Why Can't Windows Open-AudIT Discover Itself?

(and what can I do about it?)

When we run Open-AudIT Server on Windows and try to discover the IP that the server is using, we will not get a meaningful result - why is this?

When discovery runs it has no idea that the IP it is attempting to talk to is actually the local machine. It is treated just like any other IP. This means we will attempt to connect to it, over the "network", using credentials.

WMI simply does not support doing this. No credentials we supply will work, because they will be rejected by WMI on the local machine.

You can try this for yourself by running the below command on your Open-AudIT Server. Obviously substitute the IP, username, domain and password.

```
wmic /Node:"YOUR-IP" /user:"YOUR_DOMAIN\YOUR_USERNAME" /password:"YOUR_PASSWORD" csproduct get uuid
```

The result you get will be as below.

```
Node - 192.168.88.73
ERROR:
Description = User credentials cannot be used for local connections
```

And you can see this in the discovery log when we attempt to connect using WMI (ID 375 below). We don't actually retrieve a result, even with valid credentials.

So how can we audit the Open-AudIT Server?

The best option right now is to setup a scheduled task to run the audit script or to run it manually when you need to.

If you have a Collector that is able to reach the server using the required network ports, you could have that collector discover the server.

We have this as an outstanding item to be addressed in a future release.

This issue has been outstanding for a very long time, but with the work-around in place, it is not crucial to the function of Open-AudIT.

When running a discovery that includes the IP of the local server, you will receive very limited data from, the discovery but you will receive the FQDN and the MAC address. Between these two items and the default match settings, no extraneous devices will be created.

06/08/19 09:05	343	127.0.0.1	start	Discovery for 192.168.88.73 submitted for discovery 3 starting
06/08/19 09:05	344	127.0.0.1	notice	Starting discovery for 192.168.88.73
06/08/19 09:05	345	127.0.0.1	notice	Discovery for 192.168.88.73 using Nmap version 7.60 at C:\Program Files (x86)\Nmap\nmap.exe
06/08/19 09:05	346	127.0.0.1	notice	IPs in subnet: 1 Command: C:\Program Files (x86)\Nmap\nmap.exe -n -sL 192.168.88.73
06/08/19 09:05	347	127.0.0.1	notice	IPs after exclusions in subnet: 1 Command: C:\Program Files (x86)\Nmap\nmap.exe -n -sL 192.168.88.73
06/08/19 09:05	348	127.0.0.1	notice	IPs responding to Nmap ping in subnet (to be scanned): 1 Command: C:\Program Files (x86)\Nmap\nmap.exe -n -oG - -sP 192.168.88.73
06/08/19 09:05	349	192.168.88.73	notice	Scanning Host: 192.168.88.73
06/08/19 09:05	350	192.168.88.73	notice	Nmap Command Command: C:\Program Files (x86)\Nmap\nmap.exe -n -T4 -sS -p T:22,135,62078 192.168.88.73 :: Custom TCP Ports

