

# Monitoring your ILS infrastructure with PRTG

By: Wes Osborn



**CENTRAL  
LIBRARY  
CONSORTIUM**  
CONNECTED. CREATIVE. CURRENT.



# Topics

What is monitoring? Why should you monitor?

Why use PRTG?

PRTG setup tips

General ILS Monitoring

Polaris Monitoring

# What and Why

Making the case monitoring

# What is monitoring?

A tool that continuously examines critical system components. It should alert staff of problems and provide historical information on system performance.

# What is monitoring?

Disaster preventer

Troubleshooting assistant

What caused an outage or performance issue

Resource planning tool

# Why monitor?



# Why monitor?



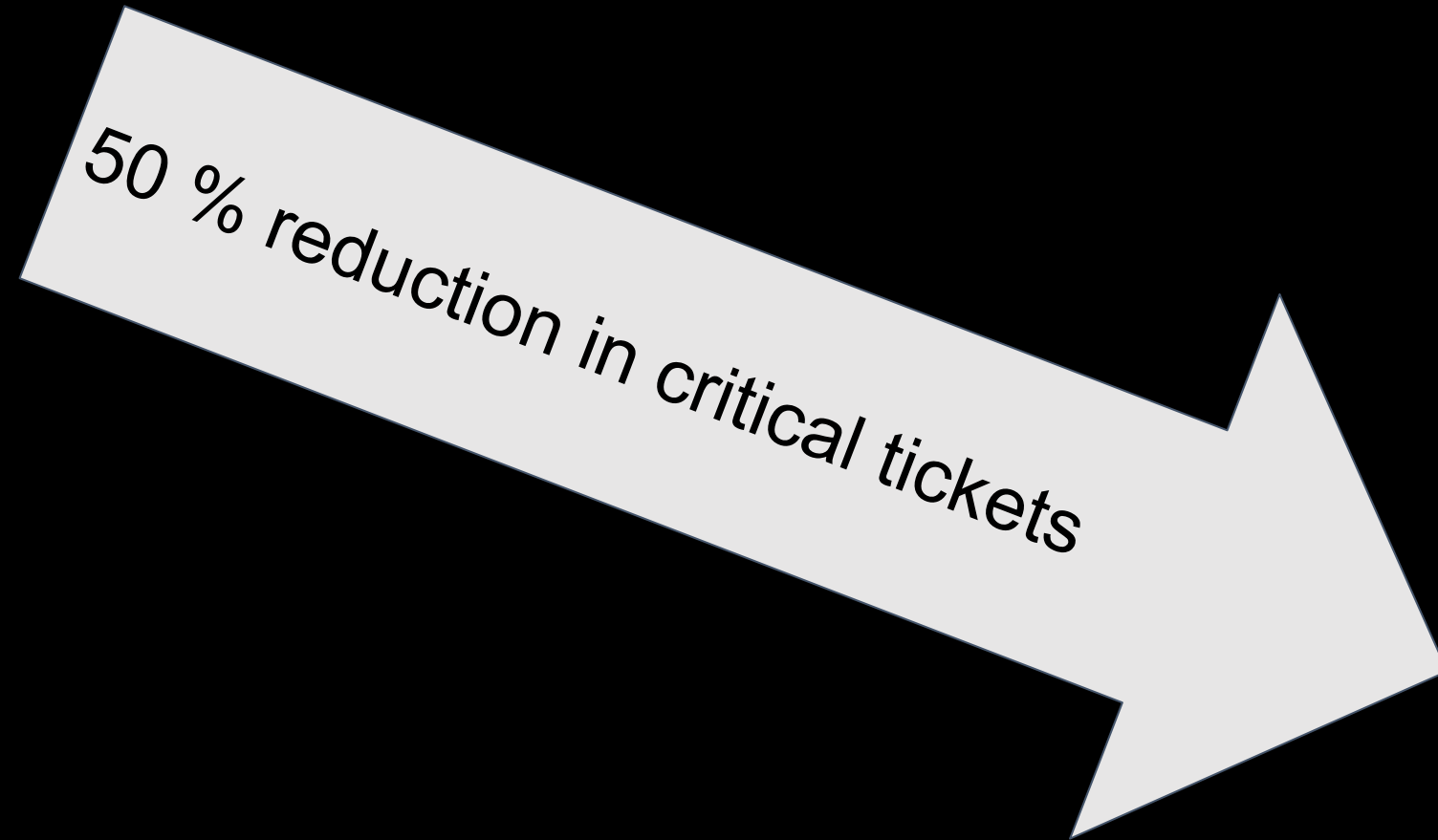
# Why monitor?





# Why monitor?

*50 % reduction in critical tickets*

A large white arrow pointing to the right, tilted slightly upwards. Inside the arrow, the text "50 % reduction in critical tickets" is written in a black, italicized font.

# Why PRTG?

There are lots of monitoring options, why choose PRTG?

# Lots of monitoring options

**Nagios®**

solarwinds® 



WhatsUpGold



# Why CLC chose PRTG?

Polaris means we're a windows shop

All in one installation

No separate DB install

Competitive price

**MONITOR**



**ALL THE THINGS!**

# Previous Monitoring Solution

Cacti for Network Bandwidth

SQL Jobs for common database / Polaris problems

Scheduled tasks for server issues

pingdom for PAC uptime



# What else does PRTG do?

Good defaults for alarms conditions

Also displays unusual activity

Multiple notification types

Full historical sensor detail (not rolled up)

Builtin reporting system (fullest disk, busiest CPU, etc.)



# PRTG UI Options

Main UI is browser based

Good Android and iOS Apps

Windows Desktop Notifier



# PRTG for Android

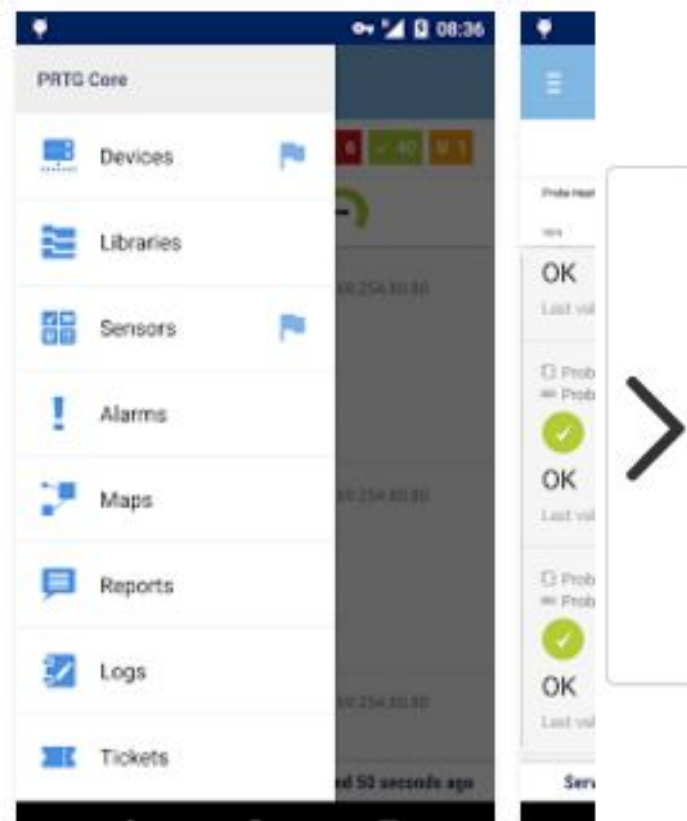
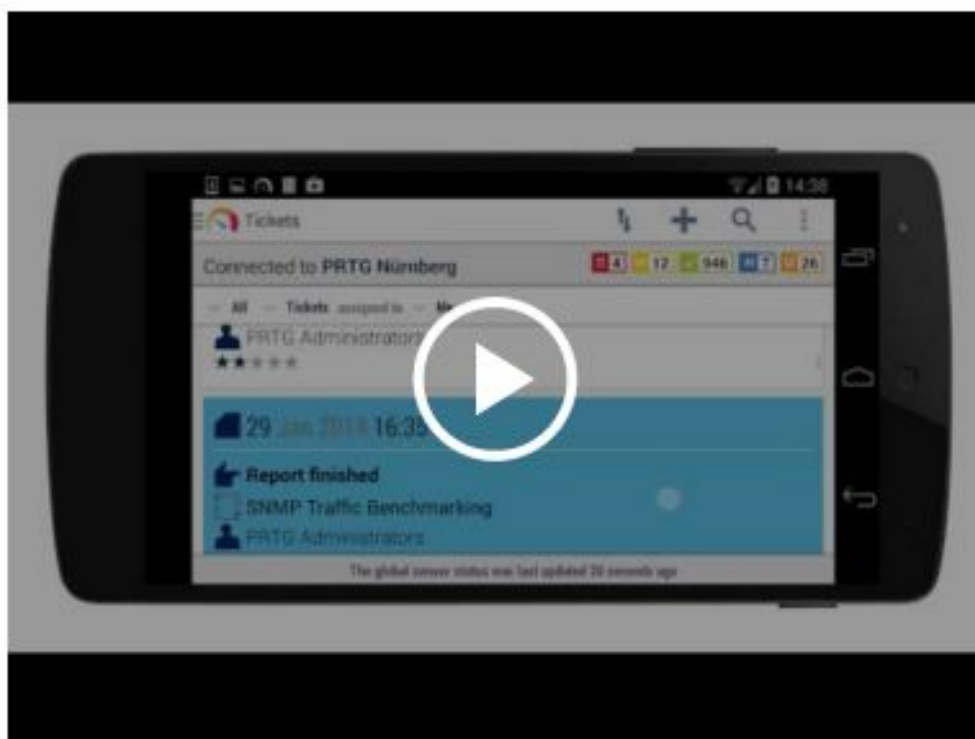
Paessler AG Business

