0(2q)

Defect ID	Symptom	Workaround
CSCua31267 CSCtx65534	Deleting a VLAN in the fabric interconnect causes the vNICs that are carrying that VLAN to flap. On deletion of one VLAN on a vNIC, traffic disruption is observed on the other VLAN.	Remove the VLANs from all the vNICs/vNIC templates and the uplinks before deleting the VLANs from a fabric interconnect.
CSCub64088	When you replace a SFP only on the IOM, UCS Manager does not update the new SFP serial number. Continues to display the old SFP serial number.	Decommission the chassis once to recommission and update the SFP serial number.
CSCtu16549	Memory DIMMs in a Cisco UCS blade may be marked as “Equipped Identity Unestablishable” if they are disabled during the power on self test. They do not have their smbios data filled in with the actual vendor data. Instead the vendor data in the smbios data is shown as “NO DIMM.”	This issue has no known workaround.
CSCtx96556	The fabric interconnect to I/O module link does not come up, or it experiences a high degree of packet CRC errors when using gen-2 10 or 7 meter twinax active cable and the 2204XP or 2208XP I/O module. This problem more likely to manifest with uplink number 3 as shown in an NX-OS CLI **show interface fex-fabric** command.	Use fiber cable or 5 meter twinax cable instead.

Table 43 Open Caveats in Release 2.0(2q) (continued)

Defect ID	Symptom	Workaround
CSCty83359	Blades reboot silently on doing any configuration change on the service profile after upgrading the Board Controller and CIMC firmware images using host firmware package and management firmware package. This is seen on B250 blades (N20-B6620-2, N20-B6625-2) when CIMC & Blade controller are updated at the same time, provided the CIMC running version is between 1.4.0 and 1.4.3s or 2.0 and 2.0.1t. These version ranges do not support board controller firmware upgrade on the above specified models. In the first association, boardControllerUpdate will get skipped if CIMC version does not support it. Any further change on the SP will reevaluate the SP and will find out that a board controller-update needs to be done and will trigger it.	Check if your current CIMC firmware version is one of the above specified ones. If yes then first upgrade your CIMC firmware to version which supports Board-controller-firmware-upgrade (i.e 1.4.3t and later and 2.0.1u and later). Once your CIMC gets upgraded then trigger Board Controller upgrade. Note that this will reboot the blade.
CSCty83542	During normal operation of an IOM, a kernel panic occurs and the IOM reboots and returns to normal operation.	This issue has no known workaround.
CSCty91945	If a fabric interconnect or IOM is used for migrating VMs hosted on a Red Hat 6.2 KVM server is rebooted during VM migration, the VM migration will not complete until the IOM or fabric interconnect comes back on line. This occurs if the IOM or fabric interconnect reboots while VM migration is in progress.	This issue has no known workaround.
CSCty93821	Server discovery fails when Cisco UCS Manager is not able to communicate with an adapter during the identification phase.	Reacknowledge or reseat the server.

Table 43 Open Caveats in Release 2.0(2q) (continued)

Defect ID	Symptom	Workaround
CSCty95396	If a server is configured to boot from an iSCSI LUN, then disabling the primary and failover NIC from the host OS will result in the host losing its connection to its boot disk which can lead to a host OS panic or BSOD. This occurs when both the primary and failover vNICs are disabled from the host OS.	Do not disable the failover iSCSI vNIC from the host OS.
CSCtz15271	There is a mismatch between the BIOS token settings definitions for "WatchdogTimerTimeout" and the actual BIOS settings on the server.	For releases prior to 2.0.(3), launch the KVM Console and update the "vpOSBootWatchdogTimerPolicy" setting.
CSCtz16082	A server running ESX can only disable C1E when using the default BIOS policy. Once a new BIOS policy is created with C1E disabled from Cisco UCS Manager, ESX does not recognize C1E as disabled while BIOS setup menu and C-state dump from EFI all show C1E is disabled in the BIOS policy from Cisco UCS Manager. So as long as the policy is either set to default (not set) or a custom default (platform default), the problem is not seen.	Leave the policy on the default settings.
CSCua50442	Third party tools such as demicode, IPMItool etc. may not parse the entire product information for the B-series server. If it does parse, you may see non-printable ASCII characters, blank or replacement ASCII characters in the Type/Version field.	Contact Cisco TAC.
CSCua68423	Under some conditions, when you add/remove a port in a port channel, you will see ENM core.	This issue has no known workaround.
CSCub54167	A Cisco UCS B230 M1 blade server fails the upgrade process during the storage service profile association.	Reacknowledge the blade after the BIOS upgrade is completed.

The following caveats were found in Release 2.0(2m)

Table 44 Open Caveats in Release 2.0(2m)

Defect ID	Symptom	Workaround
CSCug63368	Misconfiguring the gateway IP with DHCP relay agent IP instead of vPC HSRP IP can cause PXE boot fail in VPC environment with some operating system configuration.	Clear ARP entry on both vPC peers. Configure the host to use different IP address on OS from lease assigned to adapter.
CSCub71579	A blade server with VIC 1240 or VIC 1280 adapter may lose network connectivity under heavy FCoE load.	Enable 4 or more QoS system classes to avoid this issue.
CSCtz07684	Boot order in BIOS setup or F6 menus still show Local HDD even after removing Local Disk option in Cisco UCS Manager service profile. This is seen when the boot order is configured by Cisco UCS Manager service profile with PXE eth0, PXE eth1, iSCSI iscsi0, iSCSI iscsi1, Local HDD. If you decide to remove the Local HDD option by deleting it from the boot policy service profile, after server rebooting, the boot order still shows Local HDD in BIOS boot order list. This behavior does not effect booting to PXE and iSCSI devices in the order configured.	Disable Local HDD manually using the following steps: 1. Boot blade. 2. Press F2 key when message is displayed during BIOS POST. 3. Wait until BIOS completes its POST and invokes Setup utility. 4. Select the Boot Options tab. 5. Move the cursor down to Hard Drive BBS Priority and press enter to select this option. 6. Move cursor to hard drive that user want to disable and press enter to configure the drive. 7. Move cursor to Disabled option and press enter to disable the drive. 8. Save and reboot the blade.
CSCtz01783	Under some rare circumstances, issuing NX-OS CLI **show fex detail** command after an I/O module goes offline and online may cause a fabric interconnect to reload.	Use the **show fex** *fex id* **detail** command instead.
CSCty62153	After an extended period of fabric port flapping configurations on border ports are missing.	Reboot the fabric interconnect.

Table 44 Open Caveats in Release 2.0(2m) (continued)

Defect ID	Symptom	Workaround
CSCty62129	When an IOM goes offline, in some cases the forwarding resource is not freed. When the IOM comes back online, some VM-FEX interfaces may not be able to come up. This requires the chassis connectivity mode be port-channel, and only applies to the case when there are close to 1000 VM-FEX interfaces on the same chassis.	Change the chassis connectivity mode to non port-channel and re-acknowledge the chassis will recover.
CSCty36381	In very rare circumstances, an uplink on UCS-2208XP or 2204-XP may experience a rapid link up/down (less than 250 ms interval). This may result in the fabric interconnect side of the link being in link down state but the IOM side of the link being in an up state.	The server port can be disabled and re-enabled to recover.
CSCtw59783	LEDs for ports 1 and 2 on a Cisco UCS 6296 behave differently than other ports.	This issue has no known workaround.
CSCty23519	On a UCS 6120 or 6140 fabric interconnect with 20 chassis, some Cisco UCS Manager processes such as svc_sam_dme and svc_sam_bladeAG crash with the following message: `%KERN-1-SYSTEM_MSG: Proc svc_sam_dme (5082) with Total_VM 706000 KB Resident_Mem 544156 KB Anon_Resident_Mem 501068 KB being killed due to lack of memory - kernel` This issue is only seen after repeated reack, association, disassociation, decommission, and recommission of the chassis in a fully populated testbed.	This issue has no known workaround. The processes are restarted automatically.

