WNDRVR
SUPPORT NETWORK

WIND RIVER HELIX DEVICE CLOUD TROUBLESHOOTING GUIDE, EDITION 4

Corporate Headquarters

Wind River
500 Wind River Way
Alameda, CA 94501-1153
U.S.A.
Toll free (U.S.A.): +1-800-545-WIND
Telephone: +1-510-748-4100
Facsimile: +1-510-749-2010

For additional contact information, see the Wind River website:

www.windriver.com

For information on how to contact Customer Support, see:

www.windriver.com/support

Wind River Helix Device Cloud Troubleshooting Guide, Edition 4

27 January 2019

1. WIND RIVER HELIX DEVICE CLOUD TROUBLESHOOTING GUIDE, EDITION 4

2. TROUBLESHOOTING HELIX DEVICE CLOUD

Network or device configuration issues can prevent the device from connecting to the server. Before investigating issues on a specific device, ensure that port 443 is open on the firewall on the network to which the device connects or that you configured proxy server information correctly, if applicable.

For connectivity issues you can also check the status of Helix Device Cloud services at https://status.helixdevicecloud.com.

To diagnose issues on a device, you need physical or network access to the device other than through Helix Device Cloud.

To diagnose issues with software updates, you need information about the package contents and the operating system to which the update applies.

3. TROUBLESHOOTING ON WIND RIVER LINUX AND IDP XT

1. Diagnosing Initial Connectivity Failures on Wind River Linux and IDP XT

If a device running Wind River Linux or IDP XT does not appear in the device list on the management console after initial deployment, you may have a problem with the agent authentication or basic network setup.

Perform all steps in this section on the device.

Prerequisites

You need the following:

- physical access to the device or network access to the device, for example through SSH (enabled by default on devices running Wind River Linux and Wind River IDP XT)
- for SSH access, the IP address or host name of the device and an SSH client on your host
- superuser privileges on the device

Procedure

1. Verify that the agent authentication information is correct.
    1. Verify that the current device ID appears.

```
# iot-control
Looking for configuration file: /etc/iot/iot.cfg
Looking for configuration file: /var/lib/iot/iot.cfg
Looking for configuration file: /home/user/iot.cfg
Looking for configuration file: ./iot.cfg
Current device id: 5C1FB6BB-4FE8-E8FA-0FBC-AC12ABE36C18
Proxy's type (none/http/socks5/Enter to skip):
```

    In this example, the device ID is 5C1FB6BB-4FE8-E8FA-0FBC-AC12ABE36C18.

    2. To exit, press **ENTER** three times.
    3. If no device ID is present, check that the **startup.bin** file is present in the **/var/lib/iot** directory.

    If the **startup.bin** file is missing, check that you ran the iot-config.py script when you built your platform project and specified the **SECURITY_BUNDLE** key. For more information, see the following:

    Building Your Wind River Linux Platform Project for Intel Target Devices
    Building Your Wind River Linux Platform Project for ARM Target Devices
    Building Your Wind River IDP XT Platform Project

    4. If the **startup.bin** file is present, ensure that the file has read permissions for all users.

    If the **startup.bin** file has read permissions, it may not contain authentication information for your tenant. Contact your tenant administrator for help.

5. If a device ID appears, verify that the agent services are running.

```
$ iot-control --query
Service status: Mosquitto Broker... Success
Service status: Internet of Things Connection Gateway... Failed (not initialized)
Service status: Internet of Things Core Service... Success
Service status: Internet of Things Device Manager... Success
Service status: Internet of Things Mux... Success
```

6. If any of the services are not running, restart the services.

```
$ sudo iot-control --restart
Stopping service: Internet of Things Mux... Success
Stopping service: Internet of Things Device Manager... Success
Stopping service: Internet of Things Core Service... Success
Stopping service: Internet of Things Connection Gateway... Success
Starting service: Internet of Things Connection Gateway... Success
Starting service: Internet of Things Core Service... Success
Starting service: Internet of Things Device Manager... Success
Starting service: Internet of Things Mux... Success
```

After the services start, the device connects to the server.

