PNSN

Pacific Northwest Seismic Network

PNSN Review of Performance Monitoring w/Nagios

The importance of SNMP integration across all objects

By: Marc Biundo and Nathan Briley

Needs, Wants, HUGE WANTS…..

Needs:

To monitor current/ historical performance with notifications for our network devices, using an open standard network protocol.

Wants:

Have it scale with organization and help optimize system performance.

HUGE WANT:

Get instrument vendors to implement “SNMP Agents” for SOH Object Identifiers (Instrument SOH MIB/OIDs).

Two Main Instances of Nagios at PNSN

University of Washington IT Network System Monitoring / PNSN:

- Servers
- Routers
- Web Proxies

Field Operations:

- Field SOH and performance monitoring / histories
- Uptime statistics

What is SNMP?
Simple Network Management Protocol

It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network.

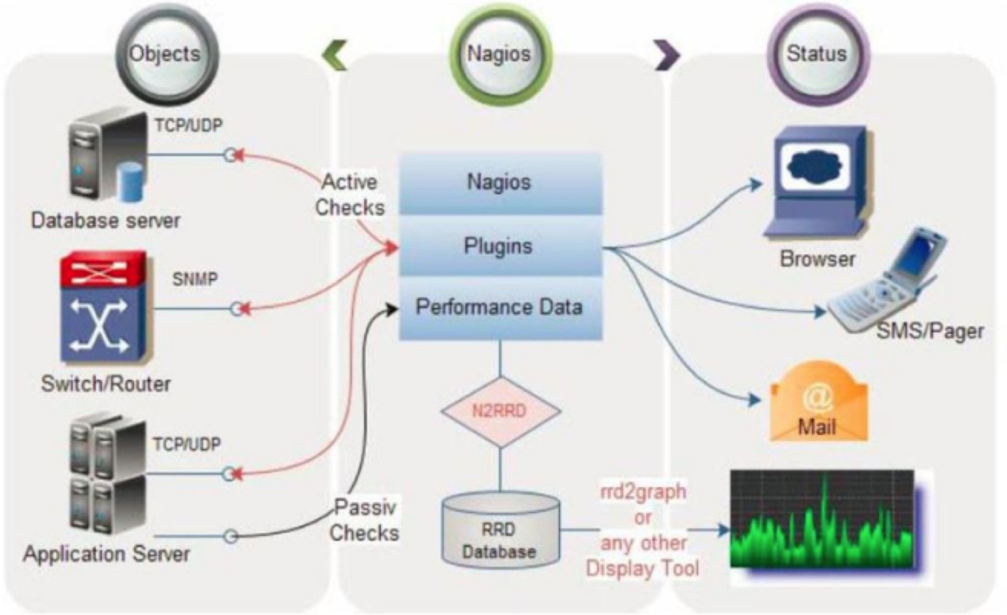
Cell modems, Radios support this protocol too.

Unfortunately: Seismic instruments don’t. **Can we change this?**

We propose the USGS make it a feature requirement for seismic instrument Purchase Agreements.

Nagios, a diagram... The Operating Principle.

