Open-AudIT and NMIS 9 Integration - customizing device selection and using multiple pollers (deprecated)

Please note that as at Open-AudIT 4.2.0, this page is no longer relevant. Please see the Integrations page.

Introduction

So you want to integrate the devices discovered in Open-AudIT with NMIS for network monitoring. But you don't want every device, and you don't want to have to manually flag devices for monitoring - you **know** you want every Juniper switch in Open-AudIT being monitored by NMIS. How can we do that without the painful effort of flagging individual devices with nmis_manage = y (even using Bulk Edit)?

As an aside, we *could* make a rule that states "if manufacturer LIKE Juniper, then set nmis_manage = y' and then use the default NMIS Integration query to solve it.

But what if we want to go one step further? What if we want Accedian routers managed by NMIS Poller A and Juniper switches monitored by NMIS Poller B? And because Poller A & B are just NMIS Pollers with no Open-AudIT installed, what gives?

Well, I'm glad you asked, read on 🙂

Selecting Devices

Integrations work by selecting a list of devices to be integrated. That list of devices is provided by a Query inside Open-AudIT. Our default query simply retrieves any devices with nmis_manage = y. But what if we create a new query to select any devices manufactured by Accedian? Well, go to menu Queries List Queries and select the query named "Integration Default for NMIS". You will see the SQL used. It is below.

```
SELECT system.id AS `system.id`, system.name AS `system.name`, system.hostname AS `system.hostname`, system.
dns_hostname AS `system.dns_hostname`, system.fqdn AS `system.fqdn`, system.dns_fqdn AS `system.dns_fqdn`,
system.ip AS `system.ip`, system.type AS `system.type`, system.credentials AS `system.credentials`, system.
nmis_group AS `system.nmis_group`, system.nmis_name AS `system.nmis_name`, system.nmis_role AS `system.
nmis_role`, system.nmis_manage AS `system.nmis_manage`, system.nmis_business_service AS `system.
nmis_business_service`, system.nmis_customer AS `system.nmis_customer`, system.nmis_poller AS `system.
nmis_poller`, system.snmp_version AS `system.snmp_version`, system.omk_uuid AS `system.omk_uuid`, locations.
name AS `locations.name`, IF(system.snmp_version != '', 'true', 'false') AS `system.collect_snmp`, IF(system.
os_group LIKE '%windows%', 'true', 'false') AS `system.collect_wmi` FROM `system` LEFT JOIN `locations` ON
system.location_id = locations.id WHERE @filter AND system.nmis_manage = 'y'
```

It's a simple matter of replacing the AND system.nmis_manage = 'y' with another condition. Our new query to select devices made by Accedian is below.

```
SELECT system.id AS `system.id`, system.name AS `system.name`, system.hostname AS `system.hostname`, system.
dns_hostname AS `system.dns_hostname`, system.fqdn AS `system.fqdn`, system.dns_fqdn AS `system.dns_fqdn`,
system.ip AS `system.ip`, system.type AS `system.type`, system.credentials AS `system.credentials`, system.
nmis_group AS `system.nmis_group`, system.nmis_name AS `system.nmis_name`, system.nmis_role AS `system.
nmis_role`, system.nmis_manage AS `system.nmis_manage`, system.nmis_business_service AS `system.
nmis_business_service`, system.nmis_customer AS `system.nmis_customer`, system.nmis_poller AS `system.
nmis_poller`, system.snmp_version AS `system.snmp_version`, system.omk_uuid AS `system.omk_uuid`, locations.
name AS `locations.name`, IF(system.snmp_version != '', 'true', 'false') AS `system.collect_snmp`, IF(system.
os_group LIKE '%windows%', 'true', 'false') AS `system.collect_wmi` FROM `system` LEFT JOIN `locations` ON
system.location_id = locations.id WHERE @filter AND system.manufacturer LIKE 'Accedian%'
```

So make a new query by menu Manage Queries Create Queries and name it ***Integration for Accedian Devices***. Paste in the SQL above and we're done.

If you want another integration for Juniper devices, repeat the above, obviously substituting Juniper for Accedian.

Now that we have our queries defined, it might be wise to test them. Just go to menu Manage Queries List Queries and Execute both of them, just to confirm the results are as expected.

Done? Great. Now make a note of the ID of each of these queries. You can see the ID on the queries read page (or in the URL when you execute the query).

Making the Integration

Now we need to go to the Pollers (assuming they're not on the same machine), and setup the individual integrations. They will work exactly the same, the only exception being the queries each runs (using the query IDs from above).

The details on how to do that are explained on the wiki page OpenAudIT-NMIS Integration, but I'll run you through it here using our example queries.

An integration run has the following steps:

1. Create the required configuration files.
2. Retrieve devices from Open-AudIT.
3. Create a node file suitable for passing into **node_admin.exe**
4. Create a new node if one does not exist, or update an existing node if it does.
5. Update the mapping of Open-AudIT devices to NMIS nodes.
6. Update the device on the Open-AudIT server if necessary.