7. If all the services are running and the device ID appears when you run iot-control, the contents of the **startup.bin** file you installed may not contain authentication information for your tenant. Contact your tenant administrator for help.

2. Verify network connectivity and configuration.
   1. Verify that the device can connect to the Internet.

```
$ ping 8.8.8.8
```

If the request times out and the device does not connect to the network through a proxy server, check all cable connections and if necessary, contact your network administrator.

2. If the device connects through a proxy server, verify that the proxy configuration is correct and that the connection is routed through the proxy server.

The output from the netstat command should show a TCP connection routed through the proxy server for the **iot-ccg** program.

In this example, **192.180.141.0** is the IP address of the device, **192.180.132.21** is the IP address of the proxy server, and **3128** is the port of the proxy server.

```
$ netstat -antp | grep EST
tcp        0      0 192.180.141.0:55520     192.180.132.21:3128     ESTABLISHED 3712/iot-ccg
```

If the connection is not routed correctly, run the **iot-control** command to configure the proxy information.

3. Verify that DNS is configured to resolve the https://helixdevicecloud.com host name.

```
$ dig helixdevicecloud.com
```

Output similar to the following should appear in the **ANSWER SECTION** of the output:

```
helixdevicecloud.com.   60      IN      A       52.200.6.230
helixdevicecloud.com.   60      IN      A       52.71.213.77
```

If not, DNS may not be configured properly. Ensure that you configure DNS with the correct settings for your network.

Related information
Connecting Your Wind River Linux and IDP XT Device to the Server

2. Diagnosing Lost Connectivity on Wind River Linux and IDP XT

Perform the steps in this section if a device running Wind River Linux or IDP XT successfully connected to the server but the status on the device details page on the management console shows **Offline** or **Unknown**.

If the status is **Device temporarily unavailable**, a software update is in progress. Do not interrupt the update.

Perform all steps in this section on the device.

Prerequisites

You need the following:

- physical access to the device or network access to the device, for example through SSH (enabled by default on devices running Wind River Linux and Wind River IDP XT)
- for SSH access, the IP address or host name of the device and an SSH client on your host
- superuser privileges on the device

Procedure

1. Verify that the agent services are running.

```
$ iot-control --query
Service status: Mosquitto Broker... Success
Service status: Internet of Things Connection Gateway... Failed (not initialized)
Service status: Internet of Things Core Service... Success
Service status: Internet of Things Device Manager... Success
Service status: Internet of Things Mux... Success
```

2. If any of the services are not running, restart the services.

```
# iot-control --restart
Stopping service: Internet of Things Device Manager... Success
Stopping service: Internet of Things Core Service... Success
Stopping service: Internet of Things Connection Gateway... Success
Stopping service: Mosquitto Broker... Success
Starting service: Mosquitto Broker... Success
Starting service: Internet of Things Connection Gateway... Success
Starting service: Internet of Things Core Service... Success
Starting service: Internet of Things Device Manager... Success
```

   After the services start, the device connects to the server.

3. If the services are running but the device is still not connected, check the connectivity to the server.

```
$ journalctl -u iot -n
```

If the output shows **Waiting for Mosquitto**, the device may not be connected to the network or there may be a problem with network connectivity.

Check all cable connections and if necessary, contact your network administrator.

4. DIAGNOSING INITIAL CONNECTIVITY FAILURES ON VXWORKS 7

If a device running VxWorks 7 does not appear in the device list on the management console after initial deployment, you may have a problem with the agent authentication or basic network setup.

Prerequisites

You need access to the device, either over the network or a serial connection. To access the device over the network, you must have included a networking component, such as telnet, in your VIP.

To run the ping and nslookup commands, you must have included the required components in your VIP.