★★★★☆ 938

**E** Everyone

**i** This app is compatible with some of your devices.

Installed



# Let's talk \$\$\$

100 sensors = Free

1000 sensors w/12 mon upgrade = \$2,020

Upgrade to 2,500 sensors w/24 mon upgrade = \$4,000

CLC System size = 60 VMs, 5 Physical Hosts, 2 Remote probes

We're using around 1,300 sensors

# PRTG Setup Tips

If you're not careful, you **WILL** be overwhelmed

# Get your accounts in order

Windows Domain Admin Account

Set up an exclusive PRTG service account

SNMP Accounts

Typically for network equipment, UPS, etc.

Database Account for running SQL Queries

Think  
**BIG**

Start  
small

# 1st rule of PRTG is Start Small

Do NOT allow PRTG to crawl your entire network

You can run the crawl later

Start with a single server

Your database server is a good idea

Do allow sensor recommendation to run

# What happens when things go wrong?

Different sensor states and how you should respond



# PRTG Sensor States

OK = Green, everything is functioning normally

Unusual = Orange, compared to average hour/day of week

Warning = Yellow, typically used for disk or memory levels

Also can be first occurrence of non-responsive sensor

Error/Down = Red, non-responsive or outside established

boundary

# Setup -> Notifications

How to know that something has gone wrong

# Notification methods

SEND EMAIL

SEND PUSH NOTIFICATION<sup>BETA</sup>

SEND SMS/PAGER MESSAGE

ADD ENTRY TO EVENT LOG

SEND SYSLOG MESSAGE

SEND SNMP TRAP

EXECUTE HTTP ACTION

URL

<http://chat.clcohoio.org/notify/sms?pn=6146649377&pn=4405446504&pn=6145629106&messz>

Postdata

EXECUTE PROGRAM

SEND AMAZON SIMPLE NOTIFICATION SERVICE MESSAGE

# Control notification volume

## NOTIFICATION SUMMARIZATION

Method

- Always notify ASAP
- Send first DOWN message ASAP, summarize others
- Send first DOWN and UP message ASAP, summarize others**
- Send all DOWN messages ASAP, summarize others
- Send all DOWN and UP messages ASAP, summarize others
- Always summarize notifications

Subject for Summarized Messages

**[%sitename] %summarycount Summarized Notifications**

Gather Notification For (Minutes)

**1**

# Conditions for notification

Setting up your notification methods

# Stacking notifications

## OBJECT TRIGGERS

Type ▼	Notifications	Actions
State Trigger	<p>When sensor state is <b>Down</b> for at least <b>60</b> seconds perform <b>HipChat Notification</b></p> <p>When sensor state is <b>Down</b> for at least <b>300</b> seconds perform <u>no notification</u> and repeat every <b>0</b> minutes</p> <p>When condition clears after a notification was triggered perform <b>HipChat Notification</b></p>	<a href="#">Edit</a> <a href="#">Delete</a>
State Trigger	<p>When sensor state is <b>Down</b> for at least <b>300</b> seconds perform <b>Email to clcdpc@clcoho.org</b></p> <p>When sensor state is <b>Down</b> for at least <b>300</b> seconds perform <u>no notification</u> and repeat every <b>0</b> minutes</p> <p>When condition clears after a notification was triggered perform <b>Email to clcdpc@clcoho.org</b></p>	<a href="#">Edit</a> <a href="#">Delete</a>
State Trigger	<p>When sensor state is <b>Down</b> for at least <b>300</b> seconds perform <b>SendTwilio SMS</b></p> <p>When sensor state is <b>Down</b> for at least <b>300</b> seconds perform <u>no notification</u> and repeat every <b>0</b> minutes</p> <p>When condition clears after a notification was triggered perform <u>no notification</u></p>	<a href="#">Edit</a> <a href="#">Delete</a>

# Other notification reasons

+ Add State Trigger

+ Add Speed Trigger

+ Add Volume Trigger

+ Add Threshold Trigger

+ Add Change Trigger

# Example speed trigger

Speed Trigger	When <input type="text" value="Primary"/> channel is <input type="text" value="Above"/> <input type="text" value="0"/> <input type="text" value="bit"/> / <input type="text" value="second"/> for at least <input type="text" value="60"/> seconds
	perform <input type="text" value="no notification"/>
	When condition clears after a notification was triggered perform <input type="text" value="no notification"/>



# Tweaking Channel Warning/Error level

## SET LIMITS CHECKED AGAINST ALL DISKS

Please use the particular channel settings to set separate error/warning limits for each disk.

Percentage Limit Check

- Only use the limits in the settings of the percentage channels
- Use the limits of both the sensor and the channel settings

Upper Error Limit

Upper Warning Limit

Lower Warning Limit

25

Lower Error Limit

10

Size Limit Check

- Only use the limits in the settings of the byte size channels
- Use the limits of both the sensor and the channel settings

Alarm on Missing/Removed  
Disk

- Deactivate alarm (default)
- Activate alarm

# 2nd rule of PRTG is never ignore errors

Error state is the most severe of the sensors states

Tweak sensors so they only alert for real problems

- Adjust schedules to work around known issues

- Remove “bad” sensors as needed

# THE BOY WHO CRIED WOLF!



You *MUST* address all errors!

You have to TRUST PRTG



# Handling Errors

Acknowledge them = takes them out of the error state


Continues to monitor the sensor, sensor can return to normal

Pause them = stops monitoring the sensor

Good option for flapping (up/down) sensors



# Acknowledging an alert


## Sensors With Status Down

Show sensors related to  Root »

✖ tagged with







1 to 1 of 1



Probe Group Device	Sensor	Status	Message
 WL Rem. »	 Probe Health	Down	Disconnected



 WL Probe Device


1 to 1 of 1

- Indefinitely
- 5m** For 5 minutes
- 15m** For 15 minutes
- 1h** For 1 hour
- 3h** For 3 hours
- 24h** For 1 day
- ?** Until

-  Settings...
-  Check Now
- Acknowledge Alarm(s) >
-  Pause >
-  Simulate Error Status
-  Priority/Favorite >
-  Delete...

Priority  Fav. 

★★★★★  

SML 

# Pausing an alert


**Sensor Probe Health** ★★★★★

Overview | Live Data | 2 days | 30 days | 365 days | Historic Data | Log | Settings | Notifications

Last Message: **Disconnected**

Last Scan:	Last Up:	Last Down:	Uptime:	Downtime:	Coverage:	Sensor Type:	Dependency:	Interval:
5 s	23 m 14 s	5 s	99.9934%	0.0066%	96%	Probe Health	Parent	every

Health



100 % 0 % 100 %

Live Graph, 2 hours

- Pause Indefinitely...
- 5m For 5 minutes...
- 15m For 15 minutes...
- 1h For 1 hour...
- 3h For 3 hours...
- 24h For 1 day...
- ? Until...
- One-time maintenance window...

Sensor Menu

- Check Now
- Details...
- Edit
- Acknowledge Alarm...
- Delete...
- Clone...
- Move
- Pause
- Simulate Error Status
- Priority/Favorite
- Historic Data
- Send Link by email
- Open Ticket



# All sensor activity is logged

Log Entries					
Items: 50 Date Range: 2016-03-06 00:00 - 2016-03-14 00:00					
Date Time	Parent	Type	Object	Status	Message
3/13/2016 12:43:00 AM	sccm01.clcdpc.org [Windows]	WMI Memory	Memory 38	Down Acknowledged	Memory is low when system is running patches (Acknowledged at 3/13/2016 12:43:00 AM by Wes Admin. Osborn until 3/13/2016 4:43:00 AM)

# PRTG UI Overview

Information dense, but for a reason

# UI Overview

Device list

Grouping and arranging

Individual Device view

Sensor list

Sensor funnels

# Dashboard

The screenshot displays the PRTG Network Monitor interface. At the top, there is a navigation menu with options like Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. A search bar is located on the right. Below the navigation, the dashboard title is "Dashboard 2". A summary bar indicates "New Log Entries 95" with a breakdown of 16 warnings (W), 1217 checks (V), 12 errors (E), and 0 unusals (U).