Table 44 Open Caveats in Release 2.0(2m) (continued)

Defect ID	Symptom	Workaround
CSCty94457	A Windows Server 2008 baremetal host loses all network configuration and sees a NIC numbering shift. For example if Windows Device Manager showed NIC 1,2,3,4 before the upgrade, after upgrade, NIC 6,7,8,9 will be created. The "new" hardware will have lost all previous configuration such as IP address, DNS server, etc. This occurs after upgrading the Cisco UCS blade adapter card firmware to 2.0(2m). This has only been observed on the Microsoft Windows 2008 ("2k8") operating system on B230 (M1 or M2 blades) and B440 with the Cisco VIC M81KR adapter card. On Cisco C-Series servers this issue has been seen on C260 and C460 servers, also running Windows 2008 R2. This has not been observed on any other supported operating systems such as ESXi, or Red Hat Linux.	Downgrading adapter to previous version reverts the NICs back to the expected numbering with configuration intact. Upgrading the adapter firmware images to Cisco UCS Release 2.0(2q) for M81KR and Cisco UCS Release 2.0(2i) for P81E adapters will also maintain the pre-upgrade NIC configuration.
CSCtr61016	The Cisco UCS Manager GUI hangs while retrieving data for the performance statistics table.	Allow the Cisco UCS Manager GUI to completely retrieve the data, then close the current Cisco UCS Manager GUI session and re-launch.
CSCtx66152	Configuring a RAID policy on a rack-mount server using an ICH10R controller fails.	After Cisco UCS Manager association completes, reset the system and configure RAID directly using the LSI Option ROM. This requires that there is no scrub policy in place in the service profile. This is to avoid deletion of RAID volumes in subsequent association operations.
CSCtk03135	If recovery is initiated for a blade with a corrupted BIOS, there is a chance that recovery will hang. This occurs approximately once in 20-30 trials.	Restart the recovery process to repair the corrupted BIOS. This issue occurs infrequently enough that a simple restart should be enough to resolve it.
CSCtx49701	When the BIOS setup is controlled by Cisco UCS Manager, the option to press F9 to load BIOS defaults in the BIOS menu is still active, which could change BIOS setup such that BIOS setup in the Cisco UCS Manager service profile might conflict with actual BIOS setup.	Do not press F9 to load BIOS defaults while in BIOS setup menu. Always control the settings via the Cisco UCS Manager service profiles.

Table 44 Open Caveats in Release 2.0(2m) (continued)

Defect ID	Symptom	Workaround
CSCtu34607	Changing the dynamic vNIC policy to change the number of vNICs may cause static vNICs to get reordered on PCIe bus. This is seen under the following conditions: 1. Create a Service Profile with Dynamic vNIC policy with count set to less than 50. 2. Create static vNICs required for ESX nk connectivity in HA setup. 3. Associate to server. Check the vNIC PCIe bus orders as seen by Host OS. 4. Increase the dynamic vNIC count to go past 56. 5. You would see PCIe orders of static vNICs are changed in Host OS. 6. Create static vNICs and then create dynamic vNICs. Either create the dynamic vNIC policy with count less than 50 or greater than 56.	There is no known workaround.

CSCtz07798	Under certain conditions, a service profile will generate a configuration failure and a blade that it is associated with is removed from the server pool. This condition can cause service profile re-association to other available blades in the pool.	If a service profile is displaying this condition, re-assign the blade from the server pool to the physical blade by running following command from the Cisco UCS Manager CLI to avoid an outage:
		`F340-31-9-1-B **scope org**`
		`F340-31-9-1-B /org # **scope service-profile server 1/8**`
		`F340-31-9-1-B /org/service-profile # **associate server 1/8**`
		`F340-31-9-1-B /org/service-profile* # **commit-buffer**`
		`F340-31-9-1-B /org/service-profile #`

Release 2.0(1)

- "Open Caveats in Release 2.0(1x)" on page 54
- "Open Caveats in Release 2.0(1w)" on page 58
- "Open Caveats in Release 2.0(1t)" on page 58
- "Open Caveats in Release 2.0(1s)" on page 58
- "Open Caveats in Release 2.0(1r)" on page 61

- "Open Caveats in Release 2.0(1q)" on page 61
- "Open Caveats in Release 2.0(1m)" on page 61

The following caveats were found in Release 2.0(1x):

Table 45 Open Caveats in Release 2.0(1x)

Defect ID	Symptom	Workaround
CSCub40588	"Waiting for FLOGI" error persists after FLOGI succeeds and the VFC comes up.	Reset the VHBA from Cisco UCS Manager to clear the state and the associated fault.
CSCtx90742	All other connections are showing up and statistics look normal except a VM itself is still not receiving traffic. This is seen when the VM's vNIC is marked as masked in the VIF list. In this condition, it will not receive traffic.	Reset the vNIC from vclient.

CSCty91471	The fabric interconnect rebooted with the following error during upgrade of fabric interconnect firmware to version 2.0(1x):
	`Reason: Kernel Panic`
	`System version:`
	`5.0(3)N2(2.1w)`
	`Service:`
		This issue has no known workaround.

CSCty59362	VFC interfaces remain down and all static veths are stuck in the CR_RE state after a full-state restore. Servers may not work properly after the full-state restore operation if the existing server's configuration does not match the configuration in the backup file used for the restore. This is because Cisco UCS Manager does not automatically reconfigure the servers after the restore operation.	When restoring using a backup file that was exported from a different system, it is strongly recommended that you use a system that has the same hardware including fabric interconnects, servers, adapters and IOM or FEX connectivity. Mismatched hardware may lead to the restored system not fully functioning. In case that there is a mismatch between the IOM/FEX links or servers on the two systems, you should acknowledge the chassis and/or servers accordingly after the restore operation.

Table 45 Open Caveats in Release 2.0(1x) (continued)

Defect ID	Symptom	Workaround
CSCtt24695	Sometimes FEX host facing ports are not created/discovered in Cisco UCS Manager at the end of chassis/server discovery. This results in Cisco UCS Manager assuming that the adapter has connectivity to only one fabric. So that blade server cannot be used to associate with a service profile which has vNICs that require both fabric or the fabric to which connectivity is not yet discovered. This happens very rarely during chassis and server discovery.	Re acknowledge the server (or chassis) so that Cisco UCS Manager attempts discovery once again.

Table 45 Open Caveats in Release 2.0(1x) (continued)

Defect ID	Symptom	Workaround
CSCtw59592	In a server using both a virtualized adapter card and a nonvirtualized card, if there are fewer service profile vNICS than the minimum required physical NIC ports then extraneous NIC ports are generated due to Cisco UCS Manager restrictions. (The minimum number of physical ports is 0 for Cisco UCS M81KR, 2 for other non-virtualized cards). This happens in the following circumstances: 1. Full width blade server with a UCS M81KR and a UCS NIC M51KR-B or UCS CNA M72KR-Q adapter card. 2. Single adapter of UCS CNA M72KR-Q with a service profile having one NIC and one HBA will still show 2 NIC and HBA on the OS side. 3. A number of vNICs were created and implicit vNIC placement was selected, so that the number of vNICs to be load-distributed on a non-virtualized adapter was less than the minimal physical NIC ports (2). The system internally creates the 2nd NIC to match to its network connectivity requirement. 4. Once the host OS boots up, it will see an extraneous vNIC being placed on non-virtualized adapter 5. No data traffic is allowed on the additional vNIC.	In a mixed adapter setup, explicitly place the vNICs on the non-virtualized adapter first and then place them on the virtualized adapter. Alternately, create at least 4 static vNICs & 4 HBAs when using dual slot blades in an HA setup.
CSCty47746	Under some rare circumstances, a hot removal and insertion of an IO module results in a timeout of backplane port creation.	Re acknowledge the chassis.
CSCtw67182	A blade with a UCS M81KR adapter shows the error “initialize error 1" during iSCSI boot.	This issue has no known workaround.

Table 45 Open Caveats in Release 2.0(1x) (continued)

Defect ID	Symptom	Workaround
CSCty27581	Any action on a trunked port-channel (such as link, enable or disable) from the Cisco UCS Manager GUI takes a long time (over 2 minutes) to reflect on CLI. Once ports are up, they show as trunking, however vSANs are stuck in initializing.	Use individual links instead of Fabric Port Channel.
CSCty26754	Blades power off unexpectedly, and stay off. A shallow discovery has happened which puts the blade into its desired power state. Some examples of actions that can trigger a shallow discovery are: • Loss of any link between the FI and the IOM • Reset of an IOM • Killing a process with debug plugin • Re-acknowledge of a chassis Blades that have been powered on with the following methods will be left in this inconsistent power state: • Pressing the physical power button on the front • Clicking the reset button on the server in the equipment tab • Right clicking the server in the list of servers on the equipment tab and selecting reset.	When a blade is powered off, only use the Power On button on the General tab to turn on the blade. If the service-profile has a desired power state of Off, but the blade is actually On, click the Set Desired Power State button that will appear on the General tab of the service-profile and change the desired power state to On. The Set Desired Power State button will disappear when the desired and actual power states match. Under the Status Details drop down, the Desired Power State will be changed to Up.
CSCtx95937	When you create a vNIC template under the LAN tab a VM-FEX Port-profile is automatically created under the VM tab. This port-profile under the VM tab is created as a convenience for VM-FEX users.	If you are not using VM-FEX you can safely delete the port-profile. Re-create the vNIC template without checking the VM checkbox or delete the port-profiles that are generated when you edit the VLAN list.

The following caveats were found in Release 2.0(1w):

Table 46 Open Caveats in Release 2.0(1w)

Defect ID	Symptom	Workaround
CSCuf47192	Under normal conditions, a slow memory leak might cause BladeAG to core on reaching the Max 200MB utilization.	This issue has no known workaround.