Procedure

1. Verify that the agent authentication information is correct.
    1. Check that the **startup.bin** file is present in the location you specified in the **HDC_DEVICE_CONFIG_PATH** parameter in your VIP.
    2. If the **startup.bin** file is not present, see Kernel Configuration Options (VIP) for information about configuring your VIP with the file location.
    3. If the **startup.bin** file is present but the **agentguid.bin** and **dxlpolicy.bin** files are missing from the location you specified in the **HDC_DEVICE_CONFIG_PATH** parameter in your VIP, verify that the **tCcgBroker** task is running.
    4. If all the files are present, the contents of the **startup.bin** file may not contain authentication information for your tenant. Contact your tenant administrator for help.
2. Verify network connectivity and configuration.
    1. Change to the VxWorks command shell.

    ```
    # cmd
    ```

    2. Verify that the device can connect to the Internet.

    ```
    # ping "8.8.8.8"
    ```

    If the request times out, check all cable connections and if necessary, contact your network administrator.

    3. Verify that DNS is configured to resolve the https://helixdevicecloud.com hostname.

    ```
    # nslookup "helixdevicecloud.com"
    ```

    Output similar to the following should appear:

    ```
    Server:  google-public-dns-a.google.com
    Address: 8.8.8.8

    Name:    helixdevicecloud.com
    Address: 52.202.232.239
             52.44.113.87
    ```

    If not, DNS may not be included in your VIP or may not be configured properly. Ensure that you include DNS in your VIP and configure DNS with the correct settings for your network.

5. TROUBLESHOOTING ON WINDOWS

1. Diagnosing Initial Connectivity Failures on Windows

If a device running Windows does not appear in the device list on the management console after initial deployment, you may have a problem with the agent authentication or basic network setup.

Perform all steps in this section on the device.

Prerequisites

You need the following:

- either physical access to the device or network access to the device, for example, through remote desktop
- for remote desktop access, the IP address or host name of the device and remote desktop enabled on the device
- a user account with administrator privileges on the Windows computer

Procedure

1. Verify that the agent authentication information is correct.
    1. Open a Command Prompt window as administrator and verify that the current device ID appears.

```
C:\Windows\System32>cd "C:\Program Files (x86)\Helix Device Cloud"\bin
C:\Program Files (x86)\Helix Device Cloud\bin>iot-control
Looking for configuration file: C:\Program Files (x86)\Helix Device Cloud\etc\iot.cfg
Looking for configuration file: C:\ProgramData\Wind River Systems\Helix Device Cloud\iot.cfg
Looking for configuration file: C:\windows\system32\iot.cfg
Looking for configuration file: C:\Program Files (x86)\Helix Device Cloud\bin\iot.cfg
Current device id: A0366CE3-D153-ACEC-D839-F34B6B5C2F06
Proxy's type (none/http/socks5/Enter to skip):
```

    In this example, the device ID is A0366CE3-D153-ACEC-D839-F34B6B5C2F06.

    2. To exit, press **ENTER** three times.
    3. If no device ID appears, see Connecting Your Windows Device to the Server for information about obtaining and installing the agent authentication file.
    4. If a device ID appears, verify that the agent services are running.

```
c:\Program Files (x86)\Helix Device Cloud\bin>iot-control --query
Service status: Mosquitto Broker... Success
Service status: Internet of Things Connection Gateway... Failed (not initialized)
Service status: Internet of Things Core Service... Success
Service status: Internet of Things Device Manager... Success
```

    5. If any of the services are not running, restart the services.

```
c:\Program Files (x86)\Helix Device Cloud\bin>iot-control --restart
Stopping service: Internet of Things Device Manager... Success
```

```
Stopping service: Internet of Things Core Service... Success
Stopping service: Internet of Things Connection Gateway... Success
Stopping service: Mosquitto Broker... Success
Starting service: Mosquitto Broker... Success
Starting service: Internet of Things Connection Gateway... Success
Starting service: Internet of Things Core Service... Success
Starting service: Internet of Things Device Manager... Success
```

After the services start, the device connects to the server.

