XFUSION Nagios Plug-in v1.1.2

User Guide

Date **2023-03-30**

Notice

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

Preface

Purpose

This document describes how to install, configure, monitor, and uninstall the Nagios plug-in.

Intended Audience

This document is intended for:

- Technical support engineers
- Maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠ CAUTION	Indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
📖 NOTE	Calls attention to important information, best practices, and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Issue	Date	Description
01	2023-03-30	This issue is the first official release.

1 Overview

Function Description

The Nagios plug-in is a plug-in integrated in the Nagios software and used for server management.Servers can be monitored after being added.

You can implement the following functions by using the Nagios plug-in:

- Monitor the alarm information of servers.
- Query the basic information and status of the PSUs, fans, CPUs, hard disks, memory, systems, and RAID controller cards of servers.

Supported Servers

- Nagios supports a maximum of 1,000 servers.
- Nagios can run on SLES 10.2 and Ubuntu 14.04.
- Table 1-1 lists the servers supported by the Nagios.

NOTE

- For V3 servers, the Nagios plug-in supports alarms in the event code format.
- Nagios plug-in supports only commas (,) as alarm delimiters. You need to change the delimiter to comma in the trap IP address registration area on the device WebUI.
- 5885H V5 and 2488H V6 servers can be added only by using SNMPv3.

Table 1-1 Supported servers

Architecture	Type	Server Model
x86	Rack server	RH2288H V2
		RH1288 V3
		RH2288 V3
		RH2288H V3
		RH5885 V3
		RH8100 V3
		1288H V5

Architecture	Type	Server Model
		2288H V5
		2488 V5
		2288X V5
		5885H V5
		1288H V6
		2288H V6
		2488H V6
		5885H V6
	Blade server	E9000(HMM910)
	High-density server	XH321 V3
		XH620 V3
		XH622 V3
		XH628 V3

Matching Versions

Software	Matching Versions
iBMC	iBMC: 2.50 or later
HMM	HMM: 6.10 or later

Software Requirements

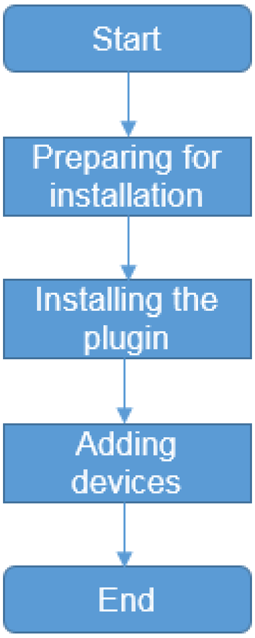
Type	Version
Nagios	nagios core 3.5.1
	nagios core 4.3.4
	nagios core 4.4.5
	nagios core 4.4.6

2 Installing the Nagios Plug-in

2.1 Installation Process

Figure 2-1 shows the process of installing the Nagios plug-in.

Figure 2-1 Installation process



2.2 Preparing for Installation

This section describes the preparations for installing the Nagios plug-in.

Software Requirements

Before installing the Nagios plug-in, ensure that the system meets the following requirements:

- The Python tool version is Python 2.7.13.
- The Nagios tool version is Nagios Core-3.5.1,Nagios Core-4.3.4 or Nagios Core-4.4.6.
- Make sure **snmpget** and **snmpwalk** command can run in you host, if not, run the follow command to install them.

  yum install net-snmp net-snmp-devel net-snmp-libs net-snmp-utils php-snmp
- The following files exist on the Nagios server:
  - pysnmp-4.2.4.tar.gz
  - pyasn1-0.1.6.tar.gz
  - pycrypto-2.3.tar.gz

NOTE

Download the **pysnmp-4.2.4.tar.gz**, **pyasn1-0.1.6.tar.gz**, and **pycrypto-2.3.tar.gz** files and upload them to any directory on the Nagios server, for example, **/usr/local**) and install the software. The procedure for software installation is as follows:

1. Run the following command to decompress the software package.

   tar xzvf *$sourcName*

   For example, If **pysnmp-4.2.4.tar.gz** is used as an example, run **tar xzvf pysnmp-4.2.4.tar.gz**.
2. Run the following command to go to the decompression directory.

   cd

   For example, if **pysnmp-4.2.4.tar.gz** is used as an example, run **cd pysnmp-4.2.4**.
3. Run the following commadn to install the software:

   python setup.py install

   If the system has multiple python versions, run the **export PATH=***$pythonPath***:$PATH** command, where **$pythonPath** indicates the directory where Python 2.7.13 is located.

Data Preparation

Table 2-1 lists the data required for installing the Nagios plug-in.