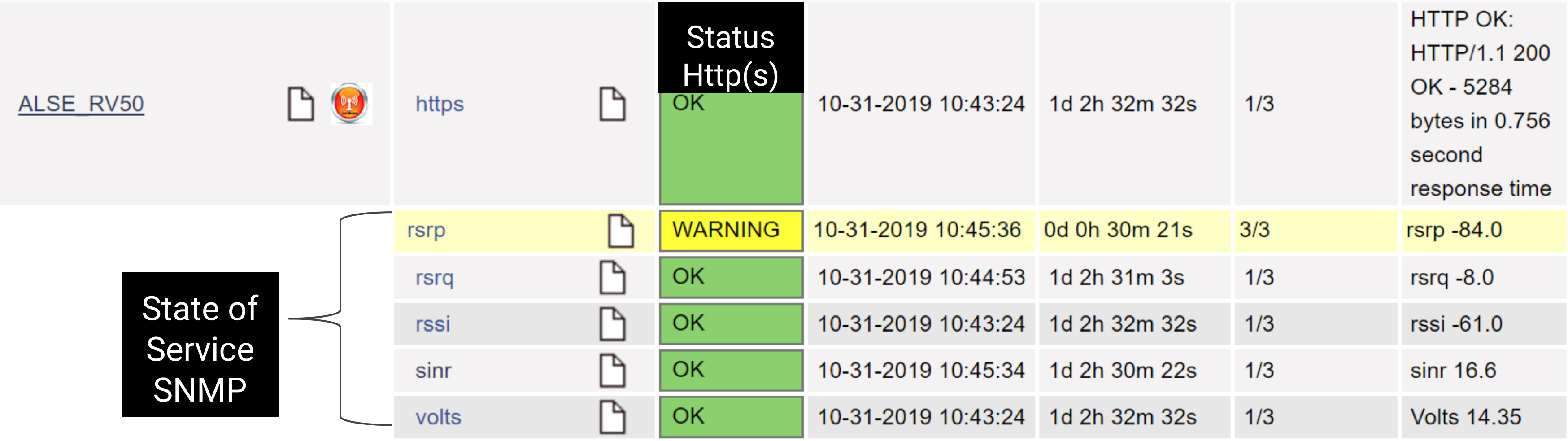
Nagios Core is open source software licensed under the GNU GPL V2.



What does Nagios communicate to user?

- Status of Devices: [UP, DOWN, Un-Reachable]

- State of Device Services: [OK, Warning, Critical] “Customizable”
  - ***NOTE*** Seismic Instruments not Included.



ALSE_RV50	https	OK	10-31-2019 10:43:24	1d 2h 32m 32s	1/3	HTTP OK: HTTP/1.1 200 OK - 5284 bytes in 0.756 second response time
	rsrp	WARNING	10-31-2019 10:45:36	0d 0h 30m 21s	3/3	rsrp -84.0
	rsrq	OK	10-31-2019 10:44:53	1d 2h 31m 3s	1/3	rsrq -8.0
	rssi	OK	10-31-2019 10:43:24	1d 2h 32m 32s	1/3	rssi -61.0
	sinr	OK	10-31-2019 10:45:34	1d 2h 30m 22s	1/3	sinr 16.6
	volts	OK	10-31-2019 10:43:24	1d 2h 32m 32s	1/3	Volts 14.35

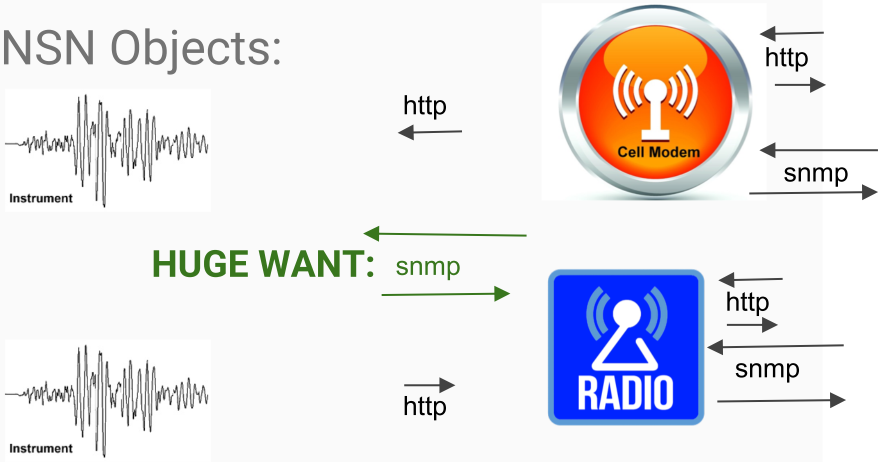
Status Http(s)

