Troubleshooting VM Lifecycle Management

Issues with Image Creation

This section includes symptoms, possible causes, and solutions for issues associated with creating an image.

Symptom: CentOS 7.X stops working after binary updates.

Possible Cause: When CentOS systems are manually or automatically updated using yum, the systems are upgraded to the latest release of CentOS 7.x. In result, CentOS 7.x stops working because the upgraded version may not be supported by Intercloud Fabric.

Note Historically, CentOS releases corresponded in a sequential manner to the minor or major releases of RHEL (for example, CentOS 6.1 release corresponded with RHEL 6.1 release). With CentOS 7.x, the model changed and versions are not upgraded in a sequential manner, but to the newest version available.

Verification and Solution: To limit kernel updates on CentOS to supported levels of CentOS 7.x and prevent automatic kernel updates, do the following:

1. Edit /etc/yum.conf.
2. Add the following to the main package repository:
   ```
   exclude=kernel* redhat-release* centos-release*
   ```

Symptom: Uploading a RHEL/CentOS 7.X OVA image during catalog creation and image upload fails with error message:

Error Message:

```
The configuration file for interfaces <interface name> cannot be found.
Fix the configuration in the Guest OS and retry importing the image.
For further details, refer to the Troubleshooting Guide.
```

Possible Cause: RHEL/CentOS systems name network devices in a predictable manner based on BIOS/PCI physical hotplug slot information. When a VM running on ESX is exported as an OVA image, sometimes VMware vSphere changes the PCI topology on the exported OVA causing a mismatch between the interface configuration file inside the OVA image and the OVA description of the NIC PCI hotplug slot. This inconsistency between what is described in the OVA compared to what is actually configured and present in the OVA image causes Intercloud Fabric to reject the image.

Verification and Solution: Deploy the OVA in the VMware vSphere environment and ensure the NIC names, as seen by the OS and device names, match. Fix any mismatched names and retry the upload.

Symptom: Image creation fails with the error "OS not compatible:VMware tools not present on VM".

Error Message:

```
Jan 24, 2015 03:26:47 GMT Image Creation in Progress: 96 %
Jan 24, 2015 03:26:47 GMT Creating Image: OS not compatible:VMware tools not present
on VM
Jan 24, 2015 03:26:47 GMT Retrying: 2
```

Verification and Solution: Confirm the following:

- The image operating system (OS) is supported.
- VMware tools are installed in the VMware vCenter client.

Symptom: Image creation fails with the error "Cannot find appropriate ICA image".

Error Message:

```
Jan 23, 2015 23:35:15 GMT Handler failed with error - Cannot find appropriate ICA image
 for the VmImage org-root/vm-img-CiscoITRH64smallscp, selectedContext=<None>
Jan 23, 2015 23:35:15 GMT Task #1 (InterCloud Create Image (Create Image in Cloud))
failed after 0 seconds
```

Verification and Solution: In the VMware vCenter client, confirm that the image is based on a supported guest OS version.

Symptom: Intercloud Fabric 2.3.1 only supports Master Boot Record (MBR)-based partition tables. As a result, disks with a GUID Partition Table (GPT) fail and display an error message.

Error Message:

```
Unsupported operating system.
```

Possible Cause: Intercloud Fabric does not support the GPT standard for disk partition tables for both Windows and Linux operating systems. Possible conditions include:

- An on-board VM is moved back to the private cloud.
- The VM is moved from the private cloud to the cloud.
- The user uploads an OVA on ICFC.

This problem might also occur during VM migration.

Verification and Solution: Check the partition style on the VM.

For Linux, run the command:

```
fdisk -lu
```

For Windows:

1. Choose **Start > Control Panel**.
2. In the Control Panel, choose **System and Security > Administrative Tools > Computer Management**.
3. Select **Disk Management**.
4. Right-click **Disk 0** and choose **Properties**.
5. Click the **Volumes** tab and check the **Partition style** for the disk.

Issues with Linux Cloud VMs

This section includes symptoms, possible causes, and solutions for issues associated with Linux VMs on public clouds.

Symptom: Red Hat/CentOS-style cloud VMs deployed in Azure with Intercloud Fabric might route traffic incorrectly.