6. If all the services are running and the device ID appears when you run iot-control, the contents of the **startup.bin** file you installed may not contain authentication information for your tenant. Contact your tenant administrator for help.

2. Verify network connectivity and configuration.
   1. Verify that the device can connect to the Internet.

```
C:\>ping 8.8.8.8
```

If the request times out and the device does not connect to the network through a proxy server, check all cable connections and if necessary, contact your network administrator.

2. If the device connects through a proxy server, verify that the proxy configuration is correct and that the connection is routed through the proxy server.

The output from the netstat command should show a TCP connection routed through the proxy server for the **iot-ccg.exe** program.

In this example, **192.180.141.0** is the IP address of the device, **192.180.132.21** is the IP address of the proxy server, and **3128** is the port of the proxy server.

```
$ netstat -abntp TCP
TCP    192.180.141.0:55415        192.180.132.21:3128    ESTABLISHED
 [iot-ccg.EXE]
```

If the connection is not routed correctly, run the **iot-control** command to configure the proxy information.

3. Verify that DNS is configured to resolve the https://helixdevicecloud.com hostname.

```
C:\>nslookup helixdevicecloud.com
```

Output similar to the following should appear:

```
Server:  UnKnown
Address:  10.0.2.2

Non-authoritative answer:
Name:    helixdevicecloud.com
Addresses:  52.202.232.239
          52.44.113.87
```

If not, DNS may not be configured properly. Ensure that you configure DNS with the correct settings for your network.

2. Diagnosing Lost Connectivity on Windows

Perform the steps in this section if a device running Windows successfully connected to the server but the status on the device details page on the management console shows **Offline** or **Unknown**.

If the status is **Device temporarily unavailable**, a software update is in progress. Do not interrupt the update.

Perform all steps in this section on the device.

Prerequisites

You need the following:

- either physical access to the device or network access to the device, for example, through remote desktop
- a user account with administrator privileges on the Windows computer

Procedure

1. Open a Command Prompt window as administrator and verify that the agent services are running.

```
C:\Windows\System32>cd "c:\Program Files (x86)\Helix Device Cloud"\bin
c:\Program Files (x86)\Helix Device Cloud\bin>iot-control --query
Service status: Mosquitto Broker... Success
Service status: Internet of Things Connection Gateway... Success
Service status: Internet of Things Core Service... Success
Service status: Internet of Things Device Manager... Success
```

2. If any of the services are not running, open a Command Prompt window as administrator and restart the services.

```
c:\Program Files (x86)\Helix Device Cloud\bin>iot-control --restart
Stopping service: Internet of Things Device Manager... Success
Stopping service: Internet of Things Core Service... Success
Stopping service: Internet of Things Connection Gateway... Success
Stopping service: Mosquitto Broker... Success
Starting service: Mosquitto Broker... Success
Starting service: Internet of Things Connection Gateway... Success
Starting service: Internet of Things Core Service... Success
Starting service: Internet of Things Device Manager... Success
```

   After the services start, the device connects to the server.

3. If the services are running but the device is still not connected, open the **C:\ProgramData\Wind River Systems\Helix Device Cloud\iot-service**_*date* file, where *date* is the most recent date.

   If the log shows output similar to the following, the device may not be connected to the network or there may be a problem with network connectivity.

```
Debug - iot_mqtt_common.c:105 - Disconnected from mqtt broker (localhost:21883); reason: The co
nnection was lost.
```

   Check all cable connections, confirm connectivity to the Internet in Network and Sharing Center, and if necessary, contact your network administrator.

6. TROUBLESHOOTING ON UBUNTU

1. Diagnosing Initial Connectivity Failures on Ubuntu

If a device running Ubuntu does not appear in the device list on the management console after initial deployment, you may have a problem with the agent authentication or basic network setup.

Perform all steps in this section on the device.

