

GESTÃO DE REDES COM SNMP

EDUARDO SILVEIRA



TCHELINUX BG 2019

APRESENTAÇÃO

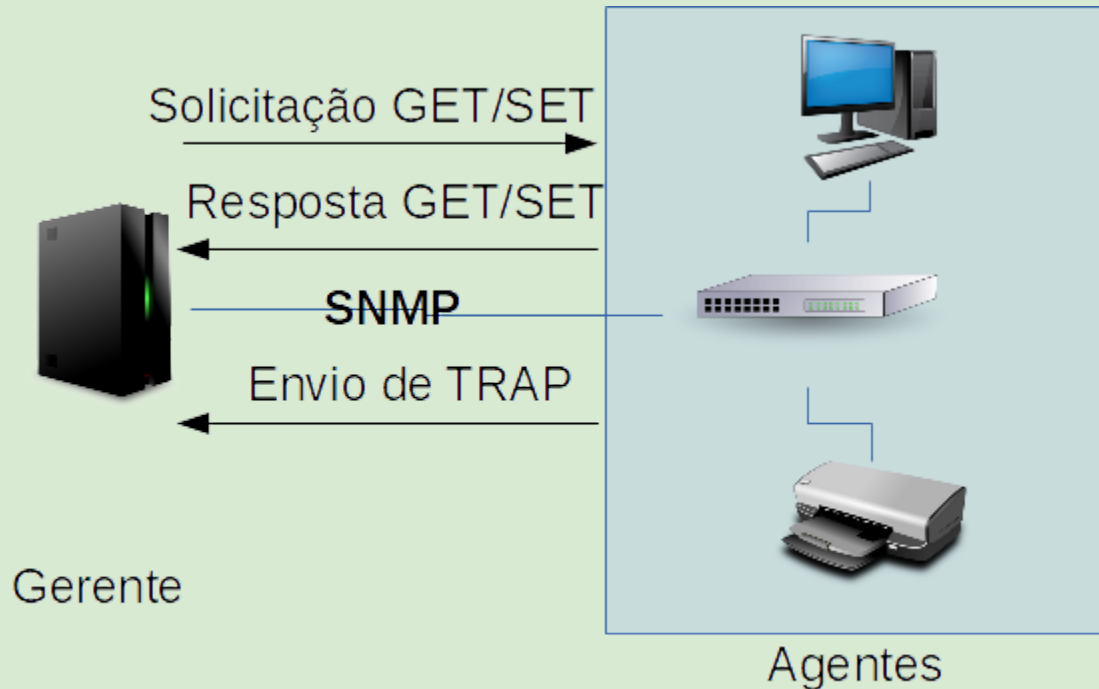
- Bacharel em Sistemas de Informação pela Universidade de Caxias do Sul.
- 12 anos trabalhando com servidores GNU/Linux, principalmente com gestão de Internet, na empresa Honos.
- Admirador do software livre e moderador do Viva o Linux durante quase 7 anos, entre 2009 e 2015.
- Podcaster e idealizador do site e podcast PADD (peloamordedeus.org.br).

O QUE É SNMP?

- Simple Network Management Protocol (SNMP) é um protocolo padrão para gerenciamento de dispositivos em redes IP.
- É utilizado na maioria das vezes no monitoramento de dispositivos conectados à rede.
- Além da comunicação direta entre o sistema de gerenciamento e os dispositivos geridos, também é possível utilizar agentes (que traduzem informações do dispositivo para o SNMP).

O QUE É SNMP?

- Sistemas de monitoramento que utilizam SNMP não seguem o modelo cliente-servidor convencional:



- Sendo assim, utilizam-se os termos gerente (para a aplicação de gerenciamento) e agente (para os dispositivos monitorados).

ONDE USAR O SNMP?

- Atualmente, o SNMP possui as versões SNMPv1, SNMPv2c e SNMPv3. Apenas o SNMPv3 possui suporte à autenticação. Por esse motivo, é comum os dispositivos gerenciados não possuírem implementada a operação Set, devido à vulnerabilidade do protocolo.
- Sendo assim, o SNMP é mais utilizado para monitoramento.
- A maioria dos dispositivos com conexão de rede (roteadores, switches, nobreaks, impressoras...) possuem SNMP, mesmo que seja a versão SNMPv1.