The main section is titled "Dashboard 2" and shows a summary of alerts: "0 Alarms, 0 Ack'ed Alarms, 16 Warnings, 34 Unusals". Below this is a table of sensor alerts:

Down for	Sensor	Status	Message	Probe Group Device	Priority
	(018) bond1.144 Traffic	Unusual	1 hour interval	10 Probe (192.168.10.1...) » CLC Firewalls » Gateway 1	★★★★
	(014) bond1.44 Traffic	Unusual	1 hour interval	10 Probe (192.168.10.1...) » CLC Firewalls » Gateway 0	★★★★
	(006) eth5 Traffic	Unusual	1 hour interval	10 Probe (192.168.10.1...) » Firewalls » UA Tremont	★★★★
	(008) eth1.20 Traffic	Unusual	1 hour interval	10 Probe (192.168.10.1...) » Firewalls » WAG Firewall	★★★★

Below the alert table is a section titled "GROUPS, DEVICES AND SENSORS". It shows a tree view starting with "Root" and "Local probe". Under "Local probe", there are several groups and their associated sensors:

- Probe Device**: Core Health (100%), Probe Health (100%), System Health (100%), Disk Free (47%), Common Saa... (100%), Microsoft Hy... (214 kbit/s), CLC Public W... (449 msec), CLC OCLC Co... (1,903 msec), ContentCafe... (291 msec), Number of o... (3,082 #), Windows Up... (33 h 36 m), CPU Load 1 (2%), XML Custom ... (No channel), Vulnerability ... (0 #), Vulnerability ... (0 #).
- Library WAN Routers**: 17 Sensors.
- Discourse & Unfi**: PING 13 (1 msec), SSL Security ... (Only Strong), SSH Disk Fre... (102,212 MB), SSL Certificat... (462 #), SSH INodes ... (0 %), SSH Load Av... (1.23), SSH Meminf... (36 %).
- Google DNS Ping**: Ping 34 (27 msec).
- prodweb.cicdpc.org**: 41 Sensors.
- prodpac**: PING 22 (1 msec), IIS Default W... (1,514 kbit/s), Disk Free 4 (70%), Memory 2 (92%), Uptime 4 (2 d 9 h 47 m), Microsoft Hy... (3,374 kbit/s), Windows Up... (33 h 35 m), Service: Elect... (57 msec), PAC Search R... (471 msec), Mobile PAC ... (304 msec), App Pool Mo... (Running), App Pool Po... (Running), App Pool We... (Running), CPU Load 76 (3%), SSL Security ... (Only Strong), RDP (Remote... (16 msec), SSL Certificat... (609 #).



# PRTG Hierarchy

Group = Any collection of devices

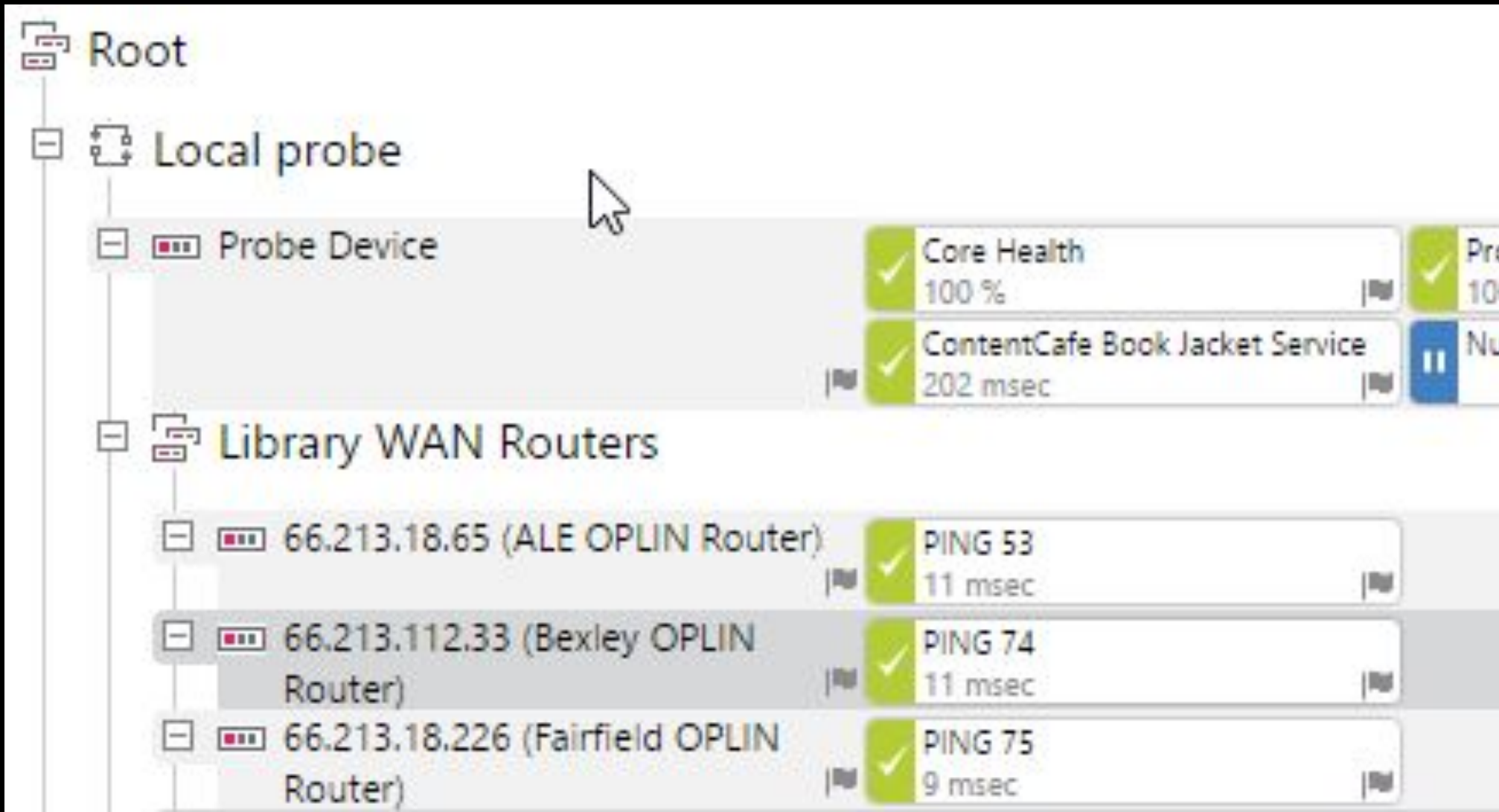
Device = Individual Server or piece of equipment

Sensor = Element of the device you want to monitor

Channel = Each sensor can have multiple channels

Percent Memory Free, Actual Megabytes Free Channels

# Tree Overview



# Adjusting the UI

## Drag&Drop

Within the same device, drag any sensor and drop it to the place where you want to have it. A grey shade will show the future position. When dropping, the sensor will be moved to this position and existing sensors will be lined up after it. This is a very easy way to reposition your sensors.

Drag sensors from one device and drop it to another to clone a sensor.

Drag and drop groups or devices to change their position or to move them into (other) groups.

## Multi-Edit


















You can use Multi-Edit for object settings: Hold down the *Ctrl* key and select multiple groups, devices, or sensors (one of a kind).