The following caveats were found in Release 2.0(1t):

Table 47 Open Caveats in Release 2.0(1t)

Defect ID	Symptom	Workaround
CSCuh22023	The data management engine (DME) might be killed by the sam_controller due to replication failure between the FIs.	If the DME is being killed continuously, restart the FI or enter the following commands: 1. `PMON STOP` 2. `PMON START`
CSCug93912	When connected to a Cisco UCS 6120XP Fabric Interconnect, the UCS Manager GUI might fail to start. The Cisco UCS Manager CLI functions correctly and displays the following error: `Fabric Interconnect A, management services have failed.`	Reboot the FI.
CSCtt94543	While accessing the fabric interconnect via SSH, the SSHD process sometimes crashes during the steady state if there is an SSH authentication failure.	This issue has no known workaround.

The following caveats were found in Release 2.0(1s):

Table 48 Open Caveats in Release 2.0(1s)

Defect ID	Symptom	Workaround
CSCug89448	The tech support collection fails on the Cisco UCS Manager GUI. The process starts, but does not complete.	Use the `show tech-support` command in the Cisco UCS Manager CLI.
CSCug59101	FI crashes due to HAP reset triggered by NTP process crash.	This issue has no known workaround.

Table 48 Open Caveats in Release 2.0(1s) (continued)

Defect ID	Symptom	Workaround
CSCuc15009	Under some conditions, the IOM upgrade fails and gets into a continuous reboot after the IOM is activated by the fabric interconnect. Rebooting the fabric interconnect on a failed IOM update does not fix this issue.	Contact Cisco TAC.
CSCub53747	The Power Consumed column on the Power Groups tab in the Cisco UCS Manager GUI displays “0” for the chassis or blades in the default power group.	Create a new power group and move the chassis to that power group. The Power Consumed column will be updated. You can then delete the new power group to move the chassis back to the default power group.
CSCtu16375	If you try to download core files from the Cisco UCS Manager GUI, the following error messages appear: “Failed to download file... reason: Server return http response code 401....." This is seen when Google analytics is enabled.	Disable Google analytics.
CSCts48719	The KVM application does not take keyboard inputs in windowed mode. This happens when the UCSM/KVM is run on a Linux Client.	This issue has no known workaround.
CSCtx12353	After a VLAN mapping change, a vNIC in ENM source pin will fail.	Change the mapping of the named VLAN default from 1 to 2 to 1.
CSCtw96111	A virtual machines using VM-FEX (Dynamic vNIC) port-profiles loses network connectivity. This occurs on ESX/ESXi 4.1 U2 with Cisco UCS B-Series blades running Cisco VIC adapter cards. Some VMs (but not necessarily all) that are connected to the VM-FEX port-profile will lose connectivity. The VM guest OS may or may not show as disconnected.	Rebooting both fabric interconnects will restore connectivity.
CSCtx35808	E2E diagnostic test was not using as much memory as possible depending on blade memory configuration. The test was updated to use as much memory as possible without running out of memory. This test is only available in manufacturing and if a blade is taken out of normal operation to run host diagnostic tests.	This issue has no known workaround.

Table 48 Open Caveats in Release 2.0(1s) (continued)

Defect ID	Symptom	Workaround
CSCtu14851	If port profiles are configured for VM-FEX, the fabric interconnect may crash during upgrade due to a heartbeat failure.	Delete port profiles using the VM tab in the Cisco UCS Manager GUI prior to upgrade
CSCtw97157	When following the steps in the Cisco upgrade guide and activating the subordinate fabric interconnect, guest virtual machines will experience a high CPU load but no other performance problems.	Try one of the three known workarounds: 1. Reboot the blade while the BIOS and adapter firmware is on previous version. 2. Finish upgrade with host firmware package to upgrade BIOS and adapter firmware. 3. Migrate the affected VM to another host.
CSCts56107	On a Service Profile (SP) configuration change, a server is rebooted before the maintenance window. This will happen if you make some configuration change on the SP which does not require a reboot. Then immediately make another change which requires a blade reboot. The blade will reboot immediately.	Please wait for the shallow association to complete and then do further changes on the SP.

The following caveats were found in Release 2.0(1r):

Table 49 Open Caveats in Release 2.0(1r)

Defect ID	Symptom	Workaround
CSCtu10771	When using a UCS 2208 IO module you see a linkState fault for the Cisco UCS Manager virtual interface corresponding to the CIMC management port (port 33 on the IO module).	This is an otherwise harmless fault and it does not affect the performance of the Cisco UCS domain in any way.

The following caveats were found in Release 2.0(1q):

Table 50 Open Caveats in Release 2.0(1q)

Defect ID	Symptom	Workaround
CSCub11507	In some conditions, a blade using a UCS M81KR adapter may lose communication to Cisco UCS Manager and prevent the OS from communicating to the network.	Reboot the blade server.
CSCtu41480	On a service profile configuration change, the changes list also shows "Networking" changes to be deployed even if there's no configuration change done in the networking area. This could happen because of various configuration changes.	This issue has no known workaround.

The following caveats were found in Release 2.0(1m):

Table 51 Open Caveats in Release 2.0(1m)

Defect ID	Symptom	Workaround
CSCtu17983	ESX boot on blades using VMWare Auto Deploy takes a long time.	This issue has no known workaround.
CSCtr30372	In the Cisco UCS Manager GUI, a power cycle with graceful operating system shutdown does not shutdown the operating system gracefully.	Using the Cisco UCS Manager GUI, execute the server power cycle in two steps. First, shutdown the server with graceful operating system shutdown option selected. Then boot the server up after clicking the Boot server option.

Table 51 Open Caveats in Release 2.0(1m) (continued)

Defect ID	Symptom	Workaround
CSCtx23541	After specifying an attribute setting in either the "General" LDAP setting or under the LDAP Provider setting, LDAPD crashes when testing LDAP. This happens with both the Cisco UCS Manager CLI and GUI.	Remove all Attribute configuration in both the "General" LDAP setting and LDAP Provider setting.
CSCtr62641	Currently in Cisco UCS Manager there is no auto-creation of IQN identifiers for iSCSI. IQNs must be manually entered for each iSCSI adapter. There is also no validation on the IQN format.	This issue has no known workaround.
CSCtz03288	Hard drives sourced from one manufacturer are two to three times slower than hard drives from another manufacturer even though both are sold under the same product id. This is seen with 300 GB SAS 10K RPM SFF drives.	This issue has no known workaround.
CSCtr10869	During upgrade from Cisco UCS 1.4 to 2.0, an SSLCert error may be written to the log files.	This issue has no known workaround. This is harmless and has not been found to impact functionality.
CSCtq30308	After kernel rebuild or update a server configured for SAN Boot of RHEL 5.6 or RHEL 5.7 may fail to boot. This is a Red Hat issue, and ticket 744330 has been filed. It is a private ticket that may be referenced when calling Red Hat support for more information.	To recover the server, modify the /etc/modprobe.conf file to add the new entry "alias scsi_hostadapter2 fnic". Also, if you have the entry "alias scsi_hostadapter2 usb-storage", modify it to: "alias scsi_hostadapter3 usb-storage".
CSCtt41541	While upgrading to Cisco UCS Release 2.0 with QoS policies defined, critical errors will be displayed for all QoS policies and VIFs with QoS policies defined on them will be down after upgrading the subordinate interconnect but before upgrading the primary fabric interconnect. Expect that during the upgrade there will be a period of downtime between when the primary restarts and when the secondary becomes primary and brings up its VIFs. During this time all blades will lose their connectivity to both LAN and SAN.	Completing the upgrade to Cisco UCS Release 2.0 by upgrading the primary interconnect will clear these faults. Alternatively you can remove all QoS policies from the affected interfaces, allowing them to come up, complete the upgrade and then reapply the QoS policies with no downtime. This issue is resolved in Cisco UCS Release 2.0(1s).

