Release Notes for Cisco UCS Central, Release 1.2

First Published: July 23, 2014
Last Updated: September 11, 2015

This document describes system requirements, new features, resolved caveats, known caveats, and open caveats with workarounds for Cisco UCS Central software Release 1.2. This document also includes information that became available after the technical documentation was published.

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

Contents

This document includes the following sections:

Revision History

Table 1 shows the revision history:

Table 1 Online Change History

Release	Date	Description
All releases	June 24, 2015	Added known limitation related to issue reported in CSCus21388.
1.2(1a)	July 23, 2014	Created release notes for Cisco UCS Central Release 1.2(1a).
	August 07, 2014	Added CSCuo69498 to resolved caveats.
	August 22, 2014	Added more resolved caveats to 1.2(1a) list.
1.2(1d)	September 30, 2014	Updated release notes for Cisco UCS Central Release 1.2(1d).
1.2(1e)	December 19, 2014	Updated release notes for Cisco UCS Central Release 1.2(1e).
1.2(1f)	February 19, 2015	Updated release notes for Cisco UCS Central Release 1.2(1f).
1.2(1d)	September 11, 2015	Added CSCur64858 to 1.2(1d) open caveats.

Introduction

Cisco UCS Central, Release 1.2 allows you to take charge of the data center environment by delivering easy to use, integrated solution for managing multiple Cisco UCS Domains in data center and remote environments, from a single management point with high availability. With Cisco UCS Central, Release 1.2, you can efficiently manage server, storage and network policies, and generate network traffic reports for your entire UCS environment in one or more data centers.

System Requirements

To access the browser based Cisco UCS Central GUI, your computer must meet or exceed the following minimum system requirements:

- Windows
  - Internet Explorer 9 and above
  - Firefox 29 and above
  - Chrome 34 and above
- Linux RHEL
  - Firefox 29 and above
  - Chrome 34 and above
- MacOS
  - Firefox 29 and above
  - Chrome 34 and above
  - Safari 6 and above

Adobe Flash Player 11.7 and above.

For the Chrome browser, remove the bundled flash player and install the flash player from Adobe.

The released OVA or ISO is supported with ESXi5.0 U3, ESXi5.1GA and ESXi5.5GA, ESXi 6.0.

The released ISO is supported with Microsoft Hyper-V Server 2008 R2 SP1 and Microsoft Hyper-V Server 2012.

Note If you are using Cisco UCS Release 1.2(1a), you must be running Cisco UCS Manager Release 2.1(2a) or higher. Some features of UCS Central 1.2(1a) may only work with later releases of Cisco UCS Manager.

New Software Features

This section contains:

Feature Support Matrix for Cisco UCS Central Releases

The following table provides a list of features in Cisco UCS Central, and Cisco UCS Manager release versions in which these features are supported:

Note Features such as specifying remote location for backup image files, 3rd party certificate, IPv6 inband management support are built in Cisco UCS Central to be compatible with upcoming Cisco UCS Manager releases.

Table 2 Cisco UCS Central Features and Supported Cisco UCS Manager Release

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions			
		2.1(2a)/ 2.1(3x)	2.2(1x)	2.2(2x)/ 2.2(3x)	3.0(1x)
Multi-version management support and viewing supported Cisco UCS Manager features	1.1(2a)	No	Yes	Yes	Yes
Importing policy/policy component and resources		No	Yes	Yes	Yes
Specifying remote location for backup files		No	No	Yes	Yes
3rd party certificates		No	No	Yes	Yes
IPv6 inband management support		No	No	Yes	Yes

Table 2 Cisco UCS Central Features and Supported Cisco UCS Manager Release (continued)

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions			
		2.1(2a)/ 2.1(3x)	2.2(1*x*)	2.2(2x)/ 2.2(3x)	3.0(1x)
Estimate Impact on Reconnect	1.2(1a)	No	No	Yes **Note**: Supported only from 2.2(3x)	Yes
Precision Boot Order Control		No	Yes	Yes	Yes
Scriptable vMedia	1.2(1e)	No	No	Yes **Note**: Supported only in 2.2(2c) and later 2.2(x) releases.	No

Note Searching for policy/policy components or resources is supported in Cisco UCS Manager, releases 2.1(2x) and 2.1(3x). To import policies, you must have Cisco UCS Manager, releases 2.2(1b) or higher

New Software Features in Release 1.2(1e)

Release 1.2(1e) Supports the following:

- Scriptable vMedia support for M3 and newer Servers
  - Non interactive OS/Driver installation and Driver Update
  - Boot from a specific vMedia device that is part of a boot policy
  - Ability to copy files from the mounted share to the local disk

New Software Features in Release 1.2(1a)

Release 1.2(1a) supports the following:

- Platform support:
  - Classic and Mini UCS Domains
  - Inventory for 6324 FI-IOM and scalability ports

  - FI Configuration for Ethernet and Uplink FI ports
- Feature enhancements:
  - Virtual MIT
  - Estimate Impact on Reconnect
  - Unified KVM Launch Manager
  - Fault Summary and Pending Activity panel
  - Precision Boot Order control
- WAN Optimization
  - Network bandwidth to 1.5 Mbps Minimum
  - Network latency to 500ms Maximum
  - Improved handling of temporary loss of connectivity between UCS Manager and UCS Central

Upgrade Paths

To deploy a fresh installation of Cisco UCS Central, Release 1.1(1b) or higher, you can use either the OVA file or the ISO image. See the *Cisco UCS Central Install and Upgrade Guides* for more information.