# Device Overview

PRODPAC

1 to 17 of 17

Pos	Sensor	Status
1.	 PING 22	Up
2.	 IIS Default Web Site	Up
3.	 Disk Free 4	Up
4.	 Memory 2	Up
5.	 Uptime 4	Up
6.	 Microsoft Hyper-V Network Adapter	Up
7.	 Windows Updates Status 2	Up
8.	 Service: Electronic Resource Management System (5.0)	Up
9.	 PAC Search Results	Paused
10.	 Mobile PAC Search	Up
11.	 App Pool MobileAppPool	Up
12.	 App Pool PowerPACAppPool	Up
13.	 App Pool WebAdminAppPool	Up
14.	 CPU Load 76	Up
15.	 SSL Security Check (Port 443) 7	Up
16.	 RDP (Remote Desktop) 29	Up
17.	 SSL Certificate Sensor (Port 443) 11	Up

1 to 17 of 17


Focusing on sensors

# Filter by Sensor Type









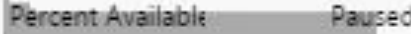




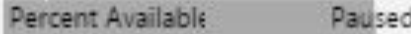




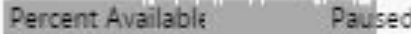



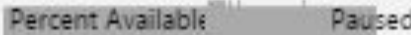
Sensors	Alarms	Maps	Reports	Logs	Tickets	Setup
All						Windows CPU Load
Add Sensor						Windows IIS 6.0 SMTP Sent
Favorite Sensors						Windows IIS Application
Top 10 Lists >						Windows Logged in Users
By Current Value >						Windows Network Card
By Current Status >						Windows Pagefile
By Uptime/Downtime >						Windows Physical Disk
By Group >						Windows System Uptime
By Type >	A...					Windows Updates Status (Powershell)
By Tag >	C...					WMI Event Log
Cross Reference >	D...					WMI Exchange Server
Compare Sensors >	E...					WMI Free Disk Space (Multi Disk)
View Historic Data	H...					WMI Logical Disk
	M...					WMI Memory
	P...					WMI Microsoft SQL Server 2014
	R...					WMI Remote Ping
	S...					WMI Service
	W...					WMI Vital System Data (V2)

# All Memory Sensors

## WMI Memory Sensors

Show sensors related to **any Object (click to select)**  tagged with

1+ ← 1 to 50 of 52 → →

Probe Group Device	Sensor	Status	Message	Last Value	Graph
 Local probe (Local Probe) »  prodweb.clcdpc.org	 Memory 8	Paused	Paused by schedule	-	 Paused
 .10 Probe (192.168.10.1... »  Non-Polaris Windows »  msscdb.clcdpc.org	 Memory 33	Paused	Paused by schedule	-	 Paused
 .10 Probe (192.168.10.1... »  Non-Polaris Windows »  mysqlprod.clcdpc.org	 Memory 34	Paused	Paused by schedule	-	 Paused
 .10 Probe (192.168.10.1... »  Non-Polaris Windows »  prodbackup.clcdpc.org [Altaro]	 WMI Memory 3	Paused	Paused by schedule	-	 Paused
 .10 Probe (192.168.10.1... »  Non-Polaris Windows »	 WMI Memory 1	Paused	Paused by schedule	-	 Paused


# Sensor state “funnels”

The screenshot displays the PRTG Network Monitor interface. At the top left, the word "Setup" is visible. The main header reads "PRTG NETWORK MONITOR". Below this, a row of five colored boxes represents different sensor states: a grey box for "New Log Entries 95", a yellow box for "w 16", a green box for "✓ 1217", a blue box for "|| 12", and an orange box for "U 34". A mouse cursor is hovering over the yellow box, which has triggered a tooltip that says "16x Warning". In the top right corner, there are icons for currency, help, and power, along with a search bar. At the bottom right, there are icons for a home page and a mail notification.

Sensor State	Count
New Log Entries	95
w (Warning)	16
✓ (OK)	1217
(Paused)	12
U (Unknown)	34




























# Funneling on unusual sensors only

## Sensors With Status Unusual

Show sensors related to  Root »

✖ tagged with

1 ← 1 to 28 of 28 → 28

Probe Group Device	Sensor	Status
 Local probe (Local Probe) »  Library WAN Routers »  rrcs-24-106-162-181.central.biz.rr.com (MPL Raymond TW modem)	 PING 86	Unusual
 .10 Probe (192.168.10.123) »  FS01 (Backup Storage - Gahanna)	 Microsoft Network Adapter Multiplexor Driver	Unusual
 .10 Probe (192.168.10.123) »  Hyper-V Hosts »  hyperv07.clcdpc.org	 Hyper-V Virtual Ethernet Adapter _2	Unusual
 .10 Probe (192.168.10.123) »  Hyper-V Hosts »  hyperv07.clcdpc.org	 Broadcom BCM57800 NetXtreme II 1 GigE [NDIS VBD Client] _239	Unusual
 .10 Probe (192.168.10.123) »  Hyper-V Hosts »  hyperv07.clcdpc.org	 Broadcom BCM57800 NetXtreme II 10 GigE [NDIS VBD Client] _237	Unusual
 .10 Probe (192.168.10.123) »  Hyper-V Hosts »  hyperv08.clcdpc.org	 Broadcom BCM57800 NetXtreme II 10 GigE [NDIS VBD Client] _221	Unusual
 .10 Probe (192.168.10.123) »  Hyper-V Hosts »  hyperv08.clcdpc.org	 Broadcom BCM5709C NetXtreme II GigE [NDIS VBD Client] _226	Unusual

# PRTG Sensors

This is where we get into the good stuff

**SO MUCH**



**AWESOME**



# Typical Sensors

Ping = All other sensors are dependent on Ping

Disk Free = Monitors all device drives

Memory Usage = VMs with Dynamic RAM can throw off

Network adapter = One sensor per adapter

System Uptime

Windows Update status (assuming Windows box)

# Add Sensor to Device Probe Device [127.0.0.1] (Step 1 of 2)

## SEARCH



251 Matching Sensor Types

### MONITOR WHAT?

- Availability/Uptime
- Bandwidth/Traffic
- Speed/Performance
- CPU Usage
- Disk Usage
- Memory Usage
- Hardware Parameters
- Network Infrastructure
- Custom Sensors

### TARGET SYSTEM TYPE?

- Windows
- Linux/MacOS
- Virtualization OS
- File Server
- Email Server
- Database
- Cloud Services

### TECHNOLOGY USED?

- Ping
- SNMP
- WMI
- Performance Counters
- HTTP
- SSH
- Packet Sniffing
- NetFlow, sFlow, jFlow
- Powershell
- Push Message Receiver
- PRTG Cloud

## MOST USED SENSOR TYPES

### PerfCounter IIS Application Pool ?

Monitors IIS Application Pools using Performance Counters



Add This ▶

### Ping ?

Monitors connectivity using Ping



Add This ▶

### SNMP Disk Free ?

Monitors the free disk space on a logical disk via SNMP



Add This ▶

### SNMP Memory ?

Monitors the memory usage via SNMP



Add This ▶

### SNMP Traffic ?

Monitors bandwidth and traffic on servers, PCs, switches, etc. using SNMP



Add This ▶

### Windows CPU Load ?

Monitors CPU load using performance counters or WMI



Add This ▶

3rd rule of PRTG,  
document all custom sensors

You'll never remember what it was for otherwise

# Sensor comments

|| Sensor Check for duplicate SimplyReport Exports 

Overview

Live Data


2 days


30 days

365 days

Historic Data

Log

 Settings

 Notifications

 !



**There are two reports scheduled to export bibs at the same time, this can cause the scheduling executive to freeze to Support ticket #227591.**

Run the following SQL to determine which reports are at risk:

Let's break out the custom sensors!



These should work for all ILS platforms



# HTTP Keyword Sensor

Make sure that the PAC is actually returning results

# HTTP Keyword monitor

## HTTP SPECIFIC

Timeout (Sec.)

60

URL

<https://catalog.clcoho.org/polaris/search/searchresults.aspx?ctx=49.1033.0.0.14&type=Keywo>

Request Method

- GET
- POST
- HEAD

Server Name Indication

prodpac.clcdpc.org



# HTTP Keyword monitor

Require Keyword

- Do not check for keyword (default)
- Set sensor to warning if keyword is missing
- Set sensor to error if keyword is missing**

Response Must Include

Tremont

Check Method

- String search (default)**
- Regular expression

Exclude Keyword

- Do not check for keyword (default)**
- Set sensor to warning if keyword is found
- Set sensor to error if keyword is found

# Checking TLS Security

Make sure that the PAC or other HTTPS services are actually secure

# SSL Certificate Sensor

Channel ▼	ID	Last Value	Minimum	Maximum	Settings
Common Name Check	7	Disabled	Disabled	Disabled	⚙️
Days to Expiration	2	599 #	599 #	635 #	⚙️
Downtime	-4				⚙️
Public Key Length	5	Good (2048)	Good (2048)	Good (2048)	⚙️
Revoked	4	No	Unable to check revocation status	No	⚙️
Root Authority Trusted	3	Yes	Yes	Yes	⚙️
Self-Signed	6	No	No	No	⚙️

# SSL Security Check Sensor

Channel ▾	ID	Last Value	Minimum	Maximum	Settings
Downtime	-4				⚙️
Security Rating	2	Only Strong Protocols Available	No Secure Protocol Available	Only Strong Protocols Available	⚙️
SSL 2.0 (Weak)	3	Denied	Denied	Denied	⚙️
SSL 3.0 (Weak)	4	Denied	Denied	Denied	⚙️
TLS 1.0 (Strong)	5	Accepted	Denied	Accepted	⚙️
TLS 1.1 (Strong)	6	Accepted	Denied	Accepted	⚙️
TLS 1.2 (Perfect)	7	Accepted	Denied	Accepted	⚙️

# More SSL Checks

<https://www.ssllabs.com/ssltest/>

# Checking 3M SIP Protocol

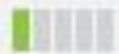
Make sure this ancient service is still limping along

# Search for “TCP” Sensor Type

## MATCHING SENSOR TYPES

Port ?

