Issues and Solutions

This chapter contains solutions to reported problems.

Administration

Lost or Unknown Administrator Password

Problem—The password to Cisco UCS Director is lost or unknown.

Possible Cause—The administrator has lost or does not know the Cisco UCS Director appliance password.

Recommended Solution—Perform the following steps:

Step 1 Log in as root on the Cisco UCS Director appliance.

Step 2 Enter the admin password reset script.

```
# opt/infra/dbPwdReset.sh
```

Note If root is not enabled on the Cisco UCS Director appliance, log in as shelladmin and use the Manage Root Access option to enable root privileges.

User Icon Menu Options Do Not Appear

Problem—In the Cisco UCS Director administrator portal, the menu options under the user icon in the header do not appear.

Recommended Solution—Perform the following steps:

Step 1 Clear your browser cache.

Step 2 Log into Cisco UCS Director.

Null Value in Tabular Reports on MSP Organization Screen and Customer Organization Screen

Problem—After upgrading from Release 5.3 or earlier to a later release, the header sections for tabular reports in the **MSP Organization** screen and **Customer Organization** screen displays null values.

Possible Cause—While upgrading, Cisco UCS Director does not persist the default setting for Service Provider feature.

Recommended Solution—Perform the following steps:

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Service Provider Feature**.

Step 3 Check **Enable Service Provider Feature**.

Step 4 Click **Submit**.

Time Mismatch Between the Cisco UCS Director System Time and the Configured NTP Server

Problem—Time mismatch noticed between the Cisco UCS Director system time and NTP server that is configured using the Shell Admin. This issue is noticed during workflow task scheduling.

Possible Cause— This problem occurs if the ESX host and the Cisco UCS Director system do not have the same NTP server or time configuration.

Resolution—Perform the following steps only when you notice this time difference:

Step 1 Log into the vCenter.

Step 2 Select the VM which is running Cisco UCS Director.

Step 3 Choose **Edit Settings**.

Step 4 Choose **Options**.

Step 5 Select **VMware Tools**.

Step 6 Clear **Synchronize guest time with host**.

Step 7 Click **OK**.

All Menu Options Not Visible in Navigation Bar

Problem—Some of the menu options in the side **Navigation** bar are not visible.

Possible Cause—The screen resolution is high (1680X1050 or 1920X1080) or you have zoomed in the Web browser above 100%. The **Navigation** bar only displays the number of options that fit in the space available.

Recommended Solution—Click **Site Map** in the **Navigation** bar to view and access all the menu options.

High Database Disk Utilization

The Diagnostic System Messages icon on the header pane of the administrator portal displays the number of diagnostic system messages that have been logged. Clicking this icon takes you to the **Diagnostic System Messages** screen that displays detailed information on the issues logged. Starting with the Base Platform Connector Pack version 6.7.4.1, this screen also displays alerts based on the database disk usage.

Problem—The **Diagnostics System Messages** screen indicates that database disk usage is exceeding the set threshold limits.

Recommended Solution—Review the data retention parameters that you have confirmed for the system, and determine if you can reduce the specified values. To review and modify these values, choose **Administration** > **System** > **System Parameters**. If you continue to notice the database disk alerts on the **Diagnostic System Messages** screen, then perform the following steps to expand the database disk size. In a multi-node configuration, perform these steps on the database node.

Note Increasing the disk size by a large range could affect the performance of the system. We recommend that you first start with increasing the disk size by about 10%. If you continue to notice that the disk is running out of space, contact Cisco TAC.

Step 1 Take a snapshot of Cisco UCS Director VM.

Step 2 Login to the vCenter and add the hard disk with the required disk size.

Step 3 Restart the VM.

Step 4 Login to the Shell Admin console and locate the newly added disk:

```
[root@local-host] # fdisk -l

Disk /dev/sda: 107.4 GB, 1073636966640 bytes
255 heads, 63 sectors/tracks, 13052 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk Identifier: 0x00046f2c

Device Boot            Start       End     Blocks     ID       System
/dev/sda/1 *             1          26      204800     83       Linux
Partition 1 does not end on cylinder boundary.

Disk /dev/sdc: 214.7 GB, 214748364800 bytes
```

```
255 heads, 63 sectors/tracks, 26108 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk Identifier: 0x00046f2c
```

Step 5 Change the mode using C on **fdisk /dev/sdc**.

Step 6 Create a partition on the disk with the default cylinder.

```
command (m for help): n
Command action
e    extended
p    primary partition (1-4)

p

partition number (1-4): 3
First cylinder (1-26108, default 1):
Using default value 1
Last cylinder, +cylinders or +size (K,M,G) (1-26108, default 26108):
Using default value 26108

Command (m for help): p

Disk /dev/sdc: 214.7 GB, 214748364800 bytes
255 heads, 63 sectors/tracks, 26108 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk Identifier: 0x00046f2c

Device Boot       Start      End    Blocks     ID     System
/dev/sdc3           1       26108   209711486  83      Linux
```

Step 7 Change the partition ID.

```
command (m for help): t
Selected partition 3
Hex code (type L to list codes): 8e
Changed system type to partition 3 to 8e (Linux LVM)

Command (m for help): w
This partition table has been altered.

Calling ioctl () to re-read partition table.
Syncing disks.
```

Step 8 Verify the disk configuration.

```
[root@local-host] # fdisk -l

Disk /dev/sdc: 214.7 GB, 214748364800 bytes
255 heads, 63 sectors/tracks, 26108 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk Identifier: 0xeb6a480
Device Boot      Start       End     Blocks        ID       System
/dev/sdc3        1        26108     209711486     8e       Linux LVM
```

Step 9 Create a physical volume and verify that the physical volume is created.

```
[root@local-host] # pvcreate /dev/sdc3

physical volume "/dev/sdc3" successfully created.

[root@local-host] # pvdisplay
"dev/sdc3" is a new physical volume of 200.00 Gib
--New Physical Volume--
PV Name        /dev/sdc3
VG Name
PV Size        200.00 Gib
Allocatable    No
PE Size        0
Total PE       0
Free PE        0
Allocated PE   0
PV UUID        T888P2c-Ov0c4-saD1-OF21-fEdv-Ibns-5HBiZ5
```

Step 10 Determine the volume group.

```
[root@local-host] # lvdisplay

----Logical Volume---
LV Path       /dev/infradb_vg/infradb_lv
LV Name       infradb_lv
VG Name       infradb_vg
```

Step 11 Extend the volume group

```
[root@local-host] # vgextend /dev/infradb_vg /dev/sdc3
Volume group "infradb_vg" successfully extended.
```

Step 12 Verify the configuration using the **vgdisplay** command.

Step 13 Extend the logical volume and then verify the configuration.

```
[root@local-host] # lvextend -L+199G /dev/infradb_vg/infradb_lv
Size of logical volume infradb_vg/infradg_lv changed from 99.99Gib to 298.099 Gib
Logical volume infradb_lv successfully resized.

[root@local-host] # lvdisplay
----Logical Volume---
LV Path       /dev/infradb_vg/infradb_lv
LV Name       infradb_lv
VG Name       infradb_vg
LV Size       298.099Gib
```

Step 14 Resize the file system.

```
[root@local-host] # resize2fs /dev/infradb_vg/infradb_lv
resize2fs 1.41.12 (11 June 2020)
Filesystem at /dev/infradb_vg/infradb_lv is mounted on /infradb; on-line resizing required
old desc_blocks = 7, new_desc_blocks = 19
Performing an on-line resize of /dev/infradb_vg/infradb_lv to 78377984 (4k) blocks
The filesystem on /dev/infradb_vg/infradb_lv is now 78377984 blocks long.
```

Step 15 Verify the disk sizes using the **df -hP** command.

Step 16 Verify the disk sizes from the Shell Admin Console.

Expanding the database disk size should resolve some of the issues displayed in the **Diagnostics System Messages** screen in the administrator portal. If you continue to see the disk-related issues even after expanding the disk size, contact Cisco TAC.

High Primary Disk Utilization

Problem—The primary disk is running out of space.

Resolution—From the Cisco UCS Director Shell Admin menu, choose the **Clean-up Patch files** option. After performing this step, check the disk utilization. If it continues to be high, check the disk to determine if files that you no longer need, such as patch files or old backup files, are retained on it. Use the command **du -a / | sort -n -r | head -n 10** to view information on folders that contain large number of files. Delete the files that you no longer need.

If you continue to notice that the primary disk is running out of space, then perform the following steps to increase the disk size. Use this procedure to increase the size of the primary disk in the application node, database node or the BMA node.

Important Increasing the disk size by a large range could affect the performance of the system. We recommend that you first start with increasing the disk size by about 10%.