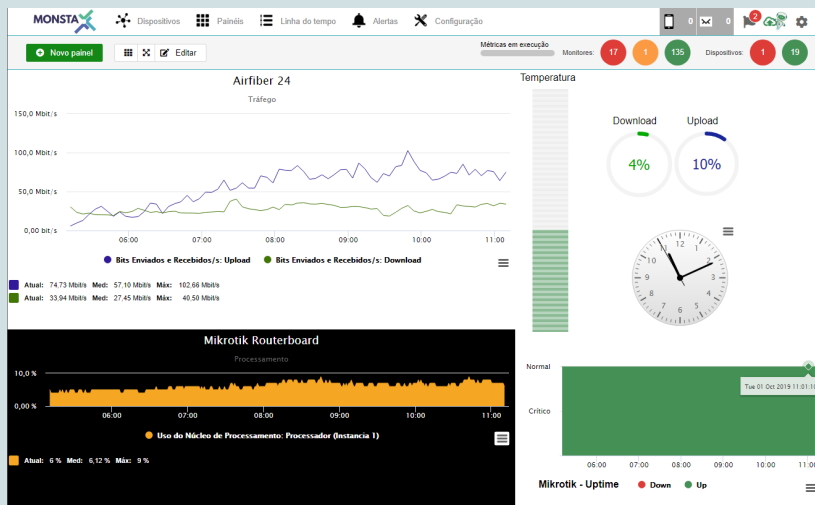
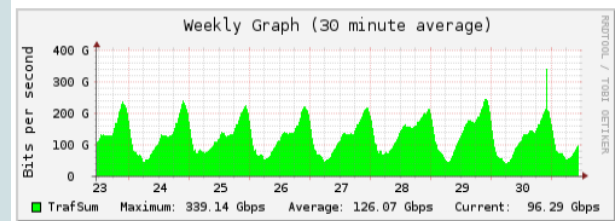
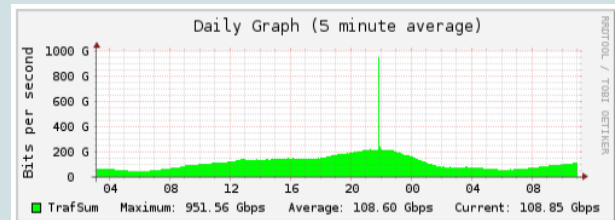
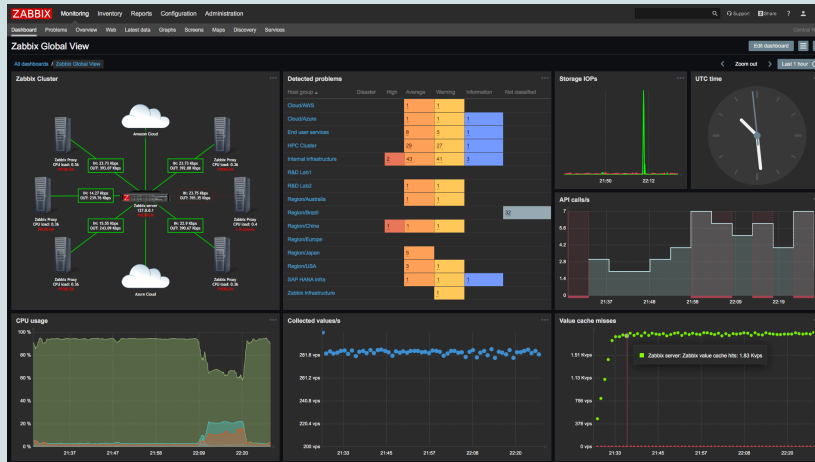
POR QUE MONITORAR?

POR QUE MONITORAR?



Fonte: https://pt.wikipedia.org/wiki/Ficheiro:Painel_Chevette_L.jpg

POR QUE MONITORAR?