Monitors a network service by connecting to its TCP/IP port.



Add This ▶

Port Range ?

Monitors a network service by connecting to various TCP/IP ports.



Add This ▶

# SIP TCP Port Monitor

## PORT SPECIFIC

Timeout (Sec.)

60

Port

5001

## TRANSPORT-LEVEL SECURITY

Security

- Do not use Transport-Level Security (default)
- Use Transport-Level Security

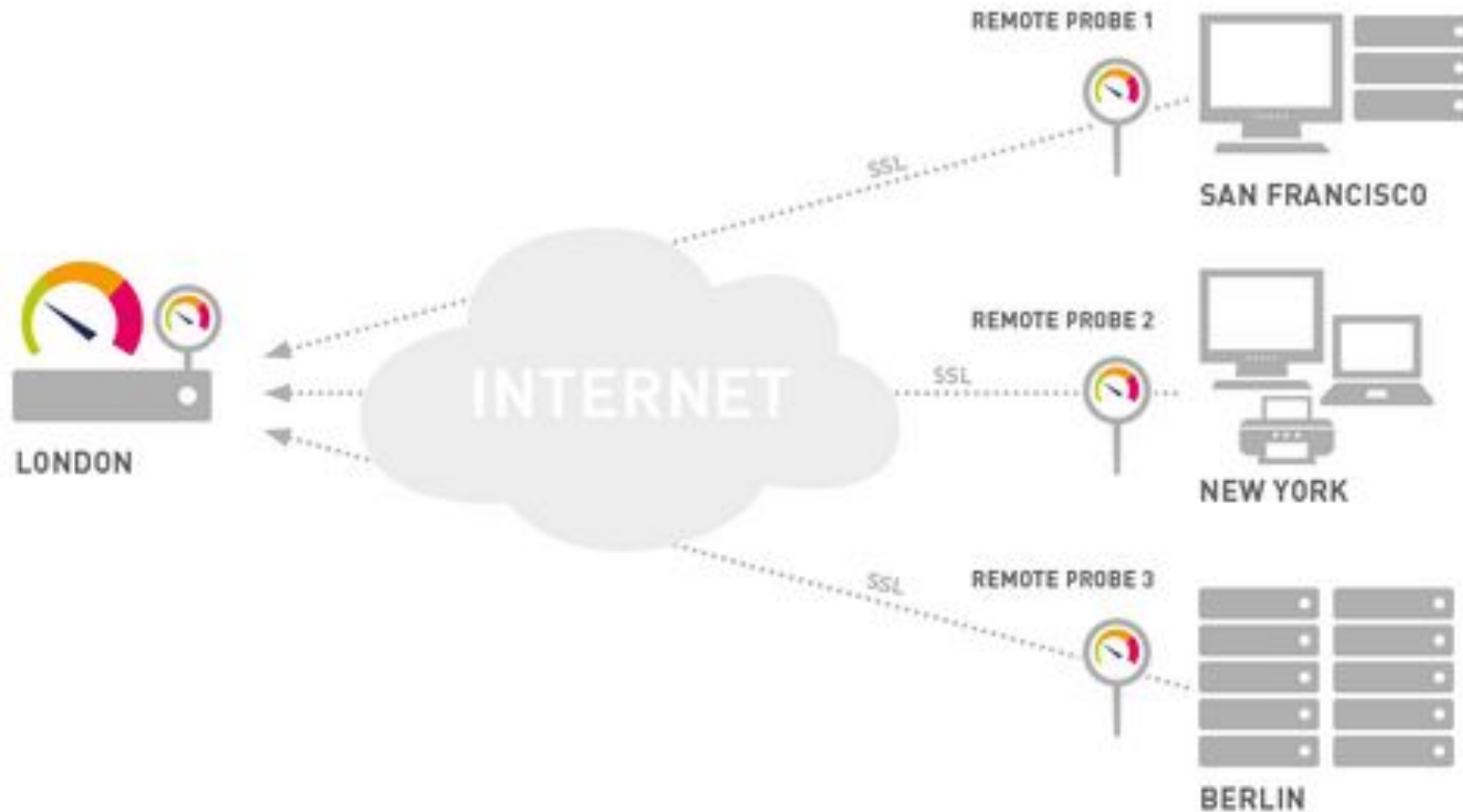
## ADVANCED SENSOR SETTINGS

Goal

- Open
- Closed



# Port tests are good for remote probes



Monitoring Remote Locations via Remote Probes

# SIP Transaction tests

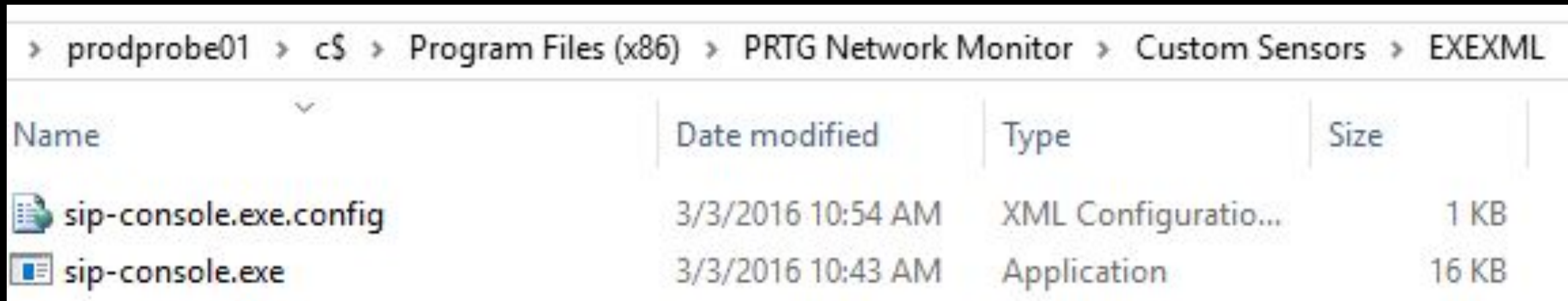
<http://www.clcohoio.org/sip-testing-tool>

# Download the command line tool



There is also a version of the command line tool that is tailored specifically to the PRTG monitoring tool that [can be found here](#). This version is configured through a config file and an example is included. It can monitor multiple SIP servers on one sensor and uses value lookups for better status reporting.

# Add the files to your PRTG Server

c:\Program Files (x86)\PRTG Network Monitor\Custom Sensors\EXEXML



The screenshot shows a Windows File Explorer window with the following path: > prodprobe01 > c\$ > Program Files (x86) > PRTG Network Monitor > Custom Sensors > EXEXML. The window displays a list of two files:

Name	Date modified	Type	Size
 sip-console.exe.config	3/3/2016 10:54 AM	XML Configuratio...	1 KB
 sip-console.exe	3/3/2016 10:43 AM	Application	16 KB