Table 51 Open Caveats in Release 2.0(1m) (continued)

Defect ID	Symptom	Workaround
CSCto59775	A host configured for iSCSI boot will always boot off a LUN exported to the Primary iSCSI VNIC by default, as iBFT is always posted on the primary iSCSI vNIC. The secondary iSCSI vNIC will post iBFT in case the LUN discovery fails on the primary iSCSI vNIC. However, if the Secondary iSCSI vNIC comes up earlier than the Primary iSCSI vNIC (due to its overlay vNIC having a lower PCI order than that of the overlay vNIC for the Primary) and LUN discovery fails on the Primary, then there is no iBFT posted and the host fails to boot.	Ensure that the PCI order of the overlay vNIC for the Primary iSCSI vNIC is always lower than that of the overlay vNIC for the Secondary iSCSI vNIC.
CSCtl04744	Network connectivity is affected (flapping on uplink ports) on both fabric interconnects during operations such as native VLAN change when the configuration change is done on both fabric interconnects at the same time.	Schedule a maintenance window to perform such configuration changes, and perform the changes separately.
CSCtt18526	After upgrade to Cisco UCS 2.0(1m), blades with UCS M81KR adapters may show the error “initialize error 4” during FC boot.	Downgrade the adapter firmware to the previous version, or upgrade to Cisco UCS Release 2.0(1q).
CSCud71175	When there is a single member port in a port channel, and an additional port is added to the fabric port channel, an HIF down event is triggered to accommodate the extra VNTAG space and provide extra VIF deployment. This occurs when the new link is added to same ASIC. The link will automatically be added and lead to the symptom. If the port is on a different ASIC, then the added link must be chassis-acknowledged. The symptom will be seen after the acknowledgement.	This issue has no known workaround. This is a rare situation that typically does not happen in a traditional port-channel deployment.

Table 51 Open Caveats in Release 2.0(1m) (continued)

Defect ID	Symptom	Workaround
CSCud71227	FWM crash and the switch reboots when you start with one link, add a second link on the same ASIC, then delete the second link and move it to a different chassis.	Acknowledge the chassis. **Note** Acknowledging the chassis will cause traffic drop.
CSCud70315	When a member of a port channel transitions between up and down states, there is a loss for traffic on the port channel, including fiber channel traffic. The throughput for fiber channel goes down and then recovers. This is caused by a SCSI time out and the recovery is triggered by the SCSI layer. The throughput may go down to 0 before recovery, but the application will not see any timeouts.	This issue has no known workaround. Proper SCSI timeout values help in recovery.

Known Limitations and Behaviors

The following known limitations found in Release 2.0(5f) are not otherwise documented:

- On platforms with 00B storage controller, Cisco UCS Manager displays usable (coerced) value in disk inventory section, which is different than the raw 'NumberOfBlocks' value displayed in catalog section. This is a non-issue; Cisco UCS Manager is designed to report the coerced, or usable, size as reported by the LSI controller. Both the host and OOB interfaces report this same value.
- While upgrading from Release 2.0(2q) to 2.0(5a) or higher, the hosts cannot login to storage due to a conflict in the FCoE VLAN ID with one of the regular VLANs. The VLAN conflict is not a supported configuration and it should be fixed prior to the upgrade.
- After the firmware upgrade from Release 1.4(3m) to any later release, vMotion fails due to AES-NI bit difference. As a workaround, disable the OEM AESNI control in BIOS for the blade that is upgraded. Once this feature is disabled and the blade is booted to ESXi, vMotion is allowed to proceed between the two hosts without any issues.

The following known limitations found in Release 2.0(5a) are not otherwise documented:

- Single chassis set up might generate an error with a warning message on accessing shared storage. This might have an impact on system's service when the fabric interconnect fails. In a multiple chassis set up, this might not cause an issue, except in IOM firmware upgrade. If this error does not clear or re occurs, do one of the following: (CSCtu17144)
  - Reboot the IO module.
  - Remove and re-seat the IO module, making sure module is firmly in contact with the backplane.

Note Do not upgrade IOM firmware until this error is cleared.

The following known limitations found in Release 2.0(3a) are not otherwise documented:

- The 2.0(3d).T catalog is not backward compatible with Release 2.0(2) or Release 2.0(1).
- The IOM reset CMC process does not complete due to an inoperable IOM. Replacing the IOM with a new IOM does not clear the state for a long time and the new IOM does not come up. This issue occurs when the reset CMC process is issued to an IOM that the Cisco UCS Manager cannot communicate with.
- The PLOGI frames can get dropped in the fabric interconnect and as a result, the hosts do not have a path to the LUNs. This issue was observed only once while adding the additional chassis to the fabric interconnect.
- When an Ethernet border port failure occurs, the host ports are repinned to a new border port. This issue could cause a few FCoE frames to be dropped. This issue is observed on a failover from one Ethernet border port to another and it can be noticed only when there is a high rate of the FCoE traffic. This is a transient issue and it recovers immediately.
- While downgrading Cisco UCS Manager from Release 2.0(x) to Release 1.4(x) with CLI commands being issued, an svc_sam_dme core dump may occur along with a CLI command failure. This issue could occur due to the following conditions:
  - When an image is activated through the GUI, CLI commands are issued.
  - When an image is activated through the CLI, CLI commands are issued from another CLI session.

  To avoid this issue, do not issue CLI commands during the process of image activation.

The following known limitations found in Release 2.0(2) are not otherwise documented:

- If upgrading from build 2.0(2m) to 2.0(2q), if you check the AES-NI control on B200 M2 and B250 M2 blades, the AES-NI setting value polarity reverses. The BIOS in build 2m defines the AES-NI NVRAM with 0 = disabled and 1 = enabled. The BIOS in build 2q defines the AES-NI NVRAM value with 0 = enabled and 1 = disabled.
- Whenever a 2232 FEX is decommissioned and re-commissioned, all the servers that are connected to that FEX must be re-acknowledged.
- During an upgrade from 2.0(1) to 2.0(2), duplicate IQNs are not allowed. Any duplicate IQNs statically entered will raise an alarm. This is seen in service profiles with duplicate IQNs assigned to multiple iSCSI vNICs. There are two fixes. One corrects the issue before the upgrade. The second fixes the issue assuming the upgrade has already been performed. Either fix will correct the issue.

  Pre Upgrade:

  Modify any service profiles or service profile templates with iSCSI vNICs to have unique IQNs. Remove any duplicates. If necessary, use the PowerShell script provided in the upgrade notes to find out which iSCSI vNICs reuse the same iSCSI name.

  Post Upgrade:

  a. Cisco UCS Manager will throw faults on iSCSI vNICs which have the shared IQN name.

  b. Enter the **show identity** *iqn* | *include iqnname* command to find which iSCSI vNIC has the IQN registered.

  c. Modify the iSCSI vNIC which is using the same IQN name but is not registered, and then edit the IQN name (manual or pooled).

  d. Make any change to the SP (ex:- Fw upgrade or modify description and so on.)

e. Re-run the **show identity** *iqn* | *include Service Profile name* command and make sure that the IQNs are registered in Cisco UCS Manager.

The details of the PowerShell script are provided in the troubleshooting and upgrade guide. (CSCty29247)

- At the end of installing ESXi 5.0 to an iSCSI LUN, an error message appears “expecting 2 boot bank, found 0". This message is not critical and a reboot of the system will start a normal boot of ESXi without any issues.
- Power-related BIOS options for C1E are disabled by default on a B200 M3.
- If the desired power state for a service profile associated with a blade server or an integrated rack-mount server is set to off, using the power button or Cisco UCS Manager to reset the server will cause the desired power state of the server to become out of sync with the actual power state and the server may unexpectedly shut down at a later time. To safely reboot a server from a power-down state, use the Boot Server action in the Cisco UCS Manager GUI.

The following known limitations found in Release 2.0(1) are not otherwise documented:

Cisco UCS Manager

- When using the Windows VIRTIO driver in a virtual machine, Ethernet performance is low when compared to Linux based VMs in a Red Hat KVM environment. Windows does not currently support the LRO feature. To minimize performance impacts, disable GRO using the **ethtool -K** *interface* **gro** command. Disabling GRO may cause higher CPU utilization with TCP traffic.
- A bonded interface will not start as a slave if the MASTER value is in double quotes. You will not be able to create NIC teaming (channel bonding) with third-party adapters.
- The HDD fault monitoring feature cannot detect failures in all possible circumstances. The disk controller may report the disk as operable even though some blocks are marked Unknown. In this circumstance, RAID creation will fail. There is no workaround. ()
- When trying to configure an FC uplink or VSAN as an FC traffic monitoring source, an error message appears stating “Error creating mon-src-mysession. FC Port (1/29) cannot be configured as ingress SPAN source due to hardware limitation.” This only happens on Cisco UCS 6200 Fabric Interconnects. ASICs in these fabric interconnects do not allow a FC port or VSAN to be added as a SPAN (traffic monitoring session) source. There is no workaround. You can still can add a VFC as a source for an Ethernet traffic monitoring session. (
- When Cisco UCS Manager and fabric interconnect activation are done together, the switch upgrade can take longer than usual. This may happen when not following the published upgrade procedure. ()
- On an adapter configured with two iSCSI VNICs, only the iSCSI VNIC designated as primary in the boot order will post the discovered iSCSI LUN to the BIOS and write an iBFT entry to the host memory during boot. There is no workaround. (CSCtr51704)
- After an upgrade from a prior release to 2.0(1), a critical fault may be raised about an overlapping or matching FCoE VLAN ID used for a vSAN and an Ethernet VLAN ID under the same fabric as the FCoE VLAN. Raising a fault is the correct behavior under this circumstance. The fault can be avoided by changing either the FCoE VLAN ID or the Ethernet VLAN ID so that they have two different IDs prior to the upgrade. Resolving the problem after the upgrade may lead to down time for the system. See the Software Advisory. (
- When using Release 2.0, BIOS versions from the 1.4 software versions may be listed. If these versions are selected when attempting a BIOS recovery, the result is a system boot failure in B440 and B200 blades, the recovery may not complete, and the system may be permanently damaged or unrecoverable. You must choose to recover the BIOS to a BIOS version from the 2.0 software release. (

- Before you delete a VLAN from a fabric interconnect, ensure that the VLAN has been removed from all vNICs and vNIC templates. If you delete a VLAN that is assigned to a vNIC or vNIC template, the vNIC could allow that VLAN to flap.