Step 1 Take a snapshot of the Cisco UCS Director VM.

Step 2 Log into the Cisco UCS Director Shell using SSH client.

Step 3 Disable swapping on the files using `swapoff -a` command.

Step 4 Reconfigure the partitions using `fdisk` command. In the following example, `fdisk /dev/device_filename` command is used to navigate to the device file and delete partition 1 and partition 2. Ensure that you delete partition 2 first.

```
fdisk /dev/device_filename

Command (m for help): d
Partition number (1,2, default 2):

Partition 2 has been deleted.

Command (m for help): d
Selected partition 1
Partition 1 has been deleted.
```

Step 5 To create a new partition, perform the following tasks:

a) Create a new device file and enter **n** to create a new partition.

The following information is displayed:

```
fdisk /dev/device_filename1

Command (m for help): n
Partition type
   p   primary (0 primary, 0 extended, 4 free)
```

```
   e   extended (container for logical partitions)
Select (default p):
```

b) Enter **p** and press **Enter**.

The following information is displayed:

```
Select (default p): p
Partition number (1-4, default 1):
```

c) Enter **1** and press **Enter**.

The following information is displayed:

```
First sector (2048-209715199, default 2048):
Last sector, +sectors or +size{K,M,G,T,P} (2048-209715199, default 209715199): +96G

Created a new partition 1 of type 'Linux' and of size 96 GiB.
```

d) Repeat Step a to Step c to create swap partition. You can add more partitions, if required.

Step 6 To change the partition type, perform the following tasks:

a) To change the partition type for partition 2, enter **t** in `fdisk` prompt and press **Enter**.

The following information is displayed:

```
Command (m for help): t
Partition number (1,2, default 2):
```

b) Enter **2** and press **Enter** to change the partition type for partition 2.

The following information is displayed:

```
Partition type (type L to list all types):
```

c) Enter **L** and press **Enter**.

The following information is displayed:

```
 0  Empty           24  NEC DOS         81  Minix / old Lin bf  Solaris
 1  FAT12           27  Hidden NTFS Win 82  Linux swap / So c1  DRDOS/sec (FAT-
 2  XENIX root      39  Plan 9          83  Linux           c4  DRDOS/sec (FAT-
 3  XENIX usr       3c  PartitionMagic  84  OS/2 hidden or  c6  DRDOS/sec (FAT-
 4  FAT16 <32M      40  Venix 80286     85  Linux extended  c7  Syrinx
 5  Extended        41  PPC PReP Boot   86  NTFS volume set da  Non-FS data
 6  FAT16           42  SFS             87  NTFS volume set db  CP/M / CTOS / .
 7  HPFS/NTFS/exFAT 4d  QNX4.x          88  Linux plaintext de  Dell Utility
 8  AIX             4e  QNX4.x 2nd part 8e  Linux LVM       df  BootIt
 9  AIX bootable    4f  QNX4.x 3rd part 93  Amoeba          e1  DOS access
 a  OS/2 Boot Manag 50  OnTrack DM      94  Amoeba BBT      e3  DOS R/O
 b  W95 FAT32       51  OnTrack DM6 Aux 9f  BSD/OS          e4  SpeedStor
 c  W95 FAT32 (LBA) 52  CP/M            a0  IBM Thinkpad hi ea  Rufus alignment
 e  W95 FAT16 (LBA) 53  OnTrack DM6 Aux a5  FreeBSD         eb  BeOS fs
 f  W95 Ext'd (LBA) 54  OnTrackDM6      a6  OpenBSD         ee  GPT
10  OPUS            55  EZ-Drive        a7  NeXTSTEP        ef  EFI (FAT-12/16/
11  Hidden FAT12    56  Golden Bow      a8  Darwin UFS      f0  Linux/PA-RISC b
12  Compaq diagnost 5c  Priam Edisk     a9  NetBSD          f1  SpeedStor
14  Hidden FAT16 <3 61  SpeedStor       ab  Darwin boot     f4  SpeedStor
16  Hidden FAT16    63  GNU HURD or Sys af  HFS / HFS+      f2  DOS secondary
17  Hidden HPFS/NTF 64  Novell Netware  b7  BSDI fs         fb  VMware VMFS
18  AST SmartSleep  65  Novell Netware  b8  BSDI swap       fc  VMware VMKCORE
```

```
1b  Hidden W95 FAT3 70  DiskSecure Mult bb  Boot Wizard hid fd  Linux raid auto
1c  Hidden W95 FAT3 75  PC/IX           bc  Acronis FAT32 L fe  LANstep
1e  Hidden W95 FAT1 80  Old Minix       be  Solaris boot    ff  BBT
```

d) Enter **82** and press **Enter**.

The following information is displayed:

```
Changed type of partition 'Linux' to 'Linux swap / Solaris'
```

e) Enter **w** and press **Enter** to save the changes.

The following information is displayed:

```
The partition table has been altered.
Calling ioctl() to re-read partition table.
Re-reading the partition table failed.: Device or resource busy

The kernel still uses the old table. The new table will be used at the next reboot or after you
 run partprobe(8) or kpartx(8).
```

Step 7 Use the `partprobe` command to update the kernel with the partition changes.

Step 8 Resize the file system on `fdisk /dev/device_filename1`.

Step 9 To enable swap, perform the following tasks:

a) Create a swap location on `fdisk /dev/device_filename1` using the `mkswap` command.
b) Edit the system configuration file using the `/etc/fstab` command.
c) Enable swap using the `swapon -a` command.

Step 10 If you continue to notice that the primary disk size is full and it is impacting performance of the system, then contact Cisco TAC.

Baremetal Agent

Cisco UCS Director Appliance with Cisco UCS Director Bare Metal Agent Installed Will Not Boot from PXE

Problem—A Cisco UCS Director appliance has Cisco UCS Director Bare Metal Agent installed but will not boot from PXE. The PXE service is running from the Cisco UCS Director web GUI, however, the following information is displayed when entering the `grep tftpd /var/log/messages` command on the Cisco UCS Director Bare Metal Agent VM:

```
Nov 16 13:49:41 localhost xinetd[5086]: Server /usr/sbin/in.tftpd is not executable
[file=/etc/xinetd.d/tftp] [line=12]

Nov 19 07:24:21 localhost xinetd[3548]: Server /usr/sbin/in.tftpd is not executable
[file=/etc/xinetd.d/tftp] [line=12]
```

Possible Cause—The Cisco UCS Director Bare Metal Agent is not using Trivial File Transfer Protocol (TFTP).

Recommended Solution—Perform the following steps:

Step 1 Verify that the Cisco UCS Director Bare Metal Agent services are running.

Example:

```
***
# /opt/infra/statusInfra.sh
 Service                  Status        PID
 ----------           ----------      -----
 broker                  RUNNING      21420
 controller              RUNNING      21443
 networkServices         RUNNING      21475

 Database Connectivity : UP
****
```

Step 2 Verify that the TFTP service is enabled.

Example:

```
# ps -ef | grep tftpd
root     21477 21475  0 Oct29 ?        00:18:57
java -Xmx1024m -Dpxe.tftpd.enable=on -Dremap=true
-DpxeServer.ip=192.0.2.1 -DpxeServer.mgmt_vlan_ip=192.0.2.254
-cp .:networkServices.jar
```

Step 3 Restart the Cisco UCS Director Bare Metal Agent services.

```
# /opt/infra/startInfraAll.sh
```

Step 4 Check the `dhcpd.conf` file to make sure that the network settings are appropriately defined. Verify that the subnet is the same.

```
# cat /etc/dhcpd.conf
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#
ddns-update-style interim;
ignore client-updates;

subnet 198.51.100.1  netmask 255.255.255.0 {
         option routers                  198.51.100.2;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.55.1;

        option time-offset              -18000; # Eastern Standard Time

        range dynamic-bootp 198.51.100.101 198.51.100.254;
        default-lease-time 21600;
        max-lease-time 43200;
        allow booting;
        allow bootp;
        next-server 198.51.100.3;
        filename "/pxelinux.0";

}
```

New Images Added to the Cisco UCS Director Bare Metal Agent Are Not Showing up in the Cisco UCS Director Appliance

Problem—After adding an image to the Cisco UCS Director Bare Metal Agent appliance, you may observe that the newly added image is still not showing up as an option in the Cisco UCS Director Setup PXE Boot task, even if the two appliances are in .

Possible Cause—A difference in the date or time between the Cisco UCS Director appliance and the Cisco UCS Director Bare Metal Agent appliance may cause this issue.