State of Service SNMP

PNSN
Pacific Northwest Seismic Network

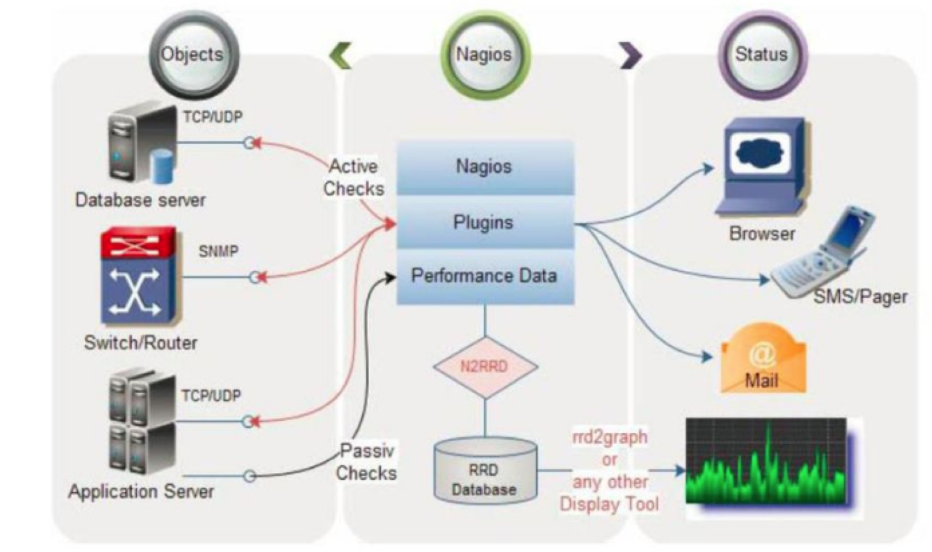
A diagram.. With PNSN Objects

PNSN Objects:



HUGE WANT: snmp

Http, Some vendors provide API's for SOH... I.E JSON API for Nanometrics.



PNSN
Pacific Northwest Seismic Network

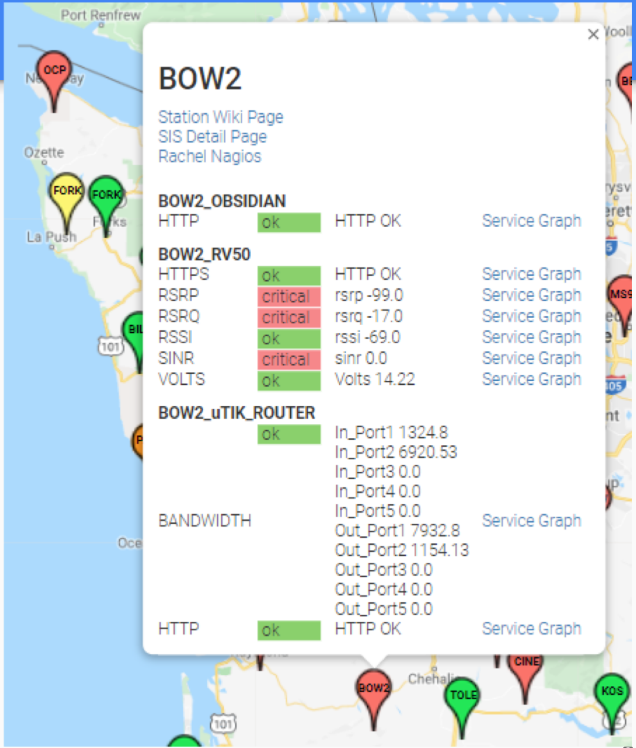
Quick look at Plugins

Mapped devices for Live Status:

Stock Google Maps API and hand coded the various integration (grouped pop ups, displays, filter, pins, etc).