OS

- If during RHEL 5.x installation to an iSCSI LUN on a blade with a Broadcom M51KR-B adapter RHEL 5.x does not detect the iSCSI LUN during OS installation, select the Broadcom M51KR-B port during the install and manually assign the initiator IP address, subnet mask, and gateway with the values from the service profile. ()

Fabric Interconnect

- When UCS is connected to an upstream Cisco Nexus 7000 Series switch (running 4.2.4 version) using port-channels, and if the port channel is configured as LACP passive on the Cisco Nexus 7000 Series switch side, it is possible that under high system stress situation, LACP may not be able to converge for the port channel. The workaround is to avoid native VLAN configuration change while system instability is in place or CPU utilization is high. Using LACP active on Cisco Nexus 7000 Series switch also reduces the likelihood of the problem occurring.
- Per- packet Veth statistics for the UCS M81KR adapter are no longer supported, and will display as 0. Supported statistics are now packets, packets mcast, packets bcast, Bytes, and packets dropped.
- When SAN port channel or a HIF port channel has FC traffic flowing through them, any link flap in the port channel can cause the FC traffic to be impacted or lost. Even multipathing does not help the FC traffic to continue as the VFC is operationally up via the other links of the port channel. Traffic will recover after a short while, but increasing SCSI timer settings can help. ()

BIOS

- When the BIOS is upgraded on a B230-M1 blade from Release 2.0(1m) to Release 2.0(1q) or later, the PCI bus enumeration will shift by one bus number. This renumbering can cause certain operating systems such as VMware ESX or Windows to see the old vNICs and vHBAs with the new PCI address and could result in those interfaces being inoperable unless the configuration is changed in the OS. In case of ESX, a workaround is to edit the esx.conf with the new PCI address and to modify the vswitch configuration. This issue results from the resolution of Caveat CSCts86890, and affects only the upgrade of this specific server between these two specific releases. See the Software Advisory.

Upgrade and Downgrade Issues

- After downgrading from Cisco UCS Manager 2.0 to 1.4(1) or 1.4(2), the fabric interconnect can become unstable and fail to boot. This is usually due to having enabled features specific to release 2.0 that are not available in the earlier release and neglecting to disable those features before attempting the downgrade. In general, it is best to contact TAC and have them walk through a downgrade with you rather than attempt it unassisted.
- After upgrading from a 1.3.x to a 1.4.x or a later release, you might see the service profile configuration disappears from an organization. To confirm that this problem has occurred, use a CLI command that begins with **show service-profile**. A NULL CLI output confirms the problem. This problem is most likely to occur if you created an organization with a space in its name while running a Cisco UCS Manager 1.0 release and then later upgraded Cisco UCS Manager to a 1.3.x release. In the 1.3.x release, spaces are not allowed in organization names and are automatically replaced with an underscore. If the system is subsequently upgraded to a 1.4.x or later release, the old organization name with a space reappears without the space to underscore conversion and all of its children (which includes service profiles, policies, and templates) are deleted. Note: An organization that was created in a Cisco UCS 1.3.x release or with a name that does not contain a space character will not have this problem.

To avoid this problem, do the following before upgrading from a 1.3.x release to a 1.4.x or a later release:

1. Change the description field of the organizations that have underscores in their names by removing the underscores and any spaces to help keep the organizations in the database.
2. Create a backup using the All Configuration option before upgrading. If a problem occurs after the upgrade, restore the configuration using the backup file. After importing the configuration file, reacknowledge all blades to restore their VIF status.

- Using any M3 server may require an upgrade to the IOM in the chassis. The third-generation adapter cards have the features that require a Cisco 2204 or 2208 IOM, and are not backward compatible with the Cisco 2104 IOM.

Open Caveats from Prior Releases

This section contains open caveats for the following releases:

Release 1.4(3)

The following caveats were found in Release 1.4(3):

Table 52 Open Caveats in Release 1.4(3)

Defect ID	Symptom	Workaround
CSCui19367	Config Import fsm fails with the following error: `Cannot create non-creatable object of class:commShellSvcLimits`	Delete commShellSvcLimits from the configuration file and then re-import.
CSCtn84926	MAC address-based port security for Emulex converged Network Adapters (N20-AE0102) is not supported. You configure MAC address-based port security through the network control policy in the service profile. When MAC address-based port security is enabled, the fabric interconnect restricts traffic to packets that contain the MAC address that it first learns. This is either the source MAC address used in the FCoE Initialization Protocol packet, or the MAC address in an ethernet packet, whichever is sent first by the adaptor. This configuration can result in either FCoE or Ethernet packets being dropped.	Disable MAC security on the service profile.
CSCty90643	The DME process on one fabric interconnect frequently crashes when the peer fabric interconnect is in an inoperable state.	Resolve the issue with the fabric interconnect in the inoperable state and the DME on the other fabric interconnect will become stable.
CSCtx41463	A fabric interconnect reboots unexpectedly. Using the **show system reset-reason** command returns “Reset triggered due to HA policy of Reset.”	This issue has no known workaround.
CSCty05262	PAA for a SPAN session does not works with 8Gb transceivers and Fibre Channel expansion modules on the fabric interconnect.	Upgrade to Cisco UCS Release 2.0(1t).

Table 52 Open Caveats in Release 1.4(3) (continued)

Defect ID	Symptom	Workaround
CSCts53607	When a UCS M81KR or UCS M71KR-E/Q (NIV) adaptor is used, and the isolated host is communicating using a MAC configured in the service profile (and registered at the interconnect via a VIC) PVLAN traffic does not flow for an isolated host. Using the **show platform fwm info hw-stm** command at the NX-OS prompt shows that the isolated host MAC is learned on the isolated VLAN, but not learned on the primary VLAN.	This issue has no known workaround. You need to upgrade to Cisco UCS Release 2.0(1s).
CSCtu17091	Blades unexpectedly reboot on Cisco UCS Manager activation when upgrading from Cisco UCS Release 1.3(1) to 1.4(3s).	Follow the upgrade path: Cisco UCS Manager 1.3(1x) -> 1.4(3r) then Cisco UCS Manager 1.4(3r) -> 1.4(3s).
CSCtu11613	When an IOM reboots after a software update on a full width blade, the HIF ports on the second adapter are not brought up by the IOM.	Reboot the IOM.
CSCtr91923	Thermal faults are confusing as they do not have meaningful details. The causes for thermal conditions are: • Threshold crossings of thermal sensors of IOM and blades. • Non availability of blade thermal sensor readings. • Loss of network connectivity between IOM and blades. • Faults in chassis fans and loss of cooling.	For threshold crossing of thermal sensors for IOM and blades, separate faults are raised. For other causes, collect IOM tech support and contact Cisco TAC. See the Cisco UCS troubleshooting guide for IOM tech support details.
CSCtu22052	A BladeAg crash is observed if a request bios_recovery_ctrl message is sent to a blade, but the response came back too late and is ignored by mcclient.	None needed. BladeAg will restart.

Release 1.4(2)

The following caveats were found in Release 1.4(2b):

Table 53 Open Caveats in Release 1.4(2b)

Defect ID	Symptom	Workaround
CSCtq84985	An Intel Westmere-EP CPU on a B200-M2 or B250-M2 blade may not be able to perform to its full extent when running a subset of 1.4.x BIOS versions. The BIOS may incorrectly initialize a value during boot up which keeps the CPU at P1 even when P0 is requested by an OS.	Please upgrade to the BIOS release for Cisco UCS Release 2.0(2m) to prevent this issue.

CSCtn09020	If the installed DIMMs do not have thermal sensors (the most likely cause as this warning is logged during initial system memory initialization) or the installed DIMMs exceeded the thermal threshold values programmed in either the memory controller or the Memory buffer, then the RankMargintest file in the CIMC shows the following warning code:
	`MRC - Warning Code:0x9 on Socket#1 Br#0 Ch#00, Ddr#00, Dimm#00, Rank#FF (if applicable)`
	`MRC - Warning Code:0x9 on Socket#1 Br#0 Ch#00, Ddr#01, Dimm#00, Rank#FF (if applicable)`
		This issue has no known workaround. The message is informational, and can be ignored.

