Monitoring using SNMP

In this article

GitHub Enterprise provides data on disk usage, CPU utilization, memory usage, and more over SNMP.

SNMP is a common standard for monitoring devices over a network. We strongly recommend enabling SNMP so you can monitor the health of your GitHub Enterprise Server instance and know when to add more memory, storage, or processor power to the host machine.

GitHub Enterprise has a standard SNMP installation, so you can take advantage of the many plugins available for Nagios or for any other monitoring system.

Configuring SNMP v2c

1. From an administrative account on GitHub Enterprise Server, in the upper-right corner of any page, click 🚀.
2. If you're not already on the "Site admin" page, in the upper-left corner, click **Site admin**.
3. In the "🚀 Site admin" sidebar, click **Management Console**.
4. In "Settings" sidebar, click **Monitoring**.
5. Under "Monitoring", select **Enable SNMP**.
6. In the **Community string** field, enter a new community string. If left blank, this defaults to `public`.
7. Under the "Settings" sidebar, click **Save settings**.

   Note: Saving settings in the Management Console restarts system services, which could result in user-visible downtime.

8. Wait for the configuration run to complete.
9. Test your SNMP configuration by running the following command on a separate workstation with SNMP support in your network:

```
# community-string is your community string
# hostname is the IP or domain of your Enterprise instance
$ snmpget -v 2c -c COMMUNITY-STRING -O e HOSTNAME hrSystemDate.0
```

This should return the system time on your GitHub Enterprise Server instance host.

User-based security

If you enable SNMP v3, you can take advantage of increased user based security through the User Security Model (USM). For each unique user, you can specify a security level:

- `noAuthNoPriv`: This security level provides no authentication and no privacy.
- `authNoPriv`: This security level provides authentication but no privacy. To query the appliance you'll need a username and password (that must be at least eight characters long). Information is sent without encryption, similar to SNMPv2. The authentication protocol can be either MD5 or SHA and defaults to SHA.
- `authPriv`: This security level provides authentication with privacy. Authentication, including a minimum eight-character authentication password, is required and responses are encrypted. A privacy password is not required, but if provided it must be at least eight characters long. If a privacy password isn't provided, the authentication password is used. The privacy protocol can be either DES or AES and defaults to AES.

Configuring users for SNMP v3

1. From an administrative account on GitHub Enterprise Server, in the upper-right corner of any page, click 🚀.
2. If you're not already on the "Site admin" page, in the upper-left corner, click **Site admin**.
3. In the "🚀 Site admin" sidebar, click **Management Console**.
4. In "Settings" sidebar, click **Monitoring**.
5. Under "Monitoring", select **Enable SNMP**.
6. Select **SNMP v3**.
7. Under "Username", type the unique username of your SNMP v3 user.
8. Select the **Security Level** dropdown menu, then click the security level for your SNMP v3 user.
9. For SNMP v3 users with the `authnopriv` security level, configure authentication.
    - Under "Authentication password", type the authentication password.
    - Next to "Authentication password", select the **Protocol** dropdown menu, then click the authentication protocol you want to use.
10. For SNMP v3 users with the `authpriv` security level, configure authentication.
    - Under "Authentication password", type the authentication password.
    - Next to "Authentication password", select the **Protocol** dropdown menu, then click the authentication protocol you want to use.
    - Optionally, under "Privacy password", type the privacy password.
    - Next to "Privacy password", select the **Protocol** dropdown menu, then click the privacy protocol method you want to use.
11. Click **Add user**.

12. Under the "Settings" sidebar, click **Save settings**.

> **Note:** Saving settings in the Management Console restarts system services, which could result in user-visible downtime.

13. Wait for the configuration run to complete.

Querying SNMP data

Both hardware and software-level information about your appliance is available with SNMP v3. Due to the lack of encryption and privacy for the `noAuthNoPriv` and `authNoPriv` security levels, we exclude the `hrSWRun` table (1.3.6.1.2.1.25.4) from the resulting SNMP reports. We include this table if you're using the `authPriv` security level. For more information, see the "OID reference documentation."

With SNMP v2c, only hardware-level information about your appliance is available. The applications and services within GitHub Enterprise do not have OIDs configured to report metrics. Several MIBs are available, which you can see by running `snmpwalk` on a separate workstation with SNMP support in your network:

```
# community-string is your community string
# hostname is the IP or domain of your Enterprise instance
$ snmpwalk -v 2c -c COMMUNITY-STRING -O e HOSTNAME
```

Of the available MIBs for SNMP, the most useful is `HOST-RESOURCES-MIB` (1.3.6.1.2.1.25). See the table below for some important objects in this MIB:

Name	OID	Description
hrSystemDate.2	1.3.6.1.2.1.25.1.2	The hosts notion of the local date and time of day.
hrSystemUptime.0	1.3.6.1.2.1.25.1.1.0	How long it's been since the host was last initialized.
hrMemorySize.0	1.3.6.1.2.1.25.2.2.0	The amount of RAM on the host.
hrSystemProcesses.0	1.3.6.1.2.1.25.1.6.0	The number of process contexts currently loaded or running on the host.
hrStorageUsed.1	1.3.6.1.2.1.25.2.3.1.6.1	The amount of storage space consumed on the host, in hrStorageAllocationUnits.
hrStorageAllocationUnits.1	1.3.6.1.2.1.25.2.3.1.4.1	The size, in bytes, of an hrStorageAllocationUnit

For example, to query for `hrMemorySize` with SNMP v3, run the following command on a separate workstation with SNMP support in your network:

```
# username is the unique username of your SNMP v3 user
# auth password is the authentication password
# privacy password is the privacy password
# hostname is the IP or domain of your Enterprise instance
$ snmpget -v 3 -u USERNAME -l authPriv \
  -A "AUTH PASSWORD" -a SHA \
```

```
  -X "PRIVACY PASSWORD" -x AES \
  -O e HOSTNAME HOST-RESOURCES-MIB::hrMemorySize.0
```

With SNMP v2c, to query for `hrMemorySize`, run the following command on a separate workstation with SNMP support in your network:

```
# community-string is your community string
# hostname is the IP or domain of your Enterprise instance
snmpget -v 2c -c COMMUNITY-STRING HOSTNAME HOST-RESOURCES-MIB::hrMemorySize.0
```

Note: To prevent leaking information about services running on your appliance, we exclude the `hrSWRun` table (1.3.6.1.2.1.25.4) from the resulting SNMP reports unless you're using the `authPriv` security level with SNMP v3. If you're using the `authPriv` security level, we include the `hrSWRun` table.

For more information on OID mappings for common system attributes in SNMP, see "Linux SNMP OID’s for CPU, Memory and Disk Statistics".