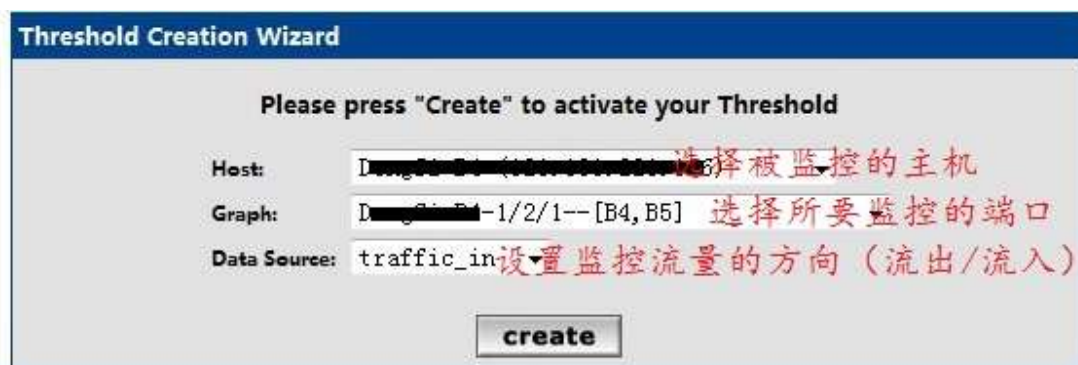


之前笔者介绍过，现在判断网络是否被攻击很多时候是基于流量判断的。比如我们的网络正常情况下使用的带宽在 50-100M，那么带宽到达 200M 的时候就显然很不正常了，造成带宽突然增大的原因有很多种，比如客户在服务器上下载上传数据、对外大量发送恶意数据包、遭受攻击等。所以，及时知道整个网络实时流量状况是非常有必要的。在工作环境中我们不可能专门有人 24 小时盯着显示器监视网络流量大小，而是需要智能解决办法，比如网络正常时带宽为 50-100M，当到达 150M 的时候给管理人员发送预警

下面我们看一下用 cacti 监控流量是如何实现阈值报警的

新建阈值模板，登录 cacti 后打开 “Console-----Thresholds-----Add”



Threshold Creation Wizard

Please press "Create" to activate your Threshold

Host: [Dropdown Menu] 选择被监控的主机

Graph: [Dropdown Menu] 选择所要监控的端口

Data Source: traffic_in 设置监控流量的方向 (流出/流入)

create

设置流入阈值报警



Linux公社（LinuxIDC.com）于2006年9月25日注册并开通网站，Linux现在已经成为一种广受关注和支持的一种操作系统，IDC是互联网数据中心，LinuxIDC就是关于Linux的数据中心。

LinuxIDC.com提供包括Ubuntu，Fedora，SUSE技术，以及最新IT资讯等Linux专业类网站。

并被收录到Google 网页目录-计算机 > 软件 > 操作系统 > Linux 目录下。

Linux公社（LinuxIDC.com）设置了有一定影响力的Linux专题栏目。

包括：

[Ubuntu专题](#)

[Fedora专题](#)

[RedHat专题](#)

[SUSE专题](#)

[红旗Linux专题](#)

[Android专题](#)

[Linux公社简介](#) - [广告服务](#) - [网站地图](#) - [帮助信息](#) - [联系我们](#)

本站（LinuxIDC）所刊载文章不代表同意其说法或描述，仅为提供更多信息，也不构成任何建议。

本站带宽由[\[6688.CC\]](#)友情提供

Copyright © 2006-2011 [Linux公社](#) All rights reserved

1: traffic_in
N/A

2: traffic_out
N/A

Data Source Item [traffic_in] - Current value: [187974.4628]

Template settings

Template Propagation Enabled

Whether or not these settings will be propagated from the threshold template.

☐ Template Propagation Enabled

Mandatory settings

Threshold Name

Provide the Thold a meaningful name.

- Traffic - Ethernet1/2/1 [traf

Threshold Enabled

Whether or not this threshold will be checked and alerted upon.

☒ Threshold Enabled

Weekend Exemption

If this is checked, this Threshold will not alert on weekends.

☐ Weekend Exemption

Disable Restoration Email

If this is checked, Thold will not send an alert when the threshold has returned to normal status.

☐ Disable Restoration Email

Threshold Type

The type of Threshold that will be monitored.

High / Low Values ▾

High / Low Settings

High Threshold

If set and data source value goes above this number, alert will be triggered

5242880 当流入流量大于5M或者低于1M

Low Threshold

If set and data source value goes below this number, alert will be triggered

1048576 是发送报警

Breach Duration

The amount of time the data source must be in breach of the threshold for an alert to be raised.

1 Minute ▾

Data Manipulation

Data Type

Special formatting for the given data.

CDEF ▾ 监控模板类型

Threshold CDEF

Apply this CDEF before returning the data.

