How to check route to SAP Cloud Platform

It can happen that SAP cloud connector cannot establish a secure tunnel to the SAP cloud platform.

The normal tunnel establishment records similar entries with INFO severity level in the *ljs_trace.log* file:

```
#INFO
#com.sap.core.connectivity.tunnel.client.handshake.ClientProtocolHandshake
#notification-client-3-1
#Sending handshake request for tunnel: account:///c012345abc/centos and host connectivitynotification.ap1.hana.ondemand.com:443|

#INFO
#com.sap.core.connectivity.tunnel.core.impl.context.TunnelRegistryImpl#notification-client-3-1
#Registered tunnel channel [id: 0xb80c2c8b, L:/xx.xx.52.129:53096 - R:connectivitynotification.ap1.hana.ondemand.com/157.133.97.47:443] for tunnel id "account:///c012345abc/centos" and client id "1C9480707A4011E8C764DF2EC0A83481"|

#INFO
#com.sap.core.connectivity.tunnel.client.notification.NotificationClient#notification-client-3-1
#Successfully established tunnel channel to notification service: [id: 0xb80c2c8b, L:/xx.xx.52.129:53096 - R:connectivitynotification.hanatrial.ondemand.com/157.133.97.47:443]|
```

However, when connection establishment fails, you need to look for the cloud connector log file *ljs_trace.log* for details:

**Connection timed out**
In this case, the SAP cloud connector cannot reach the notification server due to a timeout.

The accessibility of the notification server can be checked with networking tools:

**tracert tool**

On Windows OS check route with tracert tool:

`tracert -d <hostname>`
C:\Tools\tracert -d connectivitynotification.ap1.hana.ondemand.com

Tracing route to connectivitynotification.ap1.hana.ondemand.com
[157.133.97.47]  
over a maximum of 30 hops:

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2 ms</td>
<td>2 ms</td>
</tr>
<tr>
<td>2</td>
<td>31 ms</td>
<td>31 ms</td>
</tr>
<tr>
<td>3</td>
<td>39 ms</td>
<td>38 ms</td>
</tr>
<tr>
<td>4</td>
<td>*</td>
<td>79 ms</td>
</tr>
<tr>
<td>5</td>
<td>*</td>
<td>92 ms</td>
</tr>
<tr>
<td>6</td>
<td>71 ms</td>
<td>43 ms</td>
</tr>
<tr>
<td>7</td>
<td>50 ms</td>
<td>49 ms</td>
</tr>
<tr>
<td>8</td>
<td>82 ms</td>
<td>91 ms</td>
</tr>
<tr>
<td>9</td>
<td>*</td>
<td>54 ms</td>
</tr>
<tr>
<td>10</td>
<td>170 ms</td>
<td>*</td>
</tr>
<tr>
<td>11</td>
<td>193 ms</td>
<td>161 ms</td>
</tr>
<tr>
<td>12</td>
<td>270 ms</td>
<td>247 ms</td>
</tr>
<tr>
<td>13</td>
<td>212 ms</td>
<td>251 ms</td>
</tr>
<tr>
<td>14</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>15</td>
<td>*</td>
<td>440 ms</td>
</tr>
<tr>
<td>16</td>
<td>*</td>
<td>467 ms</td>
</tr>
<tr>
<td>17</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>18</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>19</td>
<td>453 ms</td>
<td>426 ms</td>
</tr>
</tbody>
</table>

Trace complete.

**nmap tool**

On Windows or Linux systems check route with nmap tool:

```
nmap -sn -traceroute <host name>
```
C:\Tools>nmap -sn --traceroute
connectivitynotification.ap1.hana.ondemand.com
Starting Nmap 7.70 (https://nmap.org) at 2018-08-29 09:33 W. Europe Daylight Time
Nmap scan report for connectivitynotification.ap1.hana.ondemand.com
(157.133.97.47)
Host is up (0.41s latency).

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1  0.00 ms xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.corp (xx.xx.xx.1)
2  0.00 ms xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.corp (xx.xx.xx.169)
3  0.00 ms xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.corp (xx.xx.xxx.209)
4  0.00 ms xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx (xx.xx.139.225)
5  ... 6
7  21.00 ms xx.xx.3.6
8  0.00 ms xx.xx.3.159
9  17.00 ms xx.xx.204.37
10 117.00 ms xx.xx.47.10
11 121.00 ms xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.NET (xx.xx.50.165)
12 237.00 ms xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.NET (xx.xx.15.102)
13 237.00 ms xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.NET (xx.xx.114.18)
14  ...
15 406.00 ms xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.NET (xx.xx.48.30)
16 503.00 ms xx.xx.7.202
17  ... 18
19 400.00 ms 157.133.97.47

Nmap done: 1 IP address (1 host up) scanned in 17.77 seconds

The nmap tool can be downloaded from https://nmap.org/ site.

**traceroute tool**

On Linux system execute command `traceroute -n <host name>` command:

[root@boxes ~]$ traceroute -n connectivitynotification.ap1.hana.ondemand.com

The tunnel establishment can be traced with Wireshark (www.wireshark.org) or tcpdump tools as well.