LibreNMS Alter 規則是用邏輯語言定義的。GUI 提供了建立規則的簡單方法。建立更複雜的規則，其中可能包括數學計算和 MySQL 查詢，可以使用巨集來完成。關於警報規則如何在 LibreNMS 中工作的視訊

警報規則

關於如何使用萬用字元警告規則的視訊

https://www.youtube.com/watch?v=ryv0j8GEkhM&feature=youtu.be

警戒規則萬用字元

https://www.youtube.com/watch?v=eYYioFNcrAk&feature=youtu.be

語法規則必須至少由 3 個元素組成。一個實體、一個條件和一個值。規則可以包含括弧和 Glues。實體是由資料程式庫中的表和欄位提供的。例如： ports.ifOperStatus

條件可以是以下任何一個

等於	=	在	IN	開始於	LIKE ('%...')
不等於	!=	不在	NOT IN	不開始於	NOT LIKE ('%...')
包含	LIKE ('%...%')	兩者之間	BETWEEN	結束於	LIKE ('...%')
不包含	NOT LIKE ('%...%')	不在兩者之間	NOT BETWEEN	不結束於	NOT LIKE ('...%')
是空的	= ''	IS NULL	IS NULL	大於	>
不是空的	!= '''	IS NOT NULL	IS NOT NULL	大等於	>=
				小於	<
正則表達式	*REGEXP*			小等於	<=

值可以是一個實體或任何資料。如果使用巨集作為值，你必須將巨集的名稱包含在反引號中，例如：'macros.past_60m'。

注：Regex 支持 MySQL 正則表示式。也允許進行算術運算。

選項

以下是添加提醒規則時的一些其他選項

規則名稱：與該規則相關聯的名稱

嚴重程度：該規則的 "重要程度"

最大警告次數：最大警告次數。 事件傳送的最大警報數量。-1 表示無限制。

延遲：延遲時間。判斷規則被符合后，在傳送警報傳送前等待的時間，單位為秒。

Interval（間隔時間）。事件的警告間隔時間，單位為秒，直到達到最大警告數為止。

靜音警報。禁用通過警報傳送傳送警報規則。但仍然會在 Web UI 中察看警報。

反轉符合：反轉符合。反轉符合規則（即對不符合規則的項目發出警報）。

回復警報。如果關閉，將禁用回復通知的傳送。

進階

在"進階"選項卡上，您可以為警報規則指定一些附加選項。

覆寫 SQL。如果您使用自訂查詢，請啟用此選項

查詢：用於警報的查詢。

一個例子是所有 CPU 超過 10%的平均規則。

```
 SELECT *,AVG(processors.processor_usage) as cpu_avg FROM devices,processors WHERE
(device.device_id = ? AND devices.device_id = processors.device_id) AND (device.status = 1
&& (device.disabled = 0 && devices. ignore = 0)) = 1 HAVG(processors.processor_usage) > 10
```

10 將包含平均 CPU 使用量值，你可以把這個值改成你喜歡的任何值。

你需要將其複製并黏貼到 Advanced 下的 Alert Rule 中，然后黏貼到 Query box 中，然后切換到 Override SQL。

流程

你可以通過在建立規則時給出過程的 URL 來關聯一個規則到一個過程。僅支援像"http://"這樣的鏈結，否則將傳回錯誤。配置完成后，可以通過"開啟"按鈕從 Alert 小套件中開啟過程，該按鈕可以在小套件配置框中察看/隱藏。

範例

裝置故障	device.status!=1	高記憶體使用量 <裝置啟用 且 mem 使用率大等於 90 且 mem 描述 為 virtual >	macros.device_up = 1 AND mempools.mempool_perc>= 90 AND mempools.mempool_descr REGEXP"Virtual.*"
任何通訊埠變化	ports.ifOperStatus != 'up'	CPU 使用率高(每個核心的使用率， 而不是整體) <core/per 使用率大等於 90 >	macros.device_up = 1 AND processors.processor_usage>= 90
根目錄 太滿 <指向根目錄 且 目錄使用到 **75%?** >	storage.store_descr = '/' AND storage.store_perc >= '75'	Syslog5 分內出現認證失敗 <syslog 時間標記 大等於過去 5 分 且 認證失敗 >	syslog.timestamp >=macros.past_5m AND syslog.msg REGEXP ".*authentication failure.*"
任何儲存區的使用率大等於 "警告值 "	storage.storage_perc >= storage_perc_warn	通訊埠使用率高 且 port 描述不是用戶端和 port.ifType 不是軟體回傳	macros.port_usage_perc >= 80 AND port.port_descr_type != "client" AND ports.ifType != "softwareLoopback"
若裝置是伺服器，并且使用的儲存空間高於警告級別，但舍棄了/boot 割區 <裝置類型等於 server 且 儲存描述不等於 /boot >	storage.storage_perc > storage.storage_perc_warn AND devices.type = "server" AND storage.storage_descr != "/boot"	VMware LAG 沒有使用 "源 IP 位址 hash "負載均衡	devices.os = "vmware" AND ports.ifType = "ieee8023adLag" AND ports.ifDescr REGEXP "Link Aggregation .*, load balancing algorithm: Source ip address hash"
		當 mac 位址位於你的網路上時發出警報	ipv4_mac.mac_address = "2C233A756912"

