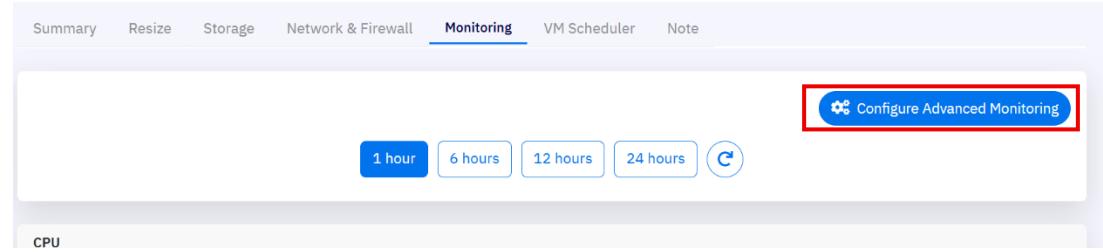
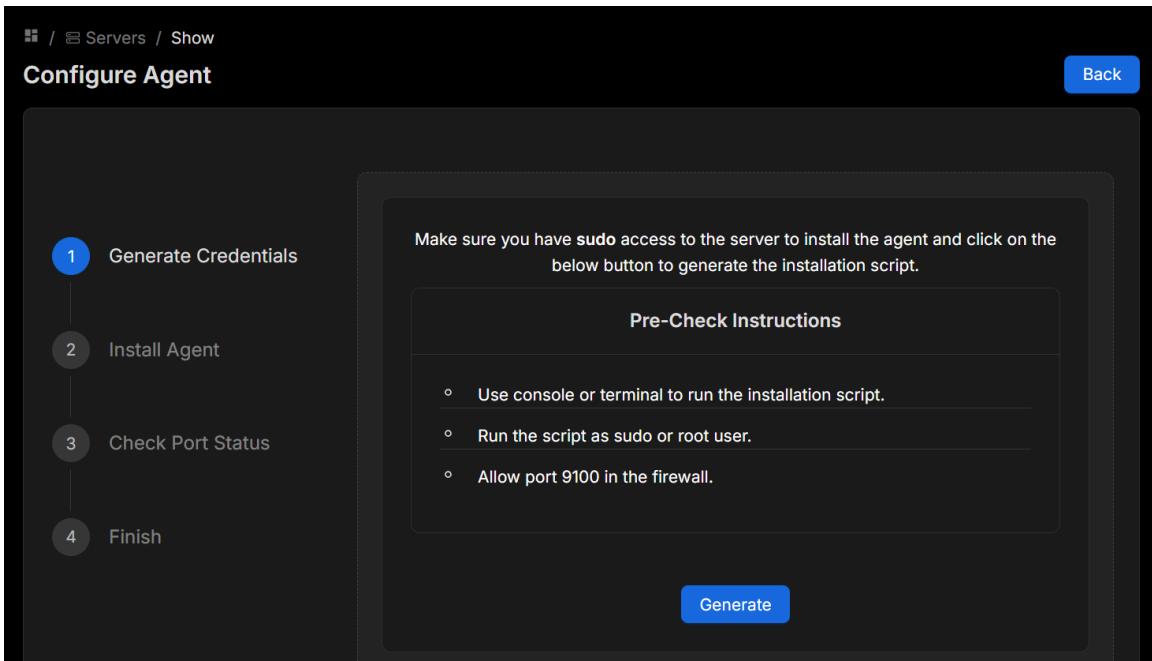


