Welcome to the "ServerHealthCheck" plugin user manual for the administrator!

Table of contents

1. Plugin installation

1.1. On the GLPI host machine, install the "ipmitool" utility with the following command:

```
sudo apt install ipmitool
```

1.2. Clone the ServerHealthCheck plugin repository to the GLPI plugins directory with the following command:

```
git clone https://github.com/friendly-zfdal/serverHealthCheck.git
```

1.3. Change the owner of the plugin directory files to "www-data" to avoid problems with the plugin accessing system functions with the following command:

```
sudo chown -R www-data:www-data /var/www/html/
```

1.4. In the side menu, go to Settings -> Plugins tab and install the plugin by clicking on the folder icon with a "+" symbol on it:

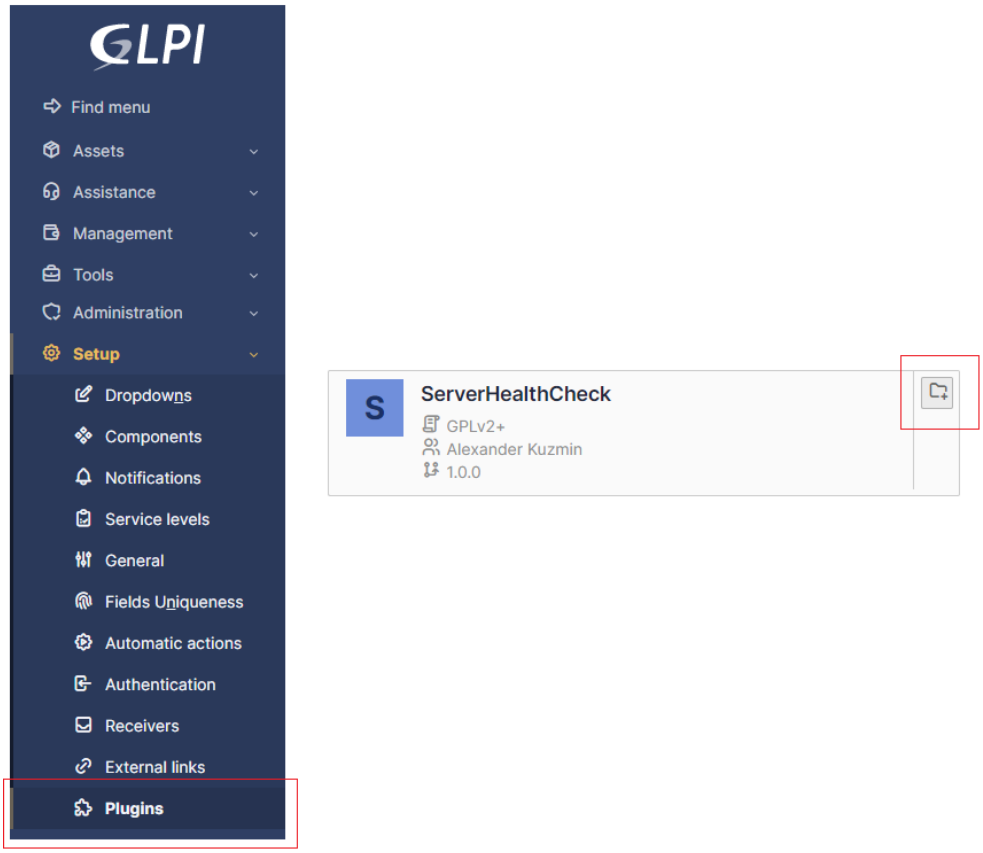

Figure 1 – Plugin installation

1.5. After successful installation, activate the plugin by clicking on the icon shown in the image below:

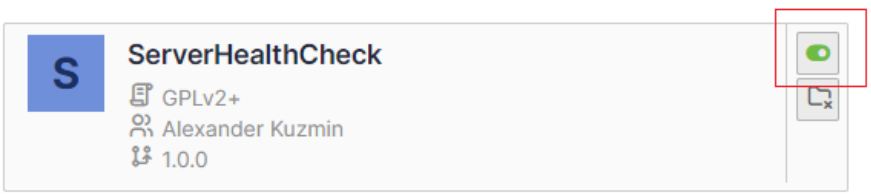

Рисунок 2 – Plugin activation