Possible Cause: There might be two default routes in the IP routing table. For example, in the Red Hat 6.1 CVM and earlier, after ICF access tunnel comes up:

- Azure provisions one cloud interface (csc0) in subnet 10.200.0.0/16 with a default route configured through 10.200.0.1.
- Intercloud Fabric provisions one overlay interface (eth0) in subnet 10.2.0.0/24 with a default route configured through 10.2.0.75.

```
[root@rhel61-lnic ~]# ip route list
168.63.129.16 via 10.200.0.1 dev csc0
168.63.129.16 via 10.200.0.1 dev csc0  proto static
10.2.0.0/24 dev eth0  proto kernel  scope link  src 10.2.0.11
169.254.0.0/16 dev csc0  scope link  metric 1002
169.254.0.0/16 dev eth0  scope link  metric 1003
10.200.0.0/16 dev csc0  proto kernel  scope link  src 10.200.0.5
default via 10.2.0.75 dev eth0 <--- default route over overlay interface 'eth0' towards
 the enterprise
default via 10.200.0.1 dev csc0  proto static <--- default route over provider interface
 'csc0'
[root@rhel61-lnic ~]#
```

Verification and Solution: Delete the default route that directs traffic over the csc0 provider interface. For example, delete the default route over the provider interface for the following Red Hat 6.1 VM:

```
[root@rhel61-lnic ~]# route delete default gw 10.200.0.1
[root@rhel61-lnic ~]# ip route list
168.63.129.16 via 10.200.0.1 dev csc0
168.63.129.16 via 10.200.0.1 dev csc0  proto static
10.2.0.0/24 dev eth0  proto kernel  scope link  src 10.2.0.11
169.254.0.0/16 dev csc0  scope link  metric 1002
169.254.0.0/16 dev eth0  scope link  metric 1003
10.200.0.0/16 dev csc0  proto kernel  scope link  src 10.200.0.5
default via 10.2.0.75 dev eth0 <---- Now there is only one default route via the overlay
 interface 'eth0'
[root@rhel61-lnic ~]#
```

Issues with Windows Cloud VMs

This section includes symptoms, possible causes, and solutions for issues associated with Windows VMs on public clouds.

Symptom: Image creation and VM migration fails for Windows 2008 R2 with the error "Missing SHA-256 sig Verification and processing Support".

Error Message:

```
Windows 2008R2: Missing SHA-256 signatures Verification and processing Support. Please install

https://technet.microsoft.com/en-us/library/security/3033929https://support.microsoft.com/en-us/kb
```

Verification and Solution: Install the following updates on the TemplGuest OS:

- Patch: https://technet.microsoft.com/en-us/library/security/3033929
- Hotfix KB: https://support.microsoft.com/en-us/kb/2921916

This step is only required for Windows Server 2008 R2.

Symptom: There is no connectivity to the Windows cloud VM.

Possible Cause: There might be a memory leak, an unopened port, or a variety of other problems.

Verification and Solution:

1. Verify Windows cloud VM reachability by using **SSH** and a public IP address, or by using **RDP** or **ping** (if available):
   a. Check the cloud VM status in the Amazon Elastic Compute Cloud (EC2) console.
   b. If the EC2 status shows "2/2 checks passed" and "running," reboot the cloud VM from the EC2 console and check connectivity.
   c. After connectivity is restored, review the system event logs for any relevant errors by using **eventvwr.msc**.
   d. If the system event logs do not contain any obvious errors, a memory leak might exist. Use **perfmon.exe** to isolate any excessive, nonpaged pool usage during upcoming boot sessions.
2. Review the EC2 firewall settings for the Windows cloud VM and ensure that the necessary ports are open:
   - TCP and UDP port 6644
   - TCP port 22

Symptom: There is an issue related to the Windows cloud VM subagent.

Possible Cause: The subagent process is not running or is not listening on the correct TCP port.

Verification and Solution: Try any of the following solutions:

- Confirm that the `sub_agent.exe` file is present in the `C:\Program Files\Cisco\ICA` folder. If the file is not present, copy it to the folder.
- In a command window, determine whether the subagent process is running.

```
c:\>tasklist /FI "imagename eq sub_agent.exe"
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
sub_agent.exe                 2616 Services                   0      4,508 K
```

  If the agent is not running, start it.