Turn Bytes into Bits ▾ 流量单位大小

Other setting

Re-Alert Cycle

Repeat alert after this amount of time has passed since the last alert.

Every Minute ▾ 报警轮询时间

Notify accounts

This is a listing of accounts that will be notified when this threshold is breached.

Extra Alert Email:

135261@139.com 接收报警地址

设置流出阈值报警

1: traffic_in

Hi: 5242880 Lo: 1048576 BL: off

2: traffic_out

Hi: 10485760 Lo: 1048576 BL: off

Data Source Item [traffic_out] - Current value: [4353183.5195]

Template settings

Template Propagation Enabled

Whether or not these settings will be propagated from the threshold template.

☐ Template Propagation Enabled

Monitoring settings

Threshold Name

Provide the Thold a meaningful name

Traffic - Ethernet1/2/1 [traf

Threshold Enabled

Whether or not this threshold will be checked and alerted upon.

☒ Threshold Enabled

Weekend Exemption

If this is checked, this Threshold will not alert on weekends.

☐ Weekend Exemption

Disable Restoration Email

If this is checked, Thold will not send an alert when the threshold has returned to normal status.

☐ Disable Restoration Email

Threshold Type

The type of Threshold that will be monitored.

High / Low Values

High / Low Settings

High Threshold

If set and data source value goes above this number, alert will be triggered

10485760 当流出流量大于10M小于1M时

Low Threshold

If set and data source value goes below this number, alert will be triggered

1048576 发送报警

Breach Duration

The amount of time the data source must be in breach of the threshold for an alert to be raised.

1 Minute

Data Manipulation

Data Type

Special formatting for the given data.

CDEF

Threshold CDEF

Apply this CDEF before returning the data.

Turn Bytes into Bits

Other setting

Re-Alert Cycle

Repeat alert after this amount of time has passed since the last alert.

Every Minute

Notify accounts

This is a listing of accounts that will be notified when this threshold is breached.

135285...@139.com

下图为流量没有超过或低于我们设置的阈值，所以显示时为蓝色

console graphs thold monitor settings

Console -> Thresholds

Logged in as jcmde (Logout)

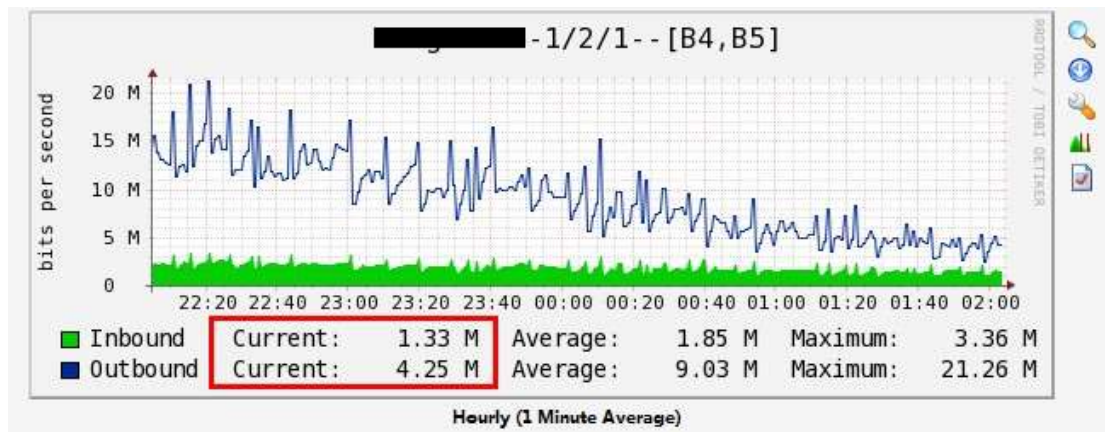
Thresholds Host Status

Threshold Status

Template: Interface - Traffic Status: All Rows: 30 Search: go clear

<< Previous		Showing Rows 1 to 2 of 2 [1]					Next >>
Actions	Name**	ID	Type	High	Low	Current	Enabled
	Traffic - Ethernet1/2/1 [traffic_in]	6	High/Low	5242880	1048576	1484664.9333	Enabled
	Traffic - Ethernet1/2/1 [traffic_out]	7	High/Low	10485760	1048576	4201861.3333	Enabled
<< Previous		Showing Rows 1 to 2 of 2 [1]					Next >>

我们还可以点击阈值左边的小图标查看当前端口的流量曲线图



下图显示的为某端口流出流量已经超过我们所设置的阈值，当超过或者低于我们设置的阈值时，显示呈红色。这个时候我们就可以收到报警邮件通知了

1352 - Traffic - Ethernet1/2/1 [traffic_in]	6	High/Low	5242880	1048576	4543771.3333	Enabled
1352 - Traffic - Ethernet1/2/1 [traffic_out]	7	High/Low	10485760	1048576	15884518.8	Enabled

下图为阈值报警的邮件内容

