Release Notes for Cisco UCS Software, Release 2.1

First Published: November 16, 2012
Updated: December 20, 2013
Part Number: OL-28313-01

This document describes system requirements, new features, resolved caveats, known caveats and workarounds for Cisco UCS Manager software Release 2.1. 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 release

Use this release note as a supplement with the other documents listed in documentation roadmap:

http://www.cisco.com/go/unifiedcomputing/b-series-doc

Contents of the various bundles for this release are described in this document:

Release Bundle Contents for Cisco UCS Software, Release 2.1

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

Contents

This document includes the following sections:

Cisco Systems, Inc.
www.cisco.com

Revision History

Table 1 shows the revision history:

Table 1 Online Change History

Part Number	Revision	Release	Date	Description
OL-28131-01	A0	2.1(1a)	November 16, 2012	Created release notes for Cisco UCS Software Release 2.1(1a).
	B0	2.1(1a)	December 12, 2012	Added notice regarding lack of support for Default Zoning from Cisco UCS, Release 2.1(1a) and later releases.
	C0	2.1(1b)	March 8, 2013	Created release notes for Cisco UCS Software Release 2.1(1b).
	D0	2.1(1d)	March 25, 2013	Created release notes for Cisco UCS Software Release 2.1(1d).
	E0	2.1(1e)	April 18, 2013	Created release notes for Cisco UCS Software Release 2.1(1e).
	F0	2.1(1e)	May 8, 2013	Updated release notes for Catalog Release 2.1.1e.T.
	G0	2.1(1f)	June 6, 2013	Updated release notes for Cisco UCS Software Release 2.1(1f).
	H0	2.1(1f)	June 7, 2013	Updated the description for CSCug93076, CSCug93221, and CSCug98662.
	I0	2.1(2a)	July 12, 2013	Updated release notes for Cisco UCS Software Release 2.1(2a).
	J0	2.1(2a)	July 17, 2013	Added known limitations and behaviors and additional resolved caveats.
	K0	2.1(2a)	July 18, 2013	Added additional caveats.
	L0	2.1(2a)	July 29, 2013	Added additional caveats.
	M0	2.1(2a)	August 9, 2013	Added additional caveats.
	N0	2.1(2c)	September 4, 2013	Updated release notes for Cisco UCS Software Release 2.1(2c).
	O0	2.1(3a)	September 10, 2013	Updated release notes for Cisco UCS Software Release 2.1(3a).
	P0	2.1(3a)	September 18, 2013	Updated PIDs for Cisco UCS Software Release 2.1(3a).
	Q0	—	October 14, 2013	Replaced resolved open caveats in various releases that had been removed from RN.

Table 1 Online Change History

Part Number	Revision	Release	Date	Description
	R0	—	November 11, 2013	Added matrix to Updating Cisco UCS Versions section.
	S0	—	November 22, 2013	Updated release notes for Catalog Release 2.1.3c.T.
	T0	2.1(3b)	December 20, 2013	Updated release notes for Release 2.1(3b)

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 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 use Cisco UCS Manager, your computer must meet or exceed the following minimum system requirements:

- The Cisco UCS Manager GUI is a Java-based application that requires Sun JRE 1.6 or later releases.
- Cisco UCS Manager uses web start and supports the following web browsers:
  - Microsoft Internet Explorer 9.0 or later
  - Mozilla Firefox 7.0 or later
  - Google Chrome 14.0 or later

  Adobe Flash Player 10 or higher is required for some features
- Cisco UCS Manager is supported on the following operating systems:
  - Microsoft Windows 7 with a minimum of 4.0 GB memory
  - Red Hat Enterprise Linux 5.0 or higher with a minimum of 4.0 GB memory

Updating Cisco UCS Releases

Starting with Software Release 2.1, the Cisco UCS Manager A bundle software (Cisco UCS Manager, Cisco NX-OS, IOM firmware) can be mixed with the previous release's B or C bundles on the servers (host firmware (FW), BIOS, CIMC, adapter FW and drivers).

Table 2 lists the mixed A, B, and C bundle versions that are supported:

Table 2 Mixed Cisco UCS Releases Supported

	Infrastructure Versions (A Bundles)									
Host FW Versions (B or C Bundles)	**1.4(3)**	**1.4(4)**	**2.0(1)**	**2.0(2)**	**2.0(3)**	**2.0(4)**	**2.0(5)**	**2.1(1)**	**2.1(2)**	**2.1(3)**
1.4(3)	Yes	—	—	—	—	—	—	—	—	—
1.4(4)	—	Yes	—	—	—	—	—	—	—	—
2.0(1)	—	—	Yes	—	—	—	—	Yes	Yes	Yes
2.0(2)	—	—	—	Yes	—	—	—	Yes	Yes	Yes
2.0(3)	—	—	—	—	Yes	—	—	Yes	Yes	Yes
2.0(4)	—	—	—	—	—	Yes	—	Yes	Yes	Yes
2.0(5)	—	—	—	—	—	—	Yes	Yes	Yes	Yes
2.1(1)	—	—	—	—	—	—	—	Yes	Yes	Yes
2.1(2)	—	—	—	—	—	—	—	—	Yes	Yes
2.1(3)	—	—	—	—	—	—	—	—	—	Yes

Note

- A mix of servers running different B-bundles may be run with a single A-bundle. However, any given server must be running the entire B/C-bundles (with associated drivers), so mixing the 2.0(3a)B BIOS with the 2.0(4b)B CIMC on a server is not supported.
- The OS hardware and software interoperability is relative to the B/C-bundle on any given server. To see what OS is supported, see the Hardware and Software Interoperability documentation associated with the B-bundle version.
- The A-bundle version must be at or above the same version(s) of any B/C-bundles running on the servers (see Table 2).

The following Cisco UCS Manager 2.1(2x) features are exceptions:

- CIMC session management
- Windows 2012 NPIV support
- ESX/Linux fNIC driver enhancements
- Cisco VIC PXE boot optimization
- FlexFlash (SD card) enablement support
- Transportable Flash Module (TFM) support
- M3 board programmable firmware upgrade

The CIMC firmware version that initially shipped on the Cisco UCS B200 M3 and Cisco UCS B22 M3 blade servers does not support the Cisco UCSM feature for updating a board controller. For Cisco UCSM to be able to update the board controller on these blade servers, you must upgrade the CIMC firmware to 2.1(2a).

The following Cisco UCS Manager 2.1(1x) features are exceptions:

- Single root I/O virtualization
- Power capping
- C-series single wire management

For detailed instructions for updating the Cisco UCS software and firmware, see the appropriate Upgrading Cisco UCS document for your installation.

Hardware and Software Interoperability

For detailed information about storage switch, operating system, adapter, adapter utility, and storage array interoperability, see the *Hardware and Software Interoperability Matrix* for this release, located at

http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html

Internal Dependencies

Table 3 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.

Table 3 Internal Dependencies

Component	Recommended Minimum Software Version	Recommended Software Version
Servers		
B22 M3	2.0(5f)	2.1(3b)
B200 M1	2.0(5f)	2.1(3b)
B200 M2	2.0(5f)	2.1(3b)
B200 M3	2.0(5f)	2.1(3b)
B230 M1	2.0(5f)	2.1(3b)
B230 M2	2.0(5f)	2.1(3b)
B250 M1	2.0(5f)	2.1(3b)
B250 M2	2.0(5f)	2.1(3b)
B420 M3	2.0(5f)	2.1(3b)
B440 M1	2.0(5f)	2.1(3b)
B440 M2	2.0(5f)	2.1(3b)
C22 M3	2.0(5f)	2.1(3b)
C22 M3L	2.1(3a)	2.1(3b)
C24 M3	2.0(5f)	2.1(3b)

Table 3 Internal Dependencies (continued)

Component	Recommended Minimum Software Version	Recommended Software Version
C24 M3L	2.1(3a)	2.1(3b)
C24 M3S2	2.1(3a)	2.1(3b)
C200 M2	2.0(5f)	2.1(3b)
C200 M2 SFF	2.0(5f)	2.1(3b)
C210 M2	2.0(5f)	2.1(3b)
C220 M3[1]	2.0(5f)	2.1(3b)
C240 M3[1]	2.0(5f)	2.1(3b)
C260 M2	2.0(5f)	2.1(3b)
C250 M2	2.0(5f)	2.1(3b)
C460 M2	2.0(5f)	2.1(3b)
C420 M3	2.1(3a)	2.1(3b)
Adapters		
UCS 82598KR-CI UCS M71KR-E UCS M71KR-Q	2.0(5f)	2.1(3b)
UCS M81KR	2.0(5f)	2.1(3b)
UCS NIC M51KR-B UCS CNA M61KR-I[2] UCS CNA M72KR-Q UCS CNA M72KR-E	2.0(5f)	2.1(3b)
UCS-VIC-M82-8P UCSB-MLOM-40G-01 UCSB-MLOM-PT-01	2.0(5f)	2.1(3b)
UCSC-PCIE-CSC-02 UCSB-MEZ-ELX-03 UCSB-MEZ-QLG-03	2.1(1a)	2.1(3b)
Fabric Interconnect		
UCS 6120XP	2.0(5f)	2.1(3b)
UCS 6140XP	2.0(5f)	2.1(3b)
UCS 6248UP	2.0(5f)	2.1(3b)
UCS 6296UP	2.0(5f)	2.1(3b)
Fabric Extender or I/OM		
UCS 2104	2.0(5f)	2.1(3b)
UCS 2208XP	2.0(5f)	2.1(3b)
UCS 2204XP	2.0(5f)	2.1(3b)
Cisco Nexus 2248[3]	1.4(1)	2.0(1x)
Cisco Nexus 2232PP	2.0(5f)	2.1(3b)

Table 3 Internal Dependencies (continued)

Component	Recommended Minimum Software Version	Recommended Software Version
Fabric Interconnect Expansion Modules		
N10-E0440 N10-E0600 N10-E0080	2.0(5f)	2.1(3b)
N10-E0060	2.0(5f)	2.1(3b)
UCS-FI-E16UP	2.0(5f)	2.1(3b)
10-GB Connections		
SFP-10G-SR, SFP-10G-LR SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M	2.0(5f)	2.1(3b)
SFP-H10GB-ACU7M SFP-H10GB-ACU10M	2.0(5f)	2.1(3b)
FET-10G	2.0(5f)	2.1(3b)
SFP-H10GB-ACU7M= SFP-H10GB-ACU10M=	2.0(5f)	2.1(3b)
8-GB Connections (FC Expansion Module N10-E0060)		
DS-SFP-FC8G-SW DS-SFP-FC8G-L	2.0(5f)	2.1(3b)
4-GB Connections (FC Expansion Module N10-E0080)		
DS-SFP-FC4G-SW DS-SFP-FC4G-LW	2.0(5f)	2.1(3b)
1-GB Connections		
GLC-T (V03 or higher) GLC-SX-MM GLC-LH-SM	2.0(5f)	2.1(3b)

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

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 2.1(x) releases work with any 2.1(x) catalog file, but not the 1.x or 2.0 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 Cisco UCS infrastructure releases. See Table 4 for details on the mapping of versions to bundles.