Recommended Solution—Perform the following steps:

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 Verify that the status for your Cisco UCS Director Bare Metal Agent account is active. If the status is inactive, generally this is due to a difference in the date or time between the two appliances.

Step 4 Reconfigure the date or time on both appliances.
Once you configure both appliances with the correct date or time, the Cisco UCS Director Bare Metal Agent status changes to active.

Baremetal Linux Workflow: How to Configure a UCS Server with 2 vNICs - One for PXE Traffic and One for Final Management (Production) IP of the Server

Problem—Server configuration with 2 vNICs.

Possible Cause—N/A.

Recommended Solution—Follow the steps listed below:

Step 1 On the BMA, navigate to the following directory `/opt/cnsaroot/templates/<your_image_name>`.

```
[root@localhost RHEL65]# pwd
```

```
/opt/cnsaroot/templates/RHEL65
```

Step 2 There will be two files in this directory, 1) *ks.cfg* and 2) *pxe.cfg*.

```
[root@localhost RHEL65]# ls
```

ks.cfg pxe.cfg

Step 3 The *pxe.cfg* file is more specific to the configuration of the PXE process, this is where we can tell the server specifically which vNIC (in our case *eth0* to use for the PXE install process. You can see below we add the *ksdevice=eth0* to tell the pxe process to use the *eth0* interface .

[root@localhost RHEL65]# vi ./pxe.cfg

ks.cfg pxe.cfg

kernel images/RHEL65/isolinux/vmlinuz

append initrd=images/RHEL65/isolinux/initrd.img ramdisk_size=9216 noapic acpi=off ip=dhcp ks=$PXE_KS_URL ksdevice=eth0

prompt 0

timeout 0

</Contents of pxe.cfg>

Step 4 Now also check the *ks.cfg*. This file pertains more specifically to the final configuration of the server. This is where we can tell the kickstart process to use *eth1* and assign the servers final IP address to *eth1*. The *-device=eth*1 parameter tells kickstart to assign the IP address to the *eth1* interface.

[root@localhost RHEL65]# vi ./ks.cfg

Look in your *ks.cfg* file for a line similar to the following:

network --bootproto=static --device=eth1 --ip=$PXE_IP --netmask=$PXE_NETMASK --gateway=$PXE_GATEWAY --vlanid=$PXE_MGMTVLAN --hostname=$PXE_NAME --onboot=on

Step 5 Make sure the UCS Service Profile vNIC that corresponds to *eth0* has the PXE VLAN allowed on it and it is set as the native VLAN for that vNIC in UCSM.

Step 6 Make sure the UCS Service Profile vNIC that corresponds to *eth0* has the Mgmt VLAN allowed on it. If you have the *-vlanid= parameter* (as seen above in green) in the kickstart file, then you do not need to set it as the native vlan. If you do not have the *-vlanid= parameter*, you will need to set it as the native vlan for this vNIC.

PXE Installation Using Cisco UCS Director Bare Metal Agent Fails During the TFTP Portion of PXE

Problem—The PXE installation using Cisco UCS Director Bare Metal Agent fails during the TFTP portion of the installation.

Possible Cause—The target server is pointed to the incorrect TFTP server, and therefore is not able to find the appropriate files using TFTP to initiate installation of the operating system.

Recommended Solution—Perform the following steps:

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 Click the row with the appropriate bare metal account.

Step 4 Click **Edit**.

Step 5 Verify that the management IP and the PXE IP addresses are correct. Once confirmed, note the IP address of the PXE Interface Address of the Cisco UCS Director Bare Metal Agent.

Step 6 Log in to the Cisco UCS Director Bare Metal Agent appliance.

Step 7 Edit the DHCP configuration file located at `/etc/dhcp/dhcpd.conf`.

Step 8 Set the `next-server` option in the DHCP configuration file to match the IP address of the PXE Interface Address of the Cisco UCS Director Bare Metal Agent.

Example:

```
[root@localhost dhcpl# cat dhcp.conf
         #
         # DHCP Server Cofiguration file.
         #   see/usr/share/doc/dhcp*/dhcp.conf.sample
         #
         ddns-update-style- interim;
         ignore client-updates;

         subnet 198.51.100.0 netmask 255.255.0.0{
               option routers                198.51.100.1;
              option subnet-mask            255.255.255.0;

              option time-offset -18000; #Easter Stadard Time;

          range dynamic-bootp 192.0.2.1, 192.0.2.254;
          default-lease-time 21600;
          max-lease-time 43200;
          allow booting;
          allow bootp;
          next-server  192.0.2.3
          filename "/pxelinux.0";
```

Step 9 Restart the DHCP servers from the Cisco UCS Director Bare Metal Agent command line using the **`service dhcp restart`** command.

PXE Boot Tasks Fail After Deploying Windows Server

Problem—After successfully installing and deploying a Windows server using Boot LUN, the PXE boot task fails, and the Monitor PXE Boot task displays the following message:

Waiting for the PXE boot to be ready.

Possible Cause—A network issue between the Windows server and Cisco UCS Director Bare Metal Agent may cause the PowerShell script that runs at the end of the PXE boot process to fail. If this process fails, the Monitor PXE boot task hangs.

Recommended Solution—Resolve the L3 network issue and resubmit the service request for the Monitor PXE Boot task.

Windows Deployment Fails After Upgrading BMA to 6.5 Version

Problem— Windows deployment fails after you upgrade the Bare Metal Agent from version 6.0 or version 6.0(x.x) to version 6.5.

Possible Cause—Upgrade process may not be complete.

Resolution— Ensure that you have followed the procedure for upgrading the BMA according to the steps outlined in the *Cisco UCS Director Upgrade Guide*.

After upgrading to Cisco UCS Director 6.5, you must complete the following steps to rectify this issue:

Step 1 When you upgrade the Bare Metal Agent from 6.0.0.0 to 6.5.0.0, wait for the upgrade to complete. Once the Bare Metal Agent appliance is up, wait for 5 minutes and then execute the following commands in the Bare Metal Agent console.

```
setsebool -P samba_export_all_ro=1 samba_export_all_rw=1
find /opt/cnsaroot/templates/ -name "Win*" -exec ln -s '{}' /var/www/html/ \;
```

Step 2 When you upgrade the Bare Metal Agent from 6.0.1.0 to 6.5.0.0, wait for the upgrade to complete and reboot the Bare Metal Agent appliance. Once the Bare Metal Agent appliance is up, wait for 5 minutes and then execute the following commands in the Bare Metal Agent console.

```
setsebool -P samba_export_all_ro=1 samba_export_all_rw=1
find /opt/cnsaroot/templates/ -name "Win*" -exec ln -s '{}' /var/www/html/ \;
```

Installing Windows 2019 Fails in Monitor PXE Boot Task

Problem—Windows 2019 deployment fails after you upgrade the Cisco Bare Metal Agent Connector Pack to the latest version.

Possible Cause—Samba password will not be updated in Windows 2019 templates, when the samba services are already enabled and running in the Bare Metal Agent.

Recommended Solution—Before provisioning Windows 2019, you should reset Samba password if the samba services are already enabled and running.

Login to Host Fails After Successful PXE Boot Request

Problem—After successful PXE boot request, login to host may fail displaying the following message:

Invalid login or password. Please verify and re-enter the credentials.

This issue exists for all OS flavors.

Possible Cause—Host login fails due to password encryption enhancement in Cisco UCS Director, Release 6.6.1.0.

Recommended Solution—Requires both the Cisco UCS Director and Bare Metal Agent to be on the same version. Ensure that you update the Bare Metal Agent to 6.6.1.0 version in order to be compatible with Cisco UCS Director.

Workflow Validation Fails for Setup Windows PXE Boot Task after Upgrading BMA to Release 6.7.4.1

Problem—Workflow validation fails for the **Setup Windows PXE Boot** task after upgrading the Bare Metal Agent from version 6.7 or version 6.7.4.0 to version 6.7.4.1.

Possible Cause—In this release, the input type for the **Password** field in the **Setup Windows PXE Boot** task is changed from **Generic Input** to **Password**. Therefore, input of the **Password** field cannot be mapped with the Generic Text Input value. Hence, the existing input mapping is lost.

Resolution— Fix the validation issue by remapping the input type for the **Password** field in the **Setup Windows PXE Boot** task.

Big Data

Monitor PXE Boot Tasks Fail During Cluster Creation

Problem—During cluster creation in Cisco UCS Director for Big Data, Monitor PXE Boot task fails with the following message:

Waiting for the PXE boot to be ready.

Possible Cause—The Monitor PXE boot task hangs when there is no enough space in the bare metal agent.

