Information about Network Ports

- Network Management Traffic for Open-AudIT installed on a Windows based server.
- Network Management Traffic for Open-AudIT installed on a Linux based server.
- Network Management User Traffic for Open-AudIT
- Optional LDAP / MS Active Directory traffic
- Optional Collector Server traffic
- Notes

For Open-AudIT to function, certain network ports must be enabled for communication.

Network Management Traffic for Open-AudIT installed on a Windows based server.

The following table shows the traffic required for using Open-AudIT and the related features that use each port.

Port #	Protocol	Service Name	Connection Initiation	Application	Notes
N/A	ICMP	ping	Server to Device	Open-AudIT	Discovery - ICMP Message Types 8 and 0
22	TCP	SSH	Server to Device	Open-AudIT	Discovery
25 or 587	TCP	SMTP	Server to Email Server	Open-AudIT	Scheduled Reports
53	UDP	DNS	Server to DNS Server	Open-AudIT	Discovery
53	TCP	DNS	Server to DNS Server	Open-AudIT	Discovery
135	TCP	WMI	Server to Device	Open-AudIT	Discovery
139	TCP	File and Print Sharing	Server to Device	Open-AudIT	Discovery
161	UDP	SNMP	Server to Device	Open-AudIT	Discovery
445	TCP	Active Directory	Server to AD Controller	Open-AudIT	Authentication and Discovery
49152-65535	TCP	WMI / AD	Server to Device	Open-AudIT	Discovery - MS Server 2008 and above, MS Vista and above targets
1025-5000	TCP	WMI / AD	Server to Device	Open-AudIT	Discovery - MS 2000, XP, 2003 targets

NOTE – See below for more details on Windows network port range requirements.

Network Management Traffic for Open-AudIT installed on a Linux based server.

The following table shows the traffic required for using Open-AudIT and the related features that use each port.

Port #	Protocol	Service Name	Connection Initiation	Application	Notes
N/A	ICMP	ping	Server to Device	Open-AudIT	Discovery - ICMP Message Types 8 and 0
22	TCP	SSH	Server to Device	Open-AudIT	Discovery
25 or 587	TCP	SMTP	Server to Email Server	Open-AudIT	Scheduled Reports
53	UDP	DNS	Server to DNS Server	Open-AudIT	Discovery
53	TCP	DNS	Server to DNS Server	Open-AudIT	Discovery
135	TCP	WMI	Server to Device	Open-AudIT	Discovery
139	TCP	Samba	Server to Device	Open-AudIT	Discovery
161	UDP	SNMP	Server to Device	Open-AudIT	Discovery
445	TCP	Samba / RPC	Server to Device	Open-AudIT	Discovery
445	TCP	Active Directory	Server to AD Controller	Open-AudIT	Authentication and Discovery

Network Management User Traffic for Open-AudIT

The following table shows the traffic required for a user to communicate with Open-AudIT or for Open-AudIT to communicate to the user.

Port #	Protocol	Service Name	Connection Initiation	App	Notes
80	TCP	HTTP	User to Server	OA	Web Interface
443	TCP	HTTPS	User to Server	OA	Web Interface

Optional LDAP / MS Active Directory traffic

If you use the optional LDAP Auth, you will likely need the below ports accessible from the Open-AudIT Server to the LDAP server.

OpenLDAP and Microsoft Active Directory require the same ports.

Port #	Protocol	Service Name	Connection Initiation	App	Notes
389	TCP	LDAP	Server to LDAP Server	OA	User authentication and/or authorisation
636	TCP	LDAPS	Server to LDAP Server	OA	User authentication and/or authorisation

Optional Collector Server traffic

If you are using Collectors for remote auditing you should consider the following.

Port #	Protocol	Service Name	Connection Initiation	App	Notes
80	TCP	HTTP	Collector to Server	OA	Not secure. Use HTTPS below instead if required
443	TCP	HTTPS	Collector to server	OA	Requires HTTPS/TLS setup on the Server to operate.

Note: You may also wish to consider the day to day administration of the operating system and open-audit configurations on the server e.g. enable ssh access to the device.

Notes

Microsoft's DCOM/WMI services typically use a large range of random ports to function.

When using a ***Windows*** installed version of Open-AudIT, RPC/DCOM/WMI uses port 135 from Open-AudIT server to client, which then informs Open-AudIT server of an available port and the target then accepts queries on that port and responds to Open-AudIT.

A typical network flow would be thus between two Windows computers (one being the Open-AudIT server, the other being the client computer being audited) would be:

1. Open-AudIT server says to client on port 135 "can we talk using DCOM/WMI?"
2. Client responds on port 135 "Yes, please use port 2000."
3. Open-AudIT server says to client on port 2000 "Here is a WMI query, please run it and return to me the result."
4. Client responds "Here is the result."

The ***Linux*** installed version of Open-AudIT does not use remote DCOM/WMI. Instead the Linux Open-AudIT server copies the audit script to the Windows target machine, then asks the Windows target machine to run the script (using RPC on port 445) and submit the result when it's finished back to the Linux Open-AudIT server. Hence, the *Linux* Open-AudIT server does not require the range of ports open that the *Windows* Open-AudIT server does.

A valuable reference for Remote WMI can be found on Microsoft's website, along with several other linked documents. Connecting to WMI on a Remote Computer - http://msdn.microsoft.com/en-us/library/aa389290(v=vs.85).aspx