Links into SIS:

It assumes the SIS entry is present and creates the link based on the pretty name format: https://anss-sis.scsn.org/sis/find/?net=UW&lookupcode=STATION



BOW2

Station Wiki Page
SIS Detail Page
Rachel Nagios

BOW2_OBSIDIAN

HTTP	ok	HTTP OK	Service Graph

BOW2_RV50

HTTPS	ok	HTTP OK	Service Graph
RSRP	critical	rsrp -99.0	Service Graph
RSRQ	critical	rsrq -17.0	Service Graph
RSSI	ok	rssi -69.0	Service Graph
SINR	critical	sinr 0.0	Service Graph
VOLTS	ok	Volts 14.22	Service Graph

BOW2_uTIK_ROUTER

BANDWIDTH	ok	In_Port1 1324.8 In_Port2 6920.53 In_Port3 0.0 In_Port4 0.0 In_Port5 0.0 Out_Port1 7932.8 Out_Port2 1154.13 Out_Port3 0.0 Out_Port4 0.0 Out_Port5 0.0	Service Graph
HTTP	ok	HTTP OK	Service Graph

PNSN
Pacific Northwest Seismic Network

Quick look at Plugins

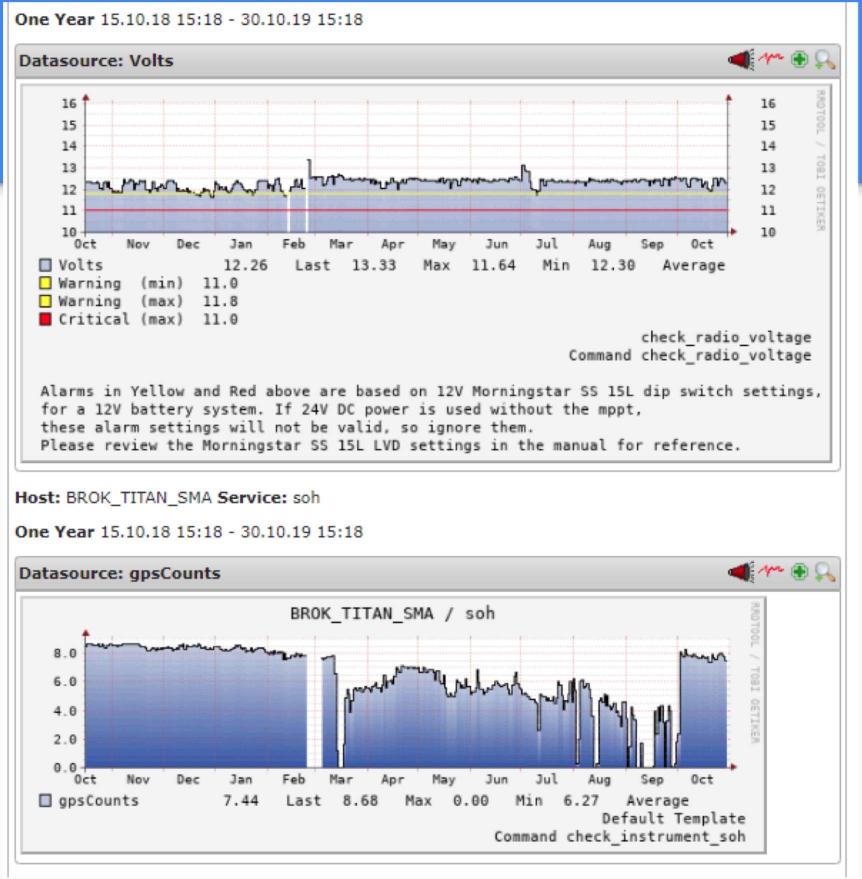
pnp4Nagios (Customizable Reports...pdf...): Easy to integrate...

PNSN_Check_SNMP(scaling...etc..etc): Used to help scale values returned.

PNSN_Check_rates(Mikrotik / Ubiquiti): Designed to convert octets to bits per second for Bandwidth....

PNSN_Check_JSON(Nanometrics SOH): This customization and TIME would not be needed if instrument vendors used SNMP.

PLUS.... This API Requires custom alarm code as well.