Recommended Solution—Search for the available space in the bare metal agent. Do one of the following:

- Search for `/var/log/messages` file in the bare metal agent. If there is no enough space in the bare metal agent, delete the files that are not required and resubmit the service request for the Monitor PXE Boot task.
- Check for the disk space using **df -k** and delete the files that are not required.

Connectivity

Troubleshooting Cisco UCS Director Connectivity

Step 1 Ensure Cisco UCS Director services are active.

Check	Do the following:
Cisco UCS Director Virtual Machine (VM)	Ensure that there is sufficient resource reservation. For more information, see the System Requirements section.
Cisco UCS Director appliance	Access the appliance using Secure Shell (SSH) and the **shelladmin** user. Ensure that all the services are running (including the database). If services are not running, restart the services and wait a few minutes before accessing Cisco UCS Director through the web interface.

Step 2 Ensure that the IP address of Cisco UCS Director can be pinged over the network.

Check	Do the following:
Cisco UCS Director network configuration	Log into vCenter and check the network configuration of the Cisco UCS Director virtual appliance and its connectivity.
Port group and management network	Ping the port group and management network.
Cisco UCS Director VM	Ensure that the **Connect** check box is checked in the VM.

Step 3 Ensure that Cisco UCS Director can be accessed through a web browser. If you cannot access Cisco UCS Director, do the following:

Note Wait for the Cisco UCS Director appliance and services to become available before connecting to Cisco UCS Director. This may take a few minutes.

Check	Do the following:
Web browser cache	Clear the web browser cache before accessing Cisco UCS Director through the web.
Web browser version	Use the recommended browser version and flash version.

Step 4 Ensure that Cisco UCS Director is able to reach all of the hardware and software.

Step 5 Ensure that Cisco UCS Director is on the same interface as Cisco UCS Director Bare Metal Agent.

Troubleshooting Connectivity with Cisco UCS Director and PowerShell Agent

Problem—You can experience a failed test connection with Cisco UCS Director. This problem can occur even though you successfully installed and configured the PowerShell Agent, and there is no issue with the network connectivity between PowerShell Agent and Cisco UCS Director.

Note This problem can occur with Windows Server 2012 R2 or other versions that use advanced cipher suites for https communication.

When you check the PowerShell Agent logs in the PowerShell Agent server, you will find an SSPI failed with inner exception error similar to the following:

```
2014-08-20 14:44:16,832 [6] ERROR cuic.ClientConnection[null] -
   Exception: A call to SSPI failed, see inner exception.
```

```
2014-08-2014:44:16,832 [6] DEBUG cuic.ClientConnection[null] - Inner exception: The message received was unexpected
 or badly formatted.
```

```
2014-08-2014:44:16,832 [6] DEBUG cuic.ClientConnection[null] - Authentication failed - closing the connection.
```

Possible Cause—The test connection fails because of the Microsoft update, in which new TLS cipher suites are added and cipher suite priorities are changed in Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2. See Microsoft kb article 2929281 for further information on this update.

Recommended Solution—Modify the SSL cipher suite group policy setting. Perform the following steps:

Step 1 At a command prompt, enter `gpedit.msc` to open your group policy editor.

Step 2 Expand **Computer Configuration** > **Administrative Templates** > **Network**, and then click **SSL Configuration Settings**.

Step 3 Under **SSL Configuration Settings**, click the **SSL Cipher Suite Order** setting.

Step 4 In the **SSL Cipher Suite Order** pane, scroll to the bottom of the pane.

Step 5 Follow the instructions labeled **How to modify this setting**.

What to do next

Restart the computer after modifying this setting for the changes to take effect.

Troubleshooting Cisco UCS Director Bare Metal Agent Connectivity

Step 1 Ensure that the DHCP service (daemon) is active.

Check	Do the following:
DHCP server	Use the following command: `/etc/init.d/dhcp status` **Note** If the status is down, restart the DHCP server.

Step 2 Ensure that the status of Cisco UCS Director Bare Metal Agent network services is active.

Check	Do the following:

Cisco UCS Director Bare Metal Agent	Use the following command:
	`ps -ef | grep java`
	Note Entering the above command should have three Java processes display. If not, restart the services and recheck to make sure all of them are active.
	`/opt/infra/stopInfraAll.sh`
	`/opt/infra/startInfraAll.sh`

Step 3 Ensure Cisco UCS Director Bare Metal Agent can ping the Cisco UCS Director Bare Metal Agent IP address. If not, check the connectivity through the network configuration of the Cisco UCS Director Bare Metal Agent appliance using vCenter.

Step 4 Ensure that Cisco UCS Director Bare Metal Agent can ping the management and blade server network.

Check	Do the following:
DHCP server	Ensure that the DHCP server that is running on the Cisco UCS Director Bare Metal Agent provides DHCP functionality for bare metal provisioning. The Cisco UCS Director Bare Metal Agent should be on the same network or interface as the manager so that it can provide Preboot Execution Environment (PXE) functionality without problems. Ensure there are no DHCP servers available in the same network as the Cisco UCS Director Bare Metal Agent.

Database Failure

Troubleshooting Inventory Database Failures

Problem—The master inventory database fails.

Possible Cause—Database failures may be caused by:

- A `mysqld` crash, which may occur if the VM is powered off abruptly.
- A power failure on the node on which the Cisco UCS Director VM is running.
- File system corruption on an external datastore on which the Cisco UCS Director VM is running.

Recommended Solution—For a multi-node setup, fail over the database by stopping the infrastructure services on the primary node and the service node, replacing the IP address of the master inventory VM with that of the backup inventory VM, and restarting services.

Note This solution is only applicable for a multi-node setup, and if you have a backup of the corrupted database node.

For a single-node setup, deploy a new Cisco UCS Director appliance and restore the database backup using the shelladmin.

Step 1 In the Cisco UCS Director shelladmin, choose `Stop services` to stop the Cisco UCS Director services on the primary node and all service nodes.

Step 2 Replace the IP address of the master inventory VM with that of the backup inventory VM in the following files:

- `/opt/infra/inframgr/service.properties`
- `/opt/infra/eventmgr/service.properties`
- `/opt/infra/idaccessmgr/service.properties`

Step 3 Start the application services on the primary node and the service node.

Troubleshooting Monitoring Database Failures

Problem—The master monitoring database fails.

Possible Cause—Database failures may be caused by:

- A `mysqld` crash, which may occur if the VM is powered off abruptly.
- A power failure on the node on which the Cisco UCS Director VM is running.
- File system corruption on an external datastore on which the Cisco UCS Director VM is running.

Recommended Solution—Fail over the database by stopping the infrastructure services on the primary node and the service node, replacing the IP address of the master monitoring VM with that of the backup monitoring VM, and restarting services.

Step 1 In the Cisco UCS Director shelladmin, choose `Stop services` to stop the Cisco UCS Director services on the primary node and all service nodes.

Step 2 Replace the IP address of the master monitoring VM with that of the backup monitoring VM in the following files:

- `/opt/infra/inframgr/service.properties`
- `/opt/infra/eventmgr/service.properties`
- `/opt/infra/idaccessmgr/service.properties`

Step 3 Start the application services on the primary node and the service node.

Backing up the Monitoring Database in a Multi-Node Setup

Problem—You are unable to back up the monitoring database in a multi-node setup.

Recommended Solution—Edit the `dbMonitoringBackupRestore.sh` script.

Step 1 Edit the `/opt/infra/dbMonitoringBackupRestore.sh` script using vi.

Step 2 Remove the `CHARGEBACK_HISTORY_ENTRY` table name from the script.

Controller Service Does Not Start When Services Are Restarted

Problem—When restarting services, the controller services does not start.

Possible Cause—The hostname of the appliance is changed from the default hostname and the change is not updated in the `/etc/hosts` file.

Recommended Solution—Edit the `/etc/hosts` file to update the hostname:

Step 1 SSH to the appliance using the root account.

Step 2 Edit the `/etc/hosts` to update the new hostname.

Example:

```
vi /etc/hosts
192.0.2.1 newhostname
192.0.2.2 CUCSD_Inventory
192.0.2.3 CUCSD_Monitoring
```

Virtualization

A Blank Screen Appears When Launching the VM Client

Problem—A blank screen appears when launching the VMRC console or the VNC console in a web browser.

Possible Cause—Undetermined.

Recommended Solution—Performing the following step:

If the screen is blank, click in the black area of the screen and press the **Enter** key.

The VMRC HTML5 Console Does Not Launch

Problem—The VMRC HTML5 console does not launch.

Possible Cause—VNC is enabled on the virtual machine.

Resolution—Perform the following steps:

Step 1 Unconfigure the VNC.