To upgrade Cisco UCS Central, you must use the ISO image. Upgrade from 1.2(1b) to any 1.2(1x) release is supported.

Note To upgrade Release 1.0(1a), you must first upgrade to 1.1(1b) release. After the upgrade has successfully completed, you can then upgrade to Release 1.2(1x). Also, make sure the registered Cisco UCS Domains are running Cisco UCS Manager, release 2.1(2a) or later.

Resolved Caveats

Resolved Caveats in Release 1.2(1f)

The following caveats are resolved in Release 1.2(1f):

Table 3 Resolved Caveats in Release 1.2(1f)

Defect ID	Description
CSCuq52593	Renaming a global service profile will not delete the ID usage for initiator IP.
CSCur97665	When you create a global service profile using the wizard with vHBAs, the vHBAs will not be missing from storage tab.
CSCus07137	Backing up UCS domains to UCS Central will not fail after performing UCS Manager upgrades.
CSCur97870	After suspending and acknowledging global boot policy, the san boot definition will not be deleted from the system.
CSCus02456	From Cisco UCS Central, when you try to associate service profile to B200 M4 servers, the association will not fail.

Table 3 Resolved Caveats in Release 1.2(1f)

Defect ID	Description
CSCuq52791	In Cisco UCS Central, if iSCSI boot parameters in a boot policy uses static IP for Initiator IP Address, changing it to a different IP pool would not cause any issues in releasing the static IP used earlier.
CSCuq54745	Statistics DB will not fill up the disk space under the /bootflash folder.
CSCus01906	After you upgrade from Cisco UCS Central 1.1(x) to 1.2(1f), any new global service profile association that uses the same boot policy with SAN boot as other global service profiles associated before upgrade, will not cause rebooting of those other service profiles.
CSCuq43213	If you do not specify the PCI order when creating a service profile in Cisco UCS Central, the PCI order will not show as ‘unspecified’.
CSCus69460	Fixed glibc GHOST vulnerability (CVE-2015-0235).
CSCun86526	The DST time zone is obsolete and has been removed from Cisco UCS Central.
CSCur14121	You will not get ‘can’t create; object already exists error’ when you modify a vSAN configuration under vNIC/vHBA placement in a global service profile.
CSCus08823	You can apply manual vNIC placement when creating a global service profile.
CSCus38084	You can successfully modify or save vNIC/vHBA order using the placement policy.

Resolved Caveats in Release 1.2(1e)

The following caveats are resolved in Release 1.2(1e):

Table 4 Resolved Caveats in Release 1.2(1e)

Defect ID	Description
CSCur04903	UCS Central will not show connectivity status as **lost connectivity** for registered Cisco UCS Domains when the connection is active.
CSCur30945	When a registered domain is not reachable, Cisco UCS Central will not become unresponsive.
CSCuq52965	Cisco UCS Central will no longer allow creation of invalid IQN block with empty suffix.

Resolved Caveats in Release 1.2(1d)

The following caveats are resolved in Release 1.2(1d):

Table 5 Resolved Caveats in Release 1.2(1d)

Defect ID	Description
CSCuq79346	When you launch KVM from UCS Central the KVM window title will display the service profile name.
CSCuq41727	You can configure the default http port 80 to use a different port number from the Cisco UCS Central CLI. The new port number must be greater than 1024.
CSCur05093	The security vulnerabilities identified by Common Vulnerability and Exposures (CVE) are fixed. See Bash Update bin.

Bash Update bin

UCS Central bash update bin (ucs-central-bash-update-3.2-33.el5_11.4.bin) provides a fix for the Security Vulnerabilities CVE-2014-6271 and CVE-2014-7169. This bash update bin is included in the 1.2(1d) and newer ISOs.

Note You are not required to upgrade to 1.2(1d) to use the bash update bin. You can use the bash update bin to just fix the security vulnerabilities on any Cisco UCS Central 1.2 releases. Download the bash update bin from here: Download bash update bin.

Do the following using the Cisco UCS Central CLI to download and install the bash bin update:

- Download the bash update bin from Cisco.com to a local scp/ftp/sftp/tftp server.
- Update the bash update bin using the following update command:

```
UCSC-VM1# connect local-mgmt
UCSC-VM1(local-mgmt)# update
<protocol>://<user_name>@<server_ip>/<file_location>/ucs-central-bash-update-3.2-33.el5_11.4.bin

protocol: protocol supported by the local server where the file is downloaded
user_name: authorized user name on the local server
server_ip: ip/hostname of the local server
file_location: location of the bin file on local server
```

Note If you have setup Cisco UCS Central in HA setup, make sure to install the bash bin update in both nodes.