Nagios

General

Home

Documentation

Current Status

Tactical Overview

Map

Hosts

Services

Host Groups

Service Groups

Summary

Grid

Problems

Services (Unhandled)

Hosts (Unhandled)

Network Outages

Quick Search:

Reports

Availability

Trends

Alerts

History

Summary

Histogram

Notifications

Event Log

System

Comments

Downtime

Process Info

Performance Info

Scheduling Queue

Configuration

Current Network Status

Last Updated: Tue Jun 7 11:46:01 CDT 2016

Updated every 30 seconds

Nagios® Core™ 4.0.5 - www.nagios.org

Logged in as nagios@mon

View History For This Host

View Notifications For This Host

View Service Status Detail For All Hosts

Host Status Totals

Up Down Unreachable Pending

1 0 0 0

All Problems All Types

0 1

Service Status Totals

OK Warning Unknown Critical Pending

12 0 5 0 0

All Problems All Types

1 13

Service Status Details For Host 'localhost'

Limit Results: 100

Host Service

localhost HTTP

localhost PING

localhost Root Partition

localhost SSH

localhost Service Status - crond

localhost Service Status - httpd

localhost Service Status - mysqld

localhost Service Status - ndo2db

localhost Service Status - npcd

localhost Service Status - rnpd

localhost Swap Usage

localhost Total Processes

Status

Last Check

Duration

Attempt

Status Information

HTTP OK: HTTP/1.1 200 OK - 3220 bytes in 0.001 second response time

PING OK - Packet loss = 0%, RTT = 0.04 ms

DISK OK - free space / 9022 MB (54% inode=84%):

SSH OK - openssh.S.3 (protocol 2.0)

crond (pid 2420) is running...

httpd (pid 41424) is running...

mysqld (pid 15755) is running...

ndo2db (pid 15862) is running...

NPDC running (pid 3546):

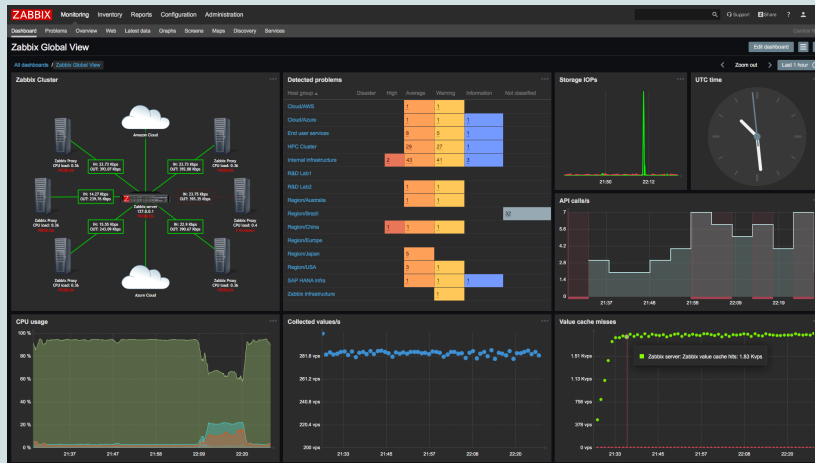
rnpd (pid 2125) is running...

SWAP OK - 100% free (2047 MB out of 2047 MB)

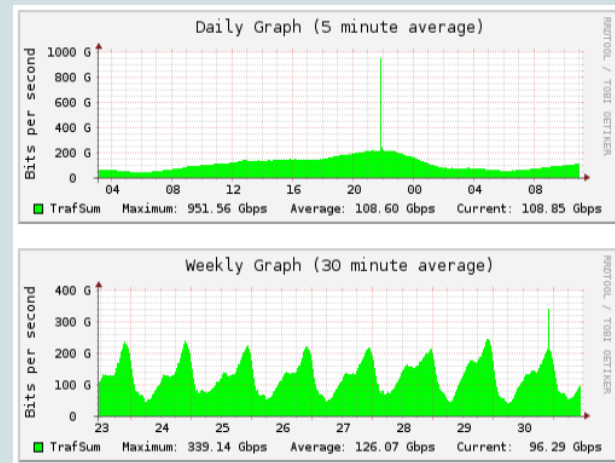
PROCS OK: 177 processes with STATE = RSZDT

