How To Monitor Hosts Using SSH In Nagios XI 5

Purpose

This document describes how to monitor hosts with Nagios XI by using SSH to execute monitoring plugins and scripts on remote machines.

If you are monitoring hosts with SSH in Nagios XI 2024, see Monitoring Hosts with SSH 2024.

SSH Overview

SSH is a secure communication protocol that can be used to login to remote servers and/or execute commands on remote servers.

Nagios XI can monitor metrics and services on remote machines by using an SSH proxy plugin called `check_by_ssh`. The `check_by_ssh` plugin allows Nagios to execute monitoring plugins and scripts on the remote machine in a secure manner, without having to supply authentication credentials.

Prerequisites

You'll need to configure SSH keys for the nagios user on your Nagios XI server before you can continue. To do this, establish a terminal session to your Nagios XI server as root and issue the following commands:

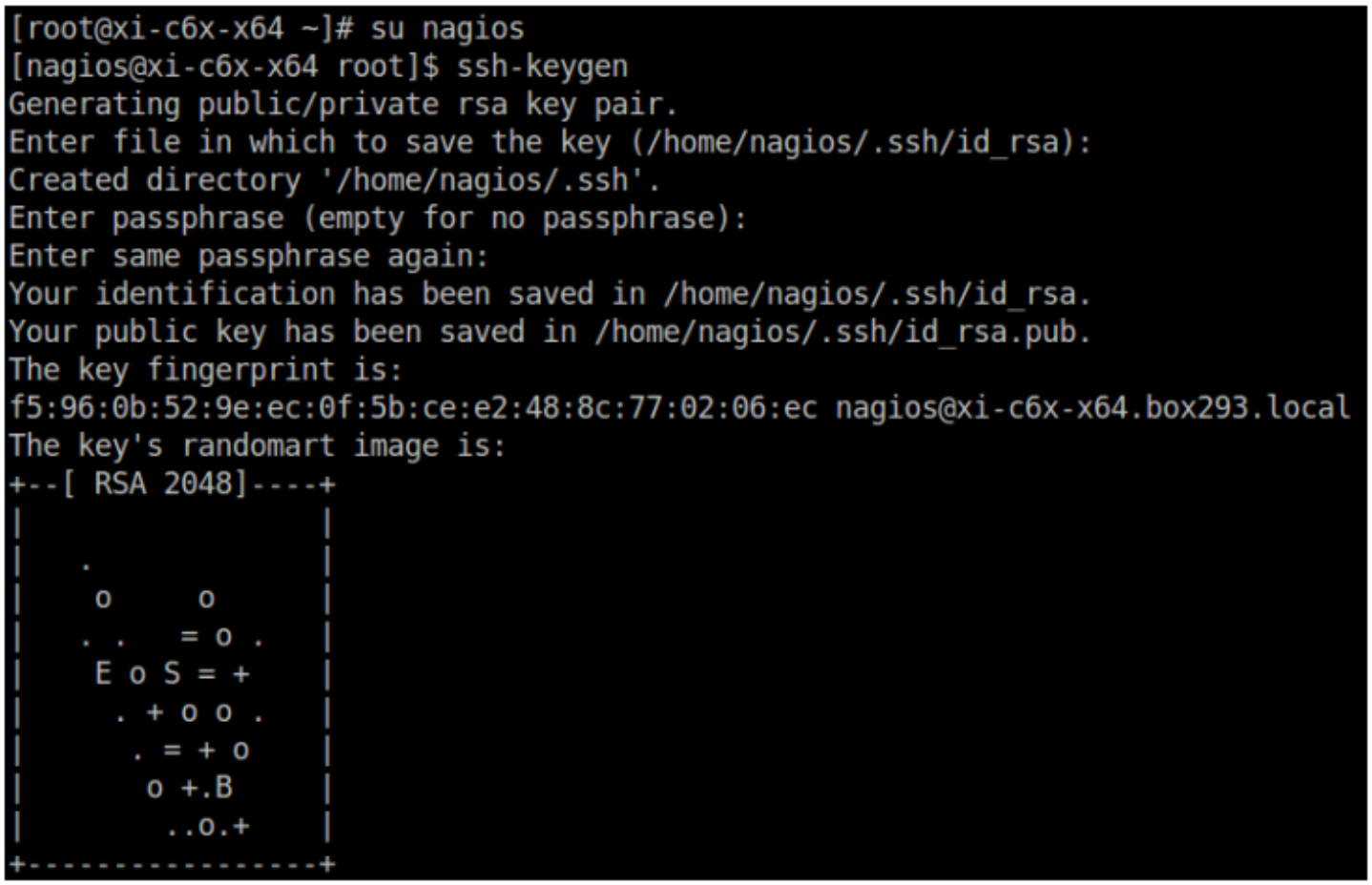
```
su nagios
ssh-keygen
```

Press **ENTER** (accepting defaults) when prompted for a filename and passphrase. Public and private SSH keys will be generated and saved in the following directory:

```
/home/nagios/.ssh
```


Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

Here is the example output from those commands:



You will need the contents of the public key file (which has a .pub extension) later. In the screenshot above it is the `id_rsa.pub` file. You will continue with the terminal session in the next step.

Before you can use the `check_by_ssh` plugin, you must install/configure the following on the remote Linux/Unix server you want to monitor:

- Create a nagios user
- Install Nagios plugins and/or monitoring scripts
- Install and configure the SSH daemon

It is assumed you have already completed those steps before proceeding.