Prerequisites

You need the following:

- physical access to the device or network access to the device, for example through SSH
- for SSH access, the IP address or host name of the device and an SSH client on your host
- superuser privileges on the device

Procedure

1. Verify that the agent authentication information is correct.
    1. Verify that the current device ID appears.

```
$ sudo iot-control
Looking for configuration file: /etc/iot/iot.cfg
Looking for configuration file: /var/lib/iot/iot.cfg
Looking for configuration file: /home/user/iot.cfg
Looking for configuration file: ./iot.cfg
Current device id: 5C1FB6BB-4FE8-E8FA-0FBC-AC12ABE36C18
Proxy's type (none/http/socks5/Enter to skip):
```

    In this example, the device ID is 5C1FB6BB-4FE8-E8FA-0FBC-AC12ABE36C18.

    2. To exit, press **ENTER** three times.
    3. If no device ID appears, see Connecting Your Ubuntu Device to the Server for information about obtaining and installing the **startup.bin** file.
    4. If a device ID appears, verify that the agent services are running.

```
$ iot-control --query
Service status: Mosquitto Broker... Success
Service status: Internet of Things Connection Gateway... Failed (not initialized)
Service status: Internet of Things Core Service... Success
Service status: Internet of Things Device Manager... Success
Service status: Internet of Things Mux... Success
```

    5. If the status of any service is not found, reinstall the agent. For more information, see Installing the HDC Agent on Ubuntu.
    6. If any of the services are not running, restart the services.

```
$ sudo iot-control --restart
Stopping service: Internet of Things Mux... Success
Stopping service: Internet of Things Device Manager... Success
Stopping service: Internet of Things Core Service... Success
Stopping service: Internet of Things Connection Gateway... Success
Starting service: Internet of Things Connection Gateway... Success
Starting service: Internet of Things Core Service... Success
Starting service: Internet of Things Device Manager... Success
Starting service: Internet of Things Mux... Success
```

After the services start, the device connects to the server.

7. If all the services are running and the device ID appears when you run iot-control, the contents of the **startup.bin** file you installed may not contain authentication information for your tenant. Contact your tenant administrator for help.

2. Verify network connectivity and configuration.
   1. Verify that the device can connect to the Internet.

```
$ ping 8.8.8.8
```

If the request times out and the device does not connect to the network through a proxy server, check all cable connections and if necessary, contact your network administrator.

2. If the device connects through a proxy server, verify that the proxy configuration is correct and that the connection is routed through the proxy server.

The output from the netstat command should show a TCP connection routed through the proxy server for the **iot-ccg** program.

In this example, **192.180.141.0** is the IP address of the device, **192.180.132.21** is the IP address of the proxy server, and **3128** is the port of the proxy server.

```
$ netstat -antp | grep EST
tcp        0      0 192.180.141.0:55520     192.180.132.21:3128     ESTABLISHED 3712/iot-ccg
```

If the connection is not routed correctly, run the **iot-control** command to configure the proxy information.

3. Verify that DNS is configured to resolve the https://helixdevicecloud.com host name.

```
$ dig helixdevicecloud.com
```

Output similar to the following should appear in the **ANSWER SECTION** of the output:

```
helixdevicecloud.com.   60      IN      A       52.200.6.230
helixdevicecloud.com.   60      IN      A       52.71.213.77
```

If not, DNS may not be configured properly. Ensure that you configure DNS with the correct settings for your network.

2. Diagnosing Lost Connectivity on Ubuntu

Perform the steps in this section if a device running Ubuntu successfully connected to the server but the status on the device details page on the management console shows **Offline** or **Unknown**.

If the status is **Device temporarily unavailable**, a software update is in progress. Do not interrupt the update.

Perform all steps in this section on the device.