Table 2-1 Table1 Required data

Item	Function	Example
IP address of the Nagios server	Used to access the server where the Nagios tool is installed and install the Nagios plug-in.	192.168.1.110
Path for uploading the installation	Used to install the Nagios plug-in installation package on the Nagios	/etc

Item	Function	Example
package to the Nagios server	server.	
Software installation path	Used to install the Nagios plug-in on the Nagios server.	/usr/local/nagios
User name for logging in to the Nagios server	Used to log in to the OS of the Nagios server.	root
Password of the Nagios server user	Used to log in to the OS operating system of the Nagios server.	xfusion123
Basic information about managed servers	You can configure information about managed servers on the Nagios server so that the Nagios server can monitor the servers. The following information is required: • IP address of the managed server • Host name of the managed server • User name for logging in to the managed server • Password for logging in to the managed server • SNMP read/write community name for communicating with the Nagios server • SNMP version. By default, only the SNMP V3 is enabled on the server side. If you need to use SNMP V1 or SNMP V2C to add a server, log in to the server to enable the SNMP V1 or SNMP V2C protocol and obtain the read and write community names of the protocol. For details, see the manuals released with the server. • Trap community name, which is used when the server reports an alarm. **NOTE** If SNMP V1 or SNMP V2C is used, the system reports only alarms related to SNMP V1 or SNMP V2C, but not alarms related to SNMP V3.	• 192.168.1.100 • xfusion-1 • root • xfusion@123 • public • v3 • xFusion12#$

Tools

PuTTY software

2.3 Installing the Nagios Plug-in and Adding Servers Manually

This section describes how to install the Nagios plug-in and add servers.

2.3.1 Installing the Nagios Plug-in

This section describes how to install theNagiosplug-in. TheNagiosplug-in for this version is not compatible with the configuration file of V100R001C00SPC201 or earlier. In the case of Nagiosplug-in installation during system upgrade, do not save the configuration file.

Prerequisites

- The Nagios plug-in installation package **XFUSION Nagios Plugin v***X.X.X***.tar** has been obtained from GitHub.
- Verify the integrity of the Nagios plug-in software package.
  a. Go to the directory where the plug-in software package and SHA256 verification file are stored.
  b. Run the **sha256sum -c < (grep** *'software package name*' *'sha256 verification file name***')** command to verify the software package.

     Example: **sha256sum -c <(grep 'XFUSION Nagios Plugin v1.1.1.tar' 'XFUSION Nagios Plugin v1.1.1.sha256.sum')**
  c. Check whether the verification result is **OK**.
     - If yes, the software package has not been tampered with and can be used.
     - If no, the software package has been tampered with. Obtain a new software package.
- The installation package has been uploaded to the Nagios server.
- You have logged in to the Nagios server as the **root** user.

Operation Procedure

Step 1 Run the following commands to decompress the installation package:

cd /etc

tar -xvf XFUSION\ Nagios\ Plugin\ v*X.X.X***.tar**

The **XFUSION Nagios Plugin v***X.X.X* folder is generated.

Step 2 Run the following commands to install the Nagios plug-in and add server information to the Nagios system:

cd XFUSION Nagios Plugin v*X.X.X*

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

The parameters are described as follows:

- The parameter following **-d** indicates the IP address of the Nagios server.
- The parameter following **-n** is the installation path of the Nagios tool.

NOTE

In the preceding command, **/usr/local/nagios** indicates the installation path. Change it based on the site requirements.

- The parameter after **-p** indicates the Nagios alarm listening port. This parameter is optional. The default port number is **10061**.

NOTE

If multiple Python versions exist in the system, the error message "check python version fail, please check you python is 2.7.13" may be displayed during the installation. If the path of the Python 2.7.13 application is **/usr/local/bin**, run **/usr/local/bin/python setup.py install -d 192.168.1.110 -p 10,061 -n /usr/local/nagios** to install the Nagios plug-in.

----End

2.3.2 Adding or Deleting Servers

After the Nagios plug-in is installed, you can add servers to be monitored on the Nagios server.

Prerequisites

- The Nagios plug-in has been installed. For details, see 2.3.1 Installing the Nagios Plug-in.
- You have obtained information about managed servers.

  If the E9000 is to be added, ensure that the static IP address of the HMM is cleared.
- The managed servers have registered a Trap IP address.
- You have logged in to the Nagios server as the **root** user.

Adding Servers Using config.py Commands

Table 2-2 describes the config.py commands.

Table 2-2 config.py command description

Command	Description
add	Add a single server.
batch	Adding servers in batches.
del	Delete a server. The server can be deleted in batches or one by one.
inquiry	Query the configured server.
version	Query the current version number.
resetserver	Clear the trap IP address of the interconnected server.

Adding a Single Server

Step 1 Switch to the directory where **config.py** is located.

```
cd /usr/local/nagios/bin/XFUSION_server
```

Step 2 Run the following command to add a server.