Configuration

The following is a sample configuration file for the integration. The configuration is written in the **.nmis** format common to other Opmantek products and is placed in, **/usr/local/omk/conf/nmisIntegration.nmis**

Details of the below fields can be found on the page linked above. Obviously you will need to use your own host, password and user values. You'll need to use one of the query IDs from your newly created queries, above (replace 36 with it).

```
%hash = (

'integration_rules_path' => 'conf/integration_rules.nmis',
  'log_path' => 'log/nmisintegration.log',
  'node_admin_path' => '/usr/local/nmis9/admin/node_admin.pl',
  'node_file_path' => '/usr/local/nmis9/conf/Nodes.nmis',
  'open_audit_details' => {
    'host' => 'http://YOUR_SERVER',
    'log_path' => 'log/openauditapi.log',
    'password' => 'YOUR_OA_PASSWORD',
    'user' => 'YOUR_OA_USER'
  },
  'open_audit_lookup_path' => 'conf/oa_nmis_lookup.nmis',
  'open_audit_query_ids' => [36]
);
```

Integration Rules

The default integration rules can be left as is, and are below. These should be placed in the file **/usr/local/omk/conf/integration_rules.nmis**.

```
%hash = (
  'nmis' => {
    'create' => {
      'active' => ['true'],
      'authkey' => [],
      'authpassword' => ['$DEVICE.credentials.snmp_v3.authentication_passphrase'],
      'authprotocol' => ['$DEVICE.credentials.snmp_v3.authentication_protocol'],
      'businessService' => ['$DEVICE.system.nmis_business_service'],
      'collect' => ['$DEVICE.system.collect'],
      'collect_snmp' => ['$DEVICE.system.collect_snmp'],
      'collect_wmi' => ['$DEVICE.system.collect_wmi'],
      'community' => ['$DEVICE.credentials.snmp.community'],
      'customer' => ['$DEVICE.system.nmis_customer'],
      'display_name' => ['$DEVICE.system.name'],
      'group' => ['$DEVICE.system.nmis_group','Open-AudIT'],
      'host' => ['$DEVICE.system.ip','$DEVICE.system.dns_fqdn'],
      'location' => ['$DEVICE.locations.name'],
      'model' => ['automatic'],
      'name' => ['$DEVICE.system.name'],
      'netType' => ['wan'],
      'notes' => [],
      'ping' => ['true'],
      'port' => [161],
      'privkey' => [],
      'privpassword' => ['$DEVICE.credentials.snmp_v3.privacy_passphrase'],
      'privprotocol' => ['$DEVICE.credentials.snmp_v3.privacy_protocol'],
      'roleType' => ['$DEVICE.system.nmis_role','core'],
      'threshold' => [],
      'username' => ['$DEVICE.credentials.snmp_v3.security_name'],
      'uuid' => ['$DEVICE.system.omk_uuid'],
      'version' => ['$DEVICE.system.snmp_version'],
      'wmipassword' => ['$DEVICE.credentials.windows.password'],
      'wmiusername' => ['$DEVICE.credentials.windows.username']
    },
    'update' => {
      'active' => ['true'],
      'authpassword' => ['$DEVICE.credentials.snmp_v3.authentication_passphrase'],
      'authprotocol' => ['$DEVICE.credentials.snmp_v3.authentication_protocol'],
      'businessService' => ['$DEVICE.system.nmis_business_service'],
      'collect' => ['$DEVICE.system.collect'],
      'collect_snmp' => ['$DEVICE.system.collect_snmp'],
      'collect_wmi' => ['$DEVICE.system.collect_wmi'],
      'community' => ['$DEVICE.credentials.snmp.community'],
      'customer' => ['$DEVICE.system.nmis_customer'],
      'display_name' => ['$DEVICE.system.name'],
      'group' => ['$DEVICE.system.nmis_group','Open-AudIT'],
      'host' => ['$DEVICE.system.ip','$DEVICE.system.dns_fqdn'],
      'location' => ['$DEVICE.locations.name'],
      'model' => ['automatic'],
      'name' => ['$DEVICE.system.name'],
      'netType' => ['wan'],
      'ping' => ['true'],
      'port' => [161],
      'privpassword' => ['$DEVICE.credentials.snmp_v3.privacy_passphrase'],
      'privprotocol' => ['$DEVICE.credentials.snmp_v3.privacy_protocol'],
      'roleType' => ['$DEVICE.system.nmis_role','core'],
      'username' => ['$DEVICE.credentials.snmp_v3.security_name'],
      'version' => ['$DEVICE.system.snmp_version'],
      'wmipassword' => ['$DEVICE.credentials.windows.password'],
      'wmiusername' => ['$DEVICE.credentials.windows.username']
    }
  }
);
```

OA_NMIS_Lookup

You will need a blank file credted in /usr/local/omk/conf/oa_nmis_lookup.json

Usage

To run the integration, simply invoke the executable and pass it a configuration file as described in the previous section. You can also invoke the tool by itself, which will look for a configuration file at **/usr/local/omk/conf/nmisIntegration.nmis** by default.

While most of the integration is driven by the options set in the configuration file, additional options can be passed at runtime. These options can be seen in the usage instructions for the integration script.

```
# Calling the tool with a custom-named configuration file
./bin/oa-nmis-integration.exe conf=conf/my_custom_config.nmis

# Calling the tool by itself (uses conf/nmisIntegration.nmis)
./bin/oa-nmis-integration.exe

# Show additional options
./bin/oa-nmis-integration.exe -h
```

And that's it!

No, not really - one more step. You'll need to create a cron job for these to run on your poller(s) at the time of your choosing.

To enable the integration to run daily at 11:05am, place the following in a suitable cron job file.

```
5 11 * * * /usr/local/omk/bin/oa-nmis-integration.exe conf=/usr/local/omk/conf/my_custom_config.nmis
```

NOW you're done 🙂

If you have any questions relating to this, Opmantek are only too happy to assist.

Mark Unwin.