Step 2 Power off and power on the VM.

Step 3 Launch the VMRC HTML5 Console again.

Establishing a VNC Session Fails on a VM with vCenter 6.5

Problem—After configuring a VNC on a VM using the **Launch VNC Console** option, the session is not established on vCenter 6.5.

Possible Cause—This issue is caused by vCenter 6.5 functionality.

Recommended Solution—Perform the following step:

To establish the VNC session, you must power off and power on the VM twice. When you unconfigure the VNC client on a VM, you must power off and power on the VM once to terminate the VNC session. This is only applicable for vCenter 6.5.

Storage Policies for a VMware Account are not Listed

Problem—After upgrading or restarting the system running Cisco UCS Director, if you run the Update Storage Policy task, the storage policy is not listed in the **VMware Storage Policy** screen. This screen appears when

you choose **Policies** > **Virtual/ Hypervisor Policies** > **Storage** > **VMware Storage Policy**. This issue occurs intermittently.

Cause—JDO issue.

Recommended Solution—Perform the following steps:

Step 1 Restart the system running Cisco UCS Director.

Step 2 Use VMware - Edit VDC Storage Policy instead of Update Storage Policy.

Issue Registering ESXi Hosts with vCenter Using FQDN

Problem—A DNS or name resolution issue causes ESXi hosts to show up by their IP addresses rather than their desired FQDNs (Fully Qualified Domain Names).

Possible Cause—You may have registered ESXi hosts with vCenter using the Register Host with vCenter task and have them labeled in vCenter by their FQDNs rather than by their IP addresses.

Recommended Solution—Edit the Register Host with vCenter task in the Workflow Designer to ensure proper DNS name resolution. Once completed, you are able to register hosts with their FQDNs.

Note The ESXi hostname and its IP address should be on DNS. Both vCenter and Cisco UCS Director should be able to resolve ESXi hostname (both short and FQDN).

Step 1 In the Workflow Designer, double-click the **Register Host with vCenter** task.

Step 2 On the **User Input Mapping** screen, uncheck **Map to User Input** for the PXE Boot Request ID and Host Node fields.

Step 3 Click **Next**.

Step 4 On the **Task Inputs** screen, uncheck **Register PXE Host**. You are required to enter a host node, user ID, and password.

You can enter the host node in either of the following formats:

${ESXI_HOSTNAME}.domain.com or

${ESXI_HOSTNAME}

Step 5 Click **Next**.

Step 6 Click **Submit**.

Unable to Access VMRC Console Using Google Chrome

Problem—Launching the VMRC console in Google Chrome fails.

Possible Cause—As of January 2015, Google Chrome has stopped supporting the Netscape Plug-in API (NPAPI), which affects the VMRC plug-in.

Recommended Solution—VMware has released a stand-alone VMRC client. You can either use the VMRC stand-alone client, or enable NPAPI and the VMRC plug-in in Chrome.

You can download the stand-alone VMRC client from VMware:

Downloading and Installing the standalone VMware Remote Console (VMRC) in vSphere 5.x and 6.0 (2091284

Note Only administrators can use the VMRC standalone client. It is not currently supported for end users.

Perform the following steps to enable NPAPI and the VMRC plug-in in Chrome:

Step 1 Enable NPAPI in Chrome.

You must enable NPAPI to get the VMRC plug-in working for both vCenter vSphere Web Client and Cisco UCS Director.

See https://support.google.com/chrome/answer/6213033?hl=en.

Step 2 Enable the VMRC plug-in.

By default, the plug-in is disabled.

See https://support.google.com/chrome/answer/142064?hl=en.

VMware Inventory Collector Takes Longer to Run When Using Service Node versus Primary Node

Problem—In a Cisco UCS Director multi-node deployment, when the VMware Inventory Collector task is set to use the service node, the execution duration is twice the time of running the task directly from the primary node.

Possible Cause—There can be various factors contributing to inventory collection performance in the deployment.

Recommended Solution—Perform the following steps:

Step 1 Check the average RTT between the following nodes using the `ping -cc 20 Peer IP or hostname` command:

a) Primary node and VMware vCenter
b) Primary node and inventory node
c) Service node and VMware vCenter
d) Service node and inventory node

Step 2 Run a basic diagnostic in primary and the service node using the diagnostics tool.

Troubleshooting Primary Node Failures

Problem—The primary node fails.

Possible Cause—A primary node failure may be caused by file system corruption on an external datastore on which the Cisco UCS Director VM is running.

Recommended Solution— Promote a service node to the primary node.

Step 1 Log in to the Cisco UCS Director shelladmin on a service node.

Step 2 In the Cisco UCS Director shelladmin, choose `Configure Multi Node Setup (Advanced Deployment).`

The following information displays:

```
Enter: [a/b/x]?
```

Step 3 Enter **a** and press the **Enter** key.

The following information displays:

```
Do you want to configure this node as Primary Node [y/n]?
```

Step 4 Enter **y** and press the **Enter** key.

The following information displays:

```
Configuring Primary Node
Stopping UCS Director Services
Select the IP version you want to configure [a) IPv4, b)IPv6] a/b:
```

Step 5 Enter **a** and press the **Enter** key.

The following information displays:

```
Provide Inventory DB IP:
```

Step 6 Enter the inventory database IP address and press the **Enter** key.

The following information displays:

```
Provide Monitoring DB IP:
```

Step 7 Enter the monitoring database IP address and press the **Enter** key.

The following information displays:

```
Disabling Database service at startup
Starting UCS Director Services
Configured Primary Node Successfully
In order for changes to take effect logout and login back
Do you want to logout [y/n]?
```

Step 8 Enter **y** and press the **Enter** key.

Troubleshooting Inventory Collection Performance Issues

Problem—In a Cisco UCS Director multi-node deployment you may experience performance issues when using a service node to perform inventory collection.

Possible Cause—The execution duration can be directly affected by the following factors:

- Poor disk I/O speed on the external datastore on which the Cisco UCS Director VM is deployed.
- Poor network latency in a multi-node setup.

- Insufficient CPU reservation in the hypervisor.
- Insufficient memory reservation in the hypervisor.

Recommended Solution—Cisco recommends that you deploy Cisco UCS Director VMs in either a local datastore with 25Mbps I/O speed, or an external datastore with 50Mbps I/O speed. Cisco recommends that you reserve at least 3000MHz CPU for the Cisco UCS Director VM in addition to the default number of vCPUs. To troubleshoot any inventory collection performance issues, determine the I/O speed for the local datastore or the external datastore, and determine the round-trip time (RTT) between the following nodes:

- Primary node and VMware vCenter
- Primary node and inventory node
- Service node and VMware vCenter
- Service node and inventory node

Step 1 Run the following command as the root user on the local datastore or the external datastore to determine the I/O speed:

```
dd if=/dev/zero of=/tmp/test1 bs=4096 count=262144 oflag=direct
```

Step 2 Check the average RTT between the nodes using the **ping -cc 20** ***Peer IP or hostname*** command.

Example:

```
ping -c 20 192.0.2.253
```

```
rtt min/avg/max/mdev = 60.474/69.888/134.199/21.529 ms
```

An average RTT below 50 ms is good.

Step 3 If the average RTT value is above 100 ms, work with your network administrator to debug any possible network latency issues to reduce the RTT to under 100 ms.

Troubleshooting VMware Console Display Issues

Problem—The VMware console does not display after an abrupt shutdown of the Cisco UCS Director VM from VMware vCenter.

Possible Cause—Occasionally after Cisco UCS Director VM is powered on, the VMware console prompt gets stuck after the process restart and does not return to the shelladmin.

Recommended Solution—After the VM is powered on, press **Alt-F1** to refresh the VMware console.

In the Cisco UCS Director VM prompt after the VM is powered on, press **Alt-F1**.

The VMware console screen is refreshed.

Unable to Unmount ISO from VM in Cisco UCS Director

Problem—Unable to unmount ISO from CD-ROM through Cisco UCS Director when the warning message is unanswered.

Possible Cause—Whenever an ISO image is mounted to CD-ROM device of a virtual machine, it may be locked by a guest operating system (behavior differs across operating system). When we try to unmount or disconnect the ISO from the CD-ROM, VMWare sometimes prompts the following message.

```
The guest operating system has locked the CD-ROM door and is probably using the CD-ROM,
which prevents the guest from recognizing media changes.
If possible, eject the CD-ROM from inside the guest before disconnecting. Disconnect anyway
 and override the lock?
```

Recommended Solution—Log into vCenter and confirm the message to unmount the ISO from the CD-ROM.