- Confirm that the subagent process is listening on TCP port 6644.

```
c:\>netstat -anB

Active Connections
  ...
  TCP    0.0.0.0:6644           0.0.0.0:0              LISTENING
 [sub_agent.exe]
  ...
```

Symptom: There is no connectivity to the SSH server.

Possible Causes:

- The `vm_trust.properties` file does not exist.
- The SSH server is not running.
- The SSH server is not listening on the correct TCP port.
- The SSH public key for the root user cannot be retrieved.

Verification and Solution: Try any of the following solutions:

- If the subagent process is running, but the process is not listening on TCP port 6644, determine whether or not the `C:\Program Files (x86)\Cisco\vm_trust.properties` file exists.

  If the `vm_trust.properties` file is absent, determine whether or not the SSH server is running:

```
c:\>sc query freesshdservice
SERVICE_NAME: freesshdservice
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

  If the SSH server is not running, confirm that the SSH server directory is populated with the necessary files:

```
c:\>dir "C:\Program Files (x86)\Cisco"\
 Volume in drive C has no label.
 Volume Serial Number is 7C21-C2FC
 Directory of C:\Program Files (x86)\Cisco
07/16/2013  05:23 AM    <DIR>          .
07/16/2013  05:23 AM    <DIR>          ..
07/16/2013  02:28 AM               672 DSAKey.cfg
07/16/2013  02:28 AM               256 freesshd.log
03/29/2013  07:33 PM         1,360,896 FreeSSHDService.exe
07/16/2013  02:28 AM             1,096 FreeSSHDService.ini
07/16/2013  02:27 AM               386 root
```

- Determine whether or not the SSH server is listening on TCP port 22 and SSH connections can be established:

```
c:\>netstat –anB

Active Connections
  ...
  TCP    0.0.0.0:22             0.0.0.0:0              LISTENING
 [FreeSSHDService.exe]
 ...
```

- Determine whether or not the SSH public key for the root user can be retrieved successfully by using the **wget.exe** command from the EC2 VM user data:

```
C:\Program Files\Cisco\ICA\wget.exe -t 1 --bind-address [peth IP] -O
C:\Windows\Temp\ec2pubkey
http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Symptom: There is an issue related to the Intercloud Agent Service (ICASVC).

Possible Cause:

- The ICASVC is not installed.
- The ICASVC is not running.
- The ICASVC is not set to the AUTO_START startup type.

Verification and Solution: Try any of the following solutions:

- If the ICASVC is not installed, determine whether or not the following registry entry is present:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\ICASvc]
"Type"=dword:00000010
"Start"=dword:00000002
"ErrorControl"=dword:00000001
"ImagePath"=hex(2):22,00,43,00,3a,00,5c,00,50,00,72,00,6f,00,67,00,72,00,61,00,\

  6d,00,20,00,46,00,69,00,6c,00,65,00,73,00,5c,00,43,00,69,00,73,00,63,00,6f,\
  00,5c,00,49,00,43,00,41,00,5c,00,49,00,63,00,61,00,53,00,76,00,63,00,2e,00,\
  65,00,78,00,65,00,22,00,00,00
"DisplayName"="Cisco InterCloud Agent Service"
"ObjectName"="LocalSystem"
"Description"="Cisco InterCloud Agent Service"
```

  If the registry entry is absent, import the ICASVC key into `HKLM\System\CCS\Services`.

- Determine whether or not the ICASVC is set to the AUTO_START startup type:

```
c:\>sc qc icasvc
[SC] QueryServiceConfig SUCCESS
SERVICE_NAME: icasvc
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\Program Files\Cisco\ICA\IcaSvc.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Cisco InterCloud Agent Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

Symptom: The ICASVC startup scripts are not running.

Possible Cause: The startup scripts are not present in the correct folder.

Verification and Solution: Confirm that the `StartIca.vbs`, `StartSubagent.vbs`, and `start_subagent.bat` files reside in the `C:\Program Files\Cisco\ICA` folder.