Release 1.4(1)

The following caveats were found in Release 1.4(1i):

Table 54 Open Caveats in Release 1.4(1i)

Defect ID	Symptom	Workaround
Upgrade		
CSCub99354	Under certain conditions, the VIC adapter fails after upgrade due to FRU corruption.	Contact Cisco TAC.
High Availability		

Table 54 Open Caveats in Release 1.4(1i) (continued)

Defect ID	Symptom	Workaround
CSCth17136	High Availability does not become ready until all 3 selected HA devices (chassis/rack-unit) have been discovered. The condition that triggers this problem is the fact that a previously functioning and fully discovered device (either chassis or rack-mount server) has failed. This may be due to connectivity problems or faulty behavior. In this case the system remains in HA NOT READY state.	The root of the problem is a failed device. Fixing the problem in the device is the first step. If the failure is persistent the faulty device can be decommissioned to resolve the problem.
CSCth69032	When Cisco UCS Manager is operated in High Availability mode, SNMP traps stop arriving as expected if the SNMP trap IP header source address field is set to the cluster virtual IP address.	SNMP trap recipients must not use the SNMP trap IP header source address, or be prepared for it to contain the management IP address of the currently primary fabric interconnect.
BIOS		
CSCtk55618	Blade and rack-mount servers that include unequal sized HDDs or SSDs have encountered various failures intermittently. Cisco UCS Manager reports “Error Configuring Local Disk Controller” in most cases during these failures, though other errors are also seen.	Verify that the servers use equal sized disks from the same vendor. This ensures that all of the disks are of identical disk capacity.

Table 54 Open Caveats in Release 1.4(1i) (continued)

Defect ID	Symptom	Workaround
CSCtj67835	The BIOS Setup shows less memory size and some DIMMs disabled on a B230. The SMBIOS table does not report memory info in Type 17 structure for the disabled DIMMs. The UCSM reports less memory size and some DIMMS disabled. This happens when the BIOS disables some DIMMs incorrectly when DIMMs on certain slots do not have the corresponding lockstep pairs installed. For example, configurations that can cause this failure include: 1. DIMM on slot C2 is not installed and slot C3 is installed - Causes DDR training failure that results in DIMM failure on slots C0,C1,C3,D0,D1,D2,D3. 2. DIMM on slot A1 is not installed - Disables DIMMs on slots A0, A2, A3. The NHM-EX CPU requires the DIMM0 in each DDR channel populated first before populating DIMM1 on that channel. This is an invalid configuration. 3. DIMM on slot B0 is not installed - Disables DIMMs on slots B1, B2, B3. The NHM-EX CPU requires the DIMM0 in each DDR channel populated first before populating DIMM1 on that channel. This is an invalid configuration.	Always populate the DIMMs in lockstep pairs, as described in the user documentation. The lockstep-ed DIMM slot pairs are A0 & A1, A2 & A3, B0 & B1, B2 & B3, C0 & C1, C2 & C3, D0 & D, and D2 & D3. Also, it is recommended to populate the DIMMs in the following order. Blue slot pairs, White slot pairs, Yellow slot pairs, Black slot pairs.
CIMC		
CSCti94391	When using mirroring mode, if a UCE error happens, there is a Redundancy SEL event and also a UCE SEL event. No other details are available for the Data Parity error.	This issue has no known workaround.
Adapters		

Table 54 Open Caveats in Release 1.4(1i) (continued)

Defect ID	Symptom	Workaround
CSCtj89468	The link from the rack-mount server adapter to the fabric interconnect port remains down if the SFP type is FET (Fabric extender transceiver). Currently the FET type is supported only between a fabric extender and a fabric interconnect. If the SFP used for the link between the IOM and the rack-mount server adapter is an FET, the link will remain down.	Replace the SFP with one of the supported SFPs for rack-mount server adapters.
CSCtj82445	CRC errors reported on an M81KR network interface on SLES 11 SP1. This is seen under High TX and RX traffic on SLES 11 SP1. The FIFO is not cleared as fast as it should because of some delays in the PCI path. An M81KR firmware devcmd storm from the host is also investigated to be one reason for the PCI stalls. These CRC errors are actually caused by FIFO overruns on the M81KR which are in turn caused by PCI stalls. They are not real CRC errors but truncated packets (due to FIFO overrun) flagged as CRC errors.	Reduce the traffic load to reduce the reported CRC errors. This assumes that the CRC errors in question are generated on M81KR and that there are no bad packets entering the adapter.
Cisco UCS Manager		
CSCtr07696	LicenseAG crashes during Cisco UCS Manager restart after downloading license files.	Erase these expiring license files from "/bootflash/license/downloaded/" through the debug plugin, and use a permanent license instead of a temporary license.
CSCtk97755	Cisco UCS Manager takes a long time to push configurations containing large number of port-profiles to the VMware Virtual Center (VC). This happens when large number of hosts and virtual machines (VMs) are configured (for example, 500 VMs on 60 hosts managed by the same VC) and a large number of port-profiles are assigned to multiple DVSes in the VCenter.	Wait until the operations complete. Configuration FSM could take more than 30 minutes. Then, configure a smaller number of port-profiles.

Table 54 Open Caveats in Release 1.4(1i) (continued)

Defect ID	Symptom	Workaround
CSCtk69231	When 15 or more chassis are configured in release 1.4(1) and the system is downgraded to release 1.3(1), chassis beyond 14 are still there. This may cause some issues as the max chassis support enabled with the 1.3(1) release is 14.	Manually decommission chassis in the system to keep the total number of chassis to 14 before downgrading to release 1.3(1) from 1.4(1).
CSCtj18969	When a rack-mount server has a local disk installed, it does not report real-time disk operability status (disk operability is reported as “N/A”).	This issue has no known workaround.
CSCtj82918	When the Cisco UCS Manager shell mode is set to s either management or local-management mode, the CLI command **terminal monitor** is not available.	Use the **terminal** command in NX-OS mode.
CSCtj62296	The minimum power cap that can currently be set is 3400W. The chassis power cap has a lower limit of 3778 W (AC), which is internally converted to 3400 W (DC).	Do not enter a cap below this requirement. This requirement was derived from the need to safely allow a chassis to simultaneously boot all blades in a chassis.
CSCti87891	The Cisco UCS Manager shell does not support redirection of **show** command output to a remote file system.	Redirect the output to a local file in either *workspace*: or *volatile*: and then transfer the file to the remote system using the **cp** command in local-mgmt mode.
CSCti86217	In Cisco UCS Manager there is no option to change the port speed of the SPAN destination port.	Un-configure the SPAN destination port and make it an “uplink”. Change the port speed on the uplink port, then reconfigure the port as a SPAN destination port. The port speed will be at the value that user set for the “uplink” port.
CSCtj51582	Cisco UCS Manager reports an unsupported DIMM as missing but does not raise a fault.	Verify that the DIMM is a Cisco DIMM supported on that server model.
Cisco UCS Manager GUI		

Table 54 Open Caveats in Release 1.4(1i) (continued)

Defect ID	Symptom	Workaround
CSCtj57838	Non-disruptive pending changes may not be shown on a service profile. When a service profile has a maintenance policy that defers the application of disrupting changes to the server, user can see what changes are pending and make further changes. Disruptive pending changes are always visible on the service profile, whereas non-disruptive changes may not be shown. Non-disruptive pending changes are only shown for user convenience. This defect has no functional impact.	This issue has no known workaround.
Cisco UCS Manager CLI		
CSCtj78998	When VIF creation does not follow V-motion, NPPM does not move the VIF to a new dynamic and the stale VIF does not carry the traffic any more. This would cause the SPAN to stop monitoring the traffic from the original VM.	Re-discover the VMs and re-create the SPAN.
Fabric Interconnect		
CSCtk35213	Fabric interconnect activation during a downgrade from 1.4(1) to 1.3(1) will fail if the setup has an active Nexus 2248 Fabric Extender.	Decommission all fabric extenders and rack-servers and completely decommission the FSM before downgrading the fabric interconnect image.

Table 54 Open Caveats in Release 1.4(1i) (continued)

Defect ID	Symptom	Workaround

CSCtk09043	The server UUID displayed by ipmitool does not match that shown by the Cisco UCS Manager CLI. UCS UUID encoding follows pre SMBIOS 2.6 specified encoding, which is big-endian encoding. Ipmitool does not work well with that encoding. The SMBIOS 2.6 specification mandates mixed encoding (first 3 fields little-endian, last 3 big-endian), which is followed by ipmitool.
	
