XFUSION Nagios Plug-in v1.1.2 用户指南

发布日期 2023-03-30

注意

由于产品版本升级或其他原因,本文档内容会不定期进行更新。除非另有约定,本文档仅作为使用指导,本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

前	吉	iv
1	简介	6
2	插件安装	8
2.1	安装流程	8
2.2	安装准备	9
2.3	安装插件并添加设备	11
2.3	.1 安装插件	11
	.2 添加或删除设备	
3	获取信息	17
4	监控服务器状态及告警	19
5 I	FAQ	21
5.1	如何卸载插件	21
5.2	如何重新启动插件服务	22
5.3	如何处理 Nagios 首页无法显示主机服务状态的详细信息	23
	如何处理 SNMP V3 告警无法上报	
A	获取技术支持	26
R	通讯矩阵	27

前言

概述

本文档提供 Nagios 插件的安装、配置、设备监控和卸载过程。

读者对象

本文档主要适用于以下工程师:

- 技术支持工程师
- 维护工程师

符号约定

在本文中可能出现下列标志,它们所代表的含义如下。

符号	说明	
▲ 危险	用于警示紧急的危险情形,若不避免,将会导致人员死亡或严重 的人身伤害。	
▲ 警告	用于警示潜在的危险情形,若不避免,可能会导致人员死亡或严 重的人身伤害。	
<u></u> 注意	用于警示潜在的危险情形,若不避免,可能会导致中度或轻微的 人身伤害。	
须知	用于传递设备或环境安全警示信息,若不避免,可能会导致设备 损坏、数据丢失、设备性能降低或其它不可预知的结果。 "注意"不涉及人身伤害。	
□ 说明	用于突出重要/关键信息、最佳实践和小窍门等。 "说明"不是安全警示信息,不涉及人身、设备及环境伤害。	

修改记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新 内容。

文档版本	发布日期	修改说明
01	2023-03-30	第一次正式发布。

1 简介

功能介绍

Nagios 插件是一个集成在 Nagios 软件中的管理服务器的插件,通过添加服务器可以实现对服务器的监控功能。

通过该插件,可以实现以下功能:

- 监控服务器的告警信息。
- 查询服务器的电源、风扇、CPU、硬盘、内存、系统和 RAID 卡的基本信息及其 状态。

支持的服务器

- Nagios 最大支持管理 1000 台设备。
- Nagios 支持 SLES 10.2 和 Ubuntu 14.04 操作系统。
- Nagios 支持的服务器如表 1-1 所示。

□ 说明

- Nagios 插件支持监控 V3 服务器的告警类型为事件码。
- Nagios 插件只支持以","为分隔符的告警类型,请在服务器的 Web 页面的"Trap IP"处将分隔符修改为","。
- 5885H V5 和 2488H V6 只能使用 SNMPv3 添加。

表1-1 支持的服务器

架构	类型	服务器型号
x86	机架服务器	RH2288H V2
		RH1288 V3
	RH2288 V3	
		RH2288H V3
		RH5885 V3

架构	类型	服务器型号
		RH8100 V3
		1288H V5
		2288H V5
		2488 V5
		2288X V5
		5885H V5
		1288H V6
		2288H V6
		2488H V6
		5885H V6
	刀片服务器	E9000 (HMM910)
	高密服务器	XH321 V3
		XH620 V3
		XH622 V3
		XH628 V3

版本配套关系

版本名称	配套版本
iBMC	iBMC: 2.50 及以上版本
HMM	HMM: 6.10 及以上版本

软件要求

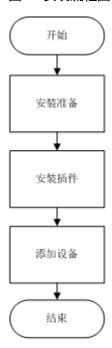
类型	版本号
Nagios	nagios core 3.5.1
	nagios core 4.3.4
	nagios core 4.4.5
	nagios core 4.4.6

- 2.1 安装流程
- 2.2 安装准备
- 2.3 安装插件并添加设备

2.1 安装流程

以流程图的方式给出插件的安装过程,安装过程如图 2-1 所示。

图2-1 安装流程图



2.2 安装准备

介绍插件安装前需要做的准备工作。

软件要求

插件安装前,请确认系统满足以下要求:

- Python 工具的版本为 Python 2.7.13。
- 支持的 Nagios 版本为 Nagios Core-3.5.1、Nagios Core-4.3.4 和 Nagios Core-4.4.6。
- 确保可以执行 snmpget 和 snmpwalk 命令,若不能,请执行以下命令安装。 yum install net-snmp net-snmp-devel net-snmp-libs net-snmp-utils php-snmp
- Nagios 服务器上存在以下三个文件:
 - "pysnmp-4.2.4.tar.gz"
 - "pyasn1-0.1.6.tar.gz"
 - "pycrypto-2.3.tar.gz"

山 说明

下载 "pysnmp-4.2.4.tar.gz"、"pyasn1-0.1.6.tar.gz" 和 "pycrypto-2.3.tar.gz" 文件, 并上传至 Nagios 服务器的任意目录 (例如: /usr/local) 进行安装。软件的安装步骤如下:

1. 执行以下命令,解压安装包。

tar xzvf \$sourcName

\$sourcName 为待解压的软件包名称,以 "pysnmp-4.2.4.tar.gz" 为例,则此处的命令为 tar xzvf pysnmp-4.2.4.tar.gz。

2. 执行以下命令, 进入解压后的文件夹。

cd

以 "pysnmp-4.2.4.tar.gz" 为例, 则此处的命令为 cd pysnmp-4.2.4。

3. 执行以下命令,安装软件。

python setup.py install

若系统中存在多个 Python 版本,请先执行 **export PATH**=\$pythonPath**:\$PATH** 命令, 其中 \$pythonPath 为 Python 2.7.13 的应用程序所在的路径。

数据准备

安装插件所需的数据如表 2-1 所示。

表2-1 安装插件所需的数据

项目	作用	样例
Nagios 服务器 的 IP 地址。	用于访问安装 Nagios 工具的服务器和安装插件。	192.168.1.110
安装包上传到 Nagios 服务器	用于在 Nagios 服务器上放置插件的安装包。	/etc

项目	作用	样例
的路径。		
软件的安装路 径。	用于在 Nagios 服务器上安装插件。	/usr/local/nagios
登录 Nagios 服 务器的用户 名。	用于访问 Nagios 服务器的操作系统。	root
Nagios 服务器 用户名的密 码。	用于访问 Nagios 服务器的操作系统。	xfusion123
被管理设备的基本信息。	用户在 Nagios 服务器上配置被管理设备的信息,使 Nagios 系统可以监控该设备。需要准备的信息包括 • 被管理设备的 IP 地址。 • 被管理设备的主机名。 • 登录被管理设备的密码。 • 与 Nagios 服务器通信的 SNMP 协议的读写团体名。 • SNMP 协议的版本设备默认只开启SNMP V3 版本协议。如果您需要使用SNMP V1 或者 V2C 版本协议资本协议,并获取该版本协议的读写团体名。并获取该版本协议的读写团体名。开启设备的 SNMP V1 和 V2C 协议以及获取该协议读写团体名的方法请参见随设备发布的手册。 • Trap 团体名,在设备上报告警时使用。 说明 使用 SNMP V1 协议或者 SNMP V2C 协议接入设备,系统只能上报 SNMP V1 或者 SNMP V2C 相关的报警,不会上报 SNMP V3 协议相关的报警。	 192.168.1.100 xfusion-1 root xfusion@123 public v3 xFusion12#\$

工具准备

请自备 PuTTY 软件。

2.3 安装插件并添加设备

介绍安装插件并同时添加设备信息的过程。

2.3.1 安装插件

介绍插件的安装过程。该版本插件和 V100R001C00SPC201 及以前版本的配置文件不兼容,如果是升级安装请在卸载插件时选择不保存配置文件。

前提条件

- 己从 GitHub 网站获取插件的安装包 "XFUSION Nagios Plugin vX.X.X.tar"。
- 检验 Nagios 插件软件包的完整性。
 - a. 进入插件软件包和 sha256 校验文件的存放目录。
 - b. 执行 **sha256sum -c <(grep '***软件包名称' 'sha256 校验文件名称'***)**命令进行校验。

如: sha256sum -c <(grep 'XFUSION Nagios Plugin v1.1.1.tar' 'XFUSION Nagios Plugin v1.1.1.sha256.sum')