1.6. Refresh the page and make sure the sidebar has a new "Plugins" tab and a "ServerHealthCheck" subtab:

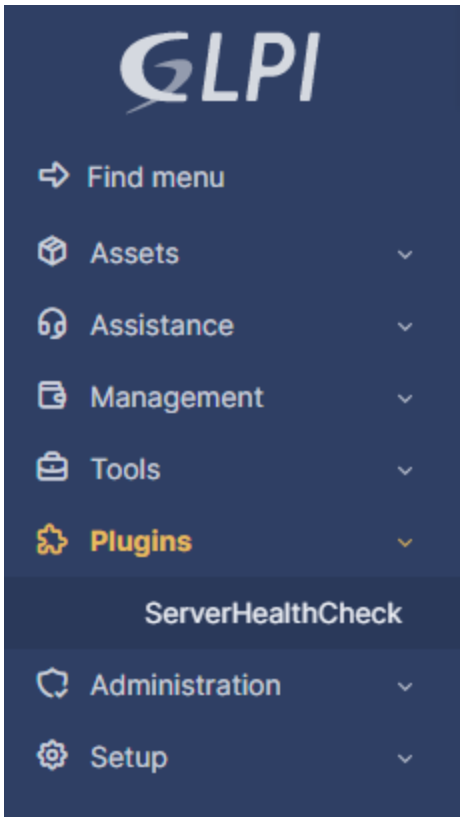

Figure 3 – Plugin tab on the sidebar

1.7. Congratulations! You have successfully installed the plugin.

2. Plugin uninstallation

2.1. Go to tab Settings-> Plugins.
2.2. Deactivate the plugin.
2.3. Remove plugin from GLPI.
2.4. Remove plugin directory from «…/glpi/plugins» folder.

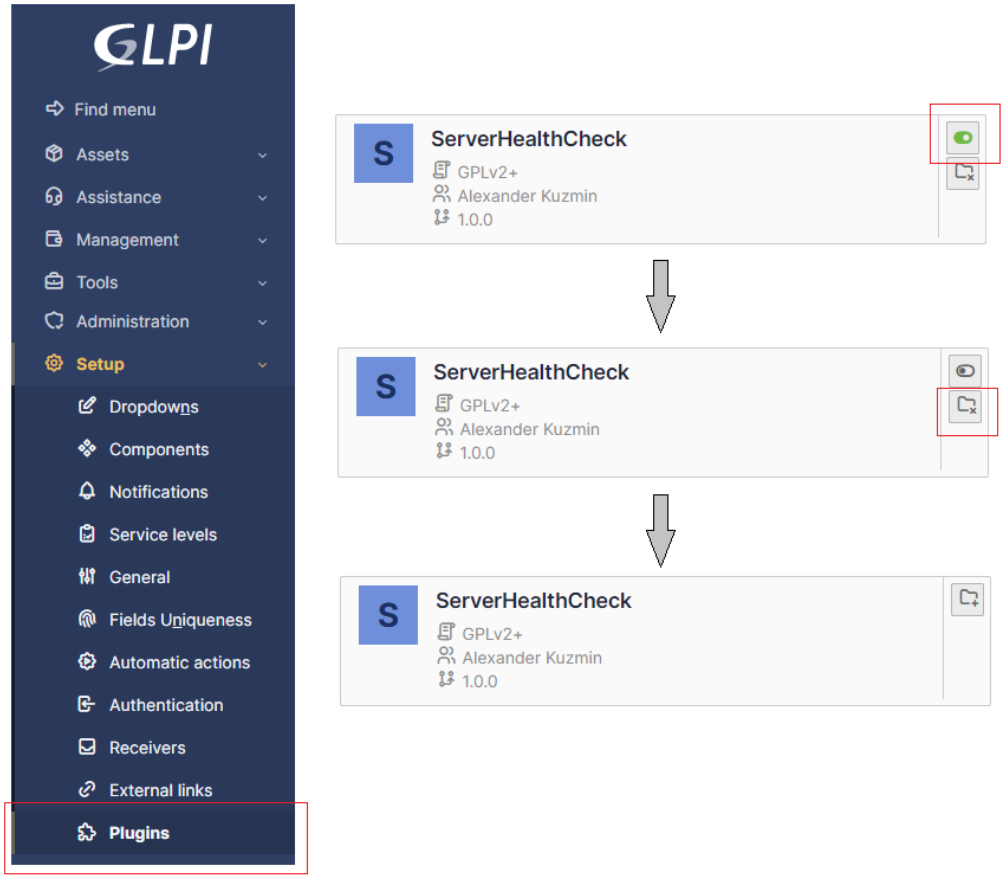

Figure 4 – Plugin uninstallation

3. The process of granting privileges to users

When the plugin is installed, a new user group "ServerHealthCheck" is created in GLPI. It is assumed that only users who have confidential information about access to servers will be added to this group. Such a restriction is necessary, since one of the plug-in report versions provides this data in an open form for the fastest remote connection to damaged systems for further more detailed diagnostics. In this regard, it is recommended to limit and control the list of persons included in this group, as well as the list of persons who can add users to this group.