# Edit .ini file to add needed info

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <configSections>
    <section name="settings" type="sip_console.CustomSettings, sip-console"/>
  </configSections>
  <settings>
    value_lookup_name="clc.custom.sip.server.status">
      <sip_servers>
        <add hostname="prodsip01" port="5002" ao="7" username="3MLogin" password="3MLogin" />
        <add hostname="prodsip02" port="5002" ao="7" username="3MLogin" password="3MLogin" />
      </sip_servers>
    </settings>
    <startup>
      <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.2" />
    </startup>
  </configuration>
```

# Add Custom/EXE Advanced Sensor

## BASIC SENSOR SETTINGS

Sensor Name

XML Custom EXE/Script Sensor 1



Parent Tags

Tags

xmlksesensor ✕

Priority



## SENSOR SETTINGS

**Important:** The EXE file has to run on the computer where the parent probe is installed, not on the parent device. The working directory for "exe" files is the probe directory, "vbs,ps1" or other script files may use different working directories.

EXE/Script

sip-console.exe



# Channels will be created for each server described in the .ini file

Channel ▼	ID	Last Value	Minimum	Maximum	Settings
Downtime	-4				⚙
prodsip01	2	Up	Up	Up	⚙
prodsip02	3	Up	Up	Up	⚙

# Enriched Content Check

Outage of book jacket service can cause havoc



# HTTP Sensor

## HTTP SPECIFIC

Timeout (Sec.)

60

URL

https://contentcafe2.btol.com/ContentCafe/Jacket.aspx?Return=1&Type=L&Value=978146543

Request Method

- GET
- POST
- HEAD

Server Name Indication

contentcafe2.btol.com

## PROXY SETTINGS FOR HTTP SENSORS

inherit from  Probe Device (Name: <empty>, Port: 8080, User: <empty>)

## SENSOR DISPLAY

Primary Channel

Loading time (msec) ▼

Chart Type

- Show channels independently (default)
- Stack channels on top of each other


# Logged in users?

Did someone forget to logout?

# Adding the sensor & adjusting the limits

**Windows Logged in Users** ?

Returns the number of users currently logged into the parent device.



**Add This** ▶

Limits

Disable Limits

**Enable Limits**

Upper Error Limit (#)

Upper Warning Limit (#)

Lower Warning Limit (#)

Lower Error Limit (#)

Error Limit Message

Warning Limit Message

# Meeting PCI DSS 6.1

How are you monitoring for security vulnerabilities?

# CVE Details website

## [Cisco](#) : Security Vulnerabilities Published In 2016 (Execute Code)

2016 : [January](#) [February](#) [March](#) [CVSS Scores Greater Than: 0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[Copy Results](#) [Download Results](#) [Select Table](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication
1	<a href="#">CVE-2016-1359</a> <a href="#">20</a>			Exec Code	2016-03-03	2016-03-04	6.5	None	Remote	Low	Single system

Cisco Prime Infrastructure 3.0 allows remote authenticated users to execute arbitrary code via a crafted HTTP request to view the contents of a log file, aka Bug ID CSCuw81494.

2	<a href="#">CVE-2016-1320</a> <a href="#">78</a>			Exec Code	2016-02-11	2016-02-25	6.8	Admin	Local	Low	Single system
---	--	--	--	-----------	------------	------------	-----	-------	-------	-----	---------------

The CLI in Cisco Prime Collaboration 9.0 and 11.0 allows local users to execute arbitrary OS commands as root by exploiting a vulnerability in the CLI, aka Bug ID CSCux69286.

3	<a href="#">CVE-2016-1308</a> <a href="#">89</a>			Exec Code Sql	2016-02-07	2016-02-16	6.5	None	Remote	Low	Single system
---	--	--	--	------------------	------------	------------	-----	------	--------	-----	---------------

SQL injection vulnerability in Cisco Unified Communications Manager 10.5(2.13900.9) allows remote authenticated users to execute arbitrary SQL commands via a crafted URL, aka Bug ID CSCux99227.

4	<a href="#">CVE-2015-6435</a> <a href="#">78</a>			Exec Code	2016-01-22	2016-01-25	10.0	None	Remote	Low	Not required