- c. 查看校验结果是否为"OK"。
 - 是:软件包未被篡改,可使用。
 - 否: 软件包已被篡改,请勿使用,请获取新软件包。
- 已上传 Nagios 安装包到服务器。
- 以"root"用户登录服务器。

操作步骤

步骤1 执行以下命令,解压安装包。

cd /etc

tar -xvf XFUSION\ Nagios\ Plugin\ vX.X.X.tar

解压后生成"XFUSION Nagios Plugin vX.X.X"文件夹。

步骤 2 执行以下命令,安装插件并自动添加设备信息到 Nagios 系统中。

cd XFUSION Nagios Plugin vX.X.X

python setup.py install -d 10.10.10.10 -p 10061 -n /usr/local/nagios

各参数的含义如下所示。

- "-d"后的参数为 Nagios 服务器的 IP 地址。
- "-n"后的参数为 Nagios 工具的安装路径。

□ 说明

"/usr/local/nagios" 为具体的安装路径,请以实际为准。

• "-p"后的参数为 Nagios 告警监听端口,可选,默认端口为 10061。

□ 说明

若系统中有多个 Python 版本,安装过程中可能会出现报错 "check python vesion fail ,please check you python is 2.7.13",若 Python 2.7.13 的应用程序所在路径为 "/usr/local/bin",则安装 Nagios 插件的命令为/usr/local/bin/python setup.py install -d 192.168.1.110 -p 10061 -n /usr/local/nagios。

----结束

2.3.2 添加或删除设备

插件安装完成后,您可以在 Nagios 服务器上添加需要监控的设备。

前提条件

- 已安装插件。具体操作请参见 2.3.1 安装插件。
- 已获取被管设备的信息。 如果需要添加的设备为 E9000,请确保其 HMM 板的静态 IP 地址已被清空。
- 被管设备已注册 Trap IP。
- 以"root"用户登录 Nagios 服务器。

使用 config.py 添加设备

表2-2 config.py 命令说明

命令	说明
add	添加单个服务器,并设置
batch	批量添加服务器
del	删除服务器,支持批量和单个删除
inquiry	查询当前已配置服务器
version	查询当前版本号
resetserver	清空对接服务器的 trap IP

添加单个服务器

步骤 1 执行以下命令,进入"config.py"所在的目录。

cd /usr/local/nagios/bin/XFUSION_server

步骤 2 执行以下命令,添加单个服务器。

执行以下命令,使用 v1 trap 添加单个服务器。
 python config.py add -i 10.10.10.10 -t Rack -p 161 -a ****** -e ****** -v v1 -u root -x SHA -d AES -V v1 -C ****** -c ******

- 执行以下命令,使用 v2 trap 添加单个服务器。
 - python config.py add -i 10.10.10.10 -t Rack -p 161 -a ****** -e ****** -v v2 -u root x SHA -d AES -V v2 -C ****** -c ******
- 执行以下命令,使用 v3 trap 添加单个服务器。

python config.py add -i 10.10.10.10 -t Rack -p 161 -a ****** -e ****** -v v3 -u root -x SHA -d AES -A ****** -E ****** -V v3 -U root -X SHA -D AES

表2-3 参数说明

参数	说明
-i	被监控服务器的 IP 地址。
-H	被监控服务器的名字,可选,不填则该项的值等于 IP 地址,不建 议填写,批量配置时不填写。
-t	被监控服务器的类型,目前支持的类型包括 Rack(机架服务器)、Blade(刀片服务器)、HighDensity(高密服务器)。
-p	被监控服务器 SNMP 服务的端口号,不填时默认为"161"。
-V	查询和设置监控服务器 SNMP 所用的协议版本,可设置为 "v1"、"v2"或者"v3"(建议选择"v3"),不填写时默认为"v3"。
-u	查询和设置监控服务器 SNMP V3 协议所用的用户名,不填写时将不能设置服务器的 trap 目的 IP 地址。
-a	查询和设置监控服务器 SNMP V3 协议所用的用户密码,不填写时将不能设置服务器的 trap 目的 IP 地址。
-e	查询和设置监控服务器 SNMP V3 协议所用的 SNMP 加密密码,不填写时默认与-a 参数的密码相同。
-X	查询和设置监控服务器 SNMP V3 协议所用的鉴权算法,可设置为 "MD5"或"SHA"。
-d	查询和设置监控服务器 SNMP V3 协议所用的加密算法,可设置为 "AES"或"DES"。
-с	查询和设置监控服务器 SNMP V1 或 SNMP V2C 协议所用的团体名,仅对 SNMP V1 和 SNMP V2C 协议适用。