- Run the following command to add a server using v1 trap:

  ```
  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 ******
  ```

- Run the following command to add a server using v2 trap:

  ```
  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 *****
  ```

- Run the following command to add a server using v3 trap:

  ```
  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
  ```

Table 2-3 Command parameters

Parameter	Description
-i	IP address of the monitored server.
-H	Name of the monitored server. This parameter is optional. If this parameter is left blank, the value is the same as the IP address. This parameter is not recommended and cannot be specified during batch configuration.
-t	Type of the monitored server. The options are as follows: • Rack • Blade • HighDensity
-p	SNMP service port of the monitored server. If this parameter is left blank, default value **161** is used.
-v	SNMP protocol version used to query and monitor the monitored server. The value can be v1, v2, or v3 (v3 is recommended). If this parameter is left blank, default value **v3** is used.
-u	User name used by the SNMP V3 protocol to query and set the monitored server. If this parameter is not specified, the trap destination IP address of the server cannot be set.
-a	Password used by the SNMP V3 protocol to query and set the monitored server. If this parameter is not specified, the trap destination IP address of the server cannot be set.
-e	If the SNMP encryption password used for querying and setting the SNMP V3 protocol of the monitored server is left blank, the value of this parameter is the same as the value of **-a** by default.

Parameter	Description
-x	authprotocol used by the SNMP V3 protocol to query and set the monitored server. The value can be **MD5** or **SHA**.
-d	privprotocol used by the SNMP V3 protocol to query and set the monitored server. The value can be **AES** or **DES**.
-c	Community name used by the SNMP V1 or SNMP V2C protocol to query and set the monitored server. This parameter is applicable only to the SNMP V1 and SNMP V2C protocols.

Table 2-4 Trap parameters

Parameter	Description
-V	SNMP version used for receiving trap messages from the monitored server. The value can be v1, v2, or v3 (v3 is recommended). If this parameter is left blank, default value **v3** is used.
-U	User name used by the SNMP V3 protocol to receive traps from the monitored server. If this parameter is left blank, the value is the same as the value of **-u** by default.
-A	Password used by the SNMP V3 protocol to receive traps from the monitored server. If this parameter is left blank, the value is the same as the value of **-a** by default.
-E	If the user SNMP encryption password used by the SNMP V3 protocol to receive the trap of the monitored server is left blank, the value of this parameter is the same as the value of **-A** by default.
-X	authprotocol used by the SNMP V3 protocol to receive traps from the monitored server. The value can be MD5 or SHA. If this parameter is not set, the value is the same as the value of **-x** by default.
-D	privprotocol used by the SNMPv3 protocol to receive traps from the monitored server. The value can be AES or DES. If this parameter is not set, the value is the same as the value of **-d** by default.
-C	Community name used by the SNMP V1 or SNMP V2C protocol to receive traps from the monitored server. This parameter is applicable only to the SNMP V1 and SNMP V2C protocols. If this parameter is not set, the value is the same as the value of **-c** by default.

After a server is added, the Nagios plug-in configures the trap parameters for the server automatically. For details about the configuration items, see Table Parameter setting.

Table 2-5 Parameter setting

Item	Description
Trap mode	Set the trap mode to event mode.
SNMP version for sending traps	Configure the SNMP version based on the **-V** parameter in Table Command parameters.
Destination IP address for sending traps	Set the IP address of the last trap. The iBMC uses the fourth address; the HMM uses the fifth address.
Destination port for sending traps	Set the port corresponding to the IP address of the last trap. The iBMC uses the port mapping to the fourth IP address; the HMM uses the port mapping to the fifth IP address.
Enable trap sending	Enable the trap sending function.

----End

Adding Servers in Batches

Step 1 Switch to the directory where **config.py** is located.

cd /usr/local/nagios/bin/XFUSION_server

Step 2 Run the following command to add servers in batches:

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* or **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* indicates that the IP addresses of the servers to be added are 10.10.10.116, 10.10.10.117, 10.10.10.118, and 10.10.10.119 (four servers in total).

-i *10.10.10.** indicates that the network segment for adding servers in batches is *10.10.10.*.

For details about other parameters, see Table Command parameters. After servers are added, the Nagios plug-in configures the trap parameters for the servers automatically. For details about the configuration items, see Table Parameter setting.

----End

Deleting a Server

Step 1 Switch to the directory where **config.py** is located.

cd /usr/local/nagios/bin/XFUSION_server

Step 2 Run the following commands to delete a server or multiple servers:

- Delete a single server:

  python config.py del -i *10.10.10.1*

- Delete servers in batches:

  python config.py del -i *10.10.10.116-119* or **python config.py del -i** *10.10.10.**

After a server is deleted, the destination address of the last trap is set to null for the server. (The iBMC is located in the fourth address, anduses theed in the fifth address.)