Table 4 Version Mapping

UCS Release	Catalog File	Adds Support for PID
2.1(1a)A	ucs-catalog.2.1.1a.T.bin	UCSC-PCIE-CSC-02 for C-Series UCSB-MEZ-ELX-03 for Cisco UCS B22 M3 and Cisco UCS B200 M3 UCSB-MEZ-QLG-03 for M3 servers
2.1(1b)A	ucs-catalog.2.1.1d.T.bin	UCS-CPU-E5-4617 UCS-CPU-E5-4650L
2.1(1d)A	ucs-catalog.2.1.1d.T.bin	—
2.1(1e)A	ucs-catalog.2.1.1d.T.bin	—
—	ucs-catalog.2.1.1e.T.bin	—
2.1(1f)A	ucs-catalog.2.1.1e.T.bin	—
2.1(2a)A	ucs-catalog.2.1.2a.T.bin	—
2.1(2c)A	—	—
2.1(3a)A	ucs-catalog.2.1.3a.T.bin	UCS-CPU-E52697B UCS-CPU-E52695B UCS-CPU-E52690B UCS-CPU-E52680B UCS-CPU-E52670B UCS-CPU-E52667B UCS-CPU-E52660B UCS-CPU-E52650B UCS-CPU-E52640B UCS-CPU-E52637B UCS-CPU-E52630B UCS-CPU-E52620B UCS-CPU-E52643B UCS-CPU-E52650LB UCS-CPU-E52630LB UCS-CPU-E52609B UCS-MR-1X082RZ-A UCS-MR-1X162RZ-A
—	ucs-catalog.2.1.3c.T.bin	UCS-ML-1X324RZ-A UCS-SD200G0KS2-EP UCS-SD400G0KS2-EP UCS-SD800G0KS2-EP UCS-CPU-E52658B
2.1(3b)A	ucs-catalog.2.1.3c.T.bin	—

Further details are in the Cisco UCS Manager Configuration Guides.

New Hardware Features in Release 2.1

Release 2.1(3a) adds support for the following:

- B200 M3, C220 M3 and C240 M3 — Intel E5-2600 v2 Series CPU.

Release 2.1(2a) adds support for the following:

- C22-M3L—C22 M3 server with large form factor HDDs
- C24-M3L—C24 M3 aerver with large form factor HDDs
- C24-M3S2—C24 M3 server with 16-HDD extender backplane with small form factor HDDs
- UCS-SD-16G—16 GB SD Card
- UCSB-FBWC-1 GB—LSI 2208R embedded; the cache option contains both the supercap and the 1 GB flash module
- UCSB-FBWC-SC—spare for supercap module for LSI 2208R
- UCSB-RAID-1 GBFM—1 GB flash module for LSI 2208R
- C240 NEBS refresh

Release 2.1(1b) adds support for the following:

- Cisco UCS B200 M3 Blade Server configurations with a single CPU

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

Release 2.1(1a) adds support for the following:

- Cisco UCS CNA M73KR-Q Adapter for B-Series M3
- Cisco UCS M73KR-E Adapter for Cisco UCS B22 M3 Blade Server and Cisco UCS B200 M3 Blade Server
- VIC 1225 Adapter for C-Series
- C420 M3 Server

New Software Features in Release 2.1

Release 2.1(2a) adds support for the following:

- Storage Enhancements
  - Windows 2012 NPIV support
  - Single IQN for iSCSI boot
  - ESX/Linux fNIC driver enhancements
  - FlexFlash (SD Card) enablement support[1]
  - Transportable Flash Module (TFM) support
- Operational Enhancements
  - CIMC session management
  - Fabric interconnect high availability firmware auto synchronization
  - VIC PXE boot optimization

1. The SD card boot support requires manual setup from the BIOS boot menu.

  - M3 board programmables firmware update
  - UCSM GUI size optimization
  - Nested Lightweight Directory Access Protocol (LDAP) group support
  - UCS Central 1.1 integration

Release 2.1(1f) adds support for the following:

- BIOS policy settings—Provides the ability to select a refresh interval rate for internal memory.
- Memory speed—Enables 1333 MHz memory speed for 8 GB/16 GB 1600-MHz RDIMMs populated with 3 DIMMs per channel/1.5 V 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 2.1(1a) adds support for the following:

- Storage
  - Cisco UCSM based FC zoning—direct connect topologies
  - Multi-hop FCoE
  - Unified appliance port
  - Inventory and discovery support for Fusion-IO and LSI PCIe mezzanine flash storage (for Cisco UCS M3 blades)
- C-Series single wire management
- Fabric
  - Sequential pool ID assignment
  - PV count optimization (VLAN compression. Only available on Cisco 6248UP/6296UP Fabric Interconnect.)
  - VLAN group
  - Multicast policy with IGMP snooping and querier
  - Org-Aware VLAN
  - LAN/SAN connectivity policies for service profile configuration
  - VCON enhancement
  - Cisco CNA NIC multi-receiving queue support
  - VM FEX for KVM SRIOV
  - VM FEX for Hyper-V SRIOV
- Operational enhancements
  - Firmware auto install
  - Mixed version support (for infra and server bundles firmware)
  - Service profile renaming
  - Fault suppression
  - UCSM upgrade validation utility
  - FSM tab enhancement
  - Native JRE 64 bits compatibility with OS and browsers
  - Lower power cap minimum for B-Series

  - RBAC enhancement
  - CIMC is included in host firmware package (management firmware package deprecated)
  - Implicit upgrade compatibility check
- Support for Cisco UCS Central

Default Zoning is Not Supported in Release 2.1(1a) and Later Releases

Default zoning has been deprecated from Cisco UCS, Release 2.1(1a) and later releases. Cisco has not supported default zoning in Cisco UCS since Cisco UCS, Release 1.4 in April 2011. Fibre Channel zoning, a more secure form of zoning, is available from Cisco UCS, Release 2.1(1a) and later releases. For more information about Fibre Channel zoning, see the *Cisco UCS Manager configuration guides* for the release to which you are planning to upgrade.

Caution All storage connectivity that relies on default zoning in your current configuration will be lost when you upgrade to Cisco UCS, Release 2.1(1a) or a later release. We recommend that you review the Fibre Channel zoning configuration documentation carefully to prepare your migration before you upgrade to Cisco UCS, Release 2.1(1a) or later releases. If you have any questions or need further assistance, contact Cisco TAC.

Resolved Caveats

The following caveats were resolved in Release 2.1(3b):

Table 5 Resolved Caveats in Release 2.1(3b)

Defect ID	Description	First Affected Bundle	Resolved in Release
CSCuj84421	Installing Java 7 update 45 no longer causes UCS Manager GUI failures.	2.1(1f)A	2.1(3b)A
CSCuj61839	Cisco UCS Blade servers running 2.1(3b) firmware on a Cisco M81KR VIC adapter no longer encounter "ASSERT FAILED @ mips/ecpu_pani.c:138" errors.	2.1(2a)B	2.1(3b)B
CSCuj99958	During heavy FC traffic, the server no longer stops responding with an `ASSERT FAILED (Exception 2 triggered!) @ mips/ecpu_panic.c:138` error.	2.1(1f)A	2.1(3b)A
CSCul21224	Cisco UCS FI reset no longer occurs due to `vlan_mgr hap reset` error.	2.0(1s)A	2.1(3b)A
CSCuj10564	Discard TX on a FC trunk port are no longer seen after hot-swapping the Cisco UCS-FI-E16UP expansion module on the Cisco UCS 6248UP FI.	2.1(1f)A	2.1(3b)A
CSCuj32124	During normal operation IOM no longer unexpectedly reboots with CPU reset.	1.4(2b)A	2.1(3b)A
CSCuj42355	When upgrading to 2.1(3b)C, the Cisco UCS C-Series integrated servers no longer lose data connectivity, and VIF paths no longer reflect an Error Unknown state after the FI reboots with the new code.	2.1(2a)A	2.1(3b)A

Table 5 Resolved Caveats in Release 2.1(3b) (continued)

Defect ID	Description	First Affected Bundle	Resolved in Release
CSCui41165	Cisco UCS Manager no longer displays “error accessing shared-storage”error or have the following issues: • Call home fan alerts are sent and cleared immediately • Errors during IOM boot-up	1.4(2b)A	2.1(3b)A
CSCui82679	FlexFlash storage is no longer disconnected from a Cisco B200 M3 server after booting ESX or ESXi from a FlexFlash card.	2.1(2a)A	2.1(3b)A
CSCui94368	A dcosAG crash is no longer observed on a system running with Call Home enabled.	2.1(1f)B	2.1(3b)A
CSCuh85553	When IPMI is enabled from Cisco UCS Manager, Cipher 0 is no longer used as the default.	2.1(1e)A	2.1(3b)A
CSCul33403	Creating multiple service profiles simultaneously no longer assigns the pool identities in reverse order.	2.1(2a)A	2.1(3b)A

The following caveats were resolved in Release 2.1(3a):

Table 6 Resolved Caveats in Release 2.1(3a)

Defect ID	Description	First Affected Bundle	Resolved in Release
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.	2.0(3a)A	2.1(3a)A
CSCua50442	BIOS will no longer remap incorrect BMC FRU data for SMBIOS table.	2.0(2q)A	2.1(3a)A
CSCuh39242	The current severity level of Upper Non-critical and Upper Critical CPU thermal faults are no longer incorrectly classified as minor faults.	2.0(2m)A	2.1(3a)A
CSCui17731	SFP validation failed error will no longer occur when you insert a supported GBIC transeiver in Fabric Extender Server ports for C-series integration.	2.1(1b)A	2.1(3a)A
CSCuh73875	SNMP polling against FI drivers will no longer cause high volume of CPU usuage.	2.1(1a)A	2.1(3a)A
CSCui37900	When you have the same authentication profile for both the iSCSI initiator and the target, upgrade from 2.0(1t) to 2.1(3a) will no longer have DME crash.	2.1(2a)A	2.1(3a)A
CSCui48112	FC VIF will no longer stay in unpinned state when you connect Cisco UCS C-series C220M3 with Cisco UCS Manager in dual-wire management mode.	2.1(2a)A	2.1(3a)A
CSCui94688	The FI no longer crashes when open file descriptions reaches beyond 10,000 in Cisco UCS Manager, release 2.1.	2.1(1f)B	2.1(3a)A
CSCuh61543	Cisco UCS Manager will no longer display configuration failure when a service profile with private VLAN and VFC is associated with Cisco UCS C-series C460M2	2.1(1e)A	2.1(3a)A

Table 6 Resolved Caveats in Release 2.1(3a) (continued)