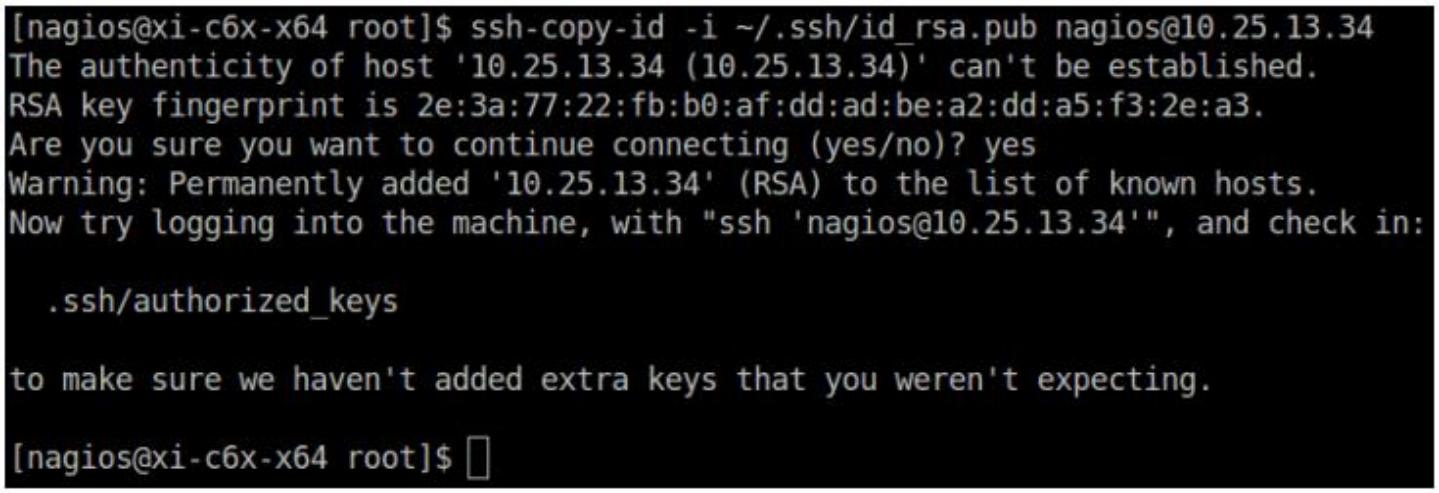
Nagios®

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

For `check_by_ssh` to work you must now copy the public key file of the nagios user on the Nagios XI server to the `authorized_keys` file for the nagios user on the remote Linux/Unix server. Continuing with the terminal session from the previous step execute the following command:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub nagios@remoteip
```

You will be prompted to add the host to the list of new hosts, you need to type yes to proceed and then you will need to type the password for the nagios user.



Note: In the step above, `remoteip` is the IP address of the Linux/Unix server you are connecting to. It is very important that:

- If you specify an IP address here, you need to use that IP address in the wizard (not a DNS record)
    - If you tried to use a DNS record in the wizard, the `check_by_ssh` plugin will not work
- If you specify a DNS record here, you need to use that DNS record in the wizard (not an IP address)
    - If you tried to use a IP address in the wizard, the `check_by_ssh` plugin will not work

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

The permissions on the `authorized_keys` files on the Linux/Unix server must be such that the file cannot be read or written to/by anyone other than the nagios user, as shown below

```
[nagios@localhost .ssh]$ ls -al
total 24
drwx------ 2 nagios users 4096 Jul 16 09:44 .
drwx------ 3 nagios users 4096 Jul 16 09:43 ..
-rw------- 1 nagios users 410 Jul 16 09:44 authorized_keys
