Nagios®
Authentication And Authorization In The CGIs

Up To: Contents
See Also: CGI Configuration File Options, Information on the CGIs

Introduction

This documentation describes how the Nagios CGIs decide who has access to view monitoring and configuration information, and who can submit commands to the Nagios daemon through the web interface.

Definitions

Before continuing, it is important that you understand the meaning of and difference between authenticated users and authenticated contacts:

- An **authenticated user** is an someone who has authenticated to the web server with a username and password and has been granted access to the Nagios web interface.
- An **authenticated contact** is an authenticated user whose username matches the short name of a contact definition.

Setting Up Authenticated Users

Assuming you configured your web server as described in the quickstart guide, it should require that you authenticate before accessing the Nagios CGIs. You should also have one user account (*nagiosadmin*) that can access the CGIs.

As you define more contacts for receiving host and service notifications, you'll most likely want to let them access the Nagios web interface. You can use the following command to add additional users who can authenticate to the CGIs. Replace <username> with the actual username you want to add. In most cases, the username should match the short name of a contact that has been defined.

```
htpasswd /usr/local/nagios/etc/htpasswd.users <username>
```

Enabling Authentication/Authorization Functionality In The CGIs

The next thing you need to do is make sure that the CGIs are configured to use the authentication and authorization functionality in determining what information and/or commands users have access to. This is done be setting the use_authentication variable in the CGI configuration file to a non-zero value. Example:

```
use_authentication=1
```

Okay, you're now done with setting up basic authentication/authorization functionality in the CGIs.

Default Permissions To CGI Information

So what default permissions do users have in the CGIs by default when the authentication/authorization functionality is enabled?

CGI Data	Authenticated Contacts*	Other Authenticated Users*
Host Status Information	Yes	No
Host Configuration Information	Yes	No
Host History	Yes	No
Host Notifications	Yes	No
Host Commands	Yes	No
Service Status Information	Yes	No
Service Configuration Information	Yes	No
Service History	Yes	No
Service Notifications	Yes	No
Service Commands	Yes	No
All Configuration Information	No	No
System/Process Information	No	No
System/Process Commands	No	No

*Authenticated contacts** are granted the following permissions for each **service** for which they are contacts (but not for services for which they are not contacts)...

- Authorization to view service status information
- Authorization to view service configuration information

- Authorization to view history and notifications for the service
- Authorization to issue service commands

*Authenticated contacts** are granted the following permissions for each **host** for which they are contacts (but not for hosts for which they are not contacts)...

- Authorization to view host status information
- Authorization to view host configuration information
- Authorization to view history and notifications for the host
- Authorization to issue host commands
- Authorization to view status information for all services on the host
- Authorization to view configuration information for all services on the host
- Authorization to view history and notification information for all services on the host
- Authorization to issue commands for all services on the host

It is important to note that by default **no one** is authorized for the following...

- Viewing the raw log file via the showlog CGI
- Viewing Nagios process information via the extended information CGI
- Issuing Nagios process commands via the command CGI
- Viewing host group, contact, contact group, time period, and command definitions via the configuration CGI

You will undoubtably want to access this information, so you'll have to assign additional rights for yourself (and possibly other users) as described below...

Granting Additional Permissions To CGI Information

You can grant *authenticated contacts* or other *authenticated users* permission to additional information in the CGIs by adding them to various authorization variables in the CGI configuration file. I realize that the available options don't allow for getting really specific about particular permissions, but its better than nothing..

Additional authorization can be given to users by adding them to the following variables in the CGI configuration file...

- authorized_for_system_information
- authorized_for_system_commands
- authorized_for_configuration_information
- authorized_for_all_hosts
- authorized_for_all_host_commands
- authorized_for_all_services
- authorized_for_all_service_commands

CGI Authorization Requirements

If you are confused about the authorization needed to access various information in the CGIs, read the ***Authorization Requirements*** section for each CGI as described here.

Authentication On Secured Web Servers

If your web server is located in a secure domain (i.e., behind a firewall) or if you are using SSL, you can define a default username that can be used to access the CGIs. This is done by defining the default_user_name option in the CGI configuration file. By defining a default username that can access the CGIs, you can allow users to access the CGIs without necessarily having to authenticate to the web server. You may want to use this to avoid having to use basic web authentication, as basic authentication transmits passwords in clear text over the Internet.

Important: Do *not* define a default username unless you are running a secure web server and are sure that everyone who has access to the CGIs has been authenticated in some manner. If you define this variable, anyone who has not authenticated to the web server will inherit all rights you assign to this user!