Results 1 - 13 of 13 Matching Services

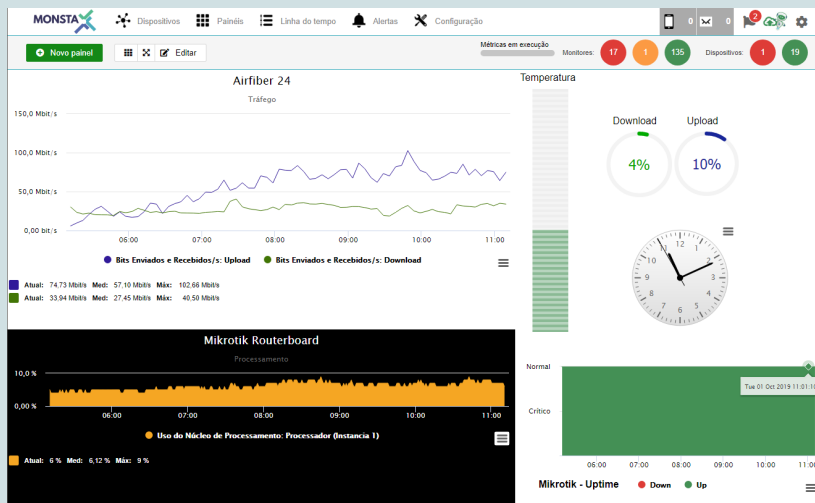
POR QUE MONITORAR?



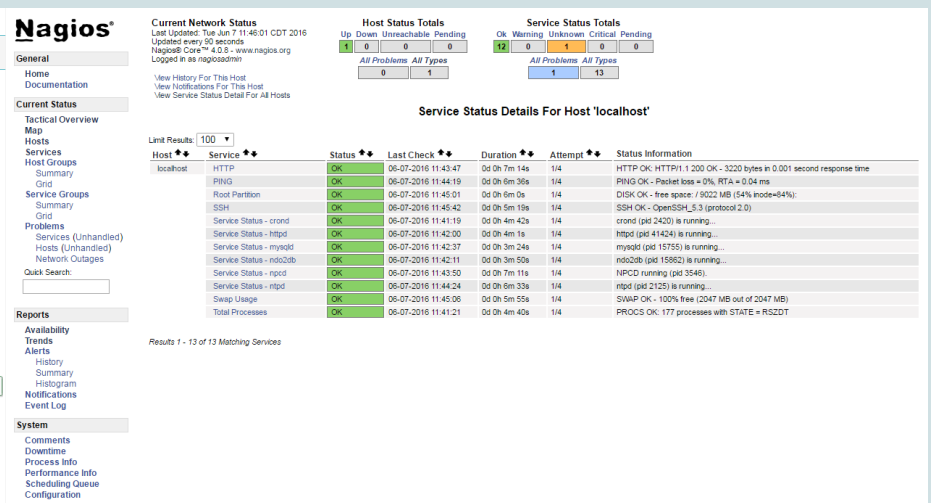
Fonte: https://commons.wikimedia.org/wiki/File:Dashboard_graphs_v4_dark_1.png



