Nagios XI - Plain Text Password Considerations

Article Number: 817 | Rating: 1/5 from 1 votes | Last Updated: Mon, Jun 18, 2018 at 8:03 PM

Overview

> *When configuring my monitoring agent I need to define the password in a plain text file. This seems very insecure, how do I encrypt it?*
>
> ***— Concerned Customer***

This is a valid question, this KB article discusses the limitations around plain text passwords and the steps you can take to keep them as secure as possible.

While this KB article is aimed at Nagios XI, it also applies to Nagios Core in regards to Nagios `.cfg` files.

What Is A Password?

What exactly is a password? Generally this is a form of authentication required to communicate with a remote system, for example:

- `check_nt` uses a password string to communicate with remote systems
- SNMP agents require a community string (v1/v2) or passphrases (v3)
- NCPA requires a token to connect to it
- `check_wmi_plus.pl` requires credentials to connect to remote windows systems

Some of the methods above send the password to the remote system as plain text over the wire. This is unavoidable with some older agents however newer methods encrypt that traffic using SSL/TLS (like NCPA).

Where Is The Password Stored?

Generally speaking, the password needs to be defined on the Nagios XI server in it's configuration files AND on the remote system. Additionally that file needs to be kept secure from prying eyes.

On the remote system you should define correct file permissions to only allow the required user/system accounts access to that configuration file. This is your first line of defence to protecting the password.

In regards to "encrypting the password", this is not as simple as it seems. The problem with encrypting a password is that it needs to be unencrypted in order to be used, and in order to unencrypt it you need the key. The key needs to be stored in plaintext otherwise it can't be used to decrypt the password. Then if you try to encrypt the key, you run into the same problem all over again.

Minimizing Exposure

As explained earlier, you should protect the configuration file on the remote system using file permissions, but what about the Nagios XI server?

All of the Nagios XI monitoring configurations are stored in the Core Config Manager (CCM) database and then they are saved into plain text files (`/usr/local/nagios/etc/`) that the Nagios Core monitoring engine reads when it starts.

Any administrator that has access to the Nagios XI server can see the password by:

- Opening CCM and looking at a service definition, the password will be stored in a `$ARGx$` field
- Using a terminal session to look at the plain text configuration file
- Performing an SQL query against the CCM database

The best solution for storing sensitive information is to define custom user macros for each password, for example `$USER87$`. These macros can then be used in the service definitions, when an administrator looks at the service definition all they will see is the macro `$USER87$` and not the password itself.

The user macros are saved in the `/usr/local/nagios/etc/`**`resource.cfg`** file, it is just a plain text and hence this file should have appropriate permissions applied.

Detailed information on user macros in Nagios XI can be found in the following documentation:

Nagios XI - Understanding The User Macros Component

Final Thoughts

For any support related questions please visit the Nagios Support Forums at:

http://support.nagios.com/forum/