	For example, the server detail from Cisco UCS Manager CLI shows:
	
	`Dynamic UUID: 0699a6f3-1b81-45f8-a9f2-c1bbe089324e`
	
	`# ipmitool -H 10.193.142.104 -U gurudev -P password mc guid System GUID: f3a69906-811b-f845-a9f2-c1bbe089324e`
	
	Compared to Cisco UCS Manager CLI or GUI output, the first 3 fields f3a69906-811b-f845 show up differently in the output of ipmitool.
		The following usage of ipmitool can be a workaround:
		
		`#ipmitool -H 10.193.142.104 -U gurudev -P password raw 0x06 0x37 06 99 a6 f3 1b 81 45 f8 a9 f2 c1 bb e0 89 32 4e`
		
		The output matches the value printed by the Cisco UCS Manager CLI.

CSCtj10809	The show port-security NX-OS CLI command returns a negative value for the Max Addresses. This will occur when a system is configured with more than 8192 Port VLAN instances and. port security is enabled on all interfaces such that more than 8192 MACs are secured.	Do not configure port-security such that secured Port VLAN instances is more than 8192.
CSCti85875	When an N2XX-ACPCI01 adapter port on a C-series server is connected to an uplink port on a UCS 6100 fabric interconnect, a fault message should appear because this connection is not supported, but there is no such fault message for this situation in this release.	This issue has no known workaround.
CIMC		

Table 54 Open Caveats in Release 1.4(1i) (continued)

Defect ID	Symptom	Workaround
CSCtj93577	The Blade CIMstic management IP address assignment is not included in backups.	Manually record the blade CIMC static management IP address assignments, and re-enter them if necessary.
RAID/Local Disk		
CSCtf73879	Cisco UCS B200 M3 and Cisco UCS B22 M3 servers currently do not support disk status, failures, fault codes, and alarms from MegaRAID controller.	This issue has no known workaround.
CSCtj03021	For the B200 and B250 blade servers, the Local Disks 'Operability' field is reported as “N/A”. The 'Operability' field of the Local Disks in B200 and B250 is expected to have a correct value and should not be reporting 'N/A'.	This issue has no known workaround.
CSCtf84982	For the MegaRAID Controller on the B440 blade server, Cisco UCS Manager fails to report BBU Status, Properties and Errors.	This issue has no known workaround.
CSCtj48519	If one or more conditions are met, Cisco UCS Manager fails to capture certain Local Disk errors. Conditions include: Mixing the SAS and SATA Local Disks in the same server; Disk spin-up or disks present but not reaching 'Ready' state; Missing Disks.	This issue has no known workaround.
CSCtf17708	Cisco UCS Manager does not include the implementation for the Write Through, Write Back, and Write back with BBU MegaRAID Battery (BBU) Write Policies for the B440 server.	This issue has no known workaround.
CSCti39470	Cisco UCS Manager currently does not support RAID 50 and RAID 60.	This issue has no known workaround.
CSCtj89447	Cisco UCS Manager fails to create a single disk striped RAID config in the Storage Controller 1064E environment.	This issue has no known workaround.

The following caveats were found in Release 1.4(1a):

Table 55 Open Caveats in Release 1.4(1a)

Defect ID	Symptom	Workaround
CSCug61578	When you remove the management cable from the primary FI, you are not able to view the SNMP trap.	There is no known workaround for this issue.

Release 1.3(1)

The following caveats were opened in Release 1.3(1c):

Table 56 Open Caveats in Release 1.3(1c)

Defect ID	Symptom	Workaround
CSCua46077	On ethernet border port failure, host ports are repinned to new border port. This could cause a few FCoE frames to be dropped. This issue is seen on failover from one ethernet border port to another, and only when there is a high rate of FCoE traffic.	This is a transient issue and recovers immediately. **Resolved**: This issue is resolved in Cisco UCS Manager Release 2.0(5a).

Release 1.2(1)

The following caveats were opened in Release 1.2(1):

Table 57 Open Caveats in Release 1.2(1)

Defect ID	Symptom	Workaround
Red Hat Linux		
CSCte73015	Loading multiple driver disks during a RHEL 5.x installation fails.	See the article at http://kbase.redhat.com/faq/docs/DOC-17753
BIOS		
CSCtb20301	Hubs that only use USB 1.0 may not properly present an attached USB device to the UCS server.	Avoid using USB hubs that are exclusively USB 1.0 capable. Virtually all USB hubs sold today are USB 1.0/2.0 capable.
CIMC		

Table 57 Open Caveats in Release 1.2(1) (continued)

Defect ID	Symptom	Workaround
CSCti94391	When using mirroring mode, if a UCE error happens, there is a Redundancy SEL event and also a UCE SEL event. No other details are available for the Data Parity error.	This issue has no known workaround.
Adapters		
CSCtj89468	The link from the rack-mount server adapter to the fabric interconnect port remains down if the SFP type is FET (Fabric extender transceiver). Currently the FET type is supported only between a fabric extender and a fabric interconnect. If the SFP used for the link between the IOM and the rack-mount server adapter is an FET, the link will remain down.	Replace the SFP with one of the supported SFPs for rack-mount server adapters.
Cisco UCS Manager		
CSCte58483	The PCIe Address for the Cisco UCS M81KR Virtual Interface Card is not seen in the GUI (or CLI). It causes no functional impact.	The only workaround is to boot some host OS onto the blade and then determine the PCI address and map it to the MAC address (and subsequently to the VNIC). In a 2.6 kernel based Linux for instance, the /sys/class/net/<device> directory has relevant information.
CSCte44668	Modification of trusted CoS policy in Service Profile does not get immediately applied to the server. If you modify the trusted CoS policy of an adapter profile in a service profile that is currently attached to a physical server, a server reboot is needed. Since it is unsafe to automatically reboot an associated server, UCSM currently does not.	Manually reboot the server or disassociate and reassociate the server to get the CoS policy to be applied.
CSCtd14055	For each Cisco UCS 82598KR-CI 10 Gigabit Ethernet Adapter, 2 interfaces show up in the OS and ethtool reports Link Detected = yes for both of them. This is only seen on Cisco UCS B250 servers.	Use the MAC that has the value provisioned in the service profile.
Cisco UCS Manager GUI		

Table 57 Open Caveats in Release 1.2(1) (continued)

Defect ID	Symptom	Workaround

CSCte58155	When upgrading from releases prior to 1.1.1, OS-specific default adapter policies will not have the current recommended default values.	After an upgrade from a release prior to 1.1.1, we recommend manually changing the adapter policy parameters to the following values:
		`Eth VMWare->RSS: Disabled`
		`Eth VMWarePassThru->RSS: Enabled`
		`Eth default->RSS: Enabled`
		
		`FC (all)->FCP Error Recovery: Disabled`
		`FC (all)->Flogi Retries: 8`
		`FC (all)->Flogi Timeout: 4000`
		`FC (all)->Plogi Timeout: 20000`
		`FC (all)->IO Throttle Count: 16`
		`FC (all)->Max LUNs Per Target: 256`

CSCta21326	Logon access is denied for user accounts where the password field was left blank during user account creation.	When creating a user account, ensure that a secure password for the account is specified.

Release 1.1(1)

This section lists the open caveats in release 1.1(1j).

Table 58 Open Caveats in Release 1.1(1j)

Defect ID	Symptom	Workaround
BIOS		
CSCtd90695	With the B-250 blade server, the displayed ESX and Linux OS HDD Boot Device Order is the reverse of the BIOS HDD Boot Order.	Review both the disks (and drive labels as applicable) during installations of ESX and Linux versions and choose the correct disk for installation.
CSCta45805	FSM gets stuck in an Error Configuring the Local Disk Controller state due to various underlying conditions. Those can include but are not limited to the following: • The Local Disks not getting discovered correctly or are “available/presence-Equipped” but not in a Ready state. • Failures that can't be correctly communicated to Cisco UCS Manager can get reported as this type of error.	Remove and insert all of the local disks from the failing server, then re-acknowledge the server.

Table 58 Open Caveats in Release 1.1(1j) (continued)

Defect ID	Symptom	Workaround
CSCsy76853	The Disk Fault/Error Codes, Disk Status, Alarms and the failures forwarded by the SAS Controller are not received by Cisco UCS Manager.	This issue has no known workaround.
CSCtb12390	After resetting the CMOS the system date needs to be reset to current.	This issue has no known workaround.
Red Hat Linux		

CSCte44548	When a vNIC is not in failover mode and a link down event occurs, the network traffic on the blades is disrupted with a system running RHEL 5.3.	This is a known issue with the ixgbe driver in RHEL 5.3 and because RHEL 5.4 is the latest release, Red Hat recommends upgrading the systems to the RHEL 5.4. If you cannot upgrade to RHEL 5.4, below are a few suggestions that has been found to work.
		1. Restart the network.
		`service network restart`
		or
		`ifdown ethx`
		`ifup ethx`
		2. Run your system with nomsi.
		• Edit /etc/grub.conf
		• Add pci=nomsi to the kernel line
		• Restart the system with this kernel
		Note that network performance may be affected since the system is running in legacy mode.