----End

Manually Clearing the Trap IP Addresses of Servers

Step 1 Switch to the directory where **config.py** is located.

cd /usr/local/nagios/bin/XFUSION_server

Step 2 Run the following commands to clear the trap IP addresses of servers:

- Clear the trap IP address of a server:

  python config.py resetserver -i *10.10.10.1* **-p** *161* **-a** ******** **-e** ******** **-v** *v3* **-u** *root* **-x** *SHA*

- Clear the trap IP addresses of servers in batches:

  python config.py resetserver -i *10.10.10.116-119* **-p** *161* **-a** ******** **-e** ******** **-v** *v3* **-u** *root* **-x** *SHA* or **python config.py resetserver -i** *10.10.10.** **-p** *161* **-a** ******** **-e** ******** **-v** *v3* **-u** *root* **-x** *SHA*

Manually set the destination address of the last trap to null for the server. (The iBMC uses the fourth address; the HMM uses the fifth address.)

----End

Querying Server IP Addresses

Step 1 Switch to the directory where **config.py** is located.

cd /usr/local/nagios/bin/XFUSION_server

Step 2 Run the following commands to query the server IP addresses:

python config.py inquiry

----End

Querying the Nagios Plug-in Version

Step 1 Switch to the directory where **config.py** is located.

cd /usr/local/nagios/bin/XFUSION_server

Step 2 Run the following commands to query the Nagios plug-in version:

python config.py version

----End

3 Obtaining Information

This chapter describes how to obtain information about rack serversuses theand high-density servers using Nagios.

Prerequisites

- The Nagios plug-in has been installed and servers have been added. For details, see 2.3.1 Installing the Nagios Plug-in and 2.3.2 Adding or Deleting Servers.
- You have logged in to the Nagios server as the **root** user.

Background Information

The Nagios enables you to obtain server information in manual or automatic mode:

- Manual mode: Log in to the Nagios server to manually run scripts to obtain information about the system, PSU, fan, CPU, DIMM, disk, PCIe card, RAID controller card, logical disk, component, sensor, and firmware version.
- Automatic mode: Configure Nagios to automatically invoke scripts to obtain information about the system, PSU, fan, CPU, DIMM, and disk.

Operation Procedure

- Manual mode:

NOTE

You must be a Nagios user when you first run the command to obtain information.

a. Run the following command to go to the **/usr/local/nagios/bin/XFUSION_server** directory:

cd /usr/local/nagios/bin/XFUSION_server

b. Run the following commands to obtain the server information:

python collect.py -a *-r resultPath*

python collect.py –f *directory /host.xml -r resultPath*

Table 3-1 Command description

Command	Description
python collect.py -a	Invoke the **XFUSION_hosts.xml** file to obtain server information. The result file is stored in

Command	Description
	/usr/local/nagios/bin/result by default.
python collect.py -a *-r resultPath*	Invoke the **XFUSION_hosts.xml** file to obtain server information. The result file is stored in a specified directory. Before running this command, ensure that the specified directory exists, the permission on the directory is 750 or higher, and the user and group to which the directory belongs are both **nagios**.
python collect.py –f *directory/host.xml*	Invoke the **host.xml** file to obtain server information. The result file is stored in **/usr/local/nagios/bin/result** by default. **NOTE** **host.xml** is the configuration file created by the user. The format of the file must be the same as that of **XFUSION_hosts.xml**, and the path of the file must be provided.
python collect.py -f *directory/host.xml -r resultPath*	Invoke the **host.xml** file to obtain server information. The result file is stored in a specified directory. **NOTE** **host.xml** is the configuration file created by the user. The format of the file must be the same as that of XFUSION_hosts.xml, and the path of the file must be provided.

- Automatic mode:

  The Nagios automatically invokes the script to obtain server information upon startup. The default polling interval is 10 minutes.

4 Monitoring Server Status andAlarms

This chapter describes how to monitor the status and alarms of rack, high-density, and blade servers in Nagios.

Prerequisites

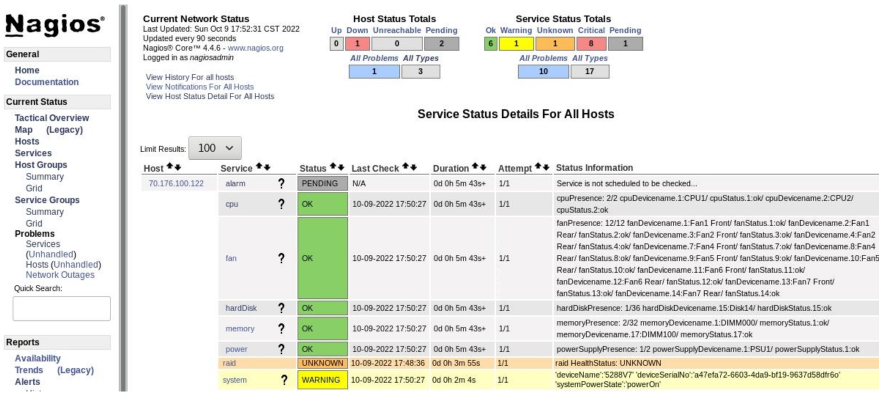
- The Nagios plug-in has been installed and servers have been added. For details, see 2.3.1 Installing the Nagios Plug-in and 2.3.2 Adding or Deleting Servers.
- You have logged in to the Nagios server as the **root** user.