Configuring Advanced Monitoring Agent

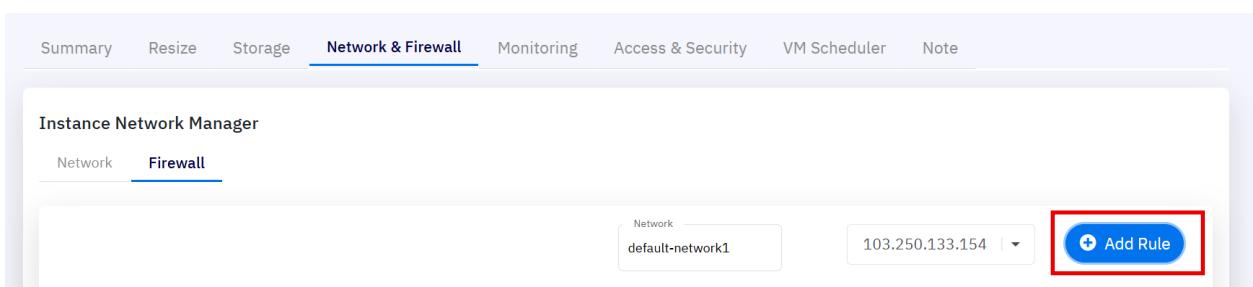
- On the Instance Details page, open the ‘Monitoring’ tab, and then click on ‘Configure Advanced Monitoring’.

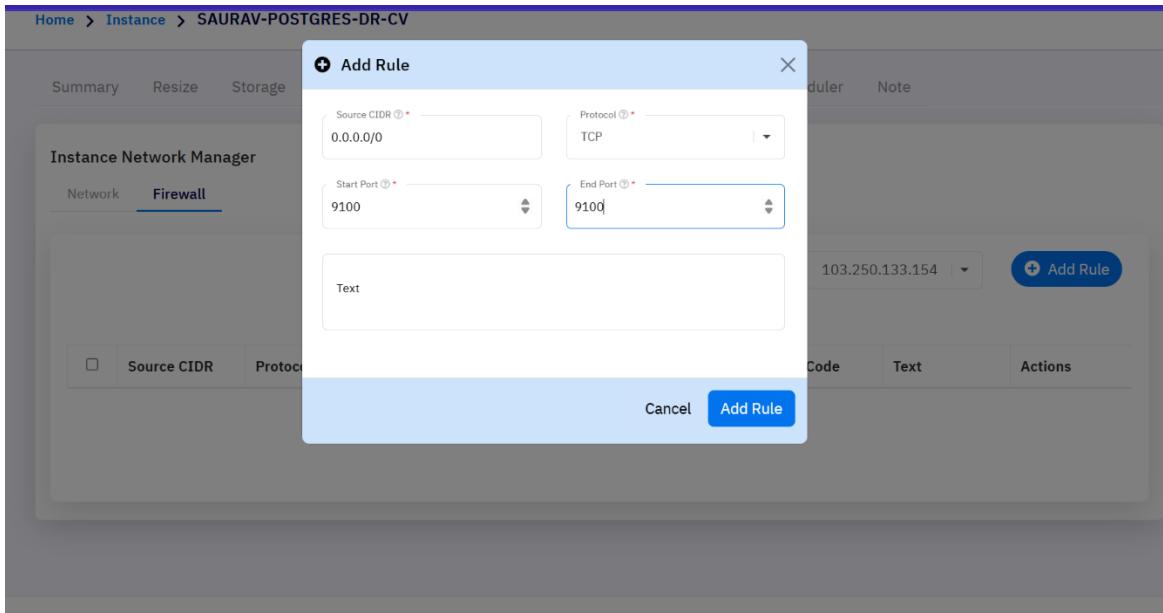


- You will be redirected to the following configuration page according to which we need to allow port 9100 in the firewall.



- Now to allow the port in the firewall, select ‘Network & Firewall’ and ‘Add Rule’





- For RedHat distribution OS, SELinux is enabled by default. This needs to be disabled.

```
[root@almaTest ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
```

- To do this, the line SELINUX inside the /etc/selinux/config should be set to disabled.
`vi /etc/selinux/config`

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
# See also:
# https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/using_selinux/changing_SELinux-states-at-time_changing_SELinux-states-and-modes
#
# NOTE: Up to RHEL 8 release included, SELINUX=disabled would also
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
SELINUX=disabled
# SELINUXTYPE= can take one of these three values:
#       targeted - Targeted processes are protected,
#       minimum - Modification of targeted policy. Only selected processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