In other words, to provide full access to the functionality of the plugin, the user must be added to the "ServerHealthCheck" group. For all other users, a public report will be available on the Tools -> Reports -> Server Health Check report tab and plugin widget information in the GLPI central dashboard.

The user "glpi" is added to the plugin's group at the moment of its installation, i.e. the system administrator initially has access to full functionality.

4. Using the "ServerHealthCheck" Plugin

In total, the plugin can display the information it collects in three forms: a private report, a public report, a widget on the main GLPI dashboard. In addition, there is the main form of the plugin, accessible only to privileged users.

4.1. Adding servers

When installing the plugin, all systems with the “server” type are automatically added to the server table. Therefore, you should specify the type of systems for computers on the Assets -> Computers tab so that the plugin can correctly collect the initial list of server systems.

In case of adding/removing servers from the Computers table **after installing the plugin**, you need to inform the plugin that you need to update the list of servers in its table. To do this, on the main form of the plugin there is a separate button "Update servers list".

4.2. Plugin main form

Figure 5 – Plugin main form

The main form of the plug-in contains a table that displays data from the plug-in table in the GLPI database and 4 buttons. Here, persons with access can correct the information necessary to access the server's BMC controller and save these changes by clicking on the "Save changes" button. For the correct operation of the plugin, IP addresses are checked for correctness, as well as passwords are checked for a length equal to or more than 8 characters for security purposes.

The "Update servers list" button updates the list of servers in the plugin table based on the list of all computers included in the GLPI.

The "Gather sensors values" button updates the data on the state of the servers in the plugin table without displaying the updated information on the screen.

The "Show report" button updates the server data (this operation may take some time) and provides the user with a private version of the report.

4.3. Private report

The private report is intended exclusively for privileged users, as it contains confidential information about the details for accessing the BMC controller of server systems in clear text. The need for such a solution was described earlier in section 3.

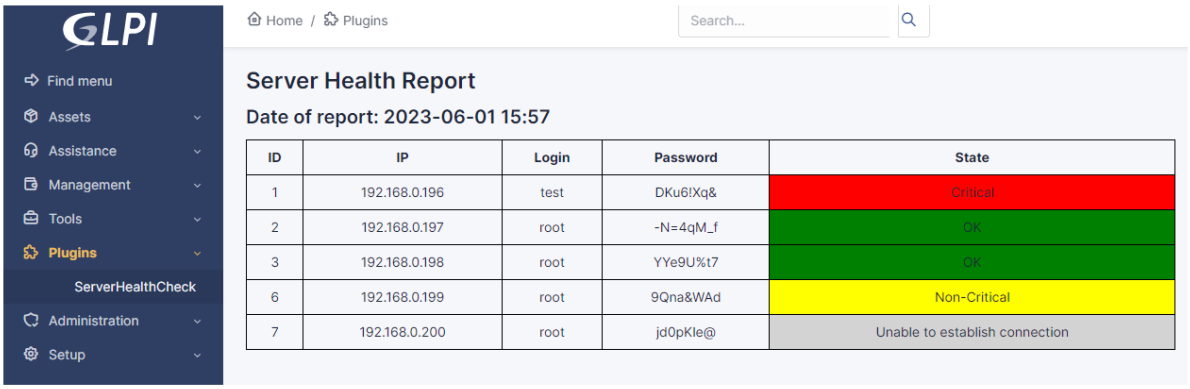

Figure 6 – Private report

4.4. Public report

For users who do not need direct access to damaged systems, but have a need to monitor the status of systems as a whole, a public report "Server Health Check report" was created on the Tools->Reports tab. This version of the report provides the same information as the private one, but without the "Login" and "Password" fields. If the user does not use the simplified GLPI interface mode and generally has access to the Tools->Reports tab, then he can view this report, which will provide up-to-date information about the state of the systems.