Cisco UCS Manager		
CSCsy80888	After the removal or insertion of one or more local disks, their full discovery fails.	Re-acknowledge the server to complete the full discovery.

Table 58 Open Caveats in Release 1.1(1j) (continued)

Defect ID	Symptom	Workaround
CSCte12163	For a given port profile with existing VIFs, if the "Max-Ports" setting is reduced from the currently configured value to a value less than the "Used-Ports" value reported for that port profile by VMware vCenter, this is a mis-configuration. The new value for "Max-Ports" for that port profile will only be updated in Cisco UCS Manager and its update in VMware Center will fail, causing a inconsistency between Cisco UCS Manager and VMware Center Server.	If the need arises to reduce the value of "Max-Ports" of a given port profile, the new value should be at least the value of "Used-Ports" reported by the VMware Center for all the DVSes for that port profile (not lower than maximum of all the "Used-Ports" values). This constraint has to be ensured manually.
Cisco UCS Manager GUI		
CSCtb35660	When a cluster configuration is set up such that I/O module 1 goes to fabric interconnect B and I/O module 2 goes to fabric interconnect A, then the Ethernet devices are given ports 1 and 0. However if the setup is straight, with I/O Module 1 connected to fabric interconnect A and I/O Module 2 to fabric interconnect B, then the devices are assigned ports 0 and 1.	Connect IOM1 to fabric-interconnect A, and IOM2 to fabric-interconnect B.
UCS Manager CLI		
CSCtc86297	The UUID of the VM changes in VMware vCenter. After a VM restarts, the virtual machine node on the VM tab shows multiple instances of the same VM with one online and one offline.	After the VM retention period configured in the VM lifecycle policy has passed, Cisco UCS Manager deletes the offline instance automatically.

Release 1.0(2)

This section lists the open caveats in release 1.0(2).

Table 59 Open Caveats in Release 1.0(2)

Defect ID	Symptom	Workaround
BIOS		
CSCtc21336	With various Local Disk Configurations, the LSI SAS Configuration Utility fails to launch while in BIOS.	The LSI SAS Controller Utility should not be used and all of the Local Disk Policy and Service Profile operations must be executed using Cisco UCS Manager.
CSCsy54097	When the memory mirroring configuration is destroyed by removing a DIMM, the BIOS will switch to the Performance mode, and will not log a message that mirroring was disabled.	Check the status of the memory mirroring in **BIOS Setup->Advanced -> Memory Configuration -> Memory RAS and Performance Configuration**.
CSCsz41907	When plugging or removing USB devices at **BIOS Setup -> Advanced -> USB**, the Setup Utility may hang.	Reboot the server.
HTTP		
CSCtc13234	HTTPD process crashed, with the following event log: Process crashed. Core file 1253640662_SAM_ucs-6120-1-A_httpd_log.3114.tar.gz (SAM/Switch Core Dump) detected on fabric interconnect A	This issue has no known workaround.
Cisco UCS Manager GUI		
CSCta94641	When waking up from sleep, the Cisco UCS Manager GUI will detect an event sequencing error and display the error: “Event Sequencing is skewed” because the JRE does not have a sleep detection mechanism.	Always shut down the UCSM GUI before putting your computer to sleep.
CSCtb45761	Downloads may be slow if TFTP is used.	If TFTP performance is slow, use SCP or another protocol.

Release 1.0(1)

This section lists the open caveats in release 1.0(1).

Table 60 Open Caveats in Release 1.0(1)

Defect ID	Symptom	Workaround
AAA		
CSCsz44814	Local user passwords cannot contain "$" character.	Do not include the "$" character in local user passwords.
Adapters		
CSCsz68887	When a service profile containing two vNICs and having failover enabled is applied to QLogic or Emulex CNAs, the failback timeout specified in the adapter policy for the second vNIC has no effect. The failback timeout specified in the adapter policy and applied to the first vNIC is applied to the whole adapter and is effective for both vNICs.	Specify the desired failback timeout in the adapter policy and apply to the first vNIC.
BIOS		
CSCsz99666	Installing EFI Native SLES 11 is currently not supported.	This issue has no known workaround.
CSCsz41107	One vNIC defined in the Cisco UCS Manager service profile boot order results in two BIOS vNICs.	Avoid defining two different pxelinux.cfg/<MAC> files that have different boot/install instructions. When booted, both vNICs should execute the same PXE configuration.
Fabric Interconnect		
CSCsx13134	When a fabric interconnect boots, the "The startup-config won't be used until the next reboot" message appears on the console. Fabric interconnect configuration is controlled by the UCS Manager, so this message has no meaning on the fabric interconnect configuration and has no functional impact.	This issue has no known workaround.
CSCsy15489	Console logon usernames on the fabric interconnect are not case sensitive. For example, there is no differentiation between admin and ADMIN.	Use case insensitive usernames.

Table 60 Open Caveats in Release 1.0(1) (continued)

Defect ID	Symptom	Workaround
CSCta09325	When the system is under high stress, with repeated port flapping (ports rapidly going up and down) and default (native) VLAN change, the FWM process may core and cause the fabric interconnect to reload.	This issue has no known workaround.
CSCta25287	The **show cdp neighbor** CLI command does not display information for CDP neighbors seen from the management interface, nor does it display the fabric interconnect CDP information corresponding to the management interface.	This issue has no known workaround.
Faults and Alerts		

CSCta76573	In rare cases the Cisco UCS Manager reports the link absence fault between the fabric interconnect server port and the fabric extender during the internal inventory collection. The following is an example of such a fault:
	`**************************`
	`Severity: Cleared`
	`Code: F0367`
	`Last Transition Time: 2009-07-15T11:47:49`
	`ID: 646445`
	`Status: None`
	`Description: No link between fabric extender port 2/1/1 and switch A:1/9`
	`Affected Object: sys/chassis-2/slot-1/fabric/port-1`
	`Name: Ether Switch Intfio Satellite Connection Absent`
	`Cause: Satellite Connection Absent`
	`Type: Connectivity`
	`Acknowledged: No`
	`Occurences: 1`
	`Creation Time: 2009-07-15T11:46:49`
	`Original Severity: Major`
	`Previous Severity: Major`
	`Highest Severity: Major`
	`****************************`
		Ignore the fault message; it will automatically get cleared after one minute. This will not impact the data path.

Inventory		

Table 60 Open Caveats in Release 1.0(1) (continued)

Defect ID	Symptom	Workaround
CSCta12005	Hardware revision numbers for fabric interconnect components are not populated in the Cisco UCS Manager.	Perform the following steps to determine the revision number for a fabric interconnect component: 1. Enter the **connect nxos** command to connect to the native NX-OS CLI. 2. Enter the appropriate **show sprom** *component* command and look for **H/W Version:** field in the command output.
Server		
CSCsy20036	The disk scrub policy needs enhancements to meet DOD compliance.	This issue has no known workaround.
SNMP		
CSCta22029	SNMP shows the fabric interconnect name rather than system name.	This issue has no known workaround.
CSCta24034	An SNMP username cannot be the same as a local username.	Select an SNMP username that does not match any local username.
SMASH		
CSCsv87256	Any SMASH command entered with wrong option should give “INVALID OPTION” error message.	This issue has no known workaround.
Cisco UCS Manager CLI		
CSCsz47512	Statistics counters cannot be cleared using the Cisco UCS Manager CLI.	Clear the counters using the Cisco UCS Manager GUI.
Cisco UCS Manager GUI		
CSCta38463	When several KVM Consoles are launched, the SUN JRE sometimes reports an error and the KVM Console fails to launch.	Launch the KVM Console again.

Table 60 Open Caveats in Release 1.0(1) (continued)

Defect ID	Symptom	Workaround
CSCta54895	In the Cisco UCS Manager GUI, if the **Reboot on boot Order Change** checkbox is checked for a boot policy, and if CD-ROM or Floppy is the last device in the boot order, then deleting or adding the device does not directly affect the boot order and the server does not reboot.	This issue has no known workaround.
CSCta66375	Fibre Channel port and server port events do not appear on the Fibre Channel port and server port **Events** tabs.	Look on the Admin **Events** tab for Fibre Channel port and server port events.

Related Documentation

For more information, you can access related documents from the following links:

- *Cisco UCS Documentation Roadmap*
- *Release Bundle Contents for Cisco UCS Software, Release 2.0*

Cisco UCS C-Series Rack Mount Server Integration with Cisco UCS Manager

For more information, refer to the related documents available at the following links:

- *Cisco UCS C-series Rack Server Integration Guides*
- *Cisco UCS C-series Software Release Notes*

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/c/en/us/td/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 delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.