SNMPv3 and Windows

The Problem

It seems that there is an issue in the SNMP PHP extension in that when we attempt to discover a device using SNMPv3 and if there are multiple credential sets that use the same security name, but different authentication and/or privacy settings, and we attempt to query a device using an incorrect credential set, subsequent attempts to query the device also fail - regardless of those subsequent attempts using the correct settings and credentials.

We have managed to work around this for Linux - we call out to the shell and run the credential tests there. This works.

Unfortunately for Windows we cannot do this.

Problem Definition

If the below all apply to you, you will be affected.

- Are running Open-AudIT on Windows
- Use SNMPv3
- Have identical security names, but differing authentication and/or privacy credentials and settings

Mitigation

For those subnet's that include these devices, you should create an individual device credential set **and** enable the match_ip config item. Once a device has been discovered, associating a specific credential set enables that credential set to be tested first. Enabling match_ip means that we will match that device without SNMP and retrieve this credential set.

Moving Forward

We plan to make assigning individual credential sets to devices easier to do. We also plan to enable the selection of a subset of credentials for a given discovery.

Both these features when combined with the above will alleviate most of the pain.

Changing Your Devices

You could always reconfigure your devices to use the exact same credentials.

Or you could add a new SNMPv3 user that is specifically for Open-AudIT and make it identical across all devices.

And don't forget you can always use the Linux version of Open-AudIT, or the Opmantek VM.

Mark Unwin.