表2-4 trap 参数

trap 参数	说明
-V	接收被监控服务器的 trap 消息所用的 SNMP 版本,可设置为 "v1"、"v2"或者"v3",不填写时默认"v3"。
-U	用 SNMP V3 协议接收被监控服务器的 trap 所用的用户名,不填写

trap 参数	说明
	时默认和-u 参数的值一致。
-A	用 SNMP V3 协议接收被监控服务器的 trap 所用的用户密码,不填写时默认和-a 参数的值一致。
-E	用 SNMP V3 协议接收被监控服务器的 trap 所用的 SNMP 加密密码,不填写时默认和-A 参数的值一致。
-X	用 SNMP V3 协议接收被监控服务器的 trap 所用的鉴权算法,可设置为"MD5"或"SHA",不填写时和-x 参数的值一致。
-D	用 SNMP V3 协议接收被监控服务器的 trap 所用的加密算法,可设置为 "AES"或 "DES",不填写时和-d 参数的值一致。
-C	用 SNMP V1 或 SNMP V2C 协议接收被监控服务器的 trap 所用的团体名,仅对 SNMP V1 和 SNMP V2C 协议适用,不填写时和-c 参数的值一致。

添加服务器后插件会配置对接服务器的 trap, 配置项如表 2-5 所示。

表2-5 trap 配置

设置项	说明					
Trap 模式	设置成事件码模式。					
Trap 发送的 snmp 版本	根据表 2-3 中的-V 参数配置。					
Trap 发送目标 IP	设置最后一个 trap 的 IP 地址,iBMC 为第四个地址,HMM 为第五个地址。					
Trap 发送的目标端口	设置最后一个 trap 的 IP 地址对应的端口,iBMC 为第四个地址对应的端口,HMM 为第五个地址对应的端口。					
Trap 发送使能	设置为使能。					

----结束

批量添加服务器

步骤 1 执行以下命令,进入"config.py"所在的目录。

cd /usr/local/nagios/bin/XFUSION_server

步骤 2 执行以下命令,批量添加服务器。

python config.py batch -i 10.10.10.116-119 -t Rack -p 161 -a ****** -e ****** -v v3 -u root -x SHA -d AES -A ****** -E ****** -V v3 -U root -X SHA -D AES 或者 python

config.py batch -i 10.10.10.* -t Rack -p 161 -a ****** -e ***** -v v3 -u root -x SHA -d AES -A ***** -E ****** -V v3 -U root -X SHA -D AES

-i 10.10.10.116-119 表明批量添加服务器的 IP 地址为 10.10.10.116、10.10.10.117、10.10.10.118、10.10.10.119,共4个服务器。

-i 10.10.10.* 表明批量添加服务器网段为 10.10.10.*。

其余参数请参考表 2-3,添加服务器后插件会配置对接服务器的 trap,配置项如表 2-5 所示。

----结束

删除服务器

步骤1 执行以下命令,进入"config.py"所在的目录。

cd /usr/local/nagios/bin/XFUSION_server

步骤 2 执行以下命令,删除服务器。

- 删除单个服务器: python config.py del -i 10.10.10.1
- 批量删除服务器: **python config.py del -i** 10.10.10.116-119 或 **python config.py del -i** 10.10.10.*

删除服务器后,会设置对应的服务器的最后一个 trap 发送目标地址为空(iBMC 为第四个地址,HMM 为第五个地址)。

----结束

手动清空服务器 trap IP 地址

步骤1 执行以下命令,进入"config.py"所在的目录。

cd /usr/local/nagios/bin/XFUSION server

步骤 2 执行以下命令,清空服务器 trap IP 地址。

- 清空单个服务器 trap IP 地址: **python config.py resetserver -i** 10.10.10.1 **-p** 161 **-a** ****** **-e** ****** **-v** v3 **-u** root **-x** SHA
- 批量清空服务器 trap IP 地址: python config.py resetserver -i 10.10.10.116-119 -p 161 -a ****** -e ****** -v v3 -u root -x SHA 或 python config.py resetserver -i 10.10.10.* -p 161 -a ****** -e ****** -v v3 -u root -x SHA