-rw------- 1 nagios users 1675 Jul 16 09:43 id_rsa
-rw-r--r-- 1 nagios users 410 Jul 16 09:43 id_rsa.pub
```

The `ssh-copy-id` command would have correctly set these permissions. If you copied the `id_rsa.pub` into the `authorized_keys` file using another method, then you need to make sure the file permissions are correct.

Solaris Steps

If your destination host is a Solaris machine then some different steps are required. First, on the Solaris server execute the following commands as the nagios user:

```
mkdir -p /export/home/nagios/.ssh
chmod 0700 /export/home/nagios/.ssh/
```

On the Nagios XI server, instead of the `ssh-copy-id` command you will need to use the following command:

```
cat ~/.ssh/id_rsa.pub | ssh nagios@10.25.13.45 'umask 077; cat >>/-
export/home/nagios/.ssh/authorized_keys'
```

Test Passwordless Login

Now to verify that you can login to the remote server without supplying a password. Continuing with the terminal session on the Nagios XI server execute the following command:

```
ssh nagios@remoteip
```

If the SSH keys are configured properly you should be able to login to the remote machine without supplying credentials. Simply type exit to close the ssh session.

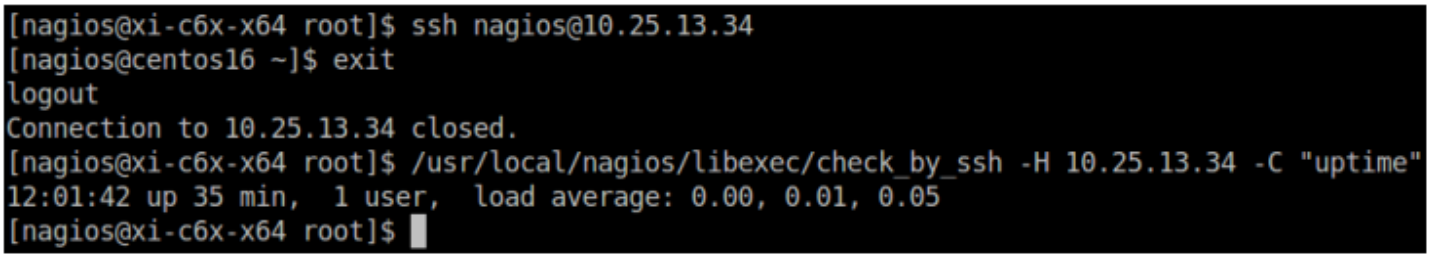
Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

Also test the `check_by_ssh` plugin, run the following command:

```
/usr/local/nagios/libexec/check_by_ssh -H remoteip -C uptime
```

If things are setup properly, you should get output from the "uptime" command on the remote server that looks similar to the following:

```
12:01:42 up 35 min, 1 user, load average: 0.00, 0.01, 0.05
```

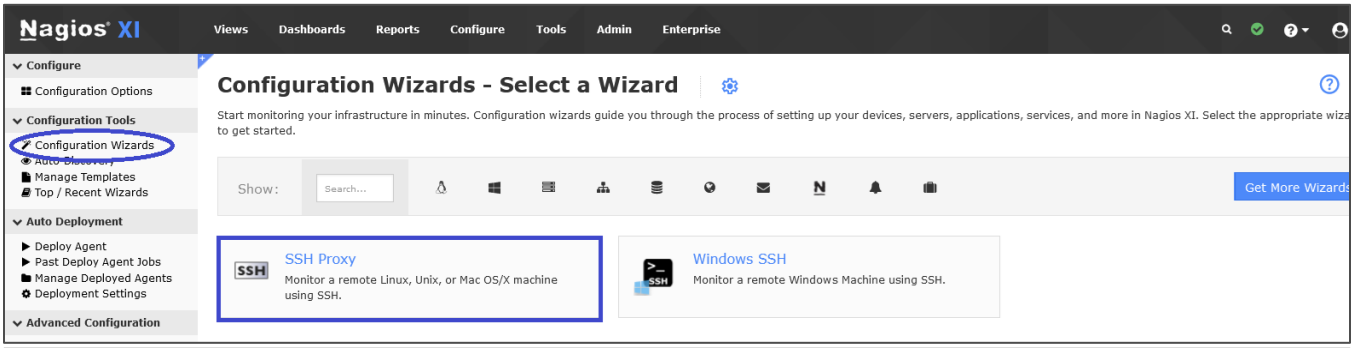


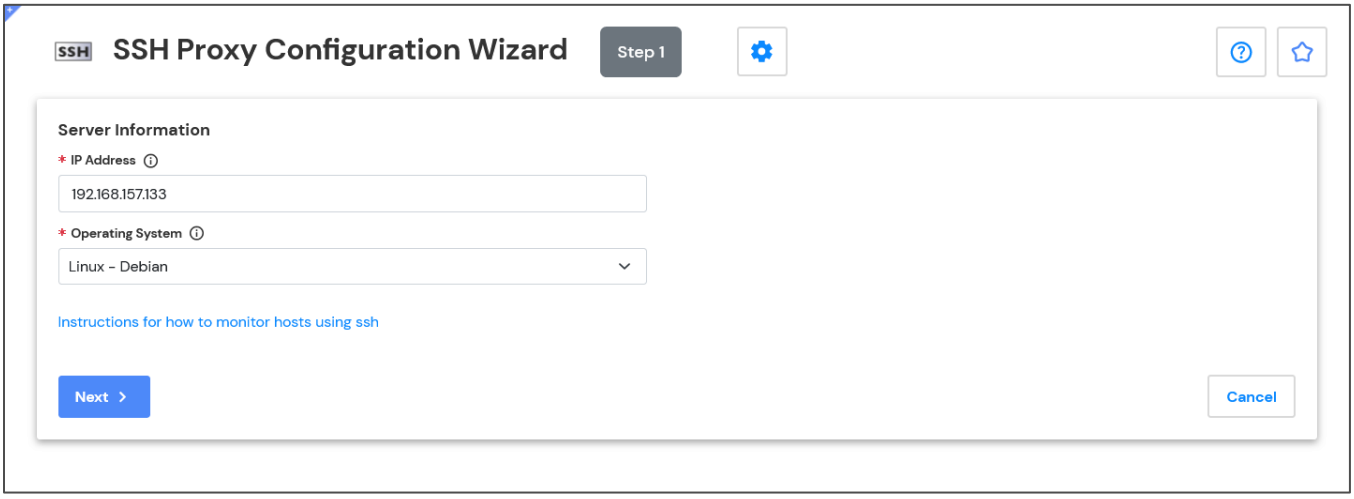
The screenshot above shows both examples that demonstrate passwordless authentication is working.

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

Using The SSH Wizard

1. To begin using the SSH Proxy wizard navigate via the top menu bar to **Configure > Run a configuring wizard** and select the **SSH Proxy wizard**. In the following screenshot you can see how the search field allows you to quickly find a wizard.

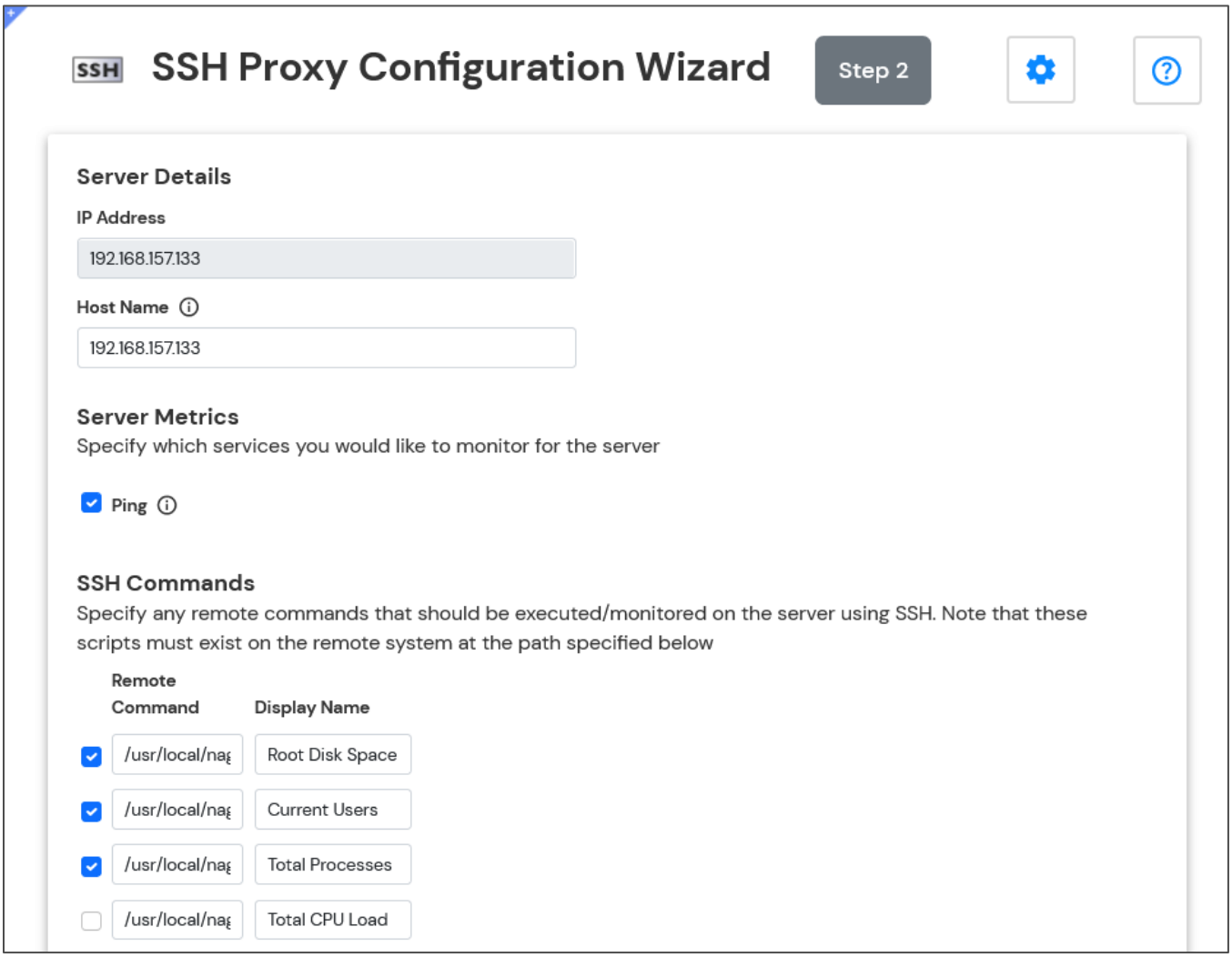




2. On **Step 1** you will be asked to supply the address of the server you will monitor via SSH.
3. You will also have to select the **Operating System** which in this example is CentOS.
4. Click **Next** to progress to **step 2**.
5. On **step 2** you will configure all of the options for monitoring.
6. To start off with make sure a valid **Host Name** has been entered.
7. The **SSH Commands** section allows you to specify which commands should be executed and monitored and what display name (service description) should be associated with each

Nagios®
Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

command. In the screenshot on the following page you can see there are three commands defined with their respective arguments.