VMware Tasks Are Stuck When VMware vCenter Is Unreachable

Problem—Loss of connectivity between the Cisco UCS Director appliance and VMware vCenter while any of VMware or VMware virtualization tasks are running results in the tasks getting stuck in the "In Progress" state until the infra service is restarted. If connectivity restored, the "In Progress" task remains stuck and does not complete.

Possible Cause—A loss of network connectivity with VMware vCenter occurs after the inventory is started. Changes to network settings in VMware vCenter during inventory can also result in a loss of network connectivity.

Recommended Solution—Update the following timeout property values in the `vmware.properties` file on the appliance and restart the service:

- **wsclient_connection_timeout**—This is the timeout value for establishing a connection between Cisco UCS Director and VMware vCenter prior to collecting any data from VMware vCenter.
- **wsclient_read_timeout**—This is the timeout value for reading data from VMware vCenter using an active connection.

Step 1 Edit the `vmware.properties` file located in the `/opt/infra/inframgr` directory using vi.

Step 2 Update the **wsclient_connection_timeout** and **wsclient_read_timeout** parameters to 45,000 and 60,000 milliseconds, respectively.

Example:

```
#wsclient connection timeout
wsclient_connection_timeout_milliseconds=45000
#wsclient read timeout
wsclient_read_timeout_milliseconds=60000
```

Note Check your network bandwidth prior to updating the timeout values. Networks with high latency may require higher timeout values for establishing connections and collecting data. The timeout values may need to be fine tuned based on the network latency.

Step 3 Restart the infra services the appliance from the shelladmin.

VM Provisioning Fails When a Storage Policy Datastore Capacity Uses the Equals Condition for Decimal Values

Problem—In Cisco UCS Director, VM provisioning fails when the datastore capacity specified in a storage policy uses the **equals** condition for decimal values. For example, if the datastore capacity value is 1109.2 GB in the datastore report, and the same value is added in the storage policy under the minimum conditions - equals 1109.2 GB, VM provisioning fails.

Cause—Cisco UCS Director rounds up the datastore capacity report value to one value after the decimal (tenths place). For example, the value of 1109.15 GB is rounded up to 1109.2 GB.

Recommended Solution—Perform the following steps:

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Storage**.

Step 2 On the **Storage** page, click **VMware Storage Policy**.

Step 3 Click the row with the storage policy that you want to edit.

Step 4 Click **Edit**.

Step 5 On the **Edit Storage Resource Allocation Policy** screen, enter the datastore capacity value rounded up to one value after the decimal in the **Filter Conditions** field.

Example:

For example if the value is 1109.15 GB, it displays as 1109.2 GB in the datastore report. For all options, you must specify any value less than 1109.2 GB but rounded to one value after the decimal, such as 1109.1 GB or 1109.0 GB.

Step 6 Click **Next**.

Step 7 On the **Additional Disk Policies** screen, click **Next**.

Step 8 On the **Hard Disk Policy** screen, click **Submit**.

Static IP Configuration Fails During VM Provisioning

Problem— Static IP address configuration fails while provisioning a VM using a standard catalog with content library templates.

Possible Cause— Static IP address is not assigned only for Ubuntu templates in vCenter 6.0 U3 version.

Resolution— Complete the following step:

Procedure

	Command or Action	Purpose
Step 1	Use vCenter 6.0 or 6.5 versions.	

Content Library Inventory Discovery Fails

Problem—Inventory discovery fails for local and subscribed content libraries.

Possible Cause—Content library inventory discovery may fail if there is a time synchronization issue between Cisco UCS Director and VMware vCenter.

Recommended Solution—Perform the following steps:

Step 1 Verify that the Cisco UCS Director and VMware vCenter systems have the same NTP server configured for content library inventory discovery.

Step 2 Perform the content library inventory discovery.

Duplicate Datastore Cluster DRS Rule Names Causes Issues When Modifying Affinity Type

Problem—When executing the Modify Datastore Cluster DRS Rule task on a datastore cluster with two different rules with the same name, the affinity type does not change.

Possible Cause—Using duplicate names causes issues with the affinity type selection when modifying the datastore cluster DRS rule.

Recommended Solution—Cisco recommends that you create DRS rules with unique names. Once a DRS rule is created, you cannot edit the rule name. If you have two datastore cluster DRS rules with the same name, delete the duplicate rule, and create a new rule with a unique name.

Step 1 Choose **Virtual** > **Storage**.

Step 2 On the **Storage** page, choose the cloud.

Step 3 On the **Storage** page, click **Datastore Clusters**.

Step 4 Click the row with the datastore cluster with the DRS rule you want to modify.

Step 5 Click **View Details**.

Step 6 Click **SDRS Rules**.

Step 7 Click the row with the rule that you want to delete.

Step 8 Click **Delete**.

Cloning a VM causes an error with Cisco Intersight

Problem—When you clone a Cisco UCS Director VM that is claimed in Cisco Intersight, the Device ID is duplicated. As a result, Cisco Intersight claims or calls the wrong Cisco UCS Director VM. The following error message is also displayed:

```
UCS Connect network error
```

Possible Cause—When you clone a Cisco UCS Director VM and set only the IP address, the cloned VM retains the GUID of the original VM. The duplicate GUID of the cloned VM results in an error in Cisco Intersight.

Recommended Solution—Perform the following step:

Assign a GUID to the cloned VM using the Cisco UCS Director Shell menu.

See section *Configuring a Network Interface* in the *Cisco UCS Director Shell Guide, Release 6.7*.

VDC-based VM Deployment Enables IPv6 address by Default

Problem—VDC-based VM deployment enables IPv6 address by default in Windows 2012 OS template.

Possible Cause—VDC based VM deployment enables IPv6 address by default, even when IPv6 is disabled in the Windows 2012 OS template. IPv6 address details are displayed in the VM report instead of IPv4 address details.

Recommended Solution—Perform the following steps:

Step 1 Convert the template to a VM.

Step 2 Run the **Get-NetIPAddress** command to check whether IPv6 address is enabled.

Step 3 Run the following PowerShell command to disable IPv6 address on the VM.

```
New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\services\TCPIP6\Parameters -Name
DisabledComponents -PropertyType DWord -Value 0xffffffff
```

Note You can do this either by launching the web console on the vCenter or by executing the **Guest Operations** task.

Step 4 Restart the Guest OS or reboot the VM.

Step 5 Convert the VM to a template and use it to provision a VM in Cisco UCS Director.

Network

Device Unreachable Error Occurs When Adding an ASA/ASAv to Cisco UCS Director

Problem—A Device Unreachable error occurs when trying to add an Adaptive Security Appliance (ASA) or Adaptive Security Virtual Appliance (ASAV) to Cisco UCS Director.

Possible Cause—Cisco UCS Director uses Internet Control Message Protocol (ICMP) to check connectivity with the management interface of an ASA/ASAv. The ASA/ASAv may not allow and accept the ICMP requests.

Recommended Solution—Ensure that the management interface of the ASA/ASAv allows and accepts ICMP request from Cisco UCS Director.

SSLHandshakeException Error Occurs When Adding an Older Version of VMware vCenter to Cisco UCS Director Version 5.4 or Later

Problem—An SSLHandshakeException occurs when an older version of vCenter is added to Cisco UCS Director version 5.4 or later.

Possible Cause—Cisco UCS Director version 5.4 and later includes a JDK update. The MD2 algorithm is disabled in the JDK so that SSL certificates are signed by default.

Note The MD2 algorithm can be enabled, however, it is disabled by default because of security implications. Enable this setting only if necessary and if you are fully aware of the security concerns.

Recommended Solution—Perform the following steps:

Step 1 Edit the `JDK_HOME/jre/lib/security/java.security` file using vi.

Step 2 Comment out the following line:

```
jdk.certpath.disabledAlgorithms=MD2
```

Example:

```
#jdk.certpath.disabledAlgorithms=MD2
```

Cisco UCS Director 5.4 now connects to older versions of VMware vCenter.

Cisco UCS Director Will Not Add Cisco ASA as a Network Device

Problem—Cisco UCS Director will not add a Cisco Adaptive Security Appliance (ASA) as a network device. The problem occurs with or without a credential policy. The Add Network Element action fails with the Device Unreachable error message.

Possible Cause—ICMP is not enabled on the ASA management port.

Recommended Solution—Enable ICMP on the ASA management port.

For information on configuring ICMP access, see the Cisco ASA Series General Operations CLI Configuration Guide.

Deployment of APIC L4-L7 Services Fails with Deployed Device Present

Problem—During L4-L7 service deployment, the Deploy APIC L4-L7 Services workflow waits for 60 seconds before trying to retrieve the deployed device information from the APIC application and fails. The workflow fails when retrieving the deployed device cluster information even though the deployed device is present on the APIC application.