Resolved Caveats in Release 1.2(1a)

The following caveats are resolved in Release 1.2(1a):

Table 6 Resolved Caveats in Release 1.2(1a)

Defect ID	Description
CSCup22584	You will no longer experience any of OpenSSL security vulnerabilities disclosed June 5, 2014.
CSCun98825	You will no longer get a failure message when using virtual media in global service profile to access UCS Manager KVM.

Table 6 Resolved Caveats in Release 1.2(1a) (continued)

Defect ID	Description
CSCuo69498	Renaming global service profile in Cisco UCS Central will no longer create orphan service profiles in Cisco UCS Manager.
CSCun79562	KVM launch icon displays within the screen for all common resolution settings.
CSCun83267	When a server that is part of the server pool in Cisco UCS Central is removed from UCS Manager, after rediscovery, the object will again be available in UCS Central server pool.
CSCun97425	SNMP host name regex will allow valid FQDNs, such as foo.lbar.com.
CSCuo05212	Setting multi core processing setting to all in BIOS policy will no longer save as all.
CSCuo28184	If you create a locale with a same name as the org in a sub-org, the locale will no longer fail in UCS Central.
CSCuo30377	Service profile identity command will display all associated IDs in the service profile.
CSCuo57907	The Desired power state will be disabled on UCS Central GSP details page when the server is in associated state.
CSCuo71712	When external statistics database connectivity status is lost, statistics manager will no longer fail to refresh connection for the oracle database.
CSCup19840	User authentication will no longer fail in UCS Central after importing backup.
CSCup41374	If a vLAN name is 32 characters long, when you assign it with an IP address for in band management, the assignment will no longer fail.
CSCup62032	Global service profiles will pick unique management IP addressed from IP pool.

Open Caveats

The following caveats are open in Release 1.2(1f):

Table 7 Open Caveats in Release 1.2(1f)

Defect ID	Symptom	Workaround
CSCus84707	Sometimes you might come across issues such as vcon order not getting saved, or vcon changes from updating template does not get reflected to the service profile.	In the case of updating template vcon changes not getting applied, log in and logout of the UCS Central GUI.
CSCus93431	If you have Cisco UCS Manager 2.2(3x) in the registered UCS domain, if a local or global service profile uses boot policy with order "1. Later" defined in Cisco UCS Central, and you try to modify the boot policy in Cisco UCS Central to add a local disk, the san boot in the boot policy will be deleted in UCS Manager.	Modify the boot policy description and save the boot policy in UCS central. Then UCS Manager will have both SAN boot and local disk properly populated.

The following caveats are open in Release 1.2(1e):

Table 8 Open Caveats in Release 1.2(1e)

Defect ID	Symptom	Workaround
CSCun37681	Cisco UCS Central does not support DNS IP configuration for inband IPv4 and inband IPv6 addresses in global service profile.	Make sure to configure policies associated to a global service profile with Actual IP addresses and not host names.

The following caveats are open in Release 1.2(1d):

Table 9 Open Caveats in Release 1.2(1d)

Defect ID	Symptom	Workaround
CSCur64858	LDAP provider bind DN password does not accept special characters.	Do not use special characters for this password. This is resolved in release 1.3(1b).

The following caveats are open in Release 1.2(1a):

Table 10 Open Caveats in Release 1.2(1a)

Defect ID	Symptom	Workaround
CSCup85700	In some cases, after restoring backup, if you change the management IP address, logging into Cisco UCS Central from the GUI fails with the following message: `fail to get connector for application:mgmt-controller,ip address:xxxxxxx`	Do the following to restart services: • Connect local-mgmt • Pmon restart

Known Limitations and Behaviors

The following known limitations and behaviors are not otherwise documented:

Table 11 Known Limitations in All Releases

Defect ID	Symptom	Workaround
CSCus21388	In a cluster set up, when the RDM link goes down on the primary node, DMEs cannot write to the database. This causes a crash on the primary node and failover to the subordinate node. The subordinate node takes over as the primary node. The database is then mounted in read-write mode on the new primary node. Because the RDM link is down, **umount** fails on the old primary node. When the RDM link comes up, the database is mounted on the old primary (current subordinate) node in read-only mode.	Restart **pmon** services on the current subordinate node or restart the node itself. Either of these processes will unmount the read-only partition and enable proper cleanup.

Related Documentation

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

- *Cisco UCS Documentation Roadmap*
- *Cisco UCS Central Install and Upgrade Guides*

Obtaining Documentation and Submitting a Service Request

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

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

This document is to be used in conjunction with the documents listed in the "Known Limitations and Behaviors" section.