Symptom: The cloud VM loses connectivity with the private data center.

Possible Cause: The certificate is not installed or is not correct.

Verification and Solution:

1. Confirm that the `ctdrv.sys` and `ctmp.sys` files are present in the `C:\Program Files\Cisco\ICA` folder.
2. Confirm that the Windows ICA driver certificate is installed:

```
C:\Program Files\Cisco\ICA>CertMgr.exe /s TrustedPublisher
==============Certificate # N ==========
Subject::
  [0,0] 2.5.4.6 (C) US
  [1,0] 2.5.4.8 (S) California
  [2,0] 2.5.4.7 (L) San Jose
  [3,0] 2.5.4.10 (O) Cisco Systems, Inc
  [4,0] 2.5.4.11 (OU) Digital ID Class 3 - Microsoft Software Validation v2
  [5,0] 2.5.4.3 (CN) Cisco Systems, Inc
...
```

Symptom: Encrypted or encapsulated packet injection is not working.

Possible Cause: Weak host sends and receives are enabled.

Verification and Solution: For encrypted or encapsulated packet injection to work, the provider adapter must have weak host sends and receives disabled, which is the default setting.

1. Determine whether weak host sends and receives are enabled or disabled:

```
> netsh interface ipv4 show interfaces level=verbose
Interface Local Area Connection 2 Parameters
...
Weak Host Sends                  : disabled
Weak Host Receives               : disabled
...
```

2. If weak host sends and receives are enabled, disable them:

```
> netsh interface ipv4 set interface [InterfaceNameOrIndex] weakhostsend=disabled
> netsh interface ipv4 set interface [InterfaceNameOrIndex] weakhostreceive=disabled
```

Symptom: The access tunnel with the Windows VM is broken.

Possible Cause: Third-party Windows Filtering Platform (WFP) filters are blocking datagrams on TCP port 6644 or the UDP port over which the subagent has initiated the Datagram Transport Layer Security (DTLS) connection.

Verification and Solution: Enter the following command and examine the output:

```
> netstat -anB
```

- To determine whether or not the UDP port is causing the problem, look for the `subagent.exe` port.
- To determine whether or not third-party WFP filters are causing the problem, look at the sysinfo section of the output for WFP filters for Windows VMs.

To resolve the issue, restart the services.

Symptom: There is an issue with the data path between the overlay miniport and the cloud provider miniport.

Possible Cause: Third-party Network Driver Interface Specification (NDIS) intermediate drivers or additional NDIS miniports are affecting the data path between the overlay miniport and the cloud provider miniport.

Verification and Solution: Enter the following command and examine the output:

```
> netstat -anB
```

All NDIS drivers are enumerated in the sysinfo section of the output for Windows VMs.

Symptom: Cloud VM deployment fails for one of the two interfaces.

Possible Cause: By default, port profiles are named "icfCloud" if a name is not provided during Intercloud Fabric tenant configuration.

Verification and Solution: When deploying cloud VM, make sure you have a network policy defined with port profiles for each vNIC that is on the same tenant. When modifying the port profiles after deploying the cloud VM, configure the appropriate tenant on the port profile that does not violate the deployment solution.

Symptom: Migrating a Windows 2012 VM or importing a Windows 2012 VM OVA fails with the error, "VM Guest OS was not shutdown gracefully. Please resume and shutdown Windows fully prior to initiating import or move actions on this VM image".

Possible Cause: ICF detected that the VM did not shut down gracefully prior to the user initiating a VM migration or exporting it as an OVA from the VMware vCenter client. Not shutting down the guest OS gracefully can corrupt the file system.

Verification and Solution: Power on the VM in the VMware vCenter client and shut down the guest OS. After the guest OS has shut down, reinitiate the request to migrate the VM or export the OVA from the VMware vCenter client.

Issues with Monitoring VMs

This section includes symptoms, possible causes, and solutions for issues associated with monitoring VMs.

Symptom: The VM statistics in the end-user portal show VMs that do not exist.

Possible Cause: The VMs were deleted from the VMware vCenter client; however, they still appear because the periodic refresh did not occur.

Verification and Solution: Manually refresh the VM list.