Possible Cause—Due to network slowness, it may take more than 60 seconds for APIC to gather and populate the deployed device information.

Recommended Solution—Increase the retry frequency to make the workflow wait for a longer period before trying to retrieve the deployed device information. Perform the following steps:

Step 1 Open the Deploy Apic L4-L7 Services workflow in the Cisco UCS Director Orchestrator Workflow Designer.

Step 2 Click the wait task inside the workflow.

Step 3 Change the wait task time interval to a value greater than 60 seconds.

Authentication Failures in Enhanced SSH Command Task Due to Incorrect Authentication Type

Problem—Error Occurs in Authentication Type in SR log.

Possible Cause—This can occur if the authentication key types are not in the supported format.

Recommended Solution—Avoid spelling mistake or invalid characters while passing the authentication type in **Enhanced SSH Command** task. The supported values for the authentication types are rsa, dsa, ecdsa, ed25519, and rsa1. The default value is rsa.

Authentication Failures in Enhanced SSH Command Task

Problem—Error occurs while reading the bytes of key files in SR log.

Possible Cause—This can occur if the given authentication type mismatch with the configured type. Also keys are generated in a custom location but service.properties and ssh_config files are not reflected with custom location.

Recommended Solution—Pass the appropriate authentication type in the task. By default, the SSH Keys will be generated and stored in the location `/root/.ssh`. **service.properties** and **ssh_config** files should get reflected with the custom location path if the user configures the custom location.

service.properties file has the specification about the private key file location for each authentication type. If you have generated the private key into the custom location, you should update the same custom location appropriately to the authentication type in both **service.properties** and **ssh_config** files, in order to connect to the Cisco UCS Director UI and Cisco UCS Director CLI without providing password.

service.properties file is available in the `/opt/infra/inframgr` location.

```
#SSH KEY FILE LOCATION
SSH_PVT_KEY_FILE_RSA=/custom_folder/.ssh/id_rsa
                SSH_PVT_KEY_FILE_DSA=/custom_folder/.ssh/id_dsa
                SSH_PVT_KEY_FILE_ECDSA=/custom_folder/.ssh/id_ecdsa
                SSH_PVT_KEY_FILE_RSA1=/custom_folder/.ssh/identity
                SSH_PVT_KEY_FILE_ED25519=/custom_folder/.ssh/id_ed25519
```

ssh_config file is available in the `/etc/ssh` location.

```
By default, all lines are commented out. Uncomment all the identity files and specify the
custom location.
   IdentityFile /custom_folder/.ssh/identity
   IdentityFile /custom_folder/.ssh/id_rsa
   IdentityFile /custom_folder/.ssh/id_dsa
   IdentityFile /custom_folder/.ssh/id_ecdsa
   IdentityFile /custom_folder/.ssh/id_ed25519
```

Orchestration

Executing Scripts Fails in Custom Tasks while Running Inframgr as Non-Root User

Problem—When executing a workflow, a file might not be accessible through a custom task. As part of the security enhancement, the inframgr service is run with non-root user privilege in the Cisco UCS Director appliance.

Possible Cause—To enhance security, inframgr will no longer run as a root user. The custom tasks which were executed with root privileges will no longer be able to perform root operations on the system. Some custom task that requires root privileges might not succeed.

Recommended Solution—Use the **sudo** command in custom task and add an entry in /etc/sudoers file to add the required permission to file.

The **sudo** command allows running programs with the security privileges of another user (by default, as the superuser).

Step 1 Log in to Cisco UCS Director user interface.

Step 2 Choose **Orchestration** > **Custom Workflow Tasks**.

Step 3 Choose and modify the required custom workflow task.

```
var builder = new ProcessBuilder();
builder.command("sudo",”<</opt/infra/testJVR.sh>>”);
 var process = builder.start();
```

Step 4 Click **Submit**.

Step 5 Log in to Cisco UCS Director as shelladmin using your SSH terminal client.

Step 6 Append the file entry in /etc/sudoers file.

```
Cmnd_Alias UCSD_COMMANDS=<</opt/infra/testJVR.sh>>
(At the end of the line, append the file entry)
```

Step 7 Provide the required permissions to file.

Step 8 In the Cisco UCS Director user interface, choose **Orchestration** > **Custom Workflow Tasks**.

Step 9 Select the required workflow and execute.

Step 10 Click **Submit**.

Folder Creation Fails in Custom Task while Running Inframgr as Non-Root User

Problem—When executing a workflow, creating a folder using the file operation in custom task might not succeed.

Possible Cause—To enhance security, inframgr will no longer run as a root user. The custom tasks which were executed with root privileges will no longer be able to perform root operations on the system. Some custom task that requires root privileges might not succeed.

Recommended Solution—Use the **sudo** command in custom task. The **sudo** command allows running programs with the security privileges of another user (by default, as the superuser).

Step 1 Log in to Cisco UCS Director.

Step 2 Choose **Orchestration** > **Custom Workflow Tasks**.

Step 3 Select and modify the required custom workflow task.

```
var builder = new ProcessBuilder();
builder.command("sudo","mkdir","<</opt/jvr>>");
 var process = builder.start();
```

Step 4 Click **Submit**.

Step 5 Choose **Orchestration** > **Workflows**.

Step 6 Select the required workflow and execute.

Step 7 Click **Submit**.

File Creation Fails in Custom Task while Running Inframgr as Non-Root User

Problem—When executing a workflow, creating a file using the file operation in custom task might not succeed.

Possible Cause—To enhance security, inframgr will no longer run as a root user. The custom tasks which were executed with root privileges will no longer be able to perform root operations on the system. Some custom task that requires root privileges might not succeed.

Recommended Solution—Use the **sudo** command in custom task. The **sudo** command allows running programs with the security privileges of another user (by default, as the superuser).

Step 1 Log in to Cisco UCS Director.

Step 2 Choose **Orchestration** > **Custom Workflow Tasks**.

Step 3 Select and modify the required custom workflow task.

```
var builder2 = new ProcessBuilder();
builder2.command("sudo","touch","<</opt/jvr/testScript.sh>>");
var process2 = builder2.start();
```

Step 4 Click **Submit**.

Step 5 Choose **Orchestration** > **Workflows**.

Step 6 Select the required workflow and execute.

Step 7 Click **Submit**.

PowerShell

Execute PowerShell Command Fails After Upgrading Cisco UCS Director

Problem—The Execute PowerShell command fails after upgrading to the latest version of Cisco UCS Director.

Possible Cause—This command may be fail due to changes to the PowerShell Agent software.

Recommended Solution—Perform the following steps:

Step 1 Check the Cisco UCS Director Release Notes for information on whether a new version of the PowerShell Agent is included in the current version of Cisco UCS Director.

Step 2 If available, download and install a new version of the PowerShell Agent from the upgraded Cisco UCS Director appliance.

Step 3 Choose **Administration** > **Virtual Accounts**.

Step 4 On the **Virtual Accounts** page, click **PowerShell Agents**.

Step 5 Click **Download Installer**.

Step 6 On the **Download Agent Installer** screen, review the installation requirements and click **Submit**.
The executable file (`PSASetup.exe`) is downloaded to your system.

Step 7 Copy the executable file to your target machine.

Step 8 Double-click the `PSASetup.exe` file.

Step 9 Follow the InstallShield Wizard prompts to install the PowerShell Agent.

Unable to Establish PowerShell Connection to Target Server

Problem—Cisco UCS Director is unable to establish the PowerShell connection to the target server.

Possible Cause— TrustedHosts is not enabled on the remote server.

Recommended Solution—Configure WinRM on your VMs.

For more information on configuring WinRM and WinRS, see the Cisco UCS Director PowerShell Agent Installation and Configuration Guide.

Step 1 On both VMs, configure the value " * " in the TrustedHosts table of WinRM by entering the **`winrm set winrm/config/client @{TrustedHosts="*"}`** command.

Example:

```
C:\Users\Administrator>winrm set winrm/config/client @{TrustedHosts="*"}
Client
NetworkDelayms = 5000
URLPrefix = wsman
AllowUnencrypted = false
Auth
Basic = true
Digest = true
Kerberos = true
Negotiate = true
```

```
Certificate = true
CredSSP = false
DefaultPorts
HTTP = 5985
HTTPS = 5986
TrustedHosts = *
```

Step 2 On your hosts, enter the **winrm quickconfig** command.

Example:

```
C:\Users\Administrator>winrm quickconfig
WinRM service is already running on this machine.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:

Configure LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.

Make these changes [y/n]?
```

Step 3 Enter **y**.