Fonte: <https://ix.br/trafego/agregado/rs>



Fonte: <https://demonstracao.monsta.com.br/index.html#/dashboard.1>



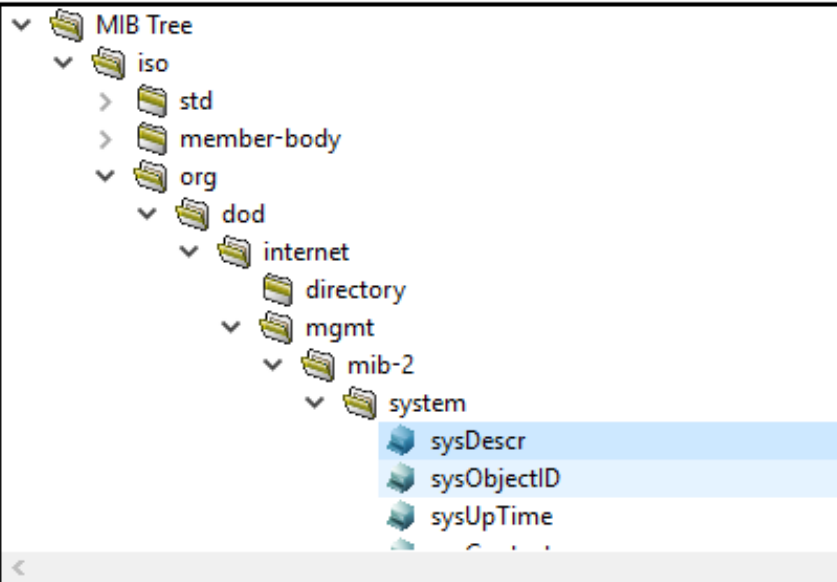
Fonte: https://commons.wikimedia.org/wiki/File:Nagios_Core_4.0.8_Host_Status.png

COMO FUNCIONA O SNMP?

- Objetos gerenciados: visão abstrata de um recurso real do sistema. As estruturas dos dados resultantes da modelagem dos recursos da rede são os objetos gerenciados.
- Management Information Base (MIB): conjunto dos objetos gerenciados, que procura abranger todas as informações necessárias para a gerência de rede. As MIBs seguem padrões de construção com sintaxe definida e estrutura lógica do tipo árvore hierárquica.
- Os objetos gerenciados são informados pelo agente para o gerente.

COMO FUNCIONA O SNMP?

MIB Tree



Node Info

Name:	sysDescr
Oid:	1.3.6.1.2.1.1.1
Composed Type:	DisplayString
Base Type:	OCTET STRING
Status:	current
Access:	read-only
Kind:	Scalar
SMI Type:	OBJECT-TYPE
Size	0 .. 255
Module:	SNMPv2-MIB
Description:	A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software.

Software: SnmpB

COMO FUNCIONA O SNMP?

MIB Tree

```
graph TD
    MIB_Tree[MIB Tree] -- 1 --> iso[iso]
    iso -- 3 --> org[org]
    org -- 6 --> dod[dod]
    dod -- 1 --> internet[internet]
    internet -- 2 --> mgmt[mgmt]
    mgmt -- 1 --> mib2[mib-2]
    mib2 -- 1 --> system[system]
    system -- 1 --> sysDescr[sysDescr]
```

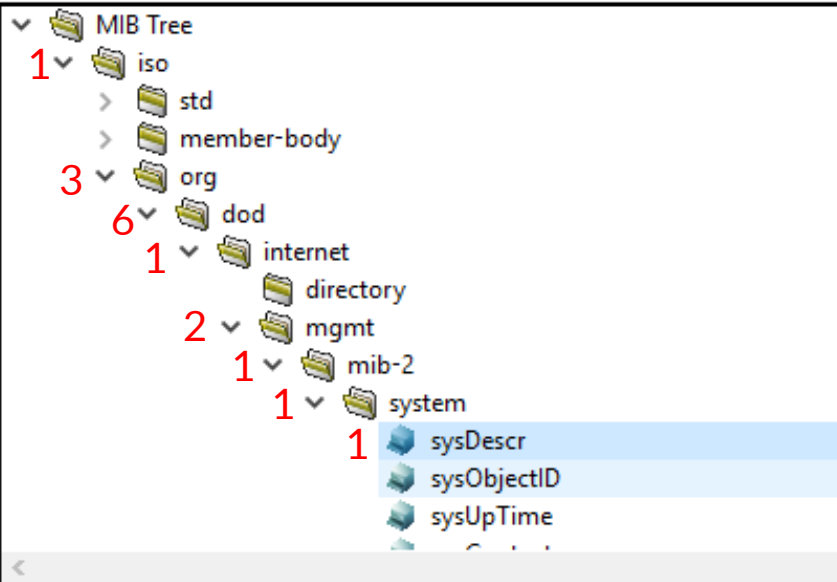
Node Info

Name:	sysDescr
Oid:	1.3.6.1.2.1.1.1
Composed Type:	DisplayString
Base Type:	OCTET STRING
Status:	current
Access:	read-only
Kind:	Scalar
SMI Type:	OBJECT-TYPE
Size	0 .. 255
Module:	SNMPv2-MIB
Description:	A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software.