One Year 15.10.18 15:18 - 30.10.19 15:18

Datasource: Volts

```
□ Volts                  12.26  Last  13.33  Max  11.64  Min  12.30  Average
□ Warning  (min)  11.0
□ Warning  (max)  11.8
■ Critical (max)  11.0
                                                         check_radio_voltage
                                                 Command check_radio_voltage

Alarms in Yellow and Red above are based on 12V Morningstar SS 15L dip switch settings,
for a 12V battery system. If 24V DC power is used without the mppt,
these alarm settings will not be valid, so ignore them.
Please review the Morningstar SS 15L LVD settings in the manual for reference.
```

Host: BROK_TITAN_SMA **Service:** soh

One Year 15.10.18 15:18 - 30.10.19 15:18

Datasource: gpsCounts

```
□ gpsCounts              7.44  Last  8.68  Max  0.00  Min  6.27  Average
                                                    Default Template
                                            Command check_instrument_soh
```

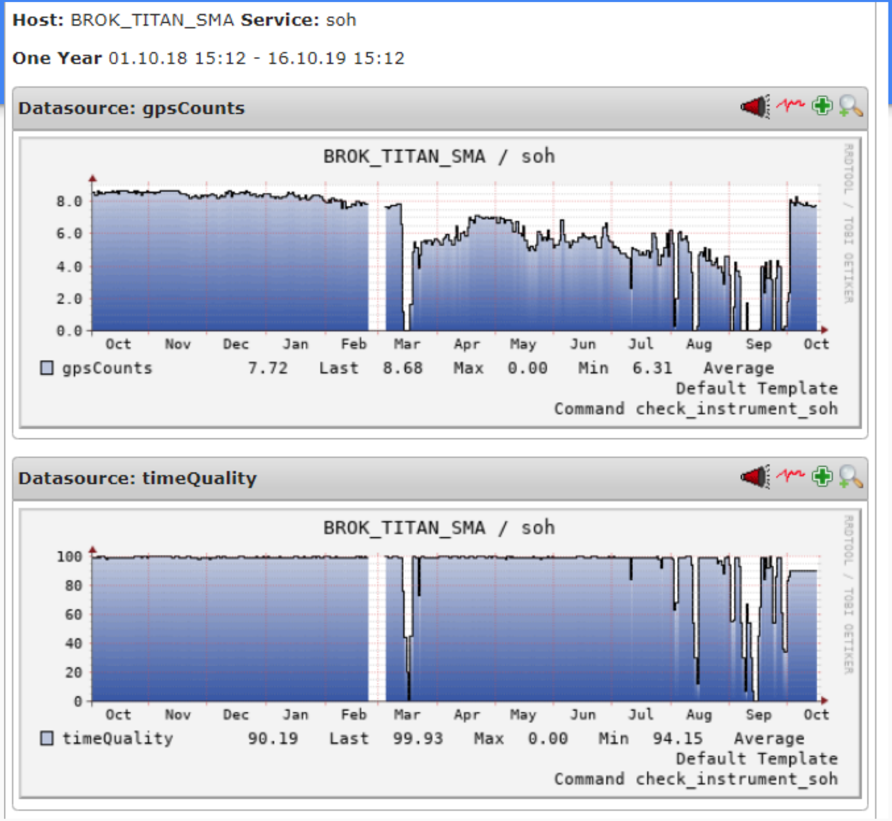
PNSN
Pacific Northwest Seismic Network

Why require SNMP in instruments? Obviously….

1. You would know if your network of sensors are having issues

2. Issues won’t sit waiting to be discovered because You can set an alarm

3. You can quickly find the root cause and rectify!



Host: BROK_TITAN_SMA **Service:** soh

One Year 01.10.18 15:12 - 16.10.19 15:12

Datasource: gpsCounts

BROK_TITAN_SMA / soh

```
□ gpsCounts        7.72  Last  8.68  Max  0.00  Min  6.31  Average
                                                  Default Template
                                        Command check_instrument_soh
```