Defect ID	Description	First Affected Bundle	Resolved in Release
CSCuc66914	A global VLAN will no longer go missing on an FI after rectifying a conflicting FCoE VLAN condition after upgrade from 1.4.1 to 2.0(4a) or later.	2.0(4a)A	2.1(3a)A
CSCud27864	BIOS will no longer hang during POST when memory mapped IO above 4 GB is enabled and CSB-MEZ-QLG-03 is present in the blade.	2.1(1a)B	2.1(3a)A
CSCug51358	FCoE uplinks to the Cisco Nexus 5548 switch will no longer experience an MTS buffer leak between the port manager request high priority and fcoe_mgr due to an FC-Map mismatch between Cisco UCS Manager and the upstream Cisco Nexus 5548 switch. This FCoE uplinks will no longer flap, and the VFCs will no longer be shown as error disabled.	2.1(1d)A	2.1(3a)A
CSCuh61202	FC storage traffic through an IOM no longer stops when the IOM is reset or reinserted, or the cable between the IOM and FI is removed or reinserted.	2.1(2a)A	2.1(3a)A
CSCui21176	When a PSU is removed from a chassis with 4 PSUs, the power state on the chassis no longer shows “redundancy-failed”.	2.1(2a)A	2.1(3a)A
CSCui45873	When the ethpm MTS queues are full, the primary FI no longer reboots with VIM core: mts_acquire_q_space() failing.	2.1(2a)A	2.1(3a)A
CSCug41743	The following BIOSes will support 3 DDR-1333 DIMMs per channel and you will no longer see high memory speed error: • B420M3.2.0.5.0.120720122110 • B420M3.2.0.5a.0.121720121433 • B420M3.2.1.1a.0.121720121615	2.1(1d)B	2.1(3a)A
CSCui45963	Some of the text and controls are no longer truncated When you create a service profile or service profile template using the wizard.The edit option for storage settings is enabled.	2.1(2a)A	2.1(3a)A
CSCug62535	BMC no longer logs the following message: `multicast_solshell.c:86:SOL Connection Attempted with SOL disabled`	2.0(5a)A	2.1(3a)A

The following caveats were resolved in Release 2.1(2c):

Table 7 Resolved Caveats in Release 2.1(2c)

Defect ID	Description	First Affected Bundle	Resolved in Release
CSCuh81555	Board controller activation no longer fails on a limited set of Cisco UCS B200 M3 blade servers, when upgrading to release 2.1(2a).	2.0(4d)B	2.1(2c)B
CSCui06351	Major faults are no longer raised for default keyring certificate status showing as unknown.	2.1(2a)A	2.1(2c)A

Table 7 Resolved Caveats in Release 2.1(2c) (continued)

Defect ID	Description	First Affected Bundle	Resolved in Release
CSCui40766	Cisco UCS Manager no longer fails to detect FlexFlash when enabled in a local disk configuration policy.	2.1(2a)A	2.1(2c)A
CSCui62823	VLAN groups are no longer applied incorrectly, which could cause an outage during update.	2.1(1d)A	2.1(2c)A

The following caveats were resolved in Release 2.1(2a):

Table 8 Resolved Caveats in Release 2.1(2a)

Defect ID	Description	First Affected Bundle	Resolved in Release
CSCuf61116	IOMs no longer crash due to a memory leak in the baseboard management controller (BMC).	2.0(1s)A	2.1(2a)A
CSCuf17523	If the port speed is changed when the port is administratively down, NX-OS no longer reports that the FI port is down, while the interface counters show it is still receiving traffic.	2.1(1a)A	2.1(2a)A
CSCuh28239	During frequent MAC address changes between FIs, you will 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 will no longer point to an incorrect destination.	2.1(1b)A	2.1(2a)A
CSCuf01402	Modifying a service profile with two iSCSI vNIC targets defined no longer prompts for a reboot before the second target can be configured.	2.1(1a)A	2.1(2a)A
CSCue47159	In a UCS chassis with one or more empty slots, UCSM no longer shows a critical alert and an "FSM Failed" warning for a slot that has no blade.	2.1(1a)A	2.1(2a)A
CSCue65877	The storage daemon (storaged) running on the blade management controller (BMC) no longer generates multiple core files.	2.1(1a)A	2.1(2a)A
CSCuf57312	FIs running Cisco UCS Manager 2.1(1a) no longer experience a bladeAG reload that results in a core dump.	2.1(1a)A	2.1(2a)A
CSCug13702	After removing the SAN Connectivity Policy from a service profile, the FC zones are deleted and no longer visible using the Cisco UCS Manager GUI or CLI.	2.1(1b)T	2.1(2a)A
CSCug19471	Blades no longer display the discovery icon in Cisco UCS Manager every 2 minutes.	2.0(2q)B	2.1(2a)B
CSCug59101	FI crashes due to HAP reset are no longer triggered by an NTP process crash.	2.0(1s)A	2.1(2a)A
CSCug40776	Running the following commands no longer cause FI reboots due to a memory leak: • connect nxos • show vlan • show run	2.0(3c)A	2.1(2a)A

Table 8 Resolved Caveats in Release 2.1(2a) (continued)

Defect ID	Description	First Affected Bundle	Resolved in Release

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`
		1.4(1j)A	2.1(2a)A

CSCuh30440	Starting with Release 2.1(2a), Cisco UCS Manager no longer hangs when disassociating a service profile with FC zoning that is running in Fibre Channel switch mode. For previous versions of Cisco UCS Manager software, use the following workaround: 1. Decommission the affected server, and then recommission it. The previous FC zone will still be included in the zone database. 2. Create a duplicate service profile to the one that was deleted, using the same name and the same organization. 3. Associate the new service profile to the recommissioned blade. The previous FC zone is deleted, and a new FC zone is created.	2.1(1d)A	2.1(2a)A
CSCud86528	Beginning with Cisco UCS Manager Release 2.1(2a), if a service profile's "Desired Power State" is in **off** state, it will be changed to **on** when the associated physical server is powered on using the reset or other server maintenance actions.	2.0(3b)B	2.1(2a)A
CSCud60153	If a link on which LLDP is configured flaps, it no longer causes memory leaks or an LLDP process crash.	2.0(2t)A	2.1(2a)A
CSCub37558	Cisco UCS Manager now displays the amber and amber blinking LED sensor states of LEDs on the blade, and raises faults in response to the color change.	2.0(3a)A	2.1(2a)A
CSCts11406	Beginning with Cisco UCS Manager Release 2.1(2a), you can delete the decommissioned server on a decommissioned and physically removed rack server from the setup, which allows you to reuse the removed server ID. Note: If you execute this command when the rack server is decommissioned but physically connected, the rack server is recommissioned and reclaims the server ID.	2.0(2t)A	2.1(2a)A
CSCuc26744	Beginning with Cisco UCS Manager Release 2.1(2a), the GUI does not have the Set Bundle option for the Activate Firmware action. Use the Auto Install feature to activate the firmware on the B/C bundle. This change avoids a firmware activation failure when the CIMC and board controller firmware being activated at the same time. This is a known hardware restriction that could result in the board's corruption.	2.0(4a)A	2.1(2a)A
CSCuc42488	Starting with Cisco UCS Manager Release 2.1(2a), the FCoE native VLAN is set to 1 where it was previously set to 4049. VLAN 1 can now communicate from upstream to a vNIC on a Cisco UCS blade without failing when the default VLAN configuration is used for the FCoE uplink.	2.1(1a)A	2.1(2a)A

Table 8 Resolved Caveats in Release 2.1(2a) (continued)

Defect ID	Description	First Affected Bundle	Resolved in Release
CSCue49383	The default power policy is changed from N+1 to Grid during initial booting when a chassis CMC reboots or is powered on. This change ensures that all power supplies power up. After boot up, the power policy setting you configured is applied.	1.4(1i)B	2.1(2a)B
CSCug26974	For servers with Cisco UCS M71KR-E or Cisco UCS CNA M71KR-Q adapters, changing the ethernet adapter's policy parameters no longer triggers a reboot on servers with the same policy.	2.1(1d)B	2.1(2a)B
CSCug43293	You no longer receive a "Configuration failed due to mac-derivation-virtualized-port" fault on service profiles when using a vNIC template that has a VM target under a suborganization.	2.1(1d)A	2.1(2a)A
CSCuf31431	Compiling rack server MIBs is now successful when performed on a CISCO-UNIFIED-COMPUTING-TC-MIB.my with 64 bit counters.	2.0(4b)C	2.1(2a)C
CSCtu17983	An ESX boot on blades that use VMware Auto Deploy no longer takes a long time to run.	2.0(1m)A	2.1(2a)B 2.1(2a)C
CSCuf78224	On a Cisco UCS B440-M2 Server with a Cisco UCS CNA M72KR-Q adapter card, VMware Auto Deploy 5.1 no longer hangs during a system boot.	2.0(4b)A	2.1(2a)B
CSCug85569	When performing an autoinstall on a server with the user ack policy, the server now proceeds with a graceful reboot. Some operating systems, such as Microsoft, no longer come up in recovery mode.	2.1(1e)A	2.1(2a)A
CSCuh35570	The fabric interconnect (FI) no longer reboots with a Kernel panic svr_sam_statsAG process error.	2.1(1e)A	2.1(2a)A
CSCue72786	VFC pinning now updates properly on the Cisco UCS M81KR VIC.	2.0(4b)A	2.1(2a)A
CSCud81176	After manually upgrading the CIMC and associating a service profile, the CIMC upgrade no longer fails while the status remains at Activating.	2.1(1a)A	2.1(2a)A
CSCud93569	The secondary FI no longer fails when you upgrade the FI firmware Cisco NX-OS software on Cisco UCS Manager.	2.0(3a)A	2.1(2a)A
CSCti87891	The Cisco UCSM shell now supports redirection of the **show** command output to a remote file system.	2.1(0.407)A	2.1(2a)A
CSCtt38889	The virtual interface on the standby vNIC is now shown as up when the vEth is up.	2.0(1m)A	2.1(2a)B
CSCud55036	With the vNIC template, the VLAN ID is now displayed correctly according to the configured VLAN number, instead of always displaying 1.	2.0(2m)A	2.1(2a)A

The following caveats were resolved in Release 2.1(1f):

Table 9 Resolved Caveats in Release 2.1(1f)