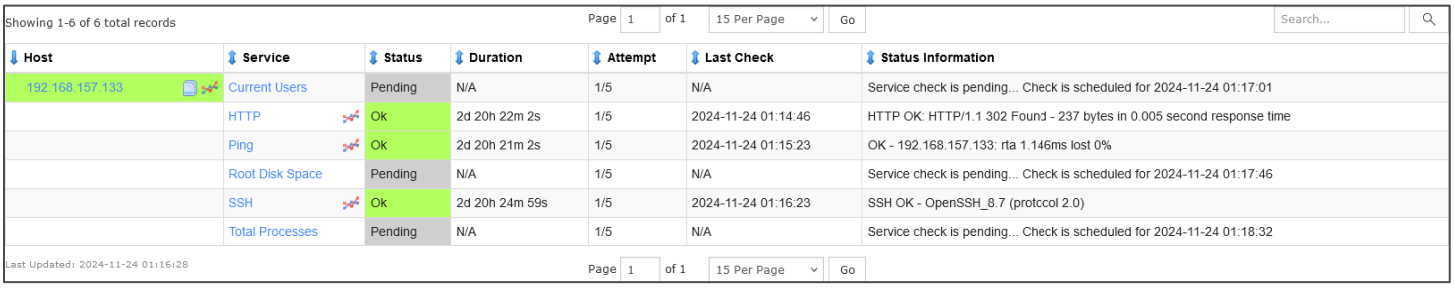


8. You have the option to **Add Row** which allows you to define more commands.
9. Once you've finished populating the commands click **Next** and then complete the wizard by choosing the required options in Step 3 – Step 5.
10. To finish up, click on **Finish** in the final step of the wizard.

This will create the new hosts and services and begin monitoring.

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.

Once the wizard applies the configuration, click the **View status details** for link to see the new host and services that were created.



Showing 1-6 of 6 total records — Page 1 of 1 — 15 Per Page — Go — Search...

Host	Service	Status	Duration	Attempt	Last Check	Status Information
192.168.157.133	Current Users	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-11-24 01:17:01
	HTTP	Ok	2d 20h 22m 2s	1/5	2024-11-24 01:14:46	HTTP OK: HTTP/1.1 302 Found - 237 bytes in 0.005 second response time
	Ping	Ok	2d 20h 21m 2s	1/5	2024-11-24 01:15:23	OK - 192.168.157.133: rta 1.146ms lost 0%
	Root Disk Space	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-11-24 01:17:46
	SSH	Ok	2d 20h 24m 59s	1/5	2024-11-24 01:16:23	SSH OK - OpenSSH_8.7 (protocol 2.0)
	Total Processes	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2024-11-24 01:18:32