WinRM is updated for remote management.

Example:

```
Make these changes [y/n]? y
WinRM has been updated for remote management.
Configured LocalAccountTokenFilterPolicy to grant administrative rights remotely to local users.
```

Step 4 Verify that WinRS is enabled by entering the **winrm g winrm/config** command at a command prompt.

Storage

File System Mounted as Read-only on Cisco UCS Director

Problem—A Linux filesystem is mounted as read-only on Cisco UCS Director.

Possible Cause—A common Linux file system approach to dealing with intermittent storage loss is that when the file system comes back up, it is mounted as read-only.

Recommended Solution—Perform the following steps:

Step 1 Unmount the file system using the **umount** command.

Example:

```
# umount /mount-point
```

Step 2 Run the **fsck** command to reset the file system state.

Example:

```
# fsck /mount-point
```

Step 3 Reboot the VM.

Reporting

Catalog Is Not Visible by End User and Group Admin

Problem—The catalog is not visible by the end user and group admin.

Possible Cause—The catalog report may be hidden on the reports customization page.

Recommended Solution—Perform the following steps to show the report:

Step 1 Choose **Administration** > **User Interface Settings**.
Step 2 On the **User Interface Settings** page, click **Reports Customization**.
Step 3 Click the row with the catalog report.
Step 4 Click **Edit**.
Step 5 On the **Customize Report** screen, uncheck **Hide Report** to show the report.
Step 6 Click **Save**.

VM Chargeback Information Does Not Appear

Problem—A cost model is applied to a VDC, but the VM chargeback information does not appear on the **Resource Accounting Details** tab.

Possible Cause—VM metering is disabled. Chargeback does not work when VM metering is disabled.

Recommended Solution—Perform the following steps to enable VM metering:

Step 1 Choose **Administration** > **System**.
Step 2 On the **System** page, click **Advanced Controls**.
Step 3 Check **Resource Metering** and **VM Metering**.
Step 4 Click **Submit**.

UCS Director Upgrade

Cisco UCS Director Fails with Flex Error 1001: Digest Mismatch with RSL

Problem—After upgrading Cisco UCS Director, access to the GUI sometimes fails with the following error, immediately after logging in:

```
Flex Error #1001: Digest mismatch with RSL
    http://10.5.40.10/app/cloudmgr/cloupia_common.swf. Redeploy the matching RSL or
    relink your application with the matching library.
```

Possible Cause—This can happen after an upgrading the Cisco UCS Director appliance. Exact conditions are currently not known.

Recommended Solution—Cisco recommends the following workarounds:

Step 1 Clear the browser cache.

Step 2 Restart the browser (or all open browsers).

Step 3 Use a different browser.

Step 4 Reset the browser as described in the following documents. This erases any previously configured browser settings.

- For Firefox, see https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings.
- For Internet Explorer, see http://windows.microsoft.com/en-us/internet-explorer/reset-ie-settings#ie=ie-11.

Cisco UCS Director Upgrade Does Not Respond

Problem—When applying a patch upgrade to the nodes of a Cisco UCS Director single-node or multi-node deployment, the upgrade does not respond.

Possible Cause—This can occur if the time on the nodes is not synchronized.

Recommended Solution—Resync the NTP time and time zone information on each node:

Step 1 Stop the upgrade in process.

Step 2 Manually resync the NTP server settings using the **Time Sync** shell admin option in the standalone (single-node) node, primary node, service node, inventory node, and monitoring node.

Step 3 Restart the upgrade process.

Websock Service Is Down After Upgrading Cisco UCS Director

Problem—After upgrading Cisco UCS Director, the websock service does not come up when the VM is powered on.

Possible Cause—The SSL or Certification Authority (CA) certificates may have not been generated for and imported into the upgraded Cisco UCS Director system.

Recommended Solution—Perform the following steps to generate and import the SSL or CA certificates:

Step 1 Generate and import the SSL or CA certificates prior to upgrading, or after upgrading from any previous release.

Note If you previously used a CA certificate, you must re-import the certificate using the shelladmin.

For information on managing SSL and CA certificates, see the Cisco UCS Director Shell Guide.

Step 2 From the Cisco UCS Director Shell menu, choose **`Start Services`** to restart the services.

Step 3 Choose **`Display Services Status`** to verify that the websock service is up.

After Upgrading to Release 6.5, Monitoring and Inventory DB nodes Do Not Show Service Status

Problem—In a multi-node evironment, after upgrading to release 6.5, the monitoring and inventory database nodes do not show the status of the services.

Possible Cause—Credential mismatch between the nodes.

Recommended Solution—Complete the following steps after upgrading the monitoring and inventory database nodes to Release 6.5:

Step 1 Login to the Shell Admin console on the monitoring and inventory database nodes.

Step 2 Select option 18 - **Reset MySQL User Password**.

Step 3 When prompted to reset the password, enter **`cloupia`** as the new password.

Step 4 Select option 2 - **Display Service Status** to determine the status of the database services.

Step 5 After verifying that all services are up and running, for better security, reset the `mysql db` password on all the nodes in the following order:

- Inventory node
- Monitoring node
- Primary node
- Service node

After Upgrading, Services on Primary and Service Nodes Do Not Start

Problem—After upgrading to release 6.5, services on the primary node and service node do not start.

Possible Cause—The database nodes (monitoring and inventory nodes) are not accessible.

Recommended Solution—Perform the following steps after upgrading the primary node and service node to release 6.5:

Step 1 On Primary and Service nodes, create a folder titled `mysql` in the `/opt/certs` location.

Step 2 Manually copy the `/opt/certs/mysql/dbkeys.key` and `/opt/certs/mysql/dbcreds.properties` files from any of the database nodes to the `/opt/certs/mysql` folder in the Primary and Service nodes.

Step 3 Reset the `mysql db` password on all the nodes in the following order:

- Inventory node
- Monitoring node

- Primary node
- Service node

Cisco UCS Director REST API

Execute REST API Fails after Upgrading Cisco UCS Director

Problem—The JSON API requests which have a payload that contains array ([ ]) as part of it are responded with a 400 bad request.

Example

```
https://x.x.x.x/app/api/rest?formatType=json&opName=userAPISubmitWorkflowServiceRequest&opData=
{param0:"sample",param1:{"list":[{"name":"sample","value":"sample"},{"name":"sample","value":"sample"}]},
param2:1000}
```

- This URL responds with a 400 status code on Cisco UCS Director release 6.7 when accessed from a browser or any other REST client.
- This URL responds with a 200 status code on Cisco UCS Director release 6.6 when accessed from a browser or any other REST client.

Possible Cause—This issue is due to modifications in Tomcat server configuration in version 6.7. Newer versions of Tomcat do not allow the array ([ ]) character in the URL of a HTTP request as it is against the HTTP 1.1 specification.

Recommended Solution—To fix this issue, URL must be encoded as shown below:

```
https://x.x.x.x/app/api/rest?formatType=json&opName=userAPISubmitWorkflowServiceRequest&opData=
%7bparam0:%22sample%22,param1:%7b%22list%22:%5b%7b%22name%22:%22sample%22,%22value%22:%22sample%22%7d,
%7b%22name%22:%22sample%22,%22value%22:%22sample%22%7d%5d%7d,param2:1000%7d
```

Other characters that need to be encoded are: |, {, }, [,], \, \\, ^, `

If encoding is not preferred, mention the characters (|, {, }, [,], \, \\, ^, and `) in the `server.xml` configuration file.

Add the following line to the `server.xml` file in the Tomcat server (in the Cisco UCS Director appliance, the file is located at the `/opt/infra/web_cloudmgr/apache-tomcat/conf` path):

```
relaxedQueryChars="|,{,},[,],\,\\,^,`"
```

Configuration now should look like this:

```
<Connector SSLEnabled="true" URIEncoding="UTF-8"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_RSA_WITH_AES_128_CBC_SHA256,
 TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA"

clientAuth="false" keystoreFile="keystore/.keystore" keystorePass="cloupia123"
maxHttpHeaderSize="65536"
maxPostSize="-1" maxThreads="150" port="8443" protocol="HTTP/1.1" scheme="https" secure="true"
 server="Web"
sslEnabledProtocols="TLSv1.2,TLSv1.1" sslProtocol="TLS" relaxedQueryChars="|,{,},[,]"/>
```

```
<Connector URIEncoding="UTF-8" maxHttpHeaderSize="65536" maxPostSize="-1" port="8080"
protocol="HTTP/1.1"
redirectPort="443" server="Web" relaxedQueryChars="|,{,},[,],\,\\,^,`"/>
```

Note The services must be restarted after making the changes.