Defect ID	Description	First Affected Bundle	Resolved in Release
CSCue04360	After a boot, the B200 M3 Server no longer hangs after a few days with PECI errors.	2.0(3a)B	2.1(1f)B
CSCuf35678	When VLAN port count optimization (VLAN compression) is enabled on a Cisco UCS 6200 Series Fabric Interconnect, traffic no longer stops if an uplink port channel port goes down.	2.1(1a)A	2.1(1f)A
CSCuf60988	Virtual Fibre Channel ports are no longer error-disabled on one FI when the server is rebooted.	2.0(4a)A	2.1(1f)A
CSCug14669	A Fibre Channel (FC) path loss no longer occurs because the Fibre Channel Forwarder (FCF) MAC address is no longer learned dynamically.	2.1(1b)A	2.1(1f)A
CSCud60746	The system no longer runs out of memory when Call Home is enabled.	2.0(2a)A	2.1(1f)A
CSCug93076 CSCug93221 CSCug98662	The Cisco UCS B200 M3, B22 M3, and B420 M3 Blade Servers no longer experience noncorrectable 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 2.1(1f). 2. Power off the host. **Caution** This step is disruptive. 3. Activate the CIMC. 4. Power on the host.	2.0(5b)B 2.0(5m)B 2.1(1a)B	2.1(1f)B
CSCue49366	Transient faults related to Cisco UCS Manager chassis SEEPROM usage and power capping no longer occur.	2.1(1a)B	2.1(1f)A
CSCue58839	The KVM launch manager now shows all service profiles when launched from a suborganization.	2.1(1a)A	2.1(1f)A
CSCuc87547	Cisco UCS Manager no longer reports PSU failures in the Cisco Nexus 2232 Fabric Extenders configured for Cisco UCS C-Series servers managed by Cisco UCS Manager.	2.0(3a)A	2.1(1f)A
CSCud13423	When the power policy is set to N+1, and an additional PSU is inserted into a slot with power, the new PSU no longer goes into spare mode instead of active mode.	2.0(1a)A	2.1(1f)B
CSCud79598	Renaming a service profile no longer increments the fault count incorrectly.	2.1(1a)A	2.1(1f)A
CSCue46382	Chassis discovery process issues, such as ports on FI-B displaying no object statistics or Cisco UCS Manager reporting incorrect states for ports on both FIs, no longer occur during a Cisco UCS Manager upgrade.	2.0(3c)A	2.1(1f)A
CSCue46600	When a Cisco UCS B440 Blade Server with a more recent Version ID (VID) is inserted in the chassis, Cisco UCS Manager no longer reports the previous VID.	2.0(4b)A	2.1(1f)A
CSCuf03602	Power supply VID data can be obtained by connecting to the IOM and running the **`show platform software cmcctrl fru psu`** command.	2.0(1m)A	2.1(1f)A

Table 9 Resolved Caveats in Release 2.1(1f) (continued)

Defect ID	Description	First Affected Bundle	Resolved in Release
CSCue48076	If there are more than 21 IP addresses in the ext-mgmt ip pool, adding a subordinate FI to a standalone FI to convert into a cluster no longer causes the console to hang.	2.1(1a)A	2.1(1f)A
CSCug40752	The KVM console now supports Java 1.7 update 17 and Java 1.6 update 43.	2.1(1b)A	2.1(1f)A

The following caveats were resolved in Release 2.1(1e):

Table 10 Resolved Caveats in Release 2.1(1e)

Defect ID	Description	First Affected Bundle	Resolved in Release
CSCuf90470	When Call Home is enabled, Online Insertion and Removal (OIR) or failure of hardware modules in the FI no longer cause the FI to reboot.	2.1(1b)A	2.1(1e)A

The following caveats were resolved in Release 2.1(1d):

Table 11 Resolved Caveats in Release 2.1(1d)

Defect ID	Description	First Affected Bundle	Resolved in Release
CSCuf14193	Upon an upgrade to Cisco UCS Manager 2.1(1d), the FI no longer reboots due to Call Home server HA policy reset when Call Home is enabled.	2.1(1b)A	2.1(1d)A

The following caveats were resolved in the Release 2.1(1b):

Table 12 Resolved Caveats in Release 2.1(1b)

Defect ID	Description	First Affected Bundle	Resolved in Release
CSCud56660	Duplicate license IDs no longer cause the LicenseAG process to core.	2.0(4d)A	2.1(1b)
CSCud10237	The eight default port licenses for flexible GEM on the FI are available for use.	2.0(3c)A	2.1(1b)
CSCue38650	The UCSM PSU policy and IOMs are no longer out of synchronization after the IOMs are rebooted.	2.1(1a)A	2.1(1b)
CSCud70368	Cisco UCS Central is now correctly creating the crossdomain.xml file on UCSM member domains.	2.1(1a)A	2.1(1b)
CSCud40412	When regenerating a new key ring or certificate, the new certificate is now successfully published to the FI web server and can be obtained by the HTTP process.	2.1(1a)A	2.1(1b)
CSCud53700	The portAG process no longer crashes while activating the Fabric Interconnect NX-OS software during an upgrade.	2.1(1a)A	2.1(1b)

Table 12 Resolved Caveats in Release 2.1(1b)

Defect ID	Description	First Affected Bundle	Resolved in Release
CSCud59230	Port channels no longer go down after upgrading to Cisco UCSM Release 2.1.	2.1(1a)A	2.1(1b)
CSCub22238	The Cisco UCS 6100 Series Fabric Interconnects no longer contain a vulnerability in the Netconf interface.	2.0(1a)A	2.1(1b)
CSCud20253	Power capping on the Cisco UCS B420 Blade Server can now support 32 GB DIMMS.	2.1(1a)A	2.1(1b)
CSCue46817	After upgrading to Release 2.1(1a) or later, a Cisco UCS B440 M1/M2 Blade Server using a RAID key attached to a LSI MegaRAID SAS 9260 no longer generates a "Missing RAID Key" fault alert.	2.1(1a)B	2.1(1b)
CSCud27494	Traffic to a blade server will no longer be dropped and forwarded to another working link when an uplink is shut down either on the fabric interconnect or from the upstream switch.	2.0(4b)A	2.1(1b)
CSCud54919	On blade servers that are not associated with a service profile, CIMC cannot respond from Cisco UCS Manager at the same time.	2.0(1t)B	2.1(1b)
CSCuc38555	Legacy USB support items can no longer be changed in the BIOS setup.	2.1(1a)B	2.1(1b)
CSCud19629	FCoE uplink interface faults are now visible in the Cisco UCS Manager GUI.	2.1(1a)A	2.1(1b)
CSCud20765	When defined through a service profile template, SRIOV virtual functions (VFs) are no longer populated incorrectly in the instantiated service profiles.	2.1(1a)A	2.1(1b)
CSCuc44209	Cisco UCS Manager no longer displays the names for PSUs connected to a Cisco Nexus 2200 Series FEX in reverse order.	1.4(3l)C	2.1(1b)

The following caveats were resolved in Release 2.1(1a):

Table 13 Resolved Caveats in Release 2.1(1a)

Defect ID	Description	First Affected Bundle	Resolved in Release
CSCub51516	DHCP will no longer fail when multiple servers are restarted at the same time.	2.0(1e)A	2.1(1a)A
CSCuc27213	The Cisco UCS B200 M2 Blade Server no longer goes into a continuous reboot loop after upgrading from Release 2.0(1s) to Release 2.0(3a).	2.0(3)A	2.1(1a)A
CSCuc26566	The Cisco UCS 6200 Series Fabric Interconnect no longer reboots without a final confirmation warning after configuration changes.	2.0(4a)A	2.1(1a)
CSCtz07798	A service profile no longer generates configuration failures if the blade it is associated with is removed from the server pool.	2.1(0.208)B	2.1(1a)
CSCuc69455	A core dump caused by a memory leak is no longer seen when multiple VLANs are assigned to a service profile's vNIC.	2.1(0.489)A	2.1(1a)
CSCth96721	There is no longer a 128 character limitation to the number of OUs or the length of the Distinguished Name (DN) when using LDAP authentication with the Active Directory.	2.0(1w)A	2.1(1a)A
CSCtt36593	The svcmonAG process no longer fails and core dumps regularly on a 14 chassis setup.	2.0(1)A	2.1(1a)A

Table 13 Resolved Caveats in Release 2.1(1a) (continued)

Defect ID	Description	First Affected Bundle	Resolved in Release
CSCty34034 CSCub48862 CSCub99354 CSCub16754	Discovery, association, or disassociation no longer fails after a BMC firmware update with a message about the VIC adapter.	1.0(2a)	2.1(1a)B
CSCuc00368 or CSCuc87155	With RAID1 mode configured with two disks on a Cisco UCS B230 Blade Server, removing and reinserting one disk no longer causes the second disk to be shown as inoperable while a RAID 1 rebuild is in progress.	2.0(3a)A	2.1(1a)A
CSCuc24817	After an FI reboot or FI failover, the vEth is no longer shown as down when Cisco NX-OS shows it as up.	2.0(3c)A	2.1(1a)A
CSCuc59752	The **snmptable** command no longer fails to return any values.	2.0(2q)A	2.1(1a)A
CSCuc09958 CSCua17646	A Java 1.7 detected error no longer occurs when downgrading from Cisco UCSM Release 2.0(3a) and later releases running JRE 1.7 to UCSM Release 2.0(2r) and earlier releases.	2.0(4a)A	2.1(1a)A
CSCtz86513	Registration emails from the SCH portal are now received after new inventory messages are sent from Cisco UCS Manager.	1.4(2b)A	2.1(1a)A
CSCtz76897	While upgrading or discovering the Cisco UCS Manager, when the chassis discovery policy is changed to the **set link-aggregation-pref port-channel** policy, the FEX no longer goes offline.	2.0(1m)A	2.1(1a)A
CSCtr45130	The Blade Server no longer reboots when activated after upgrading from Cisco UCS Manager Release 1.4(1j) to 1.4(2b).	1.4(2b)A	2.1(1a)A
CSCub64209	FCoE packets are no longer dropped when host-control is enabled in QoS policies assigned to vNICs.	2.0.67 B	2.1(1a)B
CSCtz79579	Cisco UCS Manager no longer reports an incorrect status for faulty disks that fail to power on or link up.	2.0(2.83)B	2.1(1a)B
CSCub34939 CSCty33146	After upgrading Cisco UCS Manager, an SNMP crash no longer reboots both FIs during activation.	1.4(3s)A	2.1(1a)A
CSCuc35326	The Cisco UCS B200 M3, B22 M3, and B420 M3 Blade Servers no longer experience “Server Hardware Not Supported” or discovery errors when 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.	2.0(3a)A	2.1(1a)A
CSCtw59592	In a server using both a virtualized adapter card and a nonvirtualized card, extraneous NIC ports are no longer generated if there are fewer service profile vNICs than the minimum required physical NIC ports.	2.0(1t)A	2.1(1a)A
CSCtj62296	The minimum power cap that can be set is no longer 3400 W.	1.4(1i)A	2.1(1a)A
CSCtc86297	After a VM restarts, the virtual machine node on the VM tab no longer shows multiple instances of the same VM with one online and one offline.	1.1(1j)A	2.1(1a)A
CSCta66375	Fibre Channel port and server port events now appear on the Fibre Channel port and server port **Events** tabs.	1.0(1e)A	2.1(1a)A
CSCtu34607	Changing the dynamic vNIC policy to change the number of vNICs no longer causes static vNICs to get reordered on a PCIe bus.	2.0(2m)A	2.1(1a)A

Table 13 Resolved Caveats in Release 2.1(1a) (continued)

Defect ID	Description	First Affected Bundle	Resolved in Release
CSCuc72049	When creating an access mode appliance port channel in Cisco UCS Manager, the default VLAN is no longer used instead of the specified VLAN.	2.0(3a)A	2.1(1a)A
CSCtx65534 CSCua31267	Deleting a VLAN in the fabric interconnect no longer causes the vNICs that are carrying that VLAN to flap.	2.0(2q)A	2.1(1a)A
CSCtn87981	Cisco UCS B230 and B440 Blade Servers with Cisco UCS M81KR and 82598KR-CI Adapters no longer fail with an "illegal fru" error.	2.0(1m)	2.1(1a)A

Open Caveats

The following caveats were open in Release 2.1(3b):