Operation Procedure

Step 1 In the navigation tree on the left, choose **Current Status** > **Services**.

Step 2 In the **Service Status Details For All Hosts** area in the right pane, view the information about all monitored servers and their component status, as shown in Figure 4-1.

Figure 4-1 Viewing server information



Current Network Status
Last Updated: Sun Oct 9 17:52:31 CST 2022
Updated every 90 seconds
Nagios® Core™ 4.4.6 - www.nagios.org
Logged in as *nagiosadmin*

Host Status Totals

Up	Down	Unreachable	Pending
0	1	0	2

All Problems	All Types
1	3

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
6	1	1	8	1

All Problems	All Types
10	17

Service Status Details For All Hosts

Host	Service		Status	Last Check	Duration	Attempt	Status Information
70.176.100.122	alarm	?	PENDING	N/A	0d 0h 5m 43s+	1/1	Service is not scheduled to be checked...
	cpu	?	OK	10-09-2022 17:50:27	0d 0h 5m 43s+	1/1	cpuPresence: 2/2 cpuDevicename.1:CPU1/ cpuStatus.1:ok/ cpuDevicename.2:CPU2/ cpuStatus.2:ok
	fan	?	OK	10-09-2022 17:50:27	0d 0h 5m 43s+	1/1	fanPresence: 12/12 fanDevicename.1:Fan1 Front/ fanStatus.1:ok/ fanDevicename.2:Fan1 Rear/ fanStatus.2:ok/ fanDevicename.3:Fan2 Front/ fanStatus.3:ok/ fanDevicename.4:Fan2 Rear/ fanStatus.4:ok/ fanDevicename.7:Fan4 Front/ fanStatus.7:ok/ fanDevicename.8:Fan4 Rear/ fanStatus.8:ok/ fanDevicename.9:Fan5 Front/ fanStatus.9:ok/ fanDevicename.10:Fan5 Rear/ fanStatus.10:ok/ fanDevicename.11:Fan6 Front/ fanStatus.11:ok/ fanDevicename.12:Fan6 Rear/ fanStatus.12:ok/ fanDevicename.13:Fan7 Front/ fanStatus.13:ok/ fanDevicename.14:Fan7 Rear/ fanStatus.14:ok
	hardDisk	?	OK	10-09-2022 17:50:27	0d 0h 5m 43s+	1/1	hardDiskPresence: 1/36 hardDiskDevicename.15:Disk14/ hardDiskStatus.15:ok
	memory	?	OK	10-09-2022 17:50:27	0d 0h 5m 43s+	1/1	memoryPresence: 2/32 memoryDevicename.1:DIMM000/ memoryStatus.1:ok/ memoryDevicename.17:DIMM100/ memoryStatus.17:ok
	power	?	OK	10-09-2022 17:50:27	0d 0h 5m 43s+	1/1	powerSupplyPresence: 1/2 powerSupplyDevicename.1:PSU1/ powerSupplyStatus.1:ok
	raid		UNKNOWN	10-09-2022 17:48:36	0d 0h 3m 55s	1/1	raid HealthStatus: UNKNOWN
	system	?	WARNING	10-09-2022 17:50:27	0d 0h 2m 4s	1/1	'deviceName':'5288V7' 'deviceSerialNo':'a47efa72-6603-4da9-bf19-9637d58dfr6o' 'systemPowerState':'powerOn'

- **Host**: Host name of the monitored server. You can click a host name to view details about the server.
- **XFUSION-server-plugin**: Name of the Nagios plug-in service monitored by Nagios.
- **Service**: Component or alarm of the monitored device. You can click a component to view its status.

- **Status**: Status of the monitored component.

----End

5 FAQs

5.1 How Do I Uninstall the Nagios Plug-in?

This section describes how to uninstall the Nagios plug-in.

Prerequisites

- The Nagios plug-in has been installed.
- You have logged in to the Nagios server as the **root** user.

Operation Procedure

Step 1 Run the following command to access the directory where the Nagios plug-in is installed:

cd /etc

cd XFUSION Nagios Plugin v*X.X.X*

Step 2 Run the following command to uninstall the Nagios plug-in:

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

/usr/local/nagios indicates the Nagios tool installation path. Use the actual path.

Run the following command to save the user data and uninstall the Nagios plug-in:

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

/usr/local/nagios indicates the Nagios tool installation path. Use the actual path.