Prerequisites

You need the following:

- physical access to the device or network access to the device, for example through SSH
- for SSH access, the IP address or host name of the device and an SSH client on your host
- superuser privileges on the device

Procedure

1. Verify that the agent services are running.

```
$ iot-control --query
Service status: Mosquitto Broker... Success
Service status: Internet of Things Connection Gateway... Failed (not initialized)
Service status: Internet of Things Core Service... Success
Service status: Internet of Things Device Manager... Success
Service status: Internet of Things Mux... Success
```

2. If the status of any service is not found, reinstall the agent. For more information, see Installing the HDC Agent on Ubuntu.
3. If any of the services are not running, restart the services.

```
$ sudo iot-control --restart
Stopping service: Internet of Things Mux... Success
Stopping service: Internet of Things Device Manager... Success
Stopping service: Internet of Things Core Service... Success
Stopping service: Internet of Things Connection Gateway... Success
Starting service: Internet of Things Connection Gateway... Success
Starting service: Internet of Things Core Service... Success
Starting service: Internet of Things Device Manager... Success
Starting service: Internet of Things Mux... Success
```

   After the services start, the device connects to the server.

4. If the services are running but the device is still not connected, check the connectivity to the server.

```
$ sudo journalctl -u iot -n
```

   If the output shows **Waiting for Mosquitto**, the device may not be connected to the network or there may be a problem with network connectivity.

   Check all cable connections and the status of the network interface, and if necessary, contact your network administrator.

7. DIAGNOSING REMOTE LOGIN FAILURES

Perform the steps in this section if the device successfully connects to the server but you cannot remotely log in to the device.

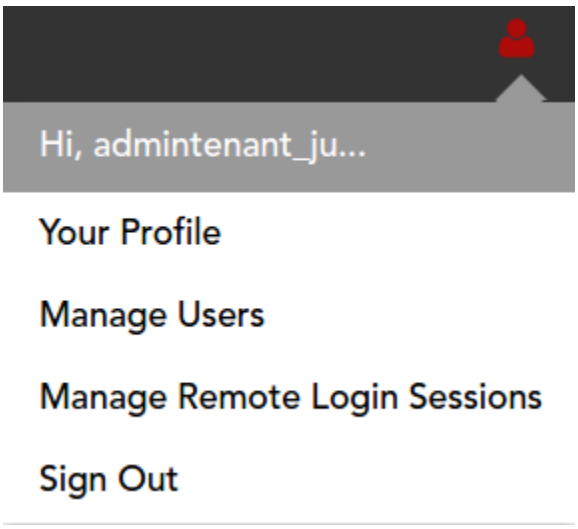
Remote login is supported on devices running Wind River Linux, Wind River IDP XT, and Ubuntu.

Ensure that the status on the device details page is **Online**. If not, resolve basic connectivity problems first.

To successfully use remote login, the device must have the correct date and time and DNS must be properly configured.

If you successfully open a remote login session to a Ubuntu device and attempt to log in as the **root** user, the message **Login incorrect** appears. You must use login credentials for a user other than the **root** user.

If you reach the maximum number of remote login sessions for a single device or for multiple devices across your tenant, a user with administrator privileges can select **Account Settings > Manage Remote Login Sessions** and delete existing sessions.



For devices that support remote login, if you have configuration problems, a message such as the following may appear when you run the **Remote Login** action:

Remote Login Failed error *xxxx*

Prerequisites

You need the following:

- physical access to the device or network access to the device, for example through SSH
- for SSH access, the IP address or host name of the device and an SSH client on your host
- superuser privileges on the device

Procedure

1. Log in to the device either through SSH or a serial connection, and ensure that the required service is running.

```
$ systemctl status iot-mux
```

The output should show **active (running)**.

2. If the service is not running, start it and check that it started successfully.

```
$ systemctl start iot-mux
$ systemctl status iot-mux
```

The output should show **active (running)**.

3. If the service fails to start, verify that the **startup.bin** file has the required configuration information.

```
$ strings /var/lib/iot/startup.bin | grep MuxHost
MuxHostmux-77d1f79a-5506-4711-9af8-9e803a313390.helixdevicecloud.com
```

If the **MuxHost** entry is not present, contact your tenant administrator for help.

