

This document empowers us to find who has interrupted the box usage.

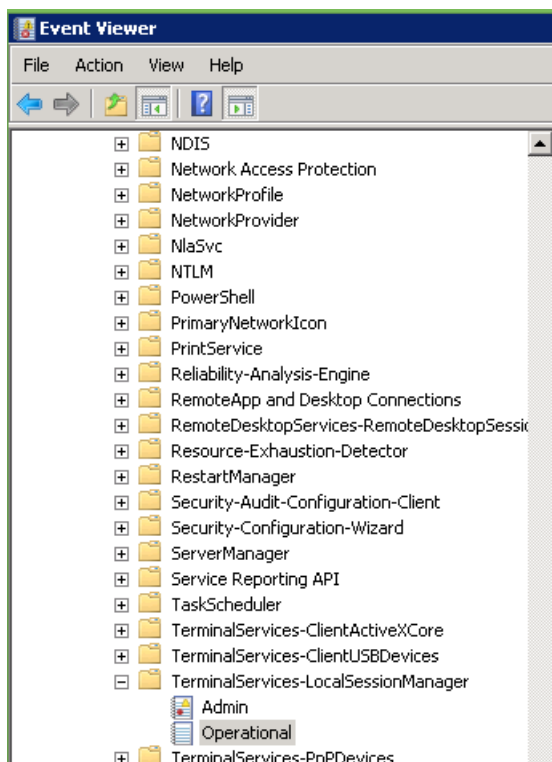
Scenario: User2 has interrupted the usage of the current user i.e. User1 for shared machine.

For demonstration, let us consider User1 is saavvaru, User2 is prmodi and Machine is '10.118.20.213'.

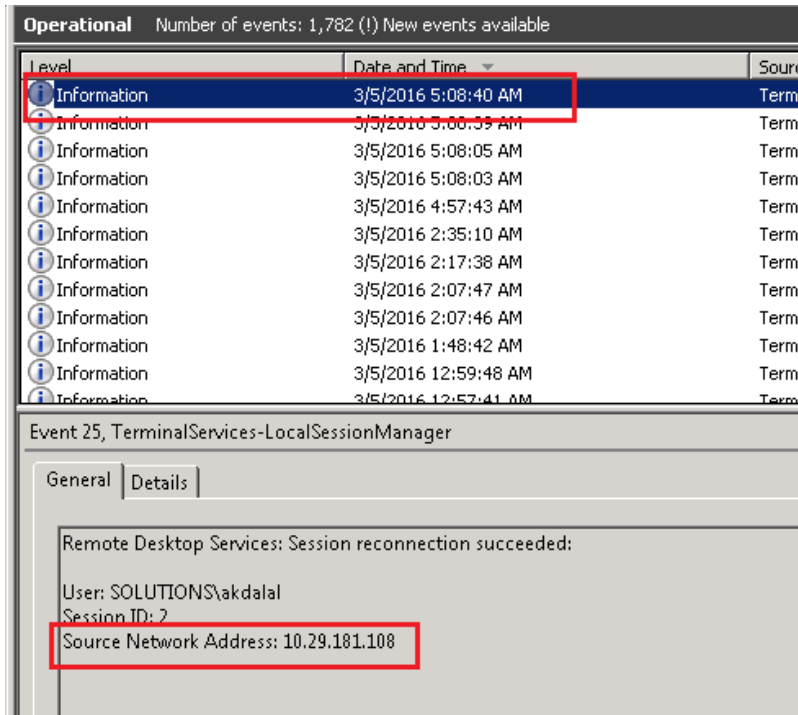
Once User1 notices that box is disconnected, he/she has to contact Box owner.

And Box owner has to follow the below steps to locate the User2 hostname.

