FAQ ref: 09022009-r009 Last Updated: 14.03.2018

PeachWorx: TFC02 - PC Discovery and Remote Agent Installation.

 ==

Sometimes, not all PCs are available for remote installation of the TFCO2 agent.

Note. The Remote PC must be on for installation of the agent to be successful.

 1.] You MUST have appropriate domain-admin privileges to remotely install anything. (Multiple server clusters may require, other, specific authentication) in addition TaskForceCO2 must be installed and run 'as administrator'.

2.] "File & Print Sharing" must be turned on at each remote workstation.

(NOTE: Items 1 and 2 are usually ok on Operating Systems; like XP, Vista and Windows7, 8 and 10 - But, possibly not, if they have been upgraded from older versions of Windows)

3.] An Admin$ share must be present and available for remote access on each remote workstation. To test if the Admin$ share is open and that you have permission to write to it follow these steps.

Execute \\remotecomputername\admin$

If that opens a remote Windows folder try creating and saving a new text file to establish that you have write permissions.

4.] Firewalls (and some anti-virus software) and some routers, may need to be configured to allow TCP and UDP conversations on various ports. (especially where multiple servers are involved).

The standard TCP and UDP ports for TFCO2 are: 6940, 6960, 6980, 0007 All of these should be configured to allow traffic "in-both-directions".

5.] If these conditions have been met and there is still a problem with communication on (some) PCs then;

a.) We may be looking at a DNS configuration issue, to determine if this might be the case;

> Ping ComputerName
>
> Ping ""FullyQualifiedDomainName"
>
> Ping KnownIPAddress
>
> If the results of all three are NOT the same a "DNS discrepancy" exists.

b.) An issue with resolving the remote PCs IP-Address from the remote PCs computer name.

> ADS uses "DNS lookup" to resolve the IPAddress from the ComputerName
>
> NetworkNeighborhood uses low level NetBIOS calls to the target PC to retrieve the IPAddress
>
> ScanByIPRange uses "reverse DNS lookup" to resolve the IPAddress

Now, consider scenario a.) above ...

c.) An issue with (historical) WINS use, versus (newer) DNS use

Any of these issues would be evidenced by a discrepancy between what (our) Central Console (individual for each product) says the IP-Address of the remote PC is and the results of the three "pings" in scenario a.) above.

If WINS is in use (and it might be, even if you have configured for DNS);

from the server: use WINS to delete any IP_Addresses which are incorrect or unused for the remote PCs which are not responding to our Central Console.

If this still leaves some PCs that are not responding then;

You may need to visit (or, open and use a remote desktop session for) each of them and use WINS locally to ensure that only the correct/current IP_Address for that PC is assigned, and then reboot that remote PC.

In our experience, this sequence of activity has always been successful in resolving such issues, and, fortunately, the last requirement, visiting some PCs, is quite rare, and has only ever involved a very small percentage of the user base.

----

ends ..