Table 14 Open Caveats in Release 2.1(3b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuj74570	A Cisco UCS B420 M3 blade with a VIC 1240 and a port expander is successfully discovered in a chassis with a 2104XP IOM, even though it is unsupported. When upgrading to the 2204XP IOM, the blade reboots for discovery.	This issue has no known workaround. The B420 M3 blade with port expander is not supported with the 2104XP IOM.	2.1(2a)B
CSCul72408	During upgrade, the following issues occured: • The IOM backplane ports show **admin down** in the Cisco UCS Manager GUI. • The VIF's show non-participating • The adapter shows DCE interfaces down.	Reboot the IOM in the affected chassis.	2.1(3a)A
CSCuj63448	When upgrading to a catalog that supports new DIMMs, some of the DIMM information is not displayed.	Reacknowledge the blade server.	1.4(4k)A

The following caveats were open in Catalog Release 2.1(3c)T:

Table 15 Open Caveats in Catalog Release 2.1(3c)T

Defect ID	Symptom	Workaround	First Bundle Affected
CSCul55015	The serial number is not displayed correctly when the following disks are used on Cisco UCS M3 servers: • Samsung MZ6ER200HAGM/003DM0B (PID = UCS-SD200G0KS2-EP) • Samsung MZ6ER400HAGL/003DM0B (PID = UCS-SD400G0KS2-EP) • Samsung MZ6ER800HAGL/003DM0B (PID = UCS-SD800G0KS2-EP)	This issue has no known workaround. All information except for the serial number is displayed correctly. There is no impact to functionality.	2.1(3c)T

The following caveats were open in Release 2.1(3a):

Table 16 Open Caveats in Release 2.1(3a)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCul99847	After upgrading to Release 2.1(3a), multiple vEthernet and vFC interfaces stay down with a `nonParticipating` error state.	This issue has no known workaround.	2.1(3a)A
CSCuj84421	Installing Java 7 update 45 causes UCS Manager GUI failures. You may see errors similar to the following: `Login Error: java.io.IOException: Invalid Http response`	Downgrade to Java 7 update 40 or below. Previous releases are located on the Oracle Java Archive website.	2.1(1f)A Resolved in 2.1(3b).
CSCui99339	When you upgrade to Release 2.1(3) from 2.1(2) using FW Auto Install to install infrastructure firmware, upgrade fails with an “Upgrade Validation Failed” error.	This issue has no known workaround.	2.1(3a)A
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`	Upgrade adapter firmware to release 2.1.3a.	2.0(5c)

The following caveats were open in Release 2.1(2c):

Table 17 Open Caveats in Release 2.1(2c)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCui17731	When a Cisco SFP 1GB Interface Converter GLC-T is inserted into a Cisco Nexus 2000 Series FEX port, it fails with a "SFP validation failed" error.	Contact Cisco TAC.	2.1(1b)A Resolved in 2.1(3a).
CSCui21176	When a PSU is removed from a chassis with 4 PSUs, the power state on the chassis may show "redundancy-failed". This occurs when the Operability of the removed PSU continues to be displayed as Operable and Power State is displayed as On.	This issue has no known workaround.	2.1(2a)A Resolved in 2.1(3a).

CSCui37900	When you upgrade to Release 2.1(2a), if a service profile template has the same authentication profile for both the iSCSI initiator and the iSCSI target, the high-availability connection between the FIs may not form, and the **`show cluster extended-state`** command displays one of the following errors:
	`A: UP, INAPPLICABLE, (Management services: DOWN)`
	`B: UP, SUBORDINATE`
	
	`A: UP, PRIMARY, (Management services: SWITCHOVER IN PROGRESS)`
	`B: UP, SUBORDINATE`
	The svc_sam_dme process may also crash.
		To avoid this issue, ensure that the authentication profile is different between the iSCSI initiator and the target before upgrading.
		If this issue occurs, contact Cisco TAC to revert to the previous code. Fix the authentication profile before resuming the upgrade.
			2.1(2a)A

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.	This issue has no known workaround.	2.1(2a)
CSCui45873	The primary FI may reboot with VIM core: mts_acquire_q_space() failing. This occurs when the ethpm MTS queues are full.	Reducing the batch size of the VM power cycle may alleviate the issue. For example, if the batch size is 80 VMs, reduce it to 20 VMs.	2.1(2a)A Resolved in 2.1(3a).
CSCui45963	When you create a service profile or service profile template using the wizard, if you choose Create a Specific Storage Policy in the Local Storage area on the Storage page, some of the text and controls are truncated. This prevents the storage settings from being edited.	When you create a service profile or service profile template using the wizard, skip the storage page and complete the rest of the wizard. After the service profile or service profile template has been created, select the service profile, click the **Storage** tab, and then click **Change Local Disk Configuration Policy** in the **Actions** area to edit the storage settings.	2.1(2a)A Resolved in 2.1(3a).

The following caveats were open in Release 2.1(2a):

Table 18 Open Caveats in Release 2.1(2a)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCui40766	Cisco UCS Manager fails to detect FlexFlash when enabled in a local disk configuration policy.	This issue has no known workaround.	2.1(2a)A Resolved in 2.1(2c).
CSCui48112	FC VIF stays in unpinned state when you connect Cisco UCS C-series C220M3 with Cisco UCS Manager in dual-wire management mode.	This issue has no known workaround.	2.1(2a)A Resolved in 2.1(3a).
CSCuh76699	The cmc pwrmgr process might stop working, causing a power cap failure in a Cisco UCS blade or chassis.	Reboot the IOM to restart the cmc pwrmgr process.	2.1(2a)A
CSCuh39242	The current severity level of Upper Noncritical and Upper Critical CPU thermal faults are incorrectly classified as minor faults. The correct classification for these should be as informational warnings because they do not indicate a problem with the hardware health or performance of the server.	This issue has no known workaround. The faults can be safely ignored.	2.1(1e)B
CSCuh64817	On a VMware VMFex setup, when you remove one of the vNICs on a powered on VM, the change does not show on the Cisco UCSM side and it still shows the extra vNIC.	This issue has no known workaround.	2.1(1a)A
CSCuh73875	High CPU usage is seen on a Cisco UCS 6140XP Fabric Interconnect, especially when running the vlan_mgr process. This process starves other lower priority processes such as svc_sam_dme, which can prevent manual failover or configuration synchronization.	Disable SNMP on the FI, or do not poll SNMP on the FI IP or VIP.	2.1(1d)A Resolved in 2.1(3a).
CSCuh94333	In rare situations, when configuring or unconfiguring FC/FCoE interface, the forwarding process crashes and the FI resets.	This issue has no known workaround.	2.0(2m)A

The following caveats were open in Release 2.1(1f):

Table 19 Open Caveats in Release 2.1(1f)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCug51358	FCoE uplinks to the Cisco Nexus 5548 switch experience an MTS buffer leak between the port manager request high priority and fcoe_mgr due to an FC-Map mismatch between Cisco UCS Manager and the upstream Cisco Nexus 5548 switch. This buffer leak causes the FCoE uplinks to flap, and the VFCs are shown as error disabled.	1. Ensure that the Cisco Nexus 5000 Series switch FC-Map is the same as the Cisco UCS Manager FC-Map. **Note** This change must be made on the Cisco Nexus 5000 Series switch. 2. Load the debug plug-in, and change the Cisco UCS Manager FC-Map using the Cisco NX-OS CLI. These options require an FI reboot if the MTS buffer is leaking. Disable the uplink ports, change the FC-Map, reboot the FI, and then reenable the uplink ports.	2.1(1d)A Resolved in 2.1(3a).
CSCug25894	During boot and reacknowledgement in the Cisco 2100 Series IOM, sysmgr cores are seen.	The system resumes normal behavior after the process is restarted. The process should take approximately three minutes.	2.0(4a)A
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.	2.0(1s)A
CSCuh01579	When the server is rebooted, or the Cisco UCS reset option is used, the Cisco UCS B200 M2 Blade Server displays a USB composite device mounted in Windows. The drive letter assigned to this device varies, which might 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.	2.1(1a)A
CSCuh12592	An FI might experience a bladeAG reload that results in a core dump due to lack of memory.	This issue has no known workaround.	2.1(1a)A
CSCuh28274	When installing XenServer 6.0.2 and adding the fNIC driver during the installation, an unrecoverable error occurs.	Install the fNIC driver after the OS is loaded.	2.1(1a)A
CSCug61578	When you remove the management cable from the primary FI, you are not able to view SNMP traps.	This issue has no known workaround and is only seen if the mgmt 0 interface of the primary FI goes down. If the mgmt interface of the secondary goes down, the traps are sent.	2.1(1b)A
CSCug63368	If the DHCP relay agent is installed as the gateway IP address instead of the HSRP IP address during a PXE boot, the PXE boot might fail in vPC environments with specific operating system configurations.	Clear the ARP entry on both vPC peers, and then configure the host to use different IP addresses on the OS from the lease assigned to the adapter.	2.1(1d)B

Table 19 Open Caveats in Release 2.1(1f) (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCug62535	BMC continuously logs the following message: `multicast_solshell.c:86:SOL Connection Attempted with SOL disabled`	This issue has no known workaround.	2.1(1a)A Resolved in 2.1(3a).
CSCug41743	With 3 DDR-1333 DIMMs installed per channel, the memory speed is not reduced to 1067 MHz under the following BIOS versions: • B420M3.2.0.5.0.120720122110 • B420M3.2.0.5a.0.121720121433 • B420M3.2.1.1a.0.121720121615	Downgrade to one of the following BIOS versions: • B420M3.2.0.4a.0.080920122056 • B420M3.2.1.1.0.100520121529	2.1(1d)B Resolved in 2.1(3a).
CSCuh28239	In some rare conditions, during frequent MAC address changes between FIs, you might see a delay in learning MAC addresses. If the MAC address changes between server ports on the same FI, the MAC address might point to an incorrect destination.	The learning delay issue has no known workaround. The problem is resolved automatically in 7-8 seconds when traffic occurs. If the MAC address points to an incorrect destination, a subsequent frame from the server sourcing MAC address will fix the issue.	2.1(1b)A Resolved in 2.1(2a).
CSCug59101	FI crashes that are due to a HAP reset are triggered by an NTP process crash.	To prevent FI reboots due to this issue, ensure that NTP server configured is reachable via DNS. If not, use the IPv4 address instead of the hostname to configure the NTP server.	2.0(1s)A Resolved in 2.1(2a).
CSCug40776	Due to a memory leak that occurs when the NTP server is configured for DNS, but is not reachable via DNS, running the following commands may cause FI reboots: • **`connect nxos`** • **`show vlan`** • **`show run`**	To prevent FI reboots due to this issue, ensure that the NTP server configured is reachable via DNS. If not, use the IPv4 address instead of the hostname to configure the NTP server.	2.0(3c)A Resolved in 2.1(2a).
CSCug85569	When performing autoinstall on a server with the user ack policy, the server does not proceed with a graceful reboot. Some operating systems, such as Microsoft, may come up in recovery mode.	This issue has no known workaround.	2.1(1b)A Resolved in 2.1(2a).