手动清空服务器 trap IP 地址后,会设置对应的服务器的最后一个 trap 发送目标地址为空(iBMC 为第四个地址,HMM 为第五个地址)。

----结束

查询已配置服务器地址

步骤 1 执行以下命令,进入 "config.py" 所在的目录。

cd /usr/local/nagios/bin/XFUSION_server

用户指南

步骤 2 执行以下命令,查询已配置服务器地址。

python config.py inquiry

----结束

查询插件版本

步骤 1 执行以下命令,进入 "config.py" 所在的目录。

cd /usr/local/nagios/bin/XFUSION_server

步骤 2 执行以下命令,查询插件版本。

python config.py version

----结束

3 获取信息

介绍在 Nagios 中获取机架和高密服务器信息的方法。

前提条件

- 已安装插件并添加设备。具体操作请参见 2.3.1 安装插件和 2.3.2 添加或删除设备。
- 以"root"用户登录 Nagios 服务器。

背景信息

在Nagios中获取设备信息的方法包括手动获取和自动获取。

- 手动获取是指用户登录 Nagios 服务器手动执行脚本,获取设备信息。可获取设备的 System、电源、风扇、CPU、内存、磁盘、pCIe 卡、RAID 卡、逻辑盘、组件、传感器、固件版本。
- 自动获取是指 Nagios 自动调用脚本,获取设备信息。可获取设备的 System、电源、风扇、CPU、内存和磁盘信息。

操作步骤

• 手动获取。

□ 说明

首次执行获取时必须是 nagios 用户。

- a. 执行以下命令,进入"/usr/local/nagios/bin/XFUSION_server"目录。 cd /usr/local/nagios/bin/XFUSION_server
- b. 执行以下命令,获取设备信息。
 python collect.py -a -r resultPath
 python collect.py -f *目录lhost.xml* -r resultPath

表3-1 命令含义

命令	含义				
python collect.py -a	调用"XFUSION_hosts.xml"文件获取设备信息,结果				

命令	含义					
	文件默认存放在"/usr/local/nagios/bin/result"目录。					
python collect.py -a -r resultPath	调用"XFUSION_hosts.xml"文件获取设备信息,结果文件存放在指定目录。 执行命令前请确保指定目录已存在,以及权限为750及以上,所属用户和组均为 nagios。					
python collect.py -f 目录 /host.xml	调用"host.xml"文件获取设备信息,结果文件默认存放在"/usr/local/nagios/bin/result"目录。 说明 "host.xml"为用户新创建的配置文件,该文件的格式必须与 "XFUSION_hosts.xml"相同,且需要给出文件所在路径。					
python collect.py -f 目录 /host.xml -r resultPath	调用"host.xml"文件获取设备信息,结果文件存放在指定目录。 说明 "host.xml"为用户新创建的配置文件,该文件的格式必须与 "XFUSION_hosts.xml"相同,且需要给出文件所在路径。					

● 自动获取。

启动 Nagios 服务后,Nagios 自动调用脚本,获取设备信息,默认轮询周期为 10 分钟。

4

监控服务器状态及告警

介绍在 Nagios 中监控机架、高密和刀片服务器状态及告警的方法。

前提条件

- 已安装插件并添加设备。具体操作请参见 2.3.1 安装插件和 2.3.2 添加或删除设备。
- 己登录 Nagios 的 Web 界面。

操作步骤

- 步骤 1 在左侧导航树中,选择 "Current Status > Services"。
- 步骤 2 在右侧信息展示区的"Service Status Details For All Hosts"列表中,查看所有被监控的设备信息及其部件状态。
 - "Service Status Details For All Hosts"列表如图 4-1 所示。

图4-1 列表信息



- "Host"列显示被监控设备的主机名。单击主机名可以查看该设备的详情。
- "XFUSION-server-plugin"为 Nagios 监控的插件服务名。
- "Service"列显示被监控设备的部件或告警(alarm)。单击部件可以查看详细的状态信息。