After this reboot to apply the changes.

```
[root@almaTest ~]# reboot
```

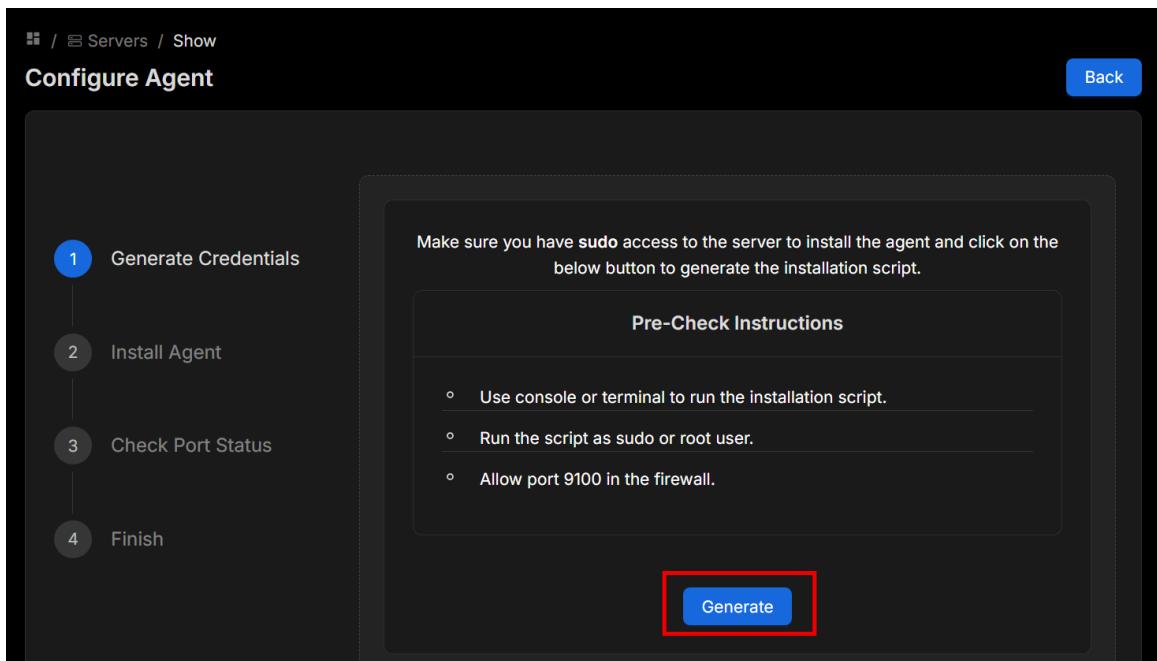
This then allows the node_exporter service to run.