Software: SnmpB

COMO FUNCIONA O SNMP?

MIB Tree



Node Info

Name:	sysDescr
Oid:	1.3.6.1.2.1.1.1
Composed Type:	DisplayString
Base Type:	OCTET STRING
Status:	current
Access:	read-only
Kind:	Scalar
SMI Type:	OBJECT-TYPE
Size:	0 .. 255
Module:	SNMPv2-MIB
Description:	A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software.

Software: SnmpB

COMO FUNCIONA O SNMP?

MIB Tree

Node Info

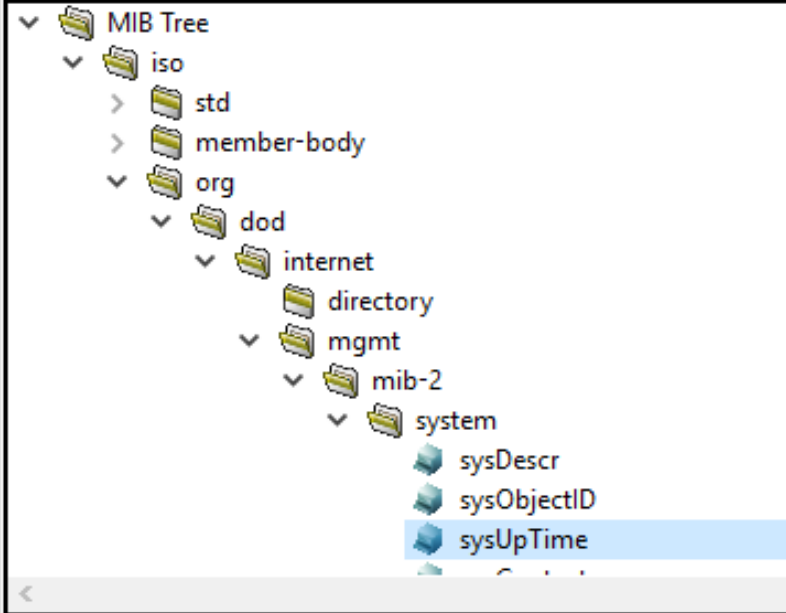
Name:	sysDescr
Oid:	1.3.6.1.2.1.1.1.1
Composed Type:	DisplayString
Base Type:	OCTET STRING
Status:	current
Access:	read-only
Kind:	Scalar
SMI Type:	OBJECT-TYPE
Size:	0 .. 255
Module:	SNMPv2-MIB
Description:	A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software.

1.3.6.1.2.1.1.1.0 = STRING: "Linux ETD-MNT 4.15.0-34-generic #37-Ubuntu SMP Mon Aug 27 15:21:48 UTC 2018 x86_64"

Software: SnmpB

COMO FUNCIONA O SNMP?