Datasource: timeQuality

BROK_TITAN_SMA / soh

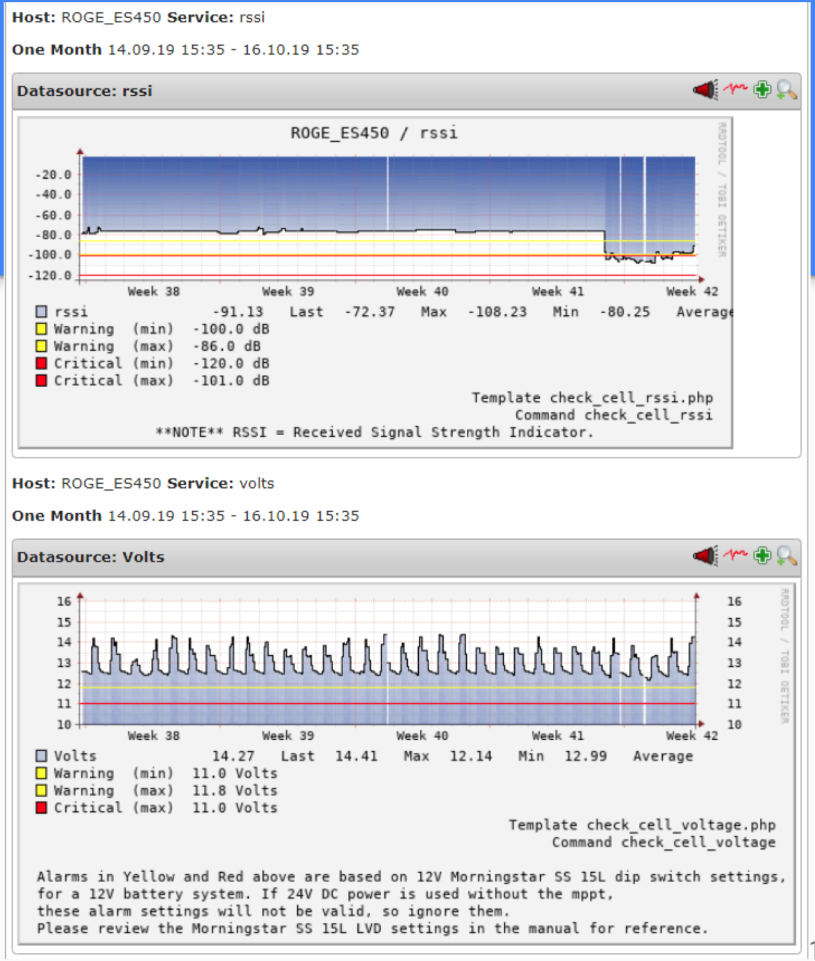
```
□ timeQuality      90.19  Last  99.93  Max  0.00  Min  94.15  Average
                                                  Default Template
                                        Command check_instrument_soh
```

PNSN
Pacific Northwest Seismic Network

A working example of an SNMP device….

We can set standard or custom alarms, system wide or site specific alarms for each device….

Using the standard, existing Alarm Handler.



Host: ROGE_ES450 **Service:** rssi

One Month 14.09.19 15:35 - 16.10.19 15:35

Datasource: rssi

```
🟦 rssi            -91.13  Last  -72.37  Max  -108.23  Min  -80.25  Average
🟨 Warning  (min)  -100.0 dB
🟨 Warning  (max)  -86.0 dB
🟥 Critical (min)  -120.0 dB
🟥 Critical (max)  -101.0 dB
                                                 Template check_cell_rssi.php
                                                   Command check_cell_rssi
                    **NOTE** RSSI = Received Signal Strength Indicator.
```