The following caveats were open in Release 2.1(1e):

Table 20 Open Caveats in Release 2.1(1e)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCug21589	When a fabric failover occurs on a VMware ESXi host with a fabric failover configured, the MAC address of the ESXi host is sent to the uplink switch. In some circumstances, the MAC address of the guest OS is not sent, which causes the network link to go down.	Generate a ping from the corresponding VM to any external hosts.	2.1(1a)T
CSCug26974	For servers with Cisco UCS M71KR-E or UCS CNA M71KR-Q adapters, changing ethernet adapters policy parameters can unnecessarily trigger a reboot on servers with that policy.	Avoid changing any ethernet adapter policy parameters except for Failback Timeout for servers equiped with Cisco UCS M71KR-E or UCS CNA M71KR-Q adapters.	2.1(1d)B Resolved in 2.1(2a).
CSCuf78224	On a Cisco UCS B440-M2 server with Cisco UCS CNA M72KR-Q adapter card, VMware Auto Deploy 5.1 hangs during boot.	Using ESXi 5.0 gPXE instead of ESXi 5.1 iPXE may work under some conditions, but booting time is slow.	2.0(4b)A Resolved in 2.1(2a).

The following caveats were open in Release 2.1(1d):

Table 21 Open Caveats in Release 2.1(1d)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuf07670	Latency spikes might be reported on ESXi servers due to the virtual machines losing connections to the storage datastores. This condition occurs when storage datastores are presented through the FCoE uplinks using Cisco UCS and Cisco Nexus 5000 Series switches.	This issue has no known workaround.	2.1(1a)A
CSCud60746	When Call Home is enabled, there is a low chance that the system may run out of memory. This occurs after 365,000 Call Home messages have been sent out, or approximately 4700 inventory messages are generated. This could result in one of the following: • The primary Fabric Interconnect may reboot with the following reset reason: `Service: callhome server hap reset` • Upgrading the firmware in the primary FI may fail due to the /isan folder filling up.	To reduce the frequency of memory leaks caused by Call Home messages: 1. Reduce the number of Call Home messages by disabling any unnecessary Call Home policies or modifying alert groups and/or profile levels. 2. Reduce inventory message generation. To completely prevent any memory leaks due to Call Home, disable Call Home. If the primary FI firmware upgrade fails, contact Cisco TAC to cleanup the /isan directory.	2.0(2a)A Resolved in 2.1(1f).

Table 21 Open Caveats in Release 2.1(1d) (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuf17523	Cisco NX-OS reports that the FI port is down, but the interface counters show it is still receiving traffic. This condition occurs when the port speed is changed when the port is administratively down.	Administratively enable and administratively disable the port.	2.1(1a)A Resolved in 2.1(2a).
CSCuf01402	Modifying a service profile with two iSCSI vNIC targets defined prompts for a reboot before the second target can be configured.	To configure the second target, modify any attribute in the service profile. Accept the reboot prompt to configure the targets properly.	2.1(1a)A Resolved in 2.1(2a).

The following caveats were open in Release 2.1(1b):

Table 22 Open Caveats in Release 2.1(1b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCud59815	When assigning FC ports on the Cisco 6200 Series FI using the slider, all ports are enabled by default. If the number of ports allocated is greater than the license allotment, license faults are generated and ports can go into the grace period.	Disable the FC ports that are not actually going to be used.	2.0(2q)A
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.	2.0(2r)A
CSCue49366	Symptoms include transient Cisco UCSM faults related to a shared Cisco UCS chassis I2C devices, such as a fan module, PSU, or the shared storage located in the Cisco UCS Chassis SEEPROM. These faults may include the terms fan inoperable, PSU, or shared storage. The detailed or brief **`tech-support`** command shows the chassis segment norxack count is high and increasing (hundreds or thousands depending on IOM uptime). This high rate of i2c access errors shows that the IOM is not backing off of the shared I2C bus for the required amount of time. As a result, one or both of the IOMs are interfering with each other's access to shared I2C resources and neither may be able to get useful work done.	This issue has no known workaround if uninterrupted high-availability service is desired. If nonredundant operation is tolerable, you could pull one IOM from the chassis. Powering down the entire chassis for 3 minutes and reapplying power might clear the condition in the short-term.	2.1(1a)B Resolved in 2.1(2a).

Table 22 Open Caveats in Release 2.1(1b) (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCud70315	When a port channel member transitions between up and down states, fabric channel traffic on the port channel is dropped. A SCSI timeout occurs, and the SCSI layer triggers the recovery.	This issue has no known workaround. Proper SCSI timeout values will help in recovery.	2.0(4a)A
CSCue29352	When you try to change the boot order without checking the option's "local storage change" and "Reboot on Boot Order Change," the server is listed in the pending activities list.	Check the Reboot on Boot Order Change check box to trigger a server reboot.	2.0(4d)A
CSCud89583	The Cisco UCS B440 Blade Server that is running Citrix XenServer 6.0.2 with E7-4830 and all C states disabled has a "CATERR_N" error and freezes. The host IP address of the blade is unreachable, and KVM, the front panel dongle, and SOL do not function.	Power cycle the blade.	2.0(3a)A Resolved in 2.1(3a).
CSCud74915	After you create a new service profile using VM-FEX, a duplicate VIF prevents you from connecting to the original blade server.	1. Disassociate both blades from their service profiles. 2. Reassociate only one blade. 3. Recreate the service profile for the other blade.	2.0(3a)A
CSCuf90470	When Call Home is enabled, Online Insertion and Removal (OIR) or failure of hardware modules (such as fans, power supply, or GEM) in the FI may cause the FI to reboot.	Disable the Call Home function.	2.1(1b)A Resolved in 2.1(1e).
CSCud27864	BIOS will no longer hang during POST when the memory mapped IO above 4 GB is enabled and CSB-MEZ-QLG-03 is present in the blade.	Disable memory mapped I/O above 4 GB.	2.1(1b)A Resolved in 2.1(3a).
CSCue47159	In a Cisco UCS chassis with one or more empty slots, UCSM may show a critical alert and a "FSM Failed" warning for a slot that has no blade.	1. Insert a spare blade into the slot that has the alert. 2. After the discovery process has completed successfully, check for the error message if it appears. 3. Decommission the server from UCSM by using the "Server Maintenance" link. 4. After the decommission process has completed successfully, remove the server from the slot.	2.1(1a)A Resolved in 2.1(2a).
CSCue65877	Under certain conditions when upgrading to Release 2.1(1), the storaged daemon generates core files.	This issue has no known workaround. The storaged daemon is a monitored daemon that restarts automatically. System operation continues and performance is not negatively impacted.	2.1(1a)A Resolved in 2.1(2a).

Table 22 Open Caveats in Release 2.1(1b) (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
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.	2.0(3b)B Resolved in 2.1(2a).
CSCud81176	After manually upgrading the CIMC and associating a service profile, the CIMC upgrade may fail while the status remains at Activating.	Remove the Management Firmware pack to activate the firmware of CIMC. A non-harmful fault is generated which can be acknowledged.	2.1(1a)A Resolved in 2.1(2a).
CSCud55036	With the vNIC template, the VLAN ID is always displayed as 1 instead of the configured VLAN number. This is a display issue only.	Use the **show vlan** command to obtain the correct VLAN ID.	2.0(2m)A Resolved in 2.1(2a).
CSCue04360	After you boot, the B200 M3 servers hang after few days, with PECI errors.	Reboot the server.	2.0(2m)A Resolved in 2.1(1f).

The following caveats were open in Release 2.1(1a):

Table 23 Open Caveats in Release 2.1(1a)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCtz15707	When the Cisco UCS C24 M3 Server has more than 16 hard disk drives installed, the 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 the number of installed hard disk drives to a maximum of 16. • Use LSI WebBIOS Configuration utility during server boot to manually create RAID 10 when more than 16 disk drives are required for the RAID 10 configuration. Press CTRL H during the server BIOS POST to launch the LSI WebBIOS configuration utility.	2.0(3a)
CSCud11400	On a scale setup, the fwm process on the FI might crash during server reack. The crash might happen when a port-channel member is being brought up. On scale setups, when there are triggers that flap the ports, a rare condition between multiple processes on the system results in incorrect cleanup that could cause the crash. The system recovers after the process restarts.	This issue has no known workaround.	2.1(1a)A

Table 23 Open Caveats in Release 2.1(1a) (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCud19629	FCoE uplink interface faults are not visible in the UCSM GUI under **SAN_Tab > Fabric A > Uplink FCoE Interfaces > FCoE Interface**.	Faults are available at the parent node level under **SAN_Tab > Fabric A**, which includes FCoE uplink interface faults.	2.1(1a)A
CSCud19730 CSCuc81667	Cisco UCS C220 and C240 servers running Cisco USM Manager Release 2.0(2) may experience a PCI bus number change when upgrading or downgrading the BIOS. This issue can cause the following: • A storage controller update failure from Cisco UCS Manager when upgrading to Release 2.1. • OS installations such as VMware might require manual intervention after bus number changes are seen.	To avoid the Cisco UCS Manager update issue either via the host firmware pack or through the firmware auto install, you should update to Release 2.0(3) before upgrading to Release 2.1. If you have already upgraded to Release 2.1 and see an "Unable to find Storage Controller Device" error, reacknowledge the servers to fix the issue. **Note** It might take up to 20 minutes for the failed firmware update attempt to timeout in Cisco UCS Manager before the server reacknowledge is started. The firmware update completes successfully during the reacknowledge task. For a VMware installation, the PCI mapping has to be manually changed using the ESX console.	2.0(3a)A
CSCud20765	When SRIOV vNICs are defined though a vnic template that is referenced by a service profile template, twice the number of VFs as specified in the dynamic connection policy are created in the instantiated service profiles. When a service profile template (with an update-template type) is updated, the SRIOV VFs in its instantiated services profiles will be erased.	Avoid using service profile templates for SRIOV VFs. Use service profiles directly.	2.1(1a)A
CSCud00607	IGMP membership might not be cleaned properly for some vEth interfaces. When IGMP joins for the same group are sent from multiple interfaces concurrently, sometimes the cleanup in the forwarding table does not happen properly. Note that the problem does not manifest when normal group expiry happens, but could happen during a reack of the server.	This issue has no known workaround.	2.1(1a)A

Table 23 Open Caveats in Release 2.1(1a) (continued)