1. Login to box/machine. Press 'windows' button and type/search for 'Event Viewer' program. Click to open.
2. In 'Event Viewer' window, navigate to *"Applications and Service Logs -> Microsoft -> Windows -> TerminalServices-LocalSessionManager -> Operational"* as shown below:



3. First record will be the current loggedin user i.e. boxowner (or) whoever is performing these steps. {So, first record can be ignored}



The host name can be found using the IP address in CMD prompt.

```
C:\WINDOWS\system32>ping -a 10.29.181.108

Pinging USHYDSAAVVARU9.us.deloitte.com [10.29.181.108] with 32 bytes of data:
Reply from 10.29.181.108: bytes=32 time=2ms TTL=128
Reply from 10.29.181.108: bytes=32 time=3ms TTL=128
Reply from 10.29.181.108: bytes=32 time=4ms TTL=128
Reply from 10.29.181.108: bytes=32 time=4ms TTL=128

Ping statistics for 10.29.181.108:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 3ms
```

In this case, USHYDSAAVVARU9 is User1.

4. This step is to find the user who has interrupted. Based on timestamp when disconnection happened, locate the record. **Make sure the 'Event ID' is 21 or 25.**

The screenshot shows the Windows Event Viewer interface. At the top, it says 'Operational' and 'Number of events: 1,782 (1) New events available'. Below this is a table with columns 'Level', 'Date and Time', and 'Source'. One event is highlighted with a red box: an 'Information' level event from 'TerminalServices-LocalSessionManager' on '3/5/2016 5:08:05 AM'. Below the table, the 'Details' tab for 'Event 25, TerminalServices-LocalSessionManager' is open. It shows the message 'Remote Desktop Services: Session reconnection succeeded:' and lists 'User: SOLUTIONS\akdalal', 'Session ID: 2', and 'Source Network Address: 10.29.155.59' (the last one is boxed in red). A large black arrow points from this address to the 'Event ID: 25' field in the 'Log Name' section at the bottom, which is also boxed in green.

Level	Date and Time	Source
Information	3/5/2016 5:08:40 AM	TerminalServices-LocalSessi...
Information	3/5/2016 5:08:39 AM	TerminalServices-LocalSessi...
Information	3/5/2016 5:08:05 AM	TerminalServices-LocalSessi...
Information	3/5/2016 5:08:03 AM	TerminalServices-LocalSessi...
Information	3/5/2016 4:57:43 AM	TerminalServices-LocalSessi...
Information	3/5/2016 2:35:10 AM	TerminalServices-LocalSessi...
Information	3/5/2016 2:17:38 AM	TerminalServices-LocalSessi...
Information	3/5/2016 2:07:47 AM	TerminalServices-LocalSessi...
Information	3/5/2016 2:07:46 AM	TerminalServices-LocalSessi...
Information	3/5/2016 1:48:42 AM	TerminalServices-LocalSessi...
Information	3/5/2016 12:59:48 AM	TerminalServices-LocalSessi...
Information	3/5/2016 12:57:41 AM	TerminalServices-LocalSessi...

Event 25, TerminalServices-LocalSessionManager

General Details

Remote Desktop Services: Session reconnection succeeded:

User: SOLUTIONS\akdalal
Session ID: 2
Source Network Address: 10.29.155.59

Log Name: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
Source: TerminalServices-LocalSessi
Event ID: 25
Level: Information
User: SYSTEM
OpCode: Info
Task Category: None
Keywords:
Computer: USSLTCSNW2614.solutions.glbsnet.com
More Information: [Event Log Online Help](#)

```
C:\WINDOWS\system32>ping -a 10.29.155.59

Pinging USHYDPRMODI1 [10.29.155.59] with 32 bytes of data:
Reply from 10.29.155.59: bytes=32 time=492ms TTL=127
Reply from 10.29.155.59: bytes=32 time=518ms TTL=127
Reply from 10.29.155.59: bytes=32 time=521ms TTL=127
Reply from 10.29.155.59: bytes=32 time=496ms TTL=127

Ping statistics for 10.29.155.59:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 492ms, Maximum = 521ms, Average = 506ms
```

In this case, USHYDORMODI1 is User2.

Event IDs

Event ID	Event Description
21	Logon
23	Logoff
24	Disconnected
25	Reconnection

If any of the above steps are unclear, please contact saavvaru@deloitte.com

Working on Windows PowerShell Script to fetch this information automatically. Watch this space for more. Please join me if interested.