---	--	--	--	-----------	------------	------------	------	------	--------	-----	--------------

An unspecified CGI script in Cisco FX-OS before 1.1.2 on Firepower 9000 devices and Cisco Unified Computing System 2.2(4b), 2.2(5) before 2.2(5a), and 3.0 before 3.0(2e) allows remote attackers to execute arbitrary shell commands via a crafted URL, aka Bug ID CSCur90888.

# Creating a PCI vulnerability sensor

Identify equipment in your cardholder data environment

Find it here: <http://www.cvedetails.com/>

Build a JSON feed

Use CLC's custom command line tool

<http://go.clcoho.org/pcisensor>

# CVE Sensor Setup Steps

Accepts JSON data via URL from [cvedetails.com](https://cvedetails.com)

URL goes in sensor setup parameters field

If any CVE's have been posted in the past 7 days, the CVE count will be returned to the console

Set channel so that it errors when limit is above zero

# PCI Vulnerability Sensor set up

## BASIC SENSOR SETTINGS

Sensor Name

Vulnerability check for Meraki MX firewall hardware

Parent Tags

Tags

exesensor ✕

Priority

★★★★★

## SENSOR SETTINGS

**Important:** The EXE file has to run on the computer where the parent probe is installed, not on the parent device. The working directory for "exe" files is the probe directory, "vbs,ps1" or other script files may use different working directories.

EXE/Script

count.ps1

Parameters

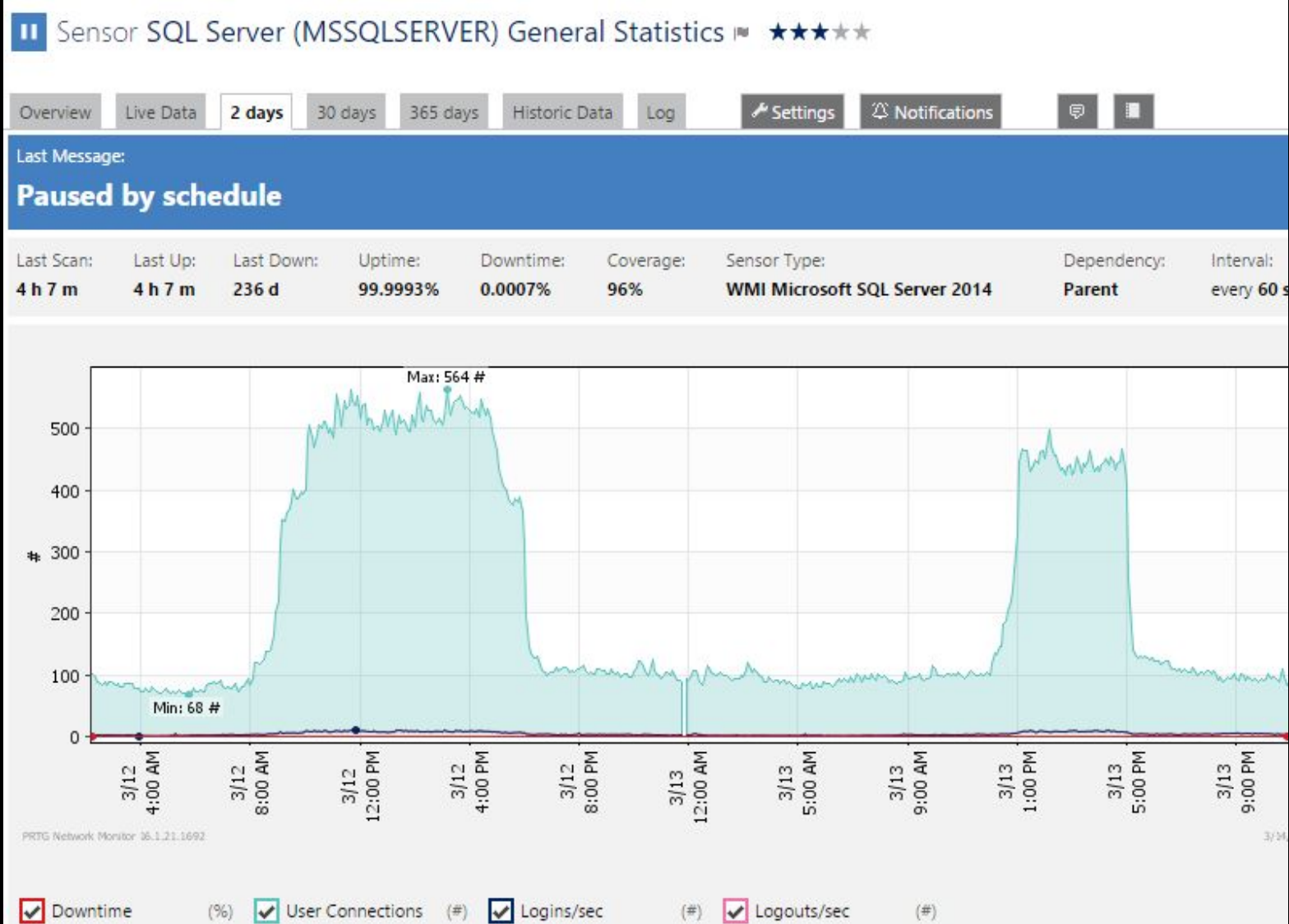
'[http://www.cvedetails.com/json-feed.php?numrows=10&vendor\\_id=16&product\\_id=30659&v](http://www.cvedetails.com/json-feed.php?numrows=10&vendor_id=16&product_id=30659&v)



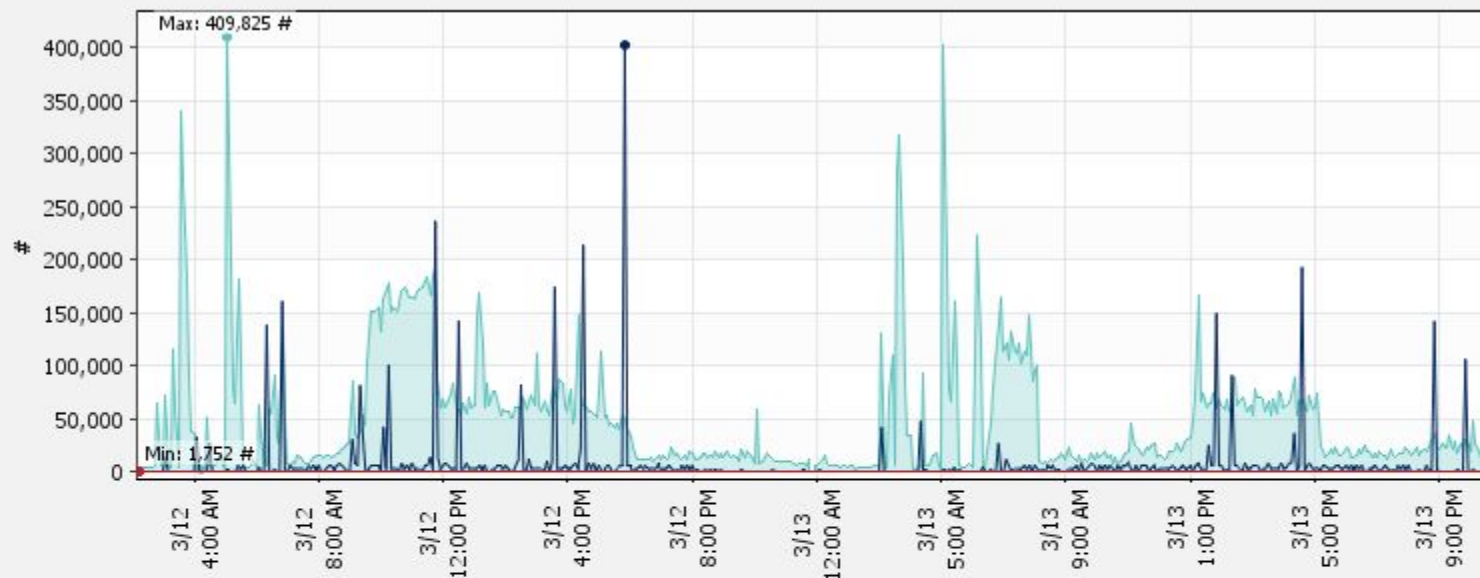
# Polaris specific sensors

Keeping an eye out for common Polaris problems

# Basic SQL status



# SQL Lock information



PRTG Network Monitor 36.1.21.1692

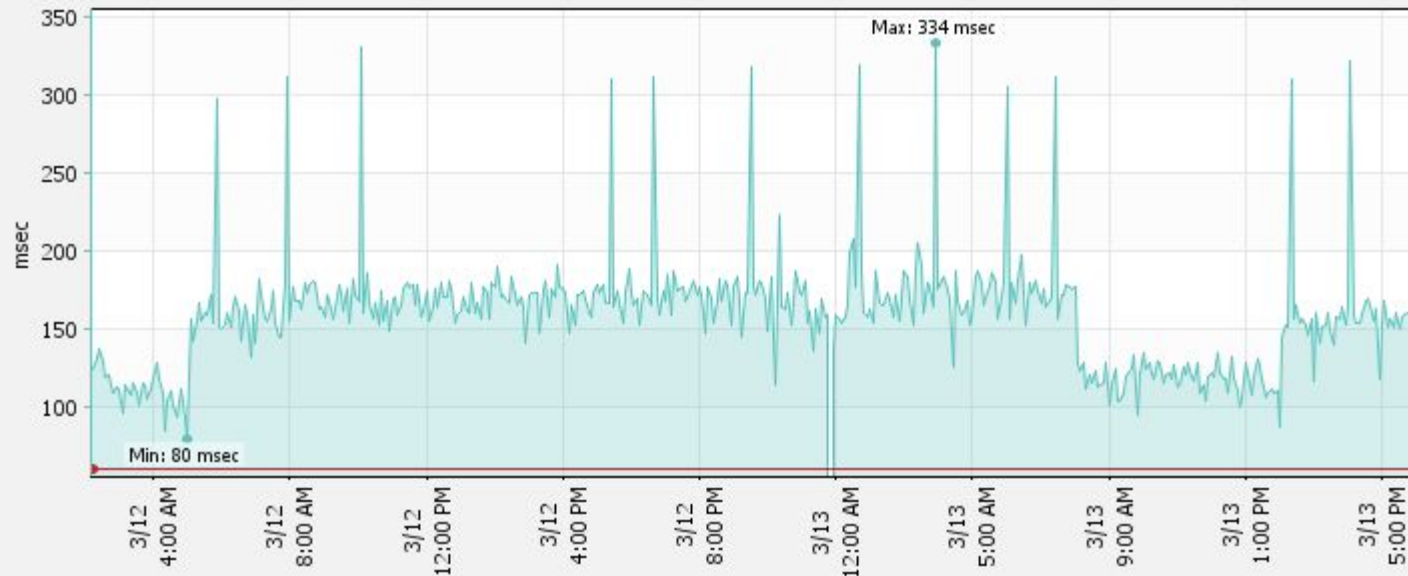
Downtime (%)  Lock Requests/sec (#)  Average Wait Time(ms)  Number of Deadlo... (#)

Date Time	Lock Requests/sec	Average Wait Time	Number of Deadlocks/sec
<b>Averages (of 575 values)</b>	44,382 #	8 ms	

1 ← 1 to 50 of 576 → 1

Date Time ▲	Lock Requests/sec	Average Wait Time	Number of Deadlocks/sec
3/13/2016 10:50:00 PM – 10:55:00 PM	22,314 #	0 ms	
3/13/2016 10:45:00 PM – 10:50:00 PM	15,574 #	0 ms	
3/13/2016 10:40:00 PM – 10:45:00 PM	19,375 #	0 ms	
3/13/2016 10:35:00 PM – 10:40:00 PM	14,532 #	0 ms	

# SQL Agent status



PRTG Network Monitor 16.1.21.1692

Downtime (%)  Sensor Executi... (msec)

Date Time	Sensor Execution Time
<b>Averages (of 575 values)</b>	155 msec

← 1 to 50 of 576 →

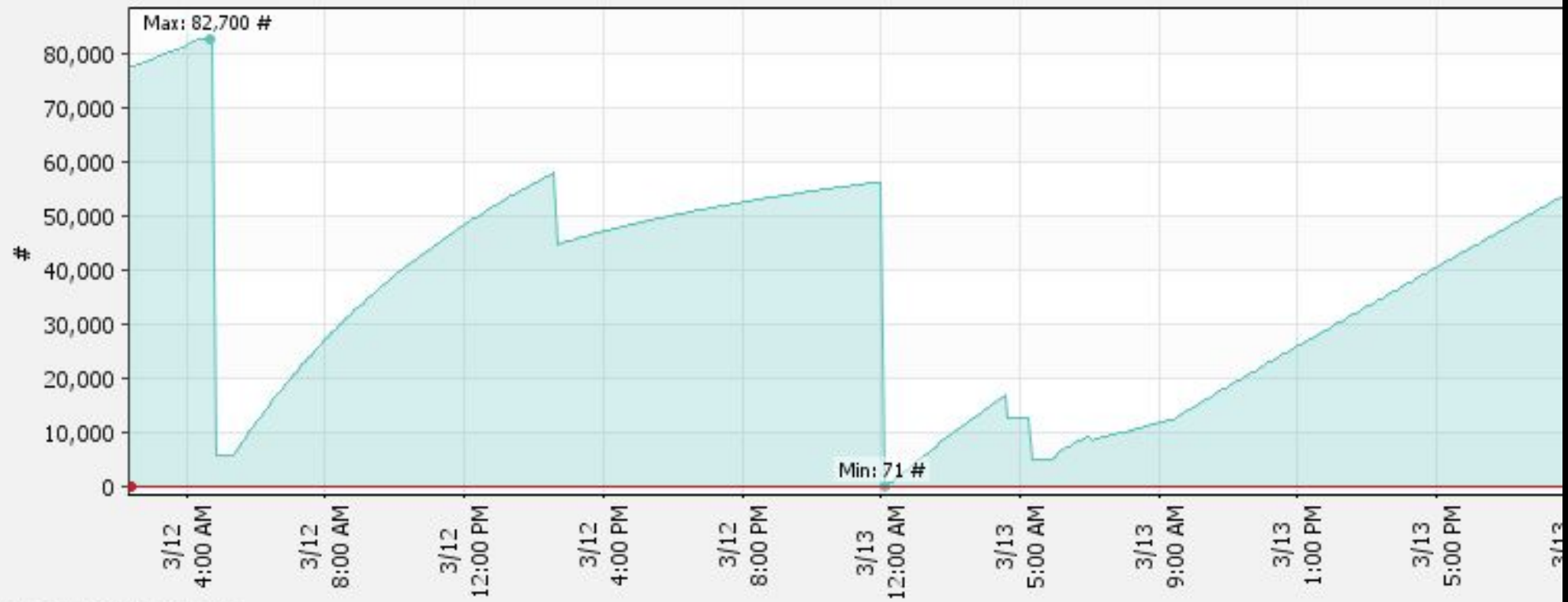
Date Time ▲	Sensor Execution Time
3/13/2016 10:55:00 PM - 11:00:00 PM	144 msec
3/13/2016 10:50:00 PM - 10:55:00 PM	152 msec
3/13/2016 10:45:00 PM - 10:50:00 PM	160 msec
3/13/2016 10:40:00 PM - 10:45:00 PM	155 msec

# Perfmon SQL Sensors

You can put anything you'd monitor via Perfmon into a sensor

`\SQLServer:Buffer Manager\Page life expectancy::count`

`\SQLServer:Memory Manager\Memory Grants Pending::count`



PRTG Network Monitor 36.1.21.1692

- Downtime (%) 
  Page life expectancy (#) 
  Memory Grants Pe... (#)

Date Time	Page life expectancy	Memory Grants Pending
<b>Averages (of 576 values)</b>	40,064 #	0 #

1 ← 1 to 50 of 576 → 2

Date Time ▲	Page life expectancy	Memory Grants Pending
3/13/2016 10:50:00 PM – 10:55:00 PM	62,012 #	0 #
3/13/2016 10:45:00 PM – 10:50:00 PM	61,711 #	0 #
3/13/2016 10:40:00 PM – 10:45:00 PM	61,409 #	0 #

<http://go.clcohoio.org/polarisprtg>

Where to find SQL scripts used in Polaris Custom Sensors

# General SQL Sensors

## MATCHING SENSOR TYPES

Microsoft SQL



Monitors a database on a Microsoft SQL Server



Add This 



# General SQL Sensor set up

## DATABASE

Database

Polaris

Authentication

- SQL Server
- Windows Authentication**

## DATA

SQL Expression

