NMIS and Open-AudIT Integrations

Introduction

So you have this great discovery and auditing tool called Open-AudIT. And you also have an amazing monitoring tool called NMIS. How can you automatically take your discovered devices and have NMIS monitor them? And why would you want to?

With version 4.2.0 of Open-AudIT, we have re-implemented Integrations in an extremely easy to use yet extremely configurable way.

Why?

Discovery provides network transparency. Monitoring provides network visibility. Both are essential to good network management and go hand in diagnosing network performance issues and device management and lifecycle. You cannot manage something if you don't know it exists and you cannot plan for the future if you don't know the current performance of your devices - be they desktops, servers, switches or routers.

Why wouldn't you want the ability to *automatically* monitor select device types (for example) as they come online? You can setup a scheduled Integration and automatically include all discovered routers and switches. Let that sink in for a minute. **Automatically** monitor devices without having to set them up individually in your monitoring solution. From discovery to monitoring automatically, on your terms. Less time spent entering details. More accurate information with zero possibility of spelling mistakes, mistyped credentials, etc. No double handling of information between systems is required. It just works.

Discover it in Open-AudIT, monitor it in NMIS - seamlessly.

How does it work?

Integrations take a list of devices from NMIS and a list of devices from Open-AudIT, matches the devices based on selected attributes, combines their attributes according to which system (NMIS or Open-AudIT) should be the point of truth and updates *both* systems based on any changes.

The list of devices may actually be empty on either side. We can restrict the devices list on either side based on device attributes. We can select attributes to be stored - even if they don't exist in Open-AudIT. And NMIS and Open-AudIT don't even need to be on the same server. There is so much flexibility!

But with great flexibility, comes (potentially) great complexity. This is an area we are particularly proud of. We have kept the creation of an Integration as easy as we can make it. At it's most simple level, if NMIS and Open-AudIT are installed on the same server, you can simply click a 'create' button and everything is done for you. You don't need to supply *any* information at all. We have chosen sensible defaults and the Integration "just works".

On the other end of the scale, you might have NMIS running on Debian and Open-AudIT running on Windows. You might wish to only integrate devices that are routers. And you might have some fields in NMIS that don't exist in Open-AudIT that you wish to track *and* be able to edit in Open-AudIT which updates NMIS. That is completely achievable with just a few clicks. More than the simple integration above, obviously - but still very easy to accomplish. No code to write, just a simple to use web interface. Oh - and there is also the JSON RESTful based Open-AudIT API as well 🙂

Questions

Now let's back up a little bit and set the scene. You've been using Open-AudIT for a while and have discovered some devices on your network. You have working credentials for these devices and can see their configuration. You may have computers, switches, printers, routers, firewalls, etc, etc.

How can we easily send some of these devices to NMIS for monitoring? When you create an Integration in Open-AudIT, by default we include all devices we have discovered that have working SNMP credentials. But you might not want every device integrated with NMIS. Some of your servers (for example) may use SNMP - but you don't need NMIS monitoring them. An integration has a section to select which devices to include from Open-AudIT. We include every device with it's "manage_in_nmis" attribute set to "y". We also have a Rule in Open-AudIT that set's this attribute if we talk to the device using SNMP. But as discussed, we don't want every SNMP talking device - in this case we only want our routers in NMIS. We can simply change the used Attribute to "type" (instead of "manage_in_nmis") and the value of that attribute to "router" (instead of "y") and we're done.

What if I want the SNMP Community string to be defined in NMIS, not Open-AudIT? An Integration contains a list of the fields used by both systems (NMIS and Open-AudIT). Each field has a flag that defines it's "priority". This can be set to either NMIS or Open-AudIT (actually stored as external or internal). Just select NMIS for the priority for the NMIS configuration.community field and if this value is changed in NMIS, the next time the Integration is run Open-AudIT will be updated.

How can I automatically run the Integration? Integrations can be scheduled within Open-AudIT just like discoveries, queries, baselines, et al. You can run an Integration on whatever time frame you choose.

What if I'm an NMIS user, have just installed Open-AudIT and don't have any devices in it? Again, just run the default Integration and your NMIS devices will be sent to Open-AudIT ***and discovered*** automatically. Open-AudIT stores more information about the make-up of a device, as opposed to NMIS's performance data. So when you run an Integration Open-AudIT has the device's IP and the device's credentials - so we run a discovery and retrieve everything Open-AudIT can. Again - this is configurable. You might not wish to run a discovery on the device - that's up to you! To enable or disable a discovery is a single attribute. Click, done!

Making it Happen

As usual, the Open-AudIT wiki has all the technical details that you should need. Just check the Integrations page here - Integrations and if there's something you don't see or questions you might have, please do ask in the Community Forums.