• "Status"列显示被监控部件的整体状态。

----结束

5 faq

- 5.1 如何卸载插件
- 5.2 如何重新启动插件服务
- 5.3 如何处理 Nagios 首页无法显示主机服务状态的详细信息
- 5.4 如何处理 SNMP V3 告警无法上报

5.1 如何卸载插件

介绍卸载插件的方法。

前提条件

- 己安装插件。
- 以"root"用户登录 Nagios 服务器。

操作步骤

步骤1 执行以下命令,进入安装插件时的目录。

cd /etc

cd XFUSION Nagios Plugin vX.X.X

步骤 2 卸载插件。

• 执行以下命令,不保留用户数据卸载插件。

python setup.py uninstall -n /usr/local/nagios

"/usr/local/nagios"为 Nagios 工具具体的安装路径,请以实际为准。

• 执行以下命令,保留用户数据卸载插件。

python setup.py uninstall -n /usr/local/nagios -s yes 或 python setup.py uninstall -n /usr/local/nagios --retain yes

"/usr/local/nagios"为 Nagios 工具具体的安装路径,请以实际为准。

步骤3 系统开始卸载插件。卸载完成后,屏幕提示以下信息。

setup.py=> [info] uninstall success.
Done.

步骤 4 检查主配置文件 "nagios.cfg" 的正确性。

1. 执行以下命令,切换到 Nagios 用户。

su - nagios

2. 执行以下命令,检查主配置文件"nagios.cfg"。

/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

□ 说明

"/usr/local/nagios" 为插件的安装路径,请以实际为准。

系统显示以下信息时表示配置文件"nagios.cfg"正确无误。

Things look okay - No serious problems were detected during the pre-flight check

3. 执行以下命令,退出到"root"用户。

exit

步骤 5 执行以下命令,重新启动 Nagios 服务。

systemctl restart nagios

----结束

5.2 如何重新启动插件服务

介绍在 Nagios 服务器中重新启动插件服务的方法。

前提条件

- 己安装插件。
- 以"root"用户登录 Nagios 服务器。

操作步骤

步骤1 执行以下命令,查看插件告警服务是否启动。

ps -ef |grep trapd.py |grep -v grep

如果屏幕显示以下信息,表示插件服务已经启动。否则,请耐心等待 2 分钟,插件服务会自动启动。

nagios 22237 1 1 18:06 ? 00:00:00 python
/usr/local/nagios/bin/XFUSION server/trapd.py

□ 说明

以上回显信息中的 "22237" 为插件的进程 ID 号。

步骤 2 执行以下命令,查看设备信息服务是否启动。

ps -ef |grep collect.py

如果屏幕显示以下信息,表示 s 设备信息服务已经启动。否则,请耐心等待 2 分钟,插件服务会自动启动。

nagios 23858 1 5 17:00 ? 00:00:01 python
/usr/local/nagios/bin/XFUSION server/collect.py -p

□ 说明

以上回显信息中的"23858"为插件的进程 ID 号。

步骤3 执行以下命令,停止插件服务。

kill -9 22237

kill -9 23858

步骤 4 等待 1 分钟,使用步骤 1 中的命令确认插件服务已启动。 插件服务被停止后会自动启动。

步骤 5 执行以下命令,重新启动 Nagios 服务。

systemctl restart nagios

□说明

Nagios 服务启动时,如果获取设备类型或者注册 Trap IP 失败,则系统会把设备的状态设置为"Unknown",表示该设备没有被 Nagios 插件所监控。