4. If the **MuxHost** entry is present, check that the device has today's date.

```
$ date
```

If not, configure the time using NTP or some other method. Ensure that the device retains the time after the device reboots.

5. If your device connects through a proxy server, do the following:
    1. Ensure that you installed the **nmap** package.

    Wind River Linux and IDP XT:

    ```
    # rpm -q nmap
    nmap-7.31-r0.0.corei7_64
    ```

    Ubuntu:

    ```
    $ apt -qq list nmap
    nmap/xenial,now 7.01-2ubuntu2 amd64 [installed,automatic]
    ```

    If the **nmap** package is not installed, install the package from your package repository, or include the package when you run the configure command and rebuild your platform project. After you install the package or deploy your platform project, run the iot-control command to configure the proxy information.

    2. If the **nmap** package is installed, confirm that the remote login connection is routed correctly.

    The output from the netstat command should show a TCP connection routed through the proxy server using the **ncat** program.

    In this example, **192.180.141.104** is the IP address of the device, **192.180.132.21** is the IP address of the proxy server, and **3128** is the port of the proxy server.

    ```
    $ netstat -antp | grep EST
    tcp        0      0 192.180.141.104:42454   192.180.132.21:3128     ESTABLISHED 17235/ncat
    ```

    You may need to run the netstat command with sudo.

    If the connection is not routed correctly, run the iot-control command to configure the proxy information.

Related information

8. DIAGNOSING SOFTWARE UPDATE FAILURES

Software updates may fail to install if the package has errors such as incorrect installation instructions or if the update process on the device is interrupted.

If your deployment included multiple devices, you need to expand the row of the deployment on the Deployments page to see the deployment status of individual devices.

To diagnose problems, you need to upload the **iot_install_updates.log** file the device creates and automatically copies to the **upload** directory during the update. For instructions, see Retrieving Files from Devices. You do not need to run the **Dump Log Files** action before retrieving the file.

See also the most recent value of the **sw_update** telemetry metric on the device details page. The most recent value for a successful software update should be **Software Update Finish... Successful !** if the update does not require a reboot or **Reboot Now...** if the update requires a reboot. For information about viewing telemetry, see Viewing Telemetry Data.

If the most recent value of the **sw_update** telemetry metric indicates that the deployment failed at a specific stage of the update, check for the following in the **iot_install_updates.log** file:

Problem	Operating System	Resolution

Errors executing commands, which are indicated by log messages similar to the following:
`Command error: sudo: no tty present and no askpass program specified`
`Command error: cmdName : Operation not permitted`
`mkdir failed - Inappropriate ioctl for device`
	Linux	Ensure that the commands you want to execute either in the boxes on the Create New Package page or in scripts you run are specified in the **/etc/sudoers** file for the **iot** user. Also ensure that you use the **sudo** command to access files and directories owned by the **root** user.
		For more information, see Software Update.

An incorrect archive type, which is indicated by the following log message: `Unarchiving the Update Package ... Failed!`	Linux and Windows	Ensure that you choose **tar.gz** for Linux-based operating systems and **zip** for Windows operating systems.

If the most recent value of the **sw_update** telemetry data shows success at the latest stage of the update but does not show **Software Update Finish... Successful !** or **Reboot Now...**, the update process on the device may have been interrupted or connectivity may have been lost during the update. The deployment status may show **Failed** or **In Progress** on the Deployments page.

Problem	Operating System	Resolution
No **iot_install_updates.log** log file available to upload.	Linux and Windows	In update packages for Windows, ensure that you start any applications in your instructions using the AT command to avoid blocking the update process. The device may have rebooted during the update. Depending on the progress of the update, you may need to deploy the update again.
The device is offline.	Linux and Windows	Check the network status of the device. If network connectivity was lost during the update, the update may have completed. When the device reconnects, retrieve the log file and check the update status. Otherwise, you need to deploy the update again. If the device reboots to complete the update, agent or network services may have failed to restart after the device rebooted. There may be a problem with the contents of the package.