Defect ID	Symptom	Workaround	First Bundle Affected

CSCuc59299	When downloading a firmware bundle, out of memory kills ethpm causing a reboot of FI, and no core is generated. The following message is shown:
	`2012 Sep 25 20:10:05 ucs-B %$ VDC-1 %$ CALLHOME-2-EVENT SW_CRASH`
	`2012 Sep 26 08:49:06 ucs-B %$ VDC-1 %$ Sep 26 08:49:06 KERN-1-SYSTEM_MSG Proc ethpm (4970) with Total_VM 249224 KB Resident_Mem 141232 KB Anon_Resident_Mem 133240 KB being killed due to lack of memory - kernel`
	`2012 Sep 26 08:49:06 ucs-B %$ VDC-1 %$ Sep 26 08:49:06 KERN-1-SYSTEM_MSG Out of Memory: Killed process 4970 (ethpm). - kernel`
	`2012 Sep 26 08:49:15 ucs-B %$ VDC-1 %$ Sep 26 08:49:15 KERN-0-SYSTEM_MSG Shutdown Ports.. - kernel`
	`2012 Sep 26 08:49:15 ucs-B %$ VDC-1 %$ Sep 26 08:49:15 KERN-0-SYSTEM_MSG writing reset reason 16, ethpm hap reset - kernel`
	This has been seen with a very large number of VIFs. For example, a setup with more than 2000 VIFs. An ethpm crash resulted in an FI reboot when sn ethpm crash occurred. The current VIF support count is 2000.
		This issue has no known workaround.	2.1(1a)A

CSCuc19701	When the fabric interconnect (FI) is reset, there is a small possibility the IOM might reboot. This has been observed only with the 2204 IOM. The IOM reboot is due to the satctrl process crashing. This is due to a race condition and is seen in scaled setups. The occurrence is rare, and the system recovers after the IOM reloads.	This issue has no known workaround.	2.1(1a)A

Table 23 Open Caveats in Release 2.1(1a) (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuc67344	In a very rare case, Cisco UCSM failed to restart due to the same UUID being allocated to two different service profiles. So far, this issue is seen only been observed for UUID pools and not for other ID's such as MAC addresses, WWXN , IP etc. This could be a day-1 implementation flaw happening in rare conditions. a) A static UUID is assigned to a service profile that is associated. b) In the single transaction, delete the service profile and create a new service profile (with a different name) with the same UUID suffix and UUID Pool. This step can be achieved only through importing (with replace option), XMLAPI, or CLI and modify the pool prefix. The expected behavior is that the UUID is correctly assigned to the new service profile and the pools reflect that. In some cases, the pool shows the allocated address as unassigned. c) Define a pool with the same UUID and create additional service profiles. This step will lead to the same UUID to be potentially allocated to the newly created service profiles.	Avoid the condition where the same UUID can be released and then allocated in the same transaction. For example, do not delete a service profile with statically assigned IDs and then create the new service profile with the same static ID in one transaction. Also avoid importing with the replace option when the existing configuration and the configuration to be imported have overlapping IDs that are assigned to different service profiles. If UCSM fails to restart, contact Cisco TAC for further assistance.	2.1(1a)A
CSCub48664	A rack server with a Cisco UCS VIC 1225 Adapter might fail discovery after decommission and recommission.	Power cycle the entire rack server.	2.1(1a)A

Table 23 Open Caveats in Release 2.1(1a) (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuc69455	The Cisco UCS Manager DME process might core dump when creating large number of service profiles with a large number of vNICs and a large number of VLANs on each vNIC in a single operation. On a Cisco 6200 Series FI, the UCSM DME process might core dump during the following large scale operations: • Creating 300 service profiles with 32 static vNICs in each service profile and 50 VLANs on each vNIC. • Creating 200 services profiles with 32 static vNICs in each service profile and 850 VLANs on each vNIC and then deleting all of the service profiles and repeating this process multiple times. The same problem could happen on a Cisco 6100 FI with a similar or smaller scale. A memory leak issue shows up when a very large number of MOs are committed in a single transaction. The same issue exists in previous releases (tested with Release 2.0[4b]) as well. It has been verified that there is no memory growth with reduced numbers such as: • Creating and then deleting 100 service profiles with two vNIC in each service profile and 100 VLANs on each vNIC. • Creating and then deleting 20 service profiles with 32 vNICs in each service profile and 50 VLANs on each vNIC.	When creating large number (>100) service profiles with large number vnics (>16) and large number of vlans (>50) on each vnic, avoid using a single operation to create all the service profiles. Break it down into multiple operations with a smaller number (such as 20) of service profiles in each operation.	2.1(1a)A
CSCuc59062	When installing ESX 5.1 to a SAN LUN using a M73KR-Q adapter, LUN discovery fails. This issue is seen because the Qlogic drivers are not present on the standard ESX 5.1 installation ISO.	Cisco will be releasing an ESX 5.1 custom ISO that will include the required M73KR-Q driver.	2.1(1a)C
CSCuc64210	The import of an all-configuration or system-configuration file fails with the error message "System is in suspend state. Policy ownership cannot be changed to GLOBAL." The all-configuration or system configuration file that was used for import was taken when the system was registered with Cisco UCS Central and was in a suspend state.	None. However, logical configurations and full-state backups taken during this state can be restored.	2.1(1a)A

Table 23 Open Caveats in Release 2.1(1a) (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuc77561	A "named-policy-unresolved" fault is suppressed during a pool-name resolution. Because the resolution can happen from remote (Cisco UCS Central), we suppressed the fault for pool name resolution for the pools of type IP, WWN, UUID, MAC, and IQN.	This issue has no known workaround. This is a change in behavior in Release 2.1.	2.1(1a)A
CSCud00607	IGMP membership might not be cleaned properly for some vEth interfaces. When IGMP joins for the same group are sent from multiple interfaces concurrently, the cleanup in the forwarding table might not occur properly. The problem does not occur for normal group expiry, but when a reack of the server occurs.	This issue has no known workaround.	2.1(1a)A
CSCuh81555	On a limited set of Cisco UCS B200 M3 blade servers, when upgrading to release 2.1(2a), board controller activation fails and the following error message is displayed: `Activation failed and Activate Status set to failed.` This is an otherwise harmless fault, and the blade continues to function normally. This occurs on servers with a particular part number. In Cisco UCS Manager, select the blade in the **Equipment** tab, then click the **General** tab in the work pane. Expand the **Part Details** area and look for the **Part Number** field. The following part numbers are affected: • 73-13217-08 • 73-13217-07 • 73-13217-06	If your Cisco UCS B200 M3 blade has one of the listed part numbers, do not use auto-install to upgrade to Release 2.1(2a). Upgrade the endpoints manually, and do not upgrade the board controller firmware for the affected Cisco UCS B200 M3 blades.	2.0(4d)B Resolved in 2.1(2c).

Open Caveats from Prior Releases

The following caveats were opened in previous Cisco UCS software releases and are still unresolved:

Table 24 Prior Open Caveats

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuf31431	Compiling rack server MIBs fails when performed on a CISCO-UNIFIED-COMPUTING-TC-MIB.my with 64 bit counters.	This issue has no known workaround.	2.0(4b)C Resolved in 2.1(2a).
CSCub55065	The service profile association failed and the server is shown as "Activating/Updating" status. This is seen when a server is running a non-interruptible configuration (such as a BIOS image update), disassociating/associating the same server may cause server configuration to stick at the "Activating/Updating" stage.	(1) Trigger "Decommission and re-commission" on the server. (2) Recover the corrupted BIOS.	2.0(3a)B
CSCuc47156	In UCS 2.1 setup, if user configured Host Firmware Package to include CIMC, after activate UCSM to 2.0, user can't update CIMC anymore.	Manually upgrade CIMC on each server.	2.0(4b)A
CSCuc26744	If a blade has a boardController firmware, then cannot use "Activate Firmware All" option from GUI. If the CIMC and BoardController firmware are activated at same time using Activate Firmware All, then activation will fail. This is known restriction from hardware. Since we use CIMC for activating BoardController, if we reboot CIMC when BoardController activation is in progress, it can cause the blade to get corrupted requiring RMA.	1. After doing "Activate Firmware ALL", go to individual BoardController components and change the startup version to same as running version. OR 2. Activate all the Board Controller components by selecting "BoardController" in the Activate Firmware filter. After this is done, then do Activate Firmware ALL for all other components	2.0(4a)A Resolved in 2.1(2a).
CSCuc82895	When downgrading UCS Manager from Release 2.0(4b) to lower 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.	2.0(4b)A
CSCuc26566	The Cisco UCS 6200 Series Fabric Interconnect reboots without a final confirmation warning after configuration changes.	This issue has no known workaround.	2.0(4a)A
CSCuc08556	A Cisco P81E CNA card installed in slot #2 on a Cisco UCS C240 might experience network disruptions with 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.	2.0(4a)A

Table 24 Prior Open Caveats (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
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. In releases 1.4 and prior a VLAN could be configured to be used both as regular Eth VLAN and as an FCoE VLAN. In the example illustrated in this defect VLAN 20 is both an FCoE VLAN for VSAN 20 and a global VLAN. In 2.0 and later releases, this is an unsupported configuration. VLAN 20 cannot be both an FCoE VLAN and regular Eth VLAN. Accordingly faults are raised when system is upgraded from any pre-Release 2.0 release to Release 2.0 or later to bring attention to the VLAN misconfiguration. Faults observed: VLAN default is error-misconfigured because of conflicting vlan-id with an fcoe-vlan VLAN20 is error-misconfigured because of conflicting vlan-id with an fcoe-vlan To rectify this, user assigned a new VLAN (2020) as the FCoE VLAN for the VSAN. This triggers re-configuration of VLAN 20 and in the process, some times, VLAN 20 may get completely removed from NXOS configuration. Due to this any host that is carrying VLAN20 will see a service outage	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 (20 in the example). 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. This error situation can only be reached through an upgrade workflow from a pre-2.0 release. In a 2.0 or later release, you are prevented from configuring a VLAN to be both FCoE and regular VLAN. So it is better to plan the re-assignment of VLANs as part of upgrade window downtime	2.0(4a)A
CSCuc47311	When a 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.	2.0(3c)B
CSCub20455	When testing the Twinax cables between IOMs and FIs or one of IOMs, blade discovery happens and displays B230M2"Mismatch Identity Unestablishable".	Try one of the following: • Reset CIMC • Change the server to a different slot.	2.0(3a)A 2.0(2r)C
CSCuc65457	In some rare conditions the bladeAG process crashes and creates a core dump.	None. The process recovers automatically after the crash as it restarts.	2.0(3a)A
CSCuc88168	6140 Fabric Interconnect reboots upon snmp crash.	The cause of this is under review. If the UCSM version is below 2.0(1t), please see CSCtt99770 Disabling SNMP on the FI may help prevent re-occurrence of the issue.	2.0(3a)A

Table 24 Prior Open Caveats (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuc65457	The svc_sam_bladeAG service crashes and creates a core dump.	This issue has no known workaround.	2.0(3a)A
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 FIs.	2.0(3a)A
CSCuc51258	When RedHat OS was left in idle for some time, the Keybooard/Mouse might become unresponsive with certain blades. This is seen randomly, and might be caused by combined error conditions. No reports of ESX hanging when running similar tests on the same hardware.	When doing disable/enable cycle on Frequency scaling from RH OS kernel, it improved the system stability and the platform previously failed within 30 minutes, but will no longer fail	2.0(3)A
CSCty23519	On a UCS 6120 or 6140 Fabric Interconnect with 20 chassis, some UCSM 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.	2.0(2r)A
CSCua31847	While upgrading from 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.	2.0(2q)A
CSCua50442	Third party tools such as demicode, IPMItool, and others, 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 technical support.	2.0(2q)A Resolved in 2.1(3a).
CSCua19893 CSCtx41004	Some of the Fibre Channel ports that are part of the san-port-channel on the Fabric Interconnect (FI) 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.	2.0(1w)A
CSCuc58056	"Inventory is not complete" errors received after displaying FI inventory.	This issue has no known workaround.	2.0(1w)A
CSCuc82601	All IOMs connected to an FI 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.	2.0(1t)A