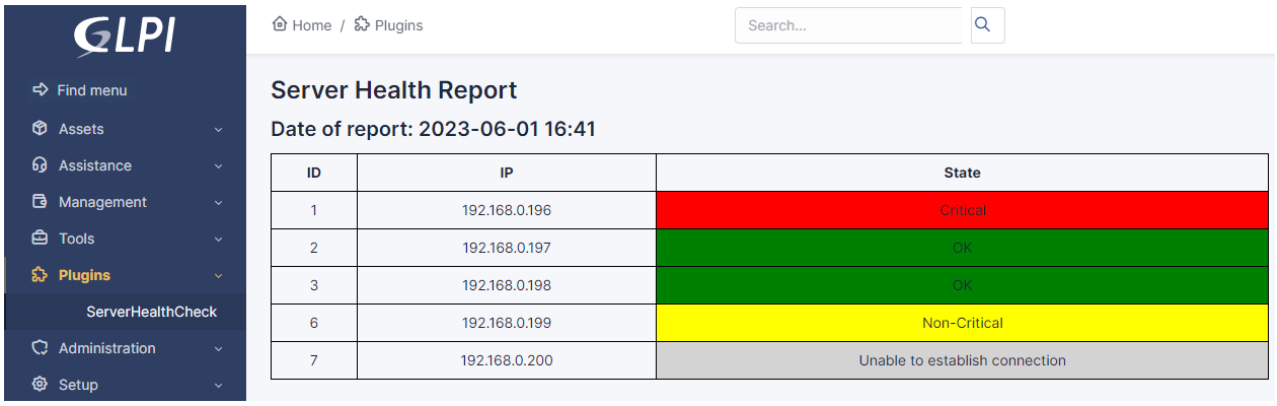

Figure 7 – Public report

4.5. Widget on the main dashboard

For quick access to the data of the last generated report, you can also add a plug-in to the main panel of the GLPI interface that provides a brief summary of the state of the organization's server park machines. This widget displays how many servers are in what state and, depending on this data, displays the overall status of the server park. The widget is available to all users who are not using the lightweight GLPI interface.

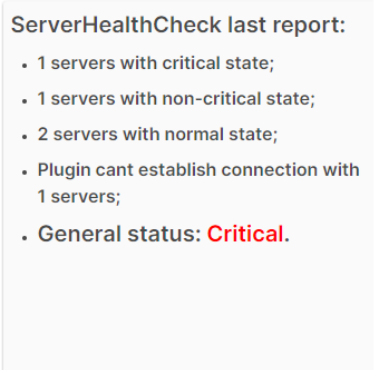

Figure 8 – Plugin widget

4.6. Displayed statuses

In total, the plugin has 5 possible statuses to indicate the state of systems and 4 possible statuses to indicate the state of the entire server park. The algorithm for setting statuses for both cases is described below.

Using the "ipmitool" utility and the "sdr" command, data on all sensors installed on the target system, their readings and statuses are read from the server system. Sensors can be "Upper Critical" and "Lower Critical" for critical sensor readings, "Upper Non-Critical" and "Lower Non-Critical" for non-critical but no longer normal values, and "OK" for normal sensor readings and " nc" for sensors that are not currently connected to the system. If the plug-in algorithm finds at least one sensor of the system, the status of which is set to "Upper Critical" or "Lower Critical", then the system is assigned the status "Critical", otherwise it is checked in the same way to find sensors with non-critical, but not normal values. If the plugin finds such sensors, then the status of the system is set to "Non-Critical". If the sensors with one of the four described values were not found, then the status "OK" is set for the system.

If the system initially failed to establish connections for any reason through the "ipmitool" utility, then the system is set to the "Unable to establish connection" status.

As you can see, the statuses have different color highlighting for the convenience of analyzing the data received from the report: "Critical" - red, "Non-Critical" - yellow, "OK" - green, "Unable to establish connection" - gray.

The general status for the server park is determined in the same way, only instead of the statuses of the sensors of a separate server, the entire server is used. That is, if there is at least one server with the “Critical” status, then the “Critical” status is set for the entire array of servers, which is displayed in the plugin widget on the main dashboard, etc.

4.7. Storage of reports

When generating public reports, they are immediately saved to the “reports” folder in the root of the plugin directory with the generation date indicated in the name so that the GLPI administrator can generate additional reporting using them.

5. Debugging the plugin in case of problems

If any problems occur during the operation of the plugin, they can be divided into three types:

- Errors in SQL queries to the database;
- PHP code execution errors;
- WEB server errors.

To view errors that occur when executing SQL queries against the database, you can view the latest events in the GLPI SQL operations log file located at «…/glpi/files/_log/sql-errors.log».

To view errors that occur when PHP scripts are executed on plugin pages, you can view the latest events in the GLPI PHP script execution log file located at «…/glpi/files/_log/php-errors.log».

To view errors that occur in the operation of the WEB server, you can view the log of its operation. In the case of the Apache WEB server and its default installation, the log file is located at «/var/log/apache2/error.log».

In accordance with the errors found, you should make the necessary changes in the plugin source code and test its performance yourself, or report the found error/required change on the plugin repository page on github.