Step 3 The system starts to uninstall the Nagios plug-in. After the uninstallation is complete, the following information is displayed:

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

Step 4 Check whether the **nagios.cfg** file is correct.

1. Run the following command to switch to the **nagios** user:

   su - nagios

2. Run the following command to check the **nagios.cfg** file:

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

   NOTE

   In the preceding command, **/usr/local/nagios** indicates the installation path. Change it based on the site requirements.

   If the following information is displayed, it indicates that the **nagios.cfg** file is correct:

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

3. Run the following command to switch to the **root** user:

   exit

Step 5 Run the following command to restart the Nagios service:

systemctl restart nagios

----End

5.2 How Do I Restart the Nagios Plug-in Service?

This section describes how to restart the Nagios plug-in service on the Nagios server.

Prerequisites

- The Nagios plug-in has been installed.
- You have logged in to the Nagios server as the **root** user.

Operation Procedure

Step 1 Run the following command to check whether the Nagios plug-in alarm service has been started:

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

If the following information is displayed, it indicates that the Nagios plug-in alarm service has been started: Otherwise, wait for 2 minutes until the Nagios plug-in service automatically starts.

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

NOTE

In the preceding command output, 22,237 indicates the process ID of the Nagios plug-in.

Step 2 Run the following command to check whether the device information service has been started:

ps -ef |grep collect.py

If the following information is displayed, the device information service has been started. Otherwise, wait for 2 minutes until the device information service automatically starts.

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

NOTE

In the preceding command output, **23858** indicates the process ID of the Nagios plug-in.

Step 3 Run the following commands to stop the Nagios plug-in service:

kill -9 22237

kill -9 23858

Step 4 Waiting 1 minute, run the command in Step 1 to check whether the Nagios plug-in service is started.

The Nagios plug-in service is automatically started after being stopped.

Step 5 Run the following command to restart the Nagios service:

# systemctl restart nagios

NOTE

If the Nagios service fails to obtain the server type or trap IP address during startup, Nagios sets the server status to **Unknown**, indicating that the server is not monitored by Nagios.

Step 6 Check whether the Nagios plug-in service and device information service are started.

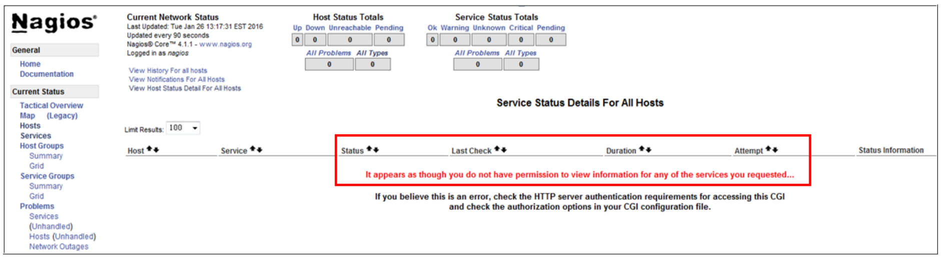
----End

5.3 What Should I Do If Host Service Status Cannot Be Displayed on the Nagios Home Page?

Symptom

The detailed information about the host service status is not displayed on the Nagios home page, as shown in Figure 5-1.

Figure 5-1 No host service status information on the Nagios home page



Current Network Status
Last Updated: Tue Jan 26 13:17:31 EST 2016
Updated every 90 seconds
Nagios® Core™ 4.1.1 - www.nagios.org
Logged in as *nagios*

Service Status Details For All Hosts

It appears as though you do not have permission to view information for any of the services you requested...

If you believe this is an error, check the HTTP server authentication requirements for accessing this CGI and check the authorization options in your CGI configuration file.

Possible Causes

The value of **use_authentication** in the **/usr/local/nagios/etc/cgi.cfg** file isset to **1**.

Operation Procedure

Step 1 Change the value of **use_authentication**.

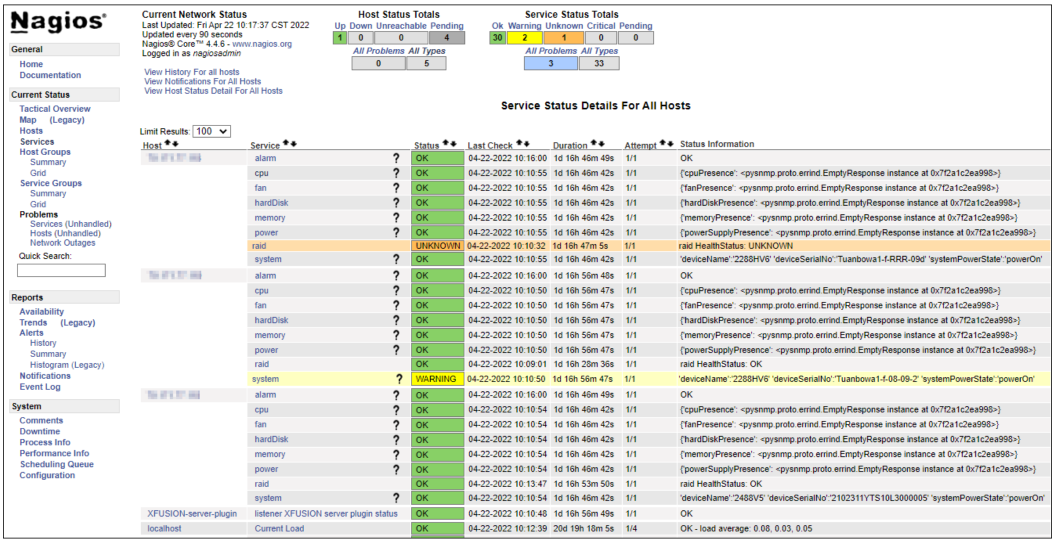
1. Open the **/usr/local/nagios/etc/cgi.cfg** file.
2. Locate the **use_authentication** file.
3. Change the value of **use_authentication** to **0**.