警報規則收集 Alert rule collection

Devices up/down	macros.device_down = "1"	Device Down! Due to no ICMP response.	macros.device_down = "1" && devices.status_reason = "icmp"
Device rebooted 裝置 開關	devices.uptime < "300" && macros.device = "1"	SNMP not responding on Device - Check on SNMP Service - Device marked Down!	macros.device_down = "1" && devices.status_reason = "snmp"
Port status up/down 端口 開關	macros.port_down = "1"	Ping Latency 網路延遲	devices.last_ping_timetaken > "10"
Service up/down 服務 開關	services.service_status != "0" && macros.device_up = "1"	Port utilisation over threshold 端口使用率超過閾值	macros.port_usage_perc >= "80" && macros.port_up = "1"
Sensor over limit - Check Device Health Settings 感應數值超過限制	sensors.sensor_current > `sensors.sensor_limit` && sensors.sensor_alert = "1" && macros.device_up = "1"	Sensor under limit - Check Device Health Settings 感應數值低於限制	sensors.sensor_current < `sensors.sensor_limit_low` && sensors.sensor_alert = "1" && macros.device_up = "1"
Wireless Sensor over limit	wireless_sensors.sensor_current >= `wireless_sensors.sensor_limit` && wireless_sensors.sensor_alert = "1" && macros.device_up = "1"	Wireless Sensor under limit	wireless_sensors.sensor_current <= `wireless_sensors.sensor_limit_low` && wireless_sensors.sensor_alert = "1" && macros.device_up = "1"
State Sensor Critical	macros.state_sensor_critical && sensors.sensor_alert = 1	State Sensor Warning	macros.state_sensor_warning && sensors.sensor_alert = 1
IPSec tunnels down	ipsec_tunnels.tunnel_status != "active" && macros.device_up = "1"	Device took too long to poll 裝置輪詢太久	devices.last_polled_timetaken >= 290
Processor usage over 85% cpu 使用率 超過 85%	processors.processor_usage > "85" && macros.device_up = "1"	Port status change from up to down 端口狀態從開到關	ports.ifOperStatus = "down" && ports.ifOperStatus_prev = "up" && macros.device_up = "1"
Device added within the last 60 minutes	devices.inserted >= `macros.past_60m`	Interface Errors Rate greater than 100 接口錯誤率大於 100	ports.ifOutErrors_rate >= "100" || ports.ifInErrors_rate >= "100"
Device discovered within the last 60 minutes	eventlog.type = "discovery" && eventlog.message ~ "@autodiscovered@" && eventlog.datetime >= `macros.past_60m`	Too many wireless clients	wireless_sensors.sensor_class = "clients" && wireless_sensors.sensor_current >= `wireless_sensors.sensor_limit` && wireless_sensors.sensor_alert = "1" && macros.device_up = "1"
Syslog, Authentication failure on Device 設備的身份驗證失敗	syslog.timestamp >= `macros.past_5m` && syslog.msg ~ "@authentication failure@"	Syslog, received Alert Priority Message Syslog · 收到警報優先級消息	syslog.timestamp >= `macros.past_5m` && syslog.priority ~ "alert"

Service warning	services.service_status = "1"	Service critical	services.service_status = "2"
Sensor over limit with linked port 連接 port 大於限制	sensors.sensor_current > sensors.sensor_limit && sensors.sensor_alert = "1" && macros.device_up = "1" && macros.sensor_port_link = "1"	Sensor under limit with linked port 連接 port 低於限制	sensors.sensor_current < sensors.sensor_limit_low && sensors.sensor_alert = "1" && macros.device_up = "1" && macros.sensor_port_link = "1"
Applications OS-Updates, New Updates Available 操作系統更新，有可用的新更新	applications.app_type = "os-updates" && applications.app_status >= "10"	Synology NAS has a failed status	devices.os = "dsm" && sensors.sensor_type = "systemStatusState" && sensors.sensor_current = "2"
Synology NAS has a bad RAID status	devices.os = "dsm" && sensors.sensor_type = "raidStatusState" && sensors.sensor_current = "[11-12]"	Synology NAS has a failed power status	devices.os = "dsm" && sensors.sensor_type = "powerStatusState" && sensors.sensor_current = "2"
Synology NAS has a bad disk status	devices.os = "dsm" && sensors.sensor_type = "diskStatusState" && sensors.sensor_current = "[4-5]"	Synology NAS has a new upgrade available	devices.os = "dsm" && sensors.sensor_type = "upgradeAvailableState" && sensors.sensor_current = "1"
Dell Server Raid Battery Failed/Degraded	sensors.sensor_current ~ "[2|6]" && sensors.sensor_oid = ".1.3.6.1.4.1.674.10893.1.20.130.15.1.4.1"	Dell Server Disk Controller State Failed/Degraded	sensors.sensor_current ~ "[2|6]" && sensors.sensor_oid = ".1.3.6.1.4.1.674.10893.1.20.130.1.1.5"
Dell Server Disk Array State Failed/Degraded	sensors.sensor_current ~ "[2|5]" && sensors.sensor_oid = ".1.3.6.1.4.1.674.10893.1.20.130.4.1.4"	Dell Server Virtual Disk Failed/Degraded	sensors.sensor_current ~ "[2|6]" && sensors.sensor_oid = ".1.3.6.1.4.1.674.10893.1.20.140.1.1.4"
SSH Connections To	%applications.app_type='portactivity' && %applications_metrics.ssh_total_to>'5'	HTTP Connections To	%applications.app_type='portactivity' && %applications_metrics.http_total_to>'100'
FTP Connections To	%applications.app_type='portactivity' && %applications_metrics.ftp_total_to>'5'	HTTPS Connections To	%applications.app_type='portactivity' && %applications_metrics.smtp_total_from>'10'
SMTP Connections From	%applications.app_type='portactivity' && %applications_metrics.smtp_total_from>'10'	IMAP Connections To	%applications.app_type='portactivity' && %applications_metrics.imap_total_to>'20'
SMTP Connections To	%applications.app_type='portactivity' && %applications_metrics.smtp_total_to>'30'	IMAPS Connections To	%applications.app_type='portactivity' && %applications_metrics.imaps_total_to>'20'