步骤 6 查看插件服务及设备信息服务是否启动。

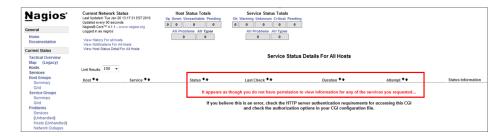
----结束

5.3 如何处理 Nagios 首页无法显示主机服务状态的详细信息

现象描述

Nagios 首页无法显示主机服务状态的详细信息,如图 5-1 所示。

图5-1 问题现象示例图



可能原因

配置文件 "/usr/local/nagios/etc/cgi.cfg"中的"use_authentication"值为"1"。

处理步骤

步骤 1 修改 "use_authentication" 值。

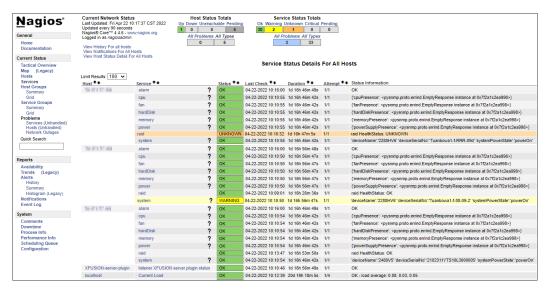
- 1. 打开文件 "/usr/local/nagios/etc/cgi.cfg"。
- 2. 定位 "use_authentication"所在位置。
- 3. 修改 "use_authentication"属性值为"0"。

步骤 2 执行以下命令,重新启动 Nagios 服务。

systemctl restart nagios

重启后 Nagios 首页主机服务状态的详细信息显示正常,如图 5-2 所示。

图5-2 主机服务状态的详细信息显示图



----结束

5.4 如何处理 SNMP V3 告警无法上报

现象描述

使用 SNMP V3 协议接入设备,主备倒换后,告警无法上报。

山 说明

刀片服务器不支持 SNMP V3 告警上报。

可能原因

- 主备板倒换、设备上下电或者设备重启后,由于设备引擎 ID 发生变化,致使告警 无法上报。
- 设备告警上报的事件码和 Trap 版本与配置不一致,导致告警无法上报。

□ 说明

设备的告警模式必须是事件码模式。

● Trap IP 未在设备上注册或端口不是 10061,导致告警无法上报。

处理步骤

步骤 1 检查服务器的 IP 地址与 Nagios 插件上的配置文件中的 IP 地址是否相同?

- 是, 步骤 4。
- 否,修改 Nagios 插件上的配置文件中的 IP 地址与服务器上的 IP 地址相同。

步骤 2 检查服务器是否处于上电状态?

- 是,步骤 4。
- 否,服务器上电。

步骤3 检查服务器告警上报是否正常?

- 是,步骤 4。
- 否,将 Trap IP 的上报模式为事件码,手动注册 Trap IP, 且将端口号设置为 10061,报文分隔符必须用","。

步骤 4 执行以下命令,查询告警获取进程号。

ps -ef | grep trapd.py

步骤 5 执行以下命令,停止告警获取进程。

kill -9 告警进程号

----结束

A 获取技术支持

如果在设备维护或故障处理过程中,遇到难以确定或难以解决的问题,通过文档的指导仍然不能解决,请通过如下方式获取技术支持。

- 联系客户服务中心。
 - 客户服务电话: 400-009-8999
 - 客户服务邮箱: support@xfusion.com
- 联系技术支持人员。

B 通讯矩阵

源设 备	源 IP	源端 口	目的设备	目的 IP	目的端位	协议	端口说明	侦听端口是否可更改	认证方式	加密方式
Nagio s 所 属设 备	Nagios 虚 拟网口 veth 的 IP	随机端口	Nagios 所属设备	iBMA 虚拟 网口 IP地 址	80	TC P	HTTP(Web) HTTP 标准协议端口,默认开启,使用的协议可配置。	是	用户名/ 密码	HTTP 协议无 加密
插所设备	插件所属 设备 IP	随加端口	iBMC 所 属设备	iBMC 虚拟 网口 veth 的 IP	161	UD P	iBMC SNMP 服务器端 口,用于 SNMP 数据 交互	不涉及	v1 v2c:团 体名 v3:用容:	以 iBMC SNMP 设置的 加密协 议 准。
Nagio s 所 属设 备	Nagios 所 属设备 IP	随机端口	SNMP Trap 服 务器	SNMP Trap 服务 器 IP	162	UD P	插件对应系 统 SNMP Trap 服务器 端口,用于 SNMP 数据 交互	不涉及	v1 v2c:团 体名 v3:用户 名/密码 说明: 使 用 v1 和	无

源设 备	源 IP	源端 口	目的设备	目的 IP	目的端侦听)	协议	端口说明	侦听端口是否可更改	认证方式	加密方式
									v2c 会降 低系统安 全性,请 谨慎操 作。	