Last Updated: 2024-11-24 01:16:28 — Page 1 of 1 — 15 Per Page — Go

This completes the steps required to monitor a host via SSH.

Troubleshooting

Here is an example where the SSH keys were not correctly configured and resulted in the services not working:

Host	Service	Status	Duration	Attempt	Last Check	Status Information
10.25.13.34	Current Users	Unknown	1m 35s	2/5	2016-12-05 13:37:41	Remote command execution failed: Host key verification failed.
	Ping	Ok	1m 35s	1/5	2016-12-05 13:36:43	OK - 10.25.13.34: rta 1.409ms, lost 0%
	Root Disk Space	Unknown	1m 35s	2/5	2016-12-05 13:37:32	Remote command execution failed: Host key verification failed.
	Total Processes	Unknown	1m 35s	2/5	2016-12-05 13:37:36	Remote command execution failed: Host key verification failed.

To resolve this, you need to check the address used in the host object and make sure this was used in the `ssh-copy-id` command. Please refer to the notes earlier in this documentation about the difference between an IP address and a DNS record.

More Information

Using Configuration Wizards

Finishing Up

This completes the documentation on monitoring hosts using SSH in Nagios XI. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum Visit Nagios Knowledge Base Visit Nagios Library

Nagios®

Copyright © 2025 Nagios Enterprises, LLC. All rights reserved.
Trademarks are the property of their respective owner.