Step 2 Run the following command to restart the Nagios service:

systemctl restart nagios

The detailed information about the host service status is displayed on the Nagios home page, as shown in Figure 5-2.

Figure 5-2 Detailed information about the host service status



Current Network Status
Last Updated: Fri Apr 22 10:17:37 CST 2022
Updated every 90 seconds
Nagios® Core™ 4.4.6 - www.nagios.org
Logged in as *nagiosadmin*

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	4

All Problems	*All Types*
0	5

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
30	2	1	0	0

All Problems	*All Types*
3	33

Service Status Details For All Hosts

Limit Results: 100

Host	Service		Status	Last Check	Duration	Attempt	Status Information
[redacted]	alarm	?	OK	04-22-2022 10:16:00	1d 16h 46m 49s	1/1	OK
	cpu	?	OK	04-22-2022 10:10:55	1d 16h 46m 42s	1/1	{'cpuPresence': <pysnmp.proto.errind.EmptyResponse instance at 0x7f2a1c2ea998>}
	fan	?	OK	04-22-2022 10:10:55	1d 16h 46m 42s	1/1	{'fanPresence': <pysnmp.proto.errind.EmptyResponse instance at 0x7f2a1c2ea998>}
	hardDisk	?	OK	04-22-2022 10:10:55	1d 16h 46m 42s	1/1	{'hardDiskPresence': <pysnmp.proto.errind.EmptyResponse instance at 0x7f2a1c2ea998>}
	memory	?	OK	04-22-2022 10:10:55	1d 16h 46m 42s	1/1	{'memoryPresence': <pysnmp.proto.errind.EmptyResponse instance at 0x7f2a1c2ea998>}
	power	?	OK	04-22-2022 10:10:55	1d 16h 46m 42s	1/1	{'powerSupplyPresence': <pysnmp.proto.errind.EmptyResponse instance at 0x7f2a1c2ea998>}
	raid		UNKNOWN	04-22-2022 10:10:32	1d 16h 47m 5s	1/1	raid HealthStatus: UNKNOWN
	system	?	OK	04-22-2022 10:10:55	1d 16h 46m 42s	1/1	'deviceName':'2288HV6' 'deviceSerialNo':'Tuanbowa1-f-RRR-09d' 'systemPowerState':'powerOn'
[redacted]	alarm	?	OK	04-22-2022 10:16:00	1d 16h 56m 48s	1/1	OK
	cpu	?	OK	04-22-2022 10:10:50	1d 16h 56m 47s	1/1	{'cpuPresence': <pysnmp.proto.errind.EmptyResponse instance at 0x7f2a1c2ea998>}
	fan	?	OK	04-22-2022 10:10:50	1d 16h 56m 47s	1/1	{'fanPresence': <pysnmp.proto.errind.EmptyResponse instance at 0x7f2a1c2ea998>}
	hardDisk	?	OK	04-22-2022 10:10:50	1d 16h 56m 47s	1/1	{'hardDiskPresence': <pysnmp.proto.errind.EmptyResponse instance at 0x7f2a1c2ea998>}
	memory	?	OK	04-22-2022 10:10:50	1d 16h 56m 47s	1/1	{'memoryPresence': <pysnmp.proto.errind.EmptyResponse instance at 0x7f2a1c2ea998>}
	power	?	OK	04-22-2022 10:10:50	1d 16h 56m 47s	1/1	{'powerSupplyPresence': <pysnmp.proto.errind.EmptyResponse instance at 0x7f2a1c2ea998>}
	raid		OK	04-22-2022 10:09:01	1d 16h 28m 36s	1/1	raid HealthStatus: OK
	system	?	WARNING	04-22-2022 10:10:50	1d 16h 56m 47s	1/1	'deviceName':'2288HV6' 'deviceSerialNo':'Tuanbowa1-f-08-09-2' 'systemPowerState':'powerOn'
[redacted]	alarm	?	OK	04-22-2022 10:16:00	1d 16h 46m 49s	1/1	OK
	cpu	?	OK	04-22-2022 10:10:54	1d 16h 46m 42s	1/1	{'cpuPresence': <pysnmp.proto.errind.EmptyResponse instance at 0x7f2a1c2ea998>}
	fan	?	OK	04-22-2022 10:10:54	1d 16h 46m 42s	1/1	{'fanPresence': <pysnmp.proto.errind.EmptyResponse instance at 0x7f2a1c2ea998>}
	hardDisk	?	OK	04-22-2022 10:10:54	1d 16h 46m 42s	1/1	{'hardDiskPresence': <pysnmp.proto.errind.EmptyResponse instance at 0x7f2a1c2ea998>}
	memory	?	OK	04-22-2022 10:10:54	1d 16h 46m 42s	1/1	{'memoryPresence': <pysnmp.proto.errind.EmptyResponse instance at 0x7f2a1c2ea998>}
	power	?	OK	04-22-2022 10:10:54	1d 16h 46m 42s	1/1	{'powerSupplyPresence': <pysnmp.proto.errind.EmptyResponse instance at 0x7f2a1c2ea998>}
	raid		OK	04-22-2022 10:13:47	1d 16h 53m 50s	1/1	raid HealthStatus: OK
	system	?	OK	04-22-2022 10:10:54	1d 16h 46m 42s	1/1	'deviceName':'2488V5' 'deviceSerialNo':'2102311YTS10L3000005' 'systemPowerState':'powerOn'
XFUSION-server-plugin	listener XFUSION server plugin status		OK	04-22-2022 10:10:48	1d 16h 56m 49s	1/1	OK
localhost	Current Load		OK	04-22-2022 10:12:39	20d 19h 18m 5s	1/4	OK - load average: 0.08, 0.03, 0.05