Host: ROGE_ES450 **Service:** volts

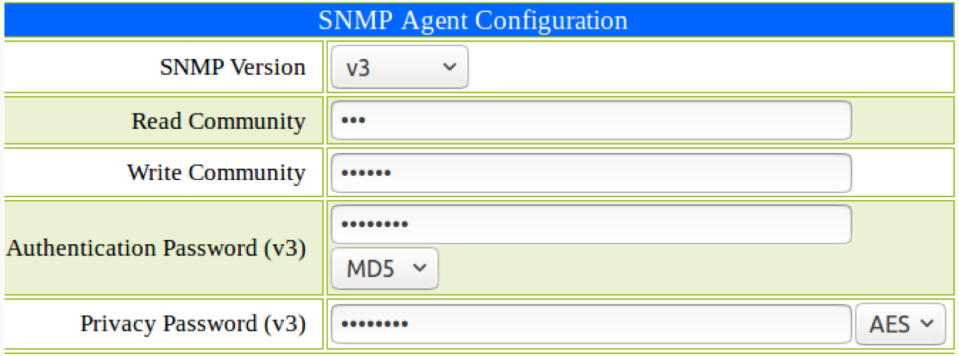
One Month 14.09.19 15:35 - 16.10.19 15:35

Datasource: Volts

```
🟦 Volts           14.27  Last  14.41  Max  12.14  Min  12.99  Average
🟨 Warning  (min)  11.0 Volts
🟨 Warning  (max)  11.8 Volts
🟥 Critical (max)  11.0 Volts
                                                 Template check_cell_voltage.php
                                                   Command check_cell_voltage

Alarms in Yellow and Red above are based on 12V Morningstar SS 15L dip switch settings,
for a 12V battery system. If 24V DC power is used without the mppt,
these alarm settings will not be valid, so ignore them.
Please review the Morningstar SS 15L LVD settings in the manual for reference.
```

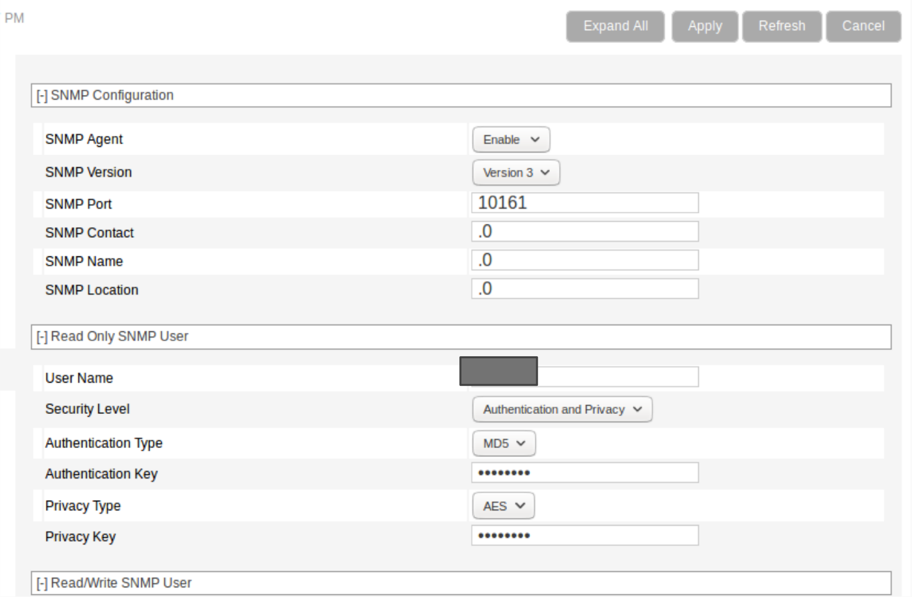
Snmp Configuration - Objects(Radio, Cell)

Easy to set in existing objects....



SNMP Agent Configuration

SNMP Version	v3
Read Community	•••
Write Community	••••••
Authentication Password (v3)	•••••••• MD5
Privacy Password (v3)	•••••••• AES



[-] SNMP Configuration

SNMP Agent	Enable
SNMP Version	Version 3
SNMP Port	10161
SNMP Contact	.0
SNMP Name	.0
SNMP Location	.0

[-] Read Only SNMP User

User Name	[redacted]
Security Level	Authentication and Privacy
Authentication Type	MD5
Authentication Key	••••••••
Privacy Type	AES
Privacy Key	••••••••

[-] Read/Write SNMP User

SOH in Meta Data?

This isn't helpful because currently it’s too cumbersome and time consuming to collect, analyse and interpret by our staff.

