Nagios XI – Monitoring Hosts Using SSH

Nagios®

The Industry Standard in IT Infrastructure Monitoring

Purpose

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

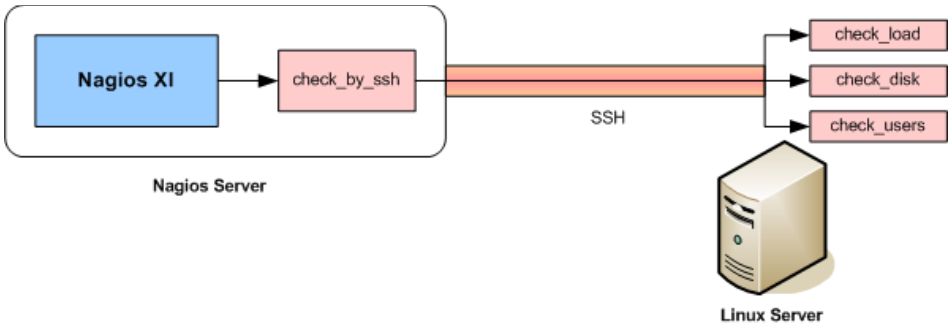
Target Audience

This document is intended for use by Nagios XI Administrators.

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 © 2010 - 2017 Nagios Enterprises, LLC

Updated – February, 2017

Here is the example output from the commands on the previous page:

```
[root@xi-c6x-x64 ~]# su nagios
[nagios@xi-c6x-x64 root]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/nagios/.ssh/id_rsa):
Created directory '/home/nagios/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/nagios/.ssh/id_rsa.
Your public key has been saved in /home/nagios/.ssh/id_rsa.pub.
The key fingerprint is:
f5:96:0b:52:9e:ec:0f:5b:ce:e2:48:8c:77:02:06:ec nagios@xi-c6x-x64.box293.local
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|   .             |
|    o     o      |
|   . .   = o .   |
|    E o S = +    |
|     . + o o .   |
|      . = + o    |
|       o +.B     |
|        ..o.+    |
+-----------------+
```

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.

Copyright © 2010 - 2017 Nagios Enterprises, LLC
Updated – February, 2017

For the called `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 ~/.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.

```
[nagios@xi-c6x-x64 root]$ ssh-copy-id -i ~/.ssh/id_rsa.pub nagios@10.25.13.34
The authenticity of host '10.25.13.34 (10.25.13.34)' can't be established.
RSA key fingerprint is 2e:3a:77:22:fb:b0:af:dd:ad:be:a2:dd:a5:f3:2e:a3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.25.13.34' (RSA) to the list of known hosts.
Now try logging into the machine, with "ssh 'nagios@10.25.13.34'", and check in:

  .ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.

[nagios@xi-c6x-x64 root]$
```

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 address). If you tried to use a DNS address in the wizard, the `check_by_ssh` plugin will not work. If you use a DNS address in the Nagos wizard, instead of `nagios@remoteip` type `nagios@remotedns` in the command above (where `remotedns` is the DNS address of the Linux/Unix server you are connecting to).

Important: 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
[nagios@localhost .ssh]$
```

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.

Copyright © 2010 - 2017 Nagios Enterprises, LLC
Updated – February, 2017

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.

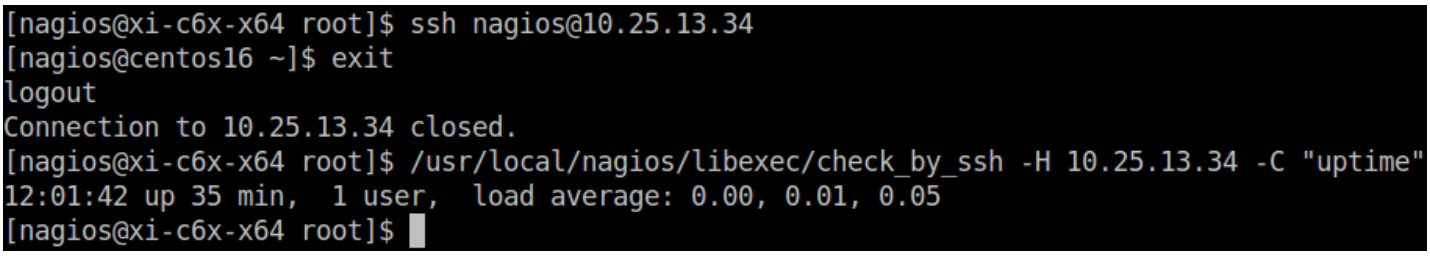
Also test the `check_by_ssh` plugin, run the following command:

```
/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
```

Important: If you are asked for a password, it means something isn't setup properly! To remedy this, search the Internet for tutorials on setting up passwordless authentication using SSH keys.

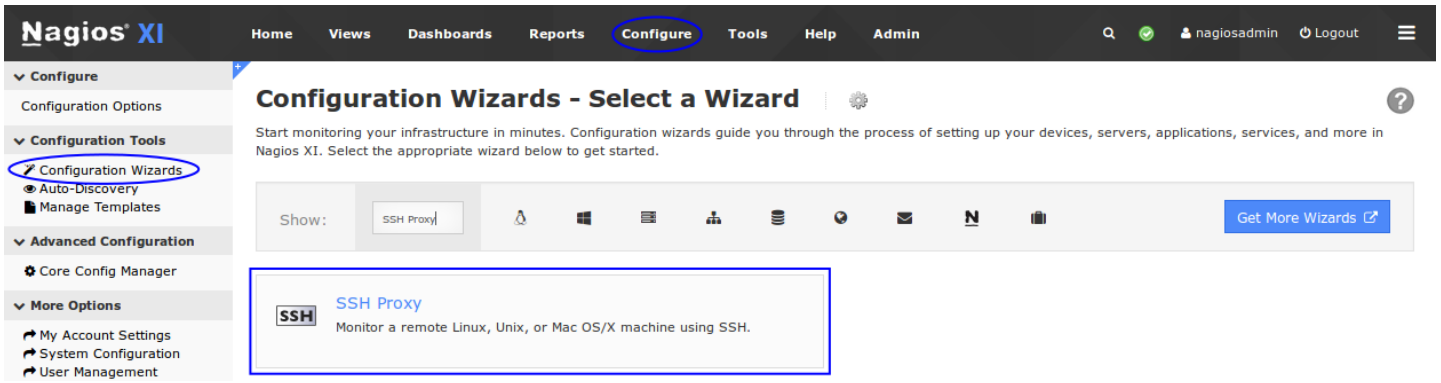


The screenshot above shows both examples which demonstrates that passwordless authentication is working.

Copyright © 2010 - 2017 Nagios Enterprises, LLC
Updated – February, 2017

Using The SSH Wizard

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.



On Step 1 you will be asked to supply the **address** of the server you will monitor via SSH.

You will also have to select the **Operating System** which in this example is CentOS.

Click Next to progress to step 2.

On step 2 you will configure all of the options for monitoring.

To start off with make sure a valid **Host Name** has been entered.

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 command.

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

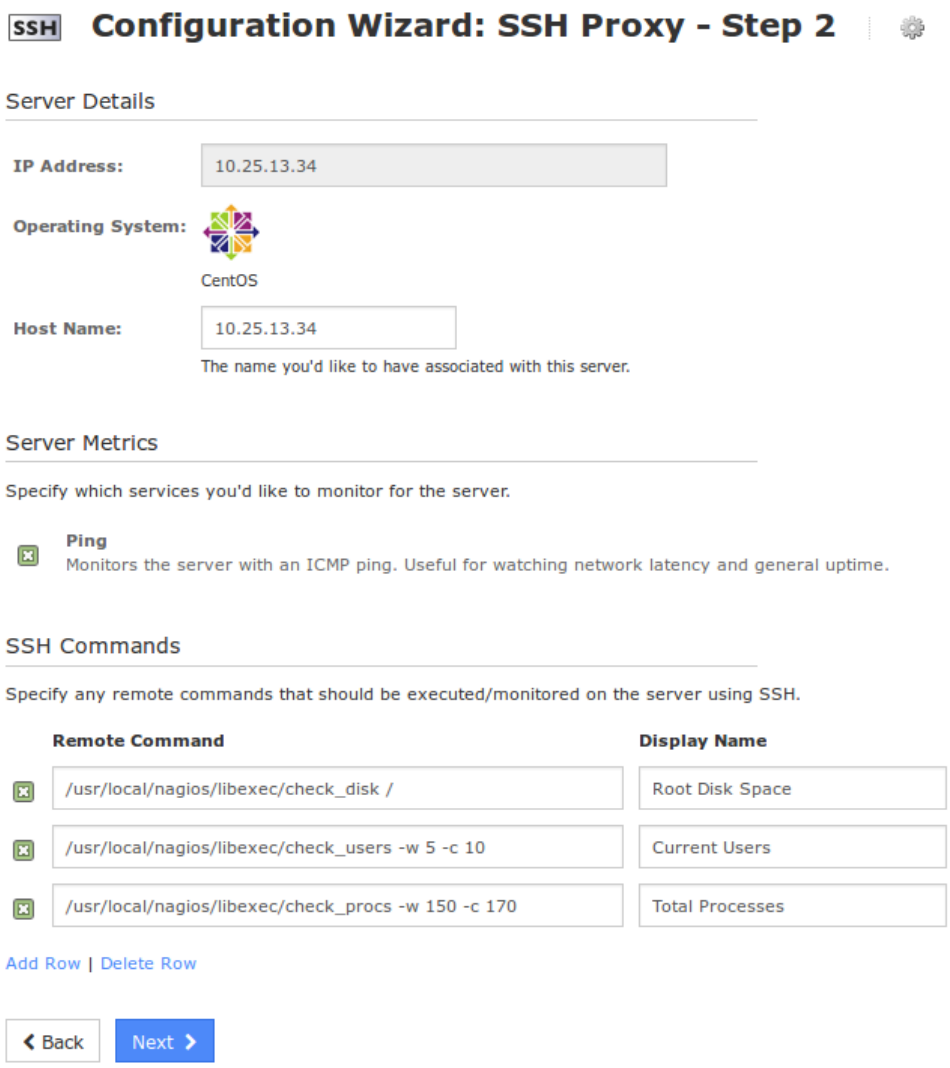
Copyright © 2010 - 2017 Nagios Enterprises, LLC
Updated – February, 2017

You have the option to **Add Row** which allows you to define more commands.

Once you've finished populating the commands click Next and then complete the wizard by choosing the required options in Step 3 – Step 5.

To finish up, click on **Finish** in the final step of the wizard.

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



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

Host	Service	Status	Duration	Attempt	Last Check	Status Information
10.25.13.34	Current Users	Ok	34s	1/5	2016-12-05 13:39:04	USERS OK - 1 users currently logged in
	Ping	Ok	2m 29s	1/5	2016-12-05 13:39:04	OK - 10.25.13.34: rta 1.883ms, lost 0%
	Root Disk Space	Ok	50s	1/5	2016-12-05 13:39:04	DISK OK - free space: / 11906 MB (90% inode=95%):
	Total Processes	Ok	42s	1/5	2016-12-05 13:39:04	PROCS OK: 79 processes

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

Copyright © 2010 - 2017 Nagios Enterprises, LLC
Updated – February, 2017

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 address being used.

Finishing Up

That's it! If you followed all the steps in these instructions, you should have basic monitoring of your servers using SSH.

If you have additional questions or other support related questions, please visit us at our Nagios Support Forums:

https://support.nagios.com/forum

Copyright © 2010 - 2017 Nagios Enterprises, LLC
Updated – February, 2017