----End

5.4 What Should I Do If SNMPv3 Alarms Cannot Be Reported?

Symptom

After an active/standby switchover between servers that use SNMP V3, alarms cannot be reported.

NOTE

Blade servers do not support SNMP V3 alarm reporting.

Possible Causes

- After an active/standby switchover, server power-on/off, or server restart, the server engine ID changes.
- The event code and trap version reported by the server are inconsistent with the configuration.

NOTE

The alarm on the server side must be in event code mode.

- The trap IP address is not registered on the server or the port is not **10061**.

Operation Procedure

Step 1 Check whether the IP address of the server is the same as the IP address in the configuration file of the Nagios plug-in.

- Yes: Go to Step 4.
- No: Change the IP address in the configuration file of the Nagios plug-in to the IP address of the server.

Step 2 Check whether the server is powered on.

- Yes: Go to Step 4.
- If no, power on the server.

Step 3 Check whether the alarm reporting function of the server is normal.

- Yes: Go to Step 4.
- No: Set the trap IP address reporting mode to event code, manually register the trap IP address, change the port number to **10061**, and set the separator to comma (,).

Step 4 Run the following command to query the alarm process ID:

ps -ef | grep trapd.py

Step 5 Run the following command to stop the alarm process:

Kill -9 *Alarm process ID*

----End

A Obtaining Technical Support

To obtain assistance, contact technical support as follows:

- Contact customer service center at support@xfusion.com.
- Contact technical support personnel.

B Communication Matrix

Source Device	Source IP Address	Source Port Number	Destination Device	Destination IP Address	Destination Port Number	Protocol	Port Description	Destination Port Configurable	Authentication Mode	Encryption Mode
Device to which Nagios belongs	IP address of the Nagios virtual network port veth	Random	Device to which Nagios belongs	Virtual network port IP address	80	TCP	HTTP(web) port, the protocol can be modified.	Yes	User name/password	HTTP: NA
Device of the plug-ins	Device IP address of the plug-ins	Random	iBMC	IP address of the iBMC virtual network port veth	161	UDP	IBMC SNMP server port is used for SNMP data interaction.	Not involved.	v1 v2c: Team name v3: Username/Password Note: using v1 and v2c will reduce security of the system. Exercise caution when performing this operation.	The encryption protocol set by iBMC SNMP shall prevail.
Device to which Nagi	IP address of the device to	Random	SNMP Trap server	SNMP Trap server IP addre	162	UDP	SNMP Trap port of the plug-ins	Not involved.	v1 v2c: Team name v3: Username/Password	None

Source Device	Source IP Address	Source Port Number	Destination Device	Destination IP Address	Destination Port Number	Protocol	Port Description	Destination Port Configurable	Authentication Mode	Encryption Mode
os belongs	which Nagios belongs			ss			on the server is used for SNMP data interaction.		Note: using v1 and v2c will reduce security of the system. Exercise caution when performing this operation.	