Table 24 Prior Open Caveats (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
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.	2.0(1t)A

CSCuc91387	UCS fault for "FSM-STAGE:sam:dme:FabricEpMgrConfigure:begin " alarms accompanied by a momentary loss of connectivity on one fabric.
	DME logs a change on nw element triggering the reconfig:
	`INFO][0xac30dbb0][Oct 20 02:21:11.425][app_sam_dme:setElement] nw element operability changed (old=1)(new=0)`
	Check quorum chassis(s) I2C logs for inability to read PSU hub:
	`segment 4 psu`
	`norxack 4`
	`timeout 13818531`
	`unfinished 17`
	`lostarbitration 1`
	`fixup 27587498`
	`pca9541clrerrprs 3`
	`pca9541seterr 8`
	`pca9541postio 1`
	`pca9541postio2 1`
	`pca9541postio3 1`
	`wait_gt_deadline 1298217`
	`hub_sw_mbb 13768948 : this looks wrong`
	`hub_sw_mbb_to 13768948 : this looks wrong`
		1. Upgrade to 2.0(4b)
		2. Ask TAC to check system against "Transient_Chassis_Thermal_Faults_or_Fan_Problems" procedure.
			2.0(1t)A

CSCub19173	When adding multiple VLANs, MAC learning fails with resource exhaustion.	Reduce the number of VLANs.	2.0(1s)A
CSCub11507	In some conditions, a blade using a UCS M81KR adapter may lose communication to UCS Manager and prevent the OS from communicating to the network.	Reboot the blade server.	2.0(1q)
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.	2.0(1m)B
CSCtw59783	LEDs for ports 1 and 2 on a UCS 6296 behave differently than other ports.	This issue has no known workaround.	2.0(1m)A
CSCtl04744	Network connectivity is affected (flapping on uplink ports) on both fabrics during operations such as native VLAN change when the configuration change is done on both interconnects at the same time.	Schedule a maintenance window to perform such configuration changes, and perform the changes separately.	2.0(1m)A
CSCtz99795	When two Cisco UCS systems push the same VLAN profile, the port profile from one Cisco UCS system disappears.	Modify the maximum port in the port profile of the first Cisco UCS system and save the configuration. The port profiles are now displayed in both the Cisco UCS systems.	1.4(3u)A

Table 24 Prior Open Caveats (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCub58460	A PortAG crash is observed during a downgrade of UCS Manager from any release that supports a 2232 FEX, to version 1.4. This is seen when the management image is downgraded to 1.4 but system and kernel images are at 2.1.	Either decomission the 2232 FEX before doing the downgrade or just ignore the crash until the downgrade is done where in all the FI images running correspond to the prior release.	1.4(3q)A
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.	1.4(3l)C
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.	1.4(1i)B

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.	1.4(1i)A

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.	1.4(1i)A
CSCtf73879	Cisco UCS B200 M3 and Cisco UCS B22 M3 servers currently do not support disk status, failures, fault codes, and alarms from the MegaRAID controller.	This issue has no known workaround.	1.4(1i)A
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.	1.4(1i)A
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.	1.4(1i)A
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.	1.4(1i)A
CSCti39470	Cisco UCS Manager currently does not support RAID 50 and RAID 60.	This issue has no known workaround.	1.4(1i)A

Table 24 Prior Open Caveats (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
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.	1.1(1j)A
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.	1.1(1j)A
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.	1.0(1e)A
CSCsy20036	The disk scrub policy needs enhancements to meet DOD compliance.	This issue has no known workaround.	1.0(1e)A
CSCsv87256	Any SMASH command entered with wrong option should give “INVALID OPTION” error message.	This issue has no known workaround.	1.0(1e)A

Table 24 Prior Open Caveats (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
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.	2.0(1o)A

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 automatically clears after 1-minute. This does not impact the data path.	

Known Limitations and Behaviors

The following known limitations and behaviors are not otherwise documented:

Table 25 Known Limitations in Release 2.1

Defect ID	Symptom	Workaround	First Bundle Affected
CSCum16710	After downgrading the Cisco UCS Manager firmware from 2.2(x) to 2.1(x), any change to a service profile whose associated server has QLogic adapter(s) may trigger a server reboot. This occurs when the host firmware package is enabled with the related adapter selected for the service profile. The affected servers include blade servers with the N20-AQ0102 adapter and rack servers with the UCSC-PCIE-QSFP adapter.	Before beginning the downgrade: • Deselect the related adapter in the user-defined host firmware package. • Check the default host firmware package and make the corresponding changes.	2.1(3a)
CSCuj80991	After the blade firmware is upgraded from Release 1.4(3m) to any later release, vMotion fails due to an AES-NI bit difference.	Disable OEM AES-NI in the BIOS on the upgraded blade.	1.4(3q)
CSCtq38888	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.	2.0(1m)
CSCuh82452	Cisco UCS Manager 2.1(1) is not supported with Cisco UCS Central 1.1(1). If you downgrade from Release 2.1(2) to Release 2.1(1), any artifacts, such as global service profiles, global policies, or VLAN/VSAN configurations, that were created on Cisco UCS Central remain in Cisco UCS Manager, but cannot be modified or deleted.	Unregister Cisco UCS Manager Release 2.1(2) from Cisco UCS Central before downgrading.	2.1(2a)A
CSCug32086	The B420 M3 Blade Server with an SD card freezes after running for one day on ESXi 5.0	This issue has no known workaround.	2.1(2a)B
CSCuf77316	Windows 2012 installed on SD flash running Cisco UCS Release 2.1(2a) fails MSFT certification.	This issue has no known workaround.	2.1(2a)B
CSCug23097	RHEL V7 storage certification tests fail on the B22M3 and B200M3 Blade Servers.	This issue has no known workaround.	2.1(2a)B

Table 25 Known Limitations in Release 2.1 (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCtz16082 or CSCtz99909	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 the BIOS setup menu and C-state dump from EFI all show C1E is disabled in the BIOS policy from Cisco UCS Manager. If 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. The message in ESX is being reported incorrectly by ESX and should be ignored. The root cause is that ESX is looking at the wrong pointer and reporting the incorrect status. This issue has no known ill effects to the function of ESX or the server.	2.0(2q)B
CSCub54167	The 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.	2.0(2q)A
CSCtz07684	Boot order in BIOS setup or F6 menus still show Local HDD even after removing the Local Disk option in the Cisco UCS Manager service profile. This is seen when the boot order is configured by the 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 the server reboots, the boot order still shows the Local HDD in the BIOS boot order list. This behavior does not affect booting to PXE and iSCSI devices in the order configured.	Disable Local HDD manually using the following steps: 1. Boot the blade. 2. Press the F2 key when the message is displayed during the BIOS POST. 3. Wait until the BIOS completes its POST and invokes the Setup utility. 4. Choose the Boot Options tab. 5. Move the cursor down to Hard Drive BBS Priority and press enter to select this option. 6. Move the cursor to the hard drive that the user wants to disable and press Enter to configure the drive. 7. Move the cursor to the Disabled option and press Enter to disable the drive. 8. Save and reboot the blade.	2.0(2m)B
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.	2.0(1m)A

Table 25 Known Limitations in Release 2.1 (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCuc22026	While creating an SNMPv3 user, if the username is already assigned to local system users, instead of displaying an error, the configuration will be accepted, but a fault is raised and the configuration will not deploy. While creating an SNMPv2 user with a community name that is the same as the local system the user will be accepted and deployed without any error or fault. While creating a local system user, if the username is already assigned to an SNMPv3 user, then instead of displaying an error, the configuration will be accepted, but a fault is raised and the configuration will not deploy. This issue happens only when the SNMPv3 username and system local username matches.	If the SNMPv3 user configuration is not deployed because of a name collision with local user, then either choose a different name for the SNMPv3 user or delete the local user for the configuration to be deployed. If a local user configuration is not deployed because of name collision with the SNMPv3 user, then either choose a different name for the local user or delete the SNMPv3 user for the configuration to be deployed.	
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.	2.0(2m)B
CSCtr10869	During an upgrade from Release 1.4 to 2.0, an SSLCert error might be written to the log files.	This issue has no known workaround. This issue is harmless and has not been found to impact functionality.	2.0(1m)A
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.	1.4(3i)
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.	1.4(1i)A

Table 25 Known Limitations in Release 2.1 (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCtj89468	The link from the rack 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 server adapter is an FET, the link will remain down.	Replace the SFP with one of the supported SFPs for rack server adapters.	1.4(1i)A
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.	1.4(1i)A
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.	1.4(1i)A
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 issue has no known workaround. This defect has no functional impact.	1.4(1i)A
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.	1.4(1i)A
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.	1.4(1i)A
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.	1.4(1i)A
CSCtd14055 or CSCtf52298	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.	1.1(1j)A

Table 25 Known Limitations in Release 2.1 (continued)

Defect ID	Symptom	Workaround	First Bundle Affected

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`
			1.1(1j)A

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 used as 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.
			1.4(1i)A

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.	1.4(1i)A
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.	1.1(1j)A

Table 25 Known Limitations in Release 2.1 (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCte12163	For a 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 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.	1.1(1j)A
CSCte73015	Loading multiple driver disks during a RHEL 5.x installation fails.	See the article at http://kbase.redhat.com/faq/docs/DOC-17753	1.1(1c)A
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.	1.0(1e)A
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.	1.0(1e)A
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.	1.0(1e)A
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.	1.0(1e)A
CSCsz41907	When plugging or removing USB devices at **BIOS Setup -> Advanced -> USB**, the Setup Utility may hang.	Reboot the server.	1.0(1e)A
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.	1.0(1e)A
CSCtb45761	Downloads may be slow if TFTP is used.	If TFTP performance is slow, use SCP or another protocol.	1.0(1e)A
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.	1.0(1e)A

Table 25 Known Limitations in Release 2.1 (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
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.	1.0(1e)A
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.	1.0(1e)A
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.	1.0(1e)A
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.	1.0(1e)A
CSCta22029	SNMP shows the fabric interconnect name rather than system name.	This issue has no known workaround.	1.0(1e)A
CSCta24034	An SNMP username cannot be the same as a local username.	Select an SNMP username that does not match any local username.	1.0(1e)A
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.	1.0(1e)A
CSCtw67182	A blade with a UCS M81KR adapter shows the error "initialize error 1" during iSCSI boot.	This issue has no known workaround.	2.0(1s)A

Table 25 Known Limitations in Release 2.1 (continued)

Defect ID	Symptom	Workaround	First Bundle Affected
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.	1.0(1e)A
CSCsz99666	Installing EFI Native SLES 11 is currently not supported.	This issue has no known workaround.	1.0(1e)A

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 2.1*

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