Matching Devices - Including OrgID

With our next release of Open-AudIT (likely 4.3.4) we are further refining how we match devices discovered to devices in the database.

This is an optional configuration option, enabled by setting discovery_use_org_id_match in the global configuration.

When you create a discovery you have an option to ***devices_assigned_to_org***. This means that any devices discovered for this discovery will be assigned (have system.org_id set to) your chosen Organisation.

Previously we have ignored this in our match rules.

From this release onward, we **will** take this into account for devices for a certain defined subset of match rules. These rules are:

- match_dbus
- match_fqdn
- match_dns_fqdn
- match_hostname
- match_dns_hostname
- match_ip
- match_ip_no_data
- match_serial
- match_serial_type
- match_sysname

You might have noticed these match rules are for items that might not be globally unique. Some examples:

- DBus - if you clone a Linux virtual machine, unless you manually regenerate this (and in my experience, people do not) it will remain the same.
- FQDN - This *should* be globally unique, but I have seen instances where it is not.
- Hostname - Think of mail.domain1.com and mail.domain2.com - same hostname.
- IP - It is not uncommon to have an overlapping address space in a given Organisation. Not ideal, but not uncommon.
- Serial - It is very common for second tier motherboard manufacturers to not set this, to set it to all 0's or even all F's.
- Sysname - This is settable by users and so even though it *should* be globally unique, there is certainly no guarantee of this.

What does this actually mean to you?

If you don't normally set ***devices_assigned_to_org***, then it will have no effect. We *only* check using the OrgID if it has been set in discovery (or manually in an audit script).

If you *do* normally set ***devices_assigned_to_org***, then the OrgID will be used to further refine the match.

If you subsequently change the OrgID of a device after discovery then you will likely have a new device created the next time the discovery runs. In this instance, you should probably just unset ***devices_assigned_to_org*** before running subsequent discoveries. This is because (in this instance) you have told Open-AudIT "these devices from this discovery belong to Org X", but then changed the Org of the device. You have changed the stored devices information. In this case - there is no no longer a device belonging to Org X, so we create a new one.

If this change does not work for you, all is not lost. We have added a configuration item (set to **n** by default, so it will use not this new option out of the box) called discovery_use_org_id_match. If you change it to **y** then the OrgID assigned to the device by the discovery will be used in the relevant match rules.