06/08/19 09:05	351	192.168.88.73	notice	Host 192.168.88.73 is up, received ssh (TCP port 22 open) response Command: C:\Program Files (x86)\Nmap\nmap.exe -n -T4 -sS -p T:22,135,62078 192.168.88.73 :: Custom TCP Ports Output: 22/tcp open ssh
06/08/19 09:05	352	192.168.88.73	notice	Host 192.168.88.73 is up, received wmi (TCP port 135 open) response Command: C:\Program Files (x86)\Nmap\nmap.exe -n -T4 -sS -p T:22,135,62078 192.168.88.73 :: Custom TCP Ports
06/08/19 09:05	353	192.168.88.73	notice	Command: C:\Program Files (x86)\Nmap\nmap.exe -n -T4 -sU -p U:161 192.168.88.73 :: Custom UDP Ports
06/08/19 09:05	354	192.168.88.73	notice	Scanning localhost, so setting WMI status to true Command: C:\Program Files (x86)\Nmap\nmap.exe -n -T4 -sU -p U:161 192.168.88.73 :: Custom UDP Ports
06/08/19 09:05	355	192.168.88.73	(1 of 1)	IP 192.168.88.73 responding, ping reply, adding to device list. SSH Status: true, WMI Status: true, SNMP Status: false. Command: http://127.0.0.1/open-audit/index.php/input/discoveries
06/08/19 09:05	356	192.168.88.73	success	The discovery_id was used to successfully retrieve information for the discovery entry named local
06/08/19 09:05	357	192.168.88.73	success	Received data for 192.168.88.73, now starting to process
06/08/19 09:05	358	192.168.88.73	success	IP 192.168.88.73 resolved to DNS hostname hel
06/08/19 09:05	359	192.168.88.73	notice	Running devices::match function.
06/08/19 09:05	360	192.168.88.73	notice	Not running match_hostname_uuid, uuid not set.
06/08/19 09:05	361	192.168.88.73	notice	Not running match_hostname_dbus, dbus_identifier not set.
06/08/19 09:05	362	192.168.88.73	notice	Not running match_hostname_serial, serial not set.
06/08/19 09:05	363	192.168.88.73	notice	Not running match_dbus, matching rule set to: n.
06/08/19 09:05	364	192.168.88.73	success	HIT on fqdn. Output: FQDN: hel.opmantek.com
06/08/19 09:05	365	192.168.88.73	success	Device with ID 2 found on initial Nmap result.
06/08/19 09:05	366	192.168.88.73	success	Delete the previous log entries for this device Command: /* input::discoveries */ DELETE FROM discovery_log WHERE system_id = 2 and discovery_id != 3
06/08/19 09:05	367	192.168.88.73	success	Update the current log entries with our new device Command: /* input::discoveries */ UPDATE discovery_log SET system_id = 2 WHERE discovery_id = 3 and ip = '192.168.88.73'
	368	192.168.88.73	notice	WMI Status is true on 192.168.88.73
06/08/19 09:05	369	192.168.88.73	notice	SSH Status is true on 192.168.88.73
06/08/19 09:05	370	192.168.88.73	notice	SNMP Status is false on 192.168.88.73
06/08/19 09:05	371	192.168.88.73	notice	SSH audit starting
06/08/19 09:05	372	192.168.88.73	warning	SSH detected but no valid SSH credentials for 192.168.88.73.
06/08/19 09:05	373	192.168.88.73	notice	Testing Windows credentials for 192.168.88.73
06/08/19 09:05	374	192.168.88.73	notice	Windows credentials starting
06/08/19 09:05	375	192.168.88.73	notice	Attempting to execute command **Command:** %comspec% /c start /b wmic /Node:"192.168.88.73" /user:"hel\administrator" /password:"*******" csproduct get uuid **Output:** ["","]
06/08/19 09:05	376	192.168.88.73	notice	Credential set for Windows named local admin not working on 192.168.88.73

06/08/19 09:05	377	192.168.88.73	warning	WMI detected but no valid Windows credentials for 192.168.88.73.
06/08/19 09:05	378	192.168.88.73	notice	MAC (input) matched to manufacturer
06/08/19 09:05	379	192.168.88.73	notice	Start of NMAP update for 192.168.88.73
06/08/19 09:05	380	192.168.88.73	notice	Formatting system details
06/08/19 09:05	381	192.168.88.73	notice	End of NMAP update for 192.168.88.73
06/08/19 09:05	382	192.168.88.73	notice	Processing found ip addresses (non-snmp) for 192.168.88.73
06/08/19 09:05	383	192.168.88.73	notice	Updating ip with ID 7
06/08/19 09:05	384	192.168.88.73	notice	Processing Nmap ports for 192.168.88.73
06/08/19 09:05	385	192.168.88.73	notice	At IP 192.168.88.73, discovery found an unknown device.
06/08/19 09:05	386	192.168.88.73	fail	No valid credentials for 192.168.88.73
06/08/19 09:05	387	192.168.88.73	notice	Audit result incoming from target.
06/08/19 09:05	388	192.168.88.73	notice	Discovery has completed processing 192.168.88.73 .
06/08/19 09:05	389	192.168.88.73	success	IP 192.168.88.73 has successfully been sent to the server. Discovery script continuing to next IP. Command: Status: 200 URL: http://127.0.0.1/open-audit/index.php/input/discoveries Output: Response:
06/08/19 09:05	390	127.0.0.1	success	The discovery_id was used to successfully retrieve information for the discovery entry named local
06/08/19 09:05	391	127.0.0.1	success	Set discovery entry status to complete
06/08/19 09:05	392	127.0.0.1	finish	Completed discovery, scanned 1 IP addresses