Items affecting Discovery times

Items affecting Discovery times

- Subnet Size
- Non Root Discovery
- SNMP Credentials
- Network Speed
- Device Speed

When running a discovery, certain items will affect how fast a discovery runs and processes devices. The below are items to consider when creating and running discoveries.

Subnet Size

Obviously the larger the provided subnet, the longer a discovery will take. ***We recommend /24's for efficiency.*** There is nothing stopping you from using a /16 (65,535 hosts) or even a /8 (16777214 hosts), but do not expect them to complete in a reasonable timeframe. The first section of the discovery script sends the non-responding IP addresses to the Open-AudIT server, so even before actually discovering a responding hosts, this section (on a large subnet) may take minutes or even hours.

If you don't know what /24's you have and do know everything on your network is contained within a /16 (for example), personally I would run a /16 ONCE to determine what networks have devices, then export the networks, massage the result in Excel and import discoveries based upon those /24's. Obviously the first scan will take a long time, but that's the price you will have to pay.

Non Root Discovery

When we audit via SSH using a credential set that is not root, we attempt toi use sudo. When we use sudo we must set a timeout and weait for that to expire, before interactively providing the password. The default for this timeout is 5 minutes and is set in the configuration as "discovery_ssh_timeout". Now before you go making this nice and small, there is a gotcha. Your audit script must finish processing within this timout or it will be incomplete and the data retrieved will cause issues in terms of changes.

Five minutes may be overly generous (most of my systems audit in well under one minute), but because we don't know how YOUR systems audit, we're overly cautious. I usually set this to 2 minutes upon install.

SNMP Credentials

When we have several sets of SNMP credentials, discovering which credentials work can take a little while. Open-AudIT will try each set in turn and wait for them to timeout before attempting the next. For each SNMP (not SNMP v3) credential set, we attempt both SNMP v1 and SNMPv2 - so two timeouts. Needless to say, when you have a lot of SNMP credential sets and the working set for a particular device is attempted last - you'll just need to be patient.

Network Speed

Network speed is a factor. We use Nmap for the initial device detection and then communicate over WMI, SMB, SSH and/or SNMP. All of these traverse the network and compete will everything else on that network. Fats network means faster discoveries.

Device Speed

When running a discovery against a computer, the rate that the computer can complete the audit script depends on that computer, not on Open-AudIT. Faster computers will complete the audit scritp faster and hence make for a faster discovery.