```
SELECT '~' + sqltext.TEXT,  
req.session_id,  
req.status,  
req.command,
```

# Check for long running jobs

```
...where req.total_elapsed_time > 10800000 and req.status in (
'running', 'suspended', 'waiting' )
```

# Long running jobs sensor setup

Record Count	<input type="radio"/> Do not count number of records
	<input checked="" type="radio"/> <b>Count number of records</b>
Post-Processing	<input type="radio"/> Ignore result set
	<input type="radio"/> Process numerical result
	<input checked="" type="radio"/> <b>Process string result</b>
	<input type="radio"/> Monitor for changes
	For string values you can use these checks
Response Must Include	
Response Must Not Include	~

# Check for open transactions

You were good and did a “begin tran” to start your SQL statement

But... you never committed it or rolled it back

Now the transaction log is filling up and other jobs won't complete

# Check for open transactions

```
SELECT '~' + hostname,spid FROM sysprocesses WHERE  
open_tran = 1 and last_batch < dateadd(hh,-1,getdate())
```

The SQL above shows any transaction that has been opened for longer than one hour

# Catching SQL Agent Job Failures

The screenshot displays the SQL Server Log File Viewer interface for the server ARSHADALI-LAP\SQL2008R2. The 'Select logs' pane on the left shows 'Job History' selected, with 'SSISProxyDemo' and 'syspolicy\_purge\_history' also checked. The main pane shows a table of log entries with a red 'X' icon indicating a failure. The selected row details show the job step 'SSISPackageCall' failed on 11/9/2010 at 6:19:17 PM. The error message states: 'Non-SysAdmins have been denied permission to run DTS Execution job steps without a proxy account. The step failed.'

Log File Viewer - ARSHADALI-LAP\SQL2008R2

Select logs:

- Database Mail
- Job History
  - SSISProxyDemo
  - syspolicy\_purge\_history
- SQL Server Agent

Log file summary: No filter applied

Date	Step ID	Server	Job Name	Step Name
11/9/2010 6:19:17 ...	0	ARSHADALI-LAP\SQL2008R2	SSISProxyDemo	(Job outcome)
11/9/2010 6:19:...	1	ARSHADALI-LAP\SQL2008R2	SSISProxyDemo	SSISPackag...

Selected row details:

Date: 11/9/2010 6:19:17 PM  
Log: Job History (SSISProxyDemo)

Step ID: 1  
Server: ARSHADALI-LAP\SQL2008R2  
Job Name: SSISProxyDemo  
Step Name: SSISPackageCall  
Duration: 00:00:00  
Sql Severity: 0  
Sql Message ID: 0  
Operator Emailed:  
Operator Net sent:  
Operator Paged:  
Retries Attempted: 0

Status

Last Refresh: 11/9/2010 6:19:24 PM

Filter: None

[View filter settings](#)

Progress

Done (1 records).

Message  
Non-SysAdmins have been denied permission to run DTS Execution job steps without a proxy account. The step failed.

# Catching SQL Agent Job Failures

```
FROM msdb.dbo.sysjobhistory SJH
```

```
...and enabled=1 and sjh.run_status = 0
```

# Other SQL sensors

Were any overdue notices sent via email?

Circ status of Out but not CKO'd to an actual patron

Requests that are held, but the item circ status is NOT held

Check for bad SIP CKO Transactions (due date: 11/30/1999)

Check for branches with different notification settings

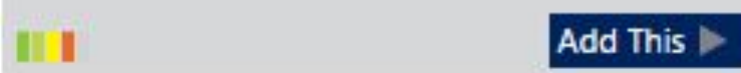


# Other Polaris Sensors

More things that can go wrong in the Polaris universe

# Is ERMS running?

WMI Service ?  
Monitors a service using WMI



Service	
<input type="checkbox"/> Distributed Transaction Coordinator	Coordinates transactions that span multiple resource managers, such as databases, message queues, an...
<input type="checkbox"/> DNS Client	The DNS Client service (dnscache) caches Domain Name System (DNS) names and registers the full compu...
<input checked="" type="checkbox"/> Electronic Resource Management System (5.0)	Provides storage, processing and access to electronic resources.
<input type="checkbox"/> Encrypting File System (EFS)	Provides the core file encryption technology used to store encrypted files on NTFS file system volum...
<input type="checkbox"/> Extensible Authentication Protocol	The Extensible Authentication Protocol (EAP) service provides network authentication in such scenari...
<input type="checkbox"/> Function Discovery Provider Host	The FDPHOST service hosts the Function Discovery (FD) network discovery providers. These FD provider...
<input type="checkbox"/> Function Discovery Resource Publication	Publishes this computer and resources attached to this computer so they can be discovered over the n...
<input type="checkbox"/> ...	...

# Monitoring the Eventlog

Using this information repository for detecting problems

# Monitor the eventlog for COM+ timeouts

## WMI EVENT LOG MONITOR

Log File		Search...
<input type="checkbox"/>	◆ Filename	◆ Number of Records
<input type="checkbox"/>	Application	19702
<input type="checkbox"/>	HardwareEvents	0
<input type="checkbox"/>	Internet Explorer	0
<input type="checkbox"/>	Key Management Service	0
<input checked="" type="checkbox"/>	Polaris Diagnostics	10275
<input type="checkbox"/>	Security	34224
<input type="checkbox"/>	System	65517
<input type="checkbox"/>	Windows PowerShell	15810

# Set New Records per second channel

Limits	<input type="radio"/> Disable Limits <input checked="" type="radio"/> <b>Enable Limits</b>
Upper Error Limit (#/s)	5
Upper Warning Limit (#/s)	
Lower Warning Limit (#/s)	
Lower Error Limit (#/s)	
Error Limit Message	<b>More than 5 errors in the Eventlog; check for COM+ issues</b>

# Counting SMS messages

Make sure the Twilio SMS stack is working

# Monitoring the monitor



[About](#)

[F.A.Q](#)

[Support](#)

[Blog](#)

[Sign-up \(free\)](#)

Downtime Happens. Get Notified!

**50 Monitors, Checked Every 5 Minutes, Totally Free.**

(Need 1-minute checks and/or more monitors?)

 **Start Monitoring (in 30 secs)**



# UptimeRobot Advantages

Up to 50 monitors

Multiple notification methods

Including webhooks (for HipChat and SMS)



Review

# The three rules of PRTG

#1 Start small when setting up

#2 Address all issues, don't allow sensors to "sit" in an error state

#3 Comment ALL custom sensors

**#4 Don't wait**

[go.clcoho.org/jobs](https://go.clcoho.org/jobs)

If this stuff sounds cool to you, come work with us

# Questions?

wosborn@clcohoio.org



CENTRAL  
LIBRARY  
CONSORTIUM  
CONNECTED. CREATIVE. CURRENT.



ICANHASCHEEZBURGER.COM