Troubleshooting the Cisco Intercloud Fabric Installation and Initial Setup

Issues with the Infrastructure Setup

This section includes symptoms, possible causes, and solutions for issues encountered while setting up the Intercloud Fabric infrastructure.

Symptom: An infrastructure update is not supported after infrastructure creation is aborted.

Error Message:

```
An infrastructure update is not supported after infrastructure creation is aborted.
Delete the existing infrastructure and recreate it. For details, see the Troubleshooting
 Guide.
```

Possible Cause: After infrastructure creation is aborted, an infrastructure update is not supported and will return an error if it is attempted.

Verification and Solution: Delete the existing infrastructure and recreate it. For details, see the Troubleshooting Guide.

Symptom: A service request remains stuck in a *Not_Started* or an *In_Progress* state.

Possible Cause: The symptom is caused by a known bug.

Verification and Solution:

If the service request remains in a *Not_Started* or an *In_Progress* state for an abnormal period of time, do the following:

1. SSH into the system console.
2. Restart services. This will result in moving the service request to a *System_Aborted* state.

After the service request is moved into a *System_Aborted* state, do the following:

1. Perform the operation again through the Intercloud Fabric UI, if allowed.
2. If the operation fails or is not permitted, you must first delete the object and then create it again.

Symptom: Logging on to Intercloud Fabric from the browser fails.

Possible Cause:

- The browser URL may be incorrect.
- Check for any services errors. In addition, log in as the administrator to the Intercloud Fabric VM CLI and check if all services are up on Intercloud Fabric by selecting option **3**, Show Services Status.

Verification and Solution: Use the obtained information to resolve the issue.

Symptom: The Intercloud Fabric browser log in fails and the CLI Show Services Status (option 3) shows that services are not running.

Verification and Solution: To resolve, log in as an administrator to the Intercloud Fabric VM CLI and use option **4** to Start Services or option **5** to Stop Services.

Symptom: Intercloud Fabric OVA deployment fails.

Possible Cause: Perform the following steps to identify the cause:

1. In VMware vCenter, review the recent tasks.
2. Review the information highlighted in red for the possible cause of the failure.
3. Select both the **Tasks** and **Events** tab and review any event highlighted in red for the possible cause of the failure.

Verification and Solution: Based on the possible causes, debug the issue accordingly.

Symptom: The Intercloud Fabric VM fails to power on after deployment.

Possible Cause: The mandatory OVA parameter fields were not correctly entered.

Verification and Solution: Reenter the mandatory OVA parameter fields.

Symptom: The Intercloud Fabric UI, API, and CLI fails to launch and you are prompted to reenter OVA parameters in the console.

Possible Cause: The mandatory IP address fields in OVA contain a value of 0.0.0.0.

Verification and Solution: Update the mandatory IP address fields in OVA.

Symptom: An error occurs when attempting to upload a Cisco Intercloud Fabric image `tar` file.

Possible Cause: This issue occurs if you use a browser other than Chrome. If you are using Chrome, it is possible that the image `tar` file did not upload completely.

Verification and Solution:

1. If you are not using the Chrome browser, use Chrome and try again.
2. If you encounter the error again, enable the root account by using the shelladmin credentials. The password for the shelladmin account is the same password that was entered when deploying the Intercloud Fabric appliance.
3. Use the **scp** command to copy the `tar` file into the `/opt/infra/uploads` folder of Intercloud Fabric.
4. On the **Images** page of the **Infrastructure Setup** dialog, click **Browse** and select the file from the local desktop.
5. Click **Next**.

   Note Do not click the **Upload** button.

6. Proceed with the remainder of the setup.

Symptom: The Intercloud Fabric image fails to successfully import into Intercloud Fabric Controller (ICFC).

Error Message:

```
Handler failed with error - Image Upload Failed: End point timed out.
Check for IP, password, space, or access related issues.
```

Possible Cause: ICFC cannot connect to Cisco Intercloud Fabric.

Verification and Solution: If the import operation does not complete within a reasonable amount of time, check the **Recent Jobs** list in ICFC for the status and any error messages. The **Task** line item lists the last error encountered, if any, while importing and the number of retries attempted.

Symptom: After restarting ICFC services, the job for importing an Intercloud Fabric image shows as running, but the job does not progress.

Possible Cause: If ICFC services are restarted while the import operation is running, the task does not resume.

Verification and Solution: Cancel the job in Intercloud Fabric and import the image again.

Symptom: The ICFC server cannot resolve hostnames to IP addresses.

Error Message:

```
ICFC cannot reach Public IP address
```

Possible Cause: The DNS server IP address is not entered correctly in the device profile. The DNS server resolves the hostname to an IP address. If ESX hosts were added to the VMware vCenter client using hostnames instead of IP addresses, those hostname-to-IP address mappings must exist in the DNS server.

Verification and Solution: Ensure that the DNS server IP address is entered correctly in the device profile, as follows:

1. In the **Policies** tab, choose **Intercloud Infrastructure Policies**.
2. If the DNS server IP address is incorrect, click **Edit** and enter the correct IP address.

For more information about configuring the DNS server IP address, see the *Cisco Intercloud Fabric Administrator Guide*.

Symptom: Intercloud Fabric displays an error regarding the shared secret.

Possible Cause: A shared secret that exceeds 11 characters was entered in Intercloud Fabric.

Verification and Solution: Ensure that the shared secret does not exceed 11 characters.

Symptom: While deploying an Intercloud Fabric OVF image, VMware vSphere displays the error, "The OVF package is invalid and cannot be deployed. The provided network mapping between OVF networks and the system network is not supported by any host."

Possible Cause: The VMware distributed virtual switch (DVS) is out of synchronization.

Verification and Solution: Ensure that the VMware DVS is properly synchronized with all hosts. For information about synchronizing the VMware DVS, see the VMware vSphere documentation.

Symptom: When using a VMware virtual switch to host the Intercloud Fabric Extender, any of the following occur:

- Traffic is lost.
- Duplicate packages are sent in private cloud and cloud VM traffic.
- Flapping occurs between the Intercloud Fabric Switch module and the Intercloud Fabric VSM.

Possible Cause: If Intercloud Fabric Extender is hosted on a VMware vSwitch or distributed switch and if the vSwitch or distributed switch is connected to multiple physical NICs, you must enable the setting **Net.ReversePathFwdCheckPromisc=1** in the ESX host where the Intercloud Fabric Extender is hosted. This situation can occur if the setting **Net.ReversePathFwdCheckPromisc=1** is not enabled in the ESX host where the Intercloud Fabric Extender resides.

Verification and Solution: Enable the setting **Net.ReversePathFwdCheckPromisc=1** in the ESX host where the Intercloud Fabric Extender is hosted. The setting is found under **Host > Configuration > Advanced Settings > Net** in the VMware vSphere GUI.

Note If the value of the *Net.ReversePathFwdCheckPromisc* configuration option is changed while the ESXi host is running, toggle (disable then re-enable) the **Promiscuous Mode** check box in the Intercloud Fabric Extender trunk port group security settings for the change to take effect.

- For a VMware virtual switch, set the trunk port group to allow **All** VLAN IDs in the VMware vSphere GUI.
- For a security policy for the trunk port group on the VMware virtual switch, set the Promiscuous Mode, MAC Address Changes, and Forged Transmits to **Accept** in the VMware vSphere GUI. This requirement applies only if you are using a VMware virtual switch. It does not apply if you are using a Cisco Nexus 1000V switch.