MIB Tree

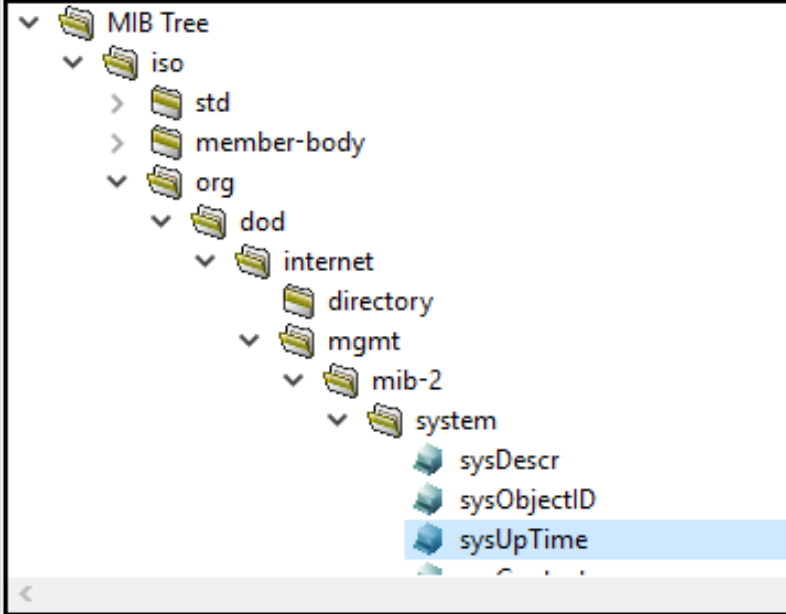


Node Info

Name:	sysUpTime
Oid:	1.3.6.1.2.1.1.3
Composed Type:	TimeTicks
Base Type:	UNSIGNED32
Status:	current
Access:	read-only
Kind:	Scalar
SMI Type:	OBJECT-TYPE
Size	0 .. 4294967295
Module:	SNMPv2-MIB
Description:	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

COMO FUNCIONA O SNMP?

MIB Tree



Node Info

Name:	sysUpTime
Oid:	1.3.6.1.2.1.1.3
Composed Type:	TimeTicks
Base Type:	UNSIGNED32
Status:	current
Access:	read-only
Kind:	Scalar
SMI Type:	OBJECT-TYPE
Size	0 .. 4294967295
Module:	SNMPv2-MIB
Description:	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

1.3.6.1.2.1.1.3.0 = Timeticks: (140045)
0:23:20.45

COMO FUNCIONA O SNMP?

MIB Tree

```
graph TD
    member-body --> org
    org --> dod
    dod --> internet
    internet --> directory
    directory --> mgmt
    mgmt --> mib-2
    mib-2 --> system
    system --> interfaces
    interfaces --> ifNumber
    ifNumber --> ifTable
    ifTable --> ifEntry
    ifEntry --> ifIndex
    ifEntry --> ifDescr
```

Node Info

Name:	ifDescr
Oid:	1.3.6.1.2.1.2.2.1.2
Composed Type:	DisplayString
Base Type:	OCTET STRING
Status:	current
Access:	read-only
Kind:	Column
SMI Type:	OBJECT-TYPE
Size	0 .. 255
Module:	IF-MIB
Description:	A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the interface hardware/software.

Query Results

-----SNMP query started-----

1: ifDescr.1 lo

2: ifDescr.2 Realtek Semiconductor Co., Ltd. RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller

3: ifDescr.3 Qualcomm Atheros AR9285 Wireless Network Adapter (PCI-Express)

-----SNMP query finished-----

Total # of Requests = 1

Total # of Objects = 4

COMO FUNCIONA O SNMP?

- Para pesquisas com snmpwalk, é necessário informar a comunidade, a versão, o host e a OID.

```
$ snmpwalk -c etdpublic -v2c localhost
```

```
iso.3.6.1.2.1.1.1.0 = STRING: "Linux ETD-MNT 4.15.0-34-generic  
#37-Ubuntu SMP Mon Aug 27 15:21:48 UTC 2018 x86_64"
```

```
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
```

```
iso.3.6.1.2.1.1.3.0 = Timeticks: (25006) 0:04:10.06
```

```
iso.3.6.1.2.1.1.4.0 = STRING: "root"
```

```
iso.3.6.1.2.1.1.5.0 = STRING: "ETD-MNT"
```

```
iso.3.6.1.2.1.1.6.0 = STRING: "\"ETD Note\""
```

```
...
```

```
$ snmpwalk -c etdpublic -v2c localhost 1.3.6.1.2.1.1.5.0
```

```
iso.3.6.1.2.1.1.5.0 = STRING: "ETD-MNT"
```

SISTEMAS DE MONITORAMENTO COM SNMP

Gratuitos

- Cacti
- Nagios Core
- Zabbix

Pagos

- Monsta (R\$ 500,00 por ano)
- Nagios XI (a partir de \$ 1995,00 para 100 nodes)
- PRTG Network Monitor from Paessler (a partir de \$ 1600,00 para 500 sensores)
- WhatsUp® Gold (licença ou assinatura anual através de contato)

OBRIGADO!

PERGUNTAS?

Slides em <http://epsilveira.github.io/>