PNSN
Pacific Northwest Seismic Network

Nagios and SNMP Summary

The design, test, integration and “evangelizing” took time, and iterations….

We added complexity internally to simplify the use, management and extensibility.

I think the team likes it and helped improve their troubleshooting skills.

It has some cool Uptime/Availability reporting options too, for holistic SOH.

We can make it better if all devices support SNMP.

The End

Standard: Snmp calls from Nagios - Usage

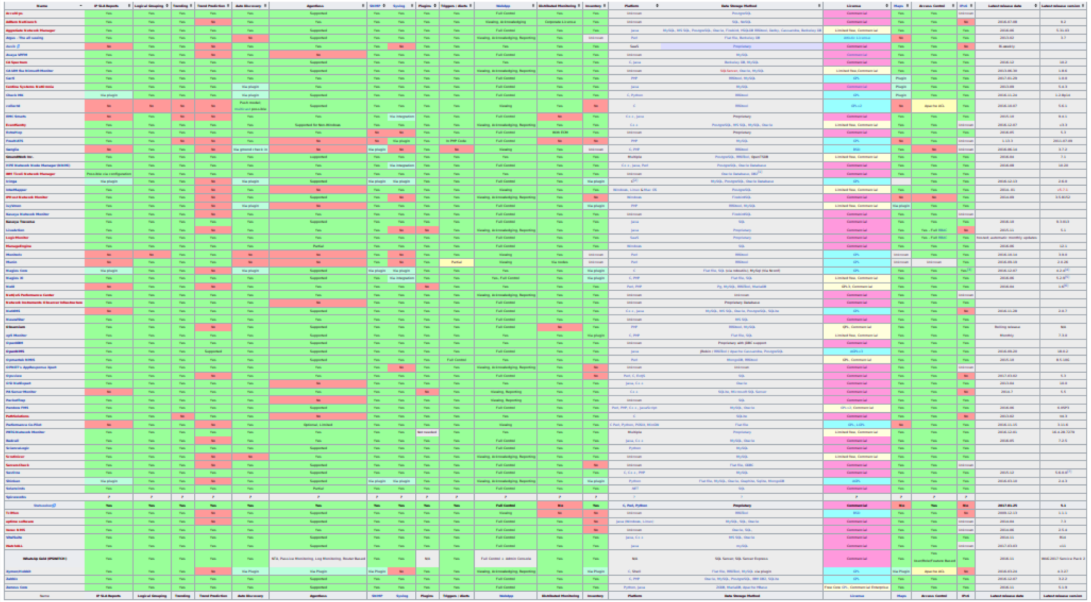
Usage:

```
check_snmp -H <ip_address> -o <OID> [-w warn_range] [-c crit_range]

[-C community] [-s string] [-r regex] [-R regexi] [-t timeout] [-e retries]

[-l label] [-u units] [-p port-number] [-d delimiter] [-D output-delimiter]

[-m miblist] [-P snmp version] [-N context] [-L seclevel] [-U secname]

[-a authproto] [-A authpasswd] [-x privproto] [-X privpasswd]
```

Network Monitoring Tools….Pick One.

Nagios,Icinga,Cacti,OpenNMS…..

- Comparison of network monitoring systems
- Icinga – A fork of Nagios Core
- Shinken – A fork of Nagios Core
- Naemon - A fork of Nagios Core



Is Nagios / SNMP Secure?

- We limit access to our Objects already… Limited connections, from UW Addresses. HTTP used for status, not PING.
- SNMP **v1** - Access or update any data using hardcoded community strings (public/private). Extremely susceptible to script kiddies
- SNMP **v2c** - May allow up to 1 secret (vendor dependent) sent in plaintext. For 1 secret setups it would protect against script kiddies but not against sniffing
- SNMP **v3** - Allows 2-3 secrets (vendor dependent) encrypted using AES or DES. Combined with firewall functionality this is extremely secure
- Why does it matter? Past examples of malicious SNMP attacks include locking out, bricking, and even physical damage of devices (printers/network gear).