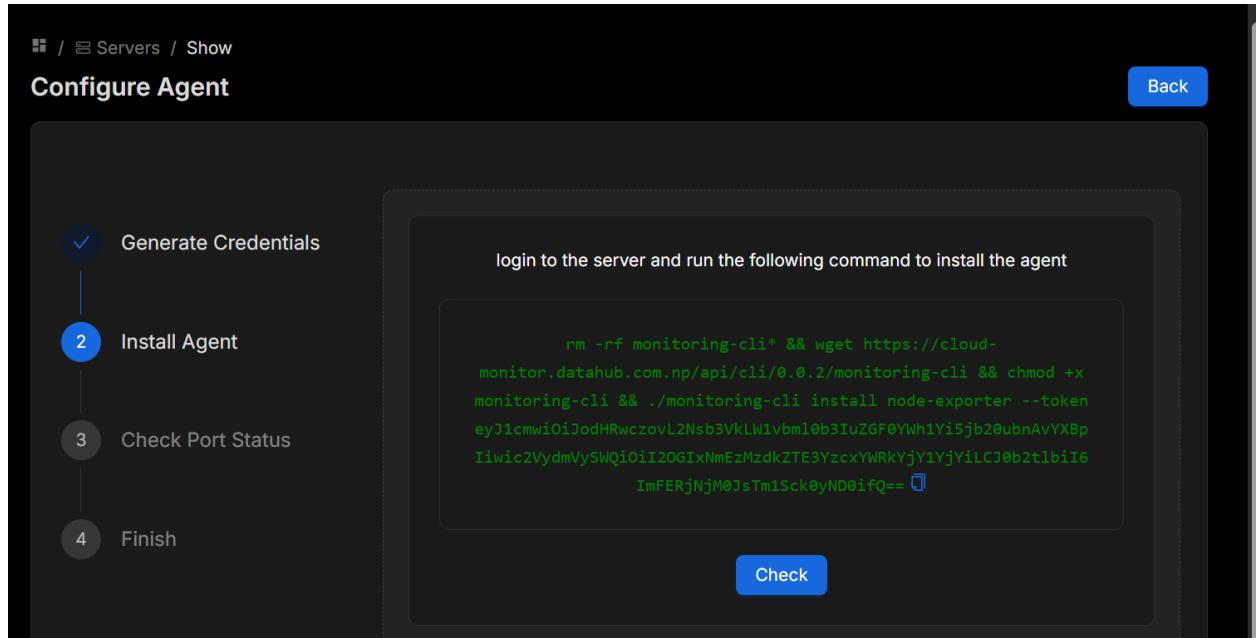
```
[root@almaTest almalinux]# sudo systemctl status node_exporter
● node_exporter.service - Node Exporter
    Loaded: loaded (/etc/systemd/system/node_exporter.service; enabled; preset: disabled)
    Active: active (running) since Fri 2025-08-29 08:10:51 EDT; 1 day 16h ago
      Main PID: 778 (node_exporter)
        Tasks: 6 (limit: 10985)
       Memory: 17.8M
          CPU: 121ms
        CGroup: /system.slice/node_exporter.service
                └─778 /usr/local/bin/node_exporter --collector.systemd --web.listen-address=:9100 --web.config.file=/etc/node_expo

Aug 29 08:10:51 almaTest node_exporter[778]: ts=2025-08-29T12:10:51.254Z caller=node_exporter.go:118 level=info collector=time
Aug 29 08:10:51 almaTest node_exporter[778]: ts=2025-08-29T12:10:51.254Z caller=node_exporter.go:118 level=info collector=timex
Aug 29 08:10:51 almaTest node_exporter[778]: ts=2025-08-29T12:10:51.254Z caller=node_exporter.go:118 level=info collector=udp_g
Aug 29 08:10:51 almaTest node_exporter[778]: ts=2025-08-29T12:10:51.254Z caller=node_exporter.go:118 level=info collector=uname
Aug 29 08:10:51 almaTest node_exporter[778]: ts=2025-08-29T12:10:51.254Z caller=node_exporter.go:118 level=info collector=vmstat
Aug 29 08:10:51 almaTest node_exporter[778]: ts=2025-08-29T12:10:51.254Z caller=node_exporter.go:118 level=info collector=watch
Aug 29 08:10:51 almaTest node_exporter[778]: ts=2025-08-29T12:10:51.254Z caller=node_exporter.go:118 level=info collector=xfs
Aug 29 08:10:51 almaTest node_exporter[778]: ts=2025-08-29T12:10:51.254Z caller=node_exporter.go:118 level=info collector=zfs
Aug 29 08:10:51 almaTest node_exporter[778]: ts=2025-08-29T12:10:51.262Z caller=tls_config.go:313 level=info msg="Listening on >
Aug 29 08:10:51 almaTest node_exporter[778]: ts=2025-08-29T12:10:51.267Z caller=tls_config.go:349 level=info msg="TLS is enable>

Lines 1-20/20 (END)
```

- Then generate the installation script.





- Copy the generated command and ssh into your VM. Switch to the root user and paste the copied command.

```
[rockylinux@SAURAV-POSTGRES-DR-CV ~]$ sudo -i
[root@SAURAV-POSTGRES-DR-CV ~]# rm -rf monitoring-cli* && wget https://cloud-monitor.datahub.com.np/api/cli/0.0.2/monitoring-cli && chmod +x monitoring-cli && ./monitoring-cli install node-exporter --token eyJlc...Ii6tMFERjNjm0JstmlSck0yND0ifQ==
--2025-08-29 05:34:15-- https://cloud-monitor.datahub.com.np/api/cli/0.0.2/monitoring-cli
Resolving cloud-monitor.datahub.com.np (cloud-monitor.datahub.com.np)... 202.51.75.24
Connecting to cloud-monitor.datahub.com.np (cloud-monitor.datahub.com.np)|202.51.75.24|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7606424 (7.3M) [application/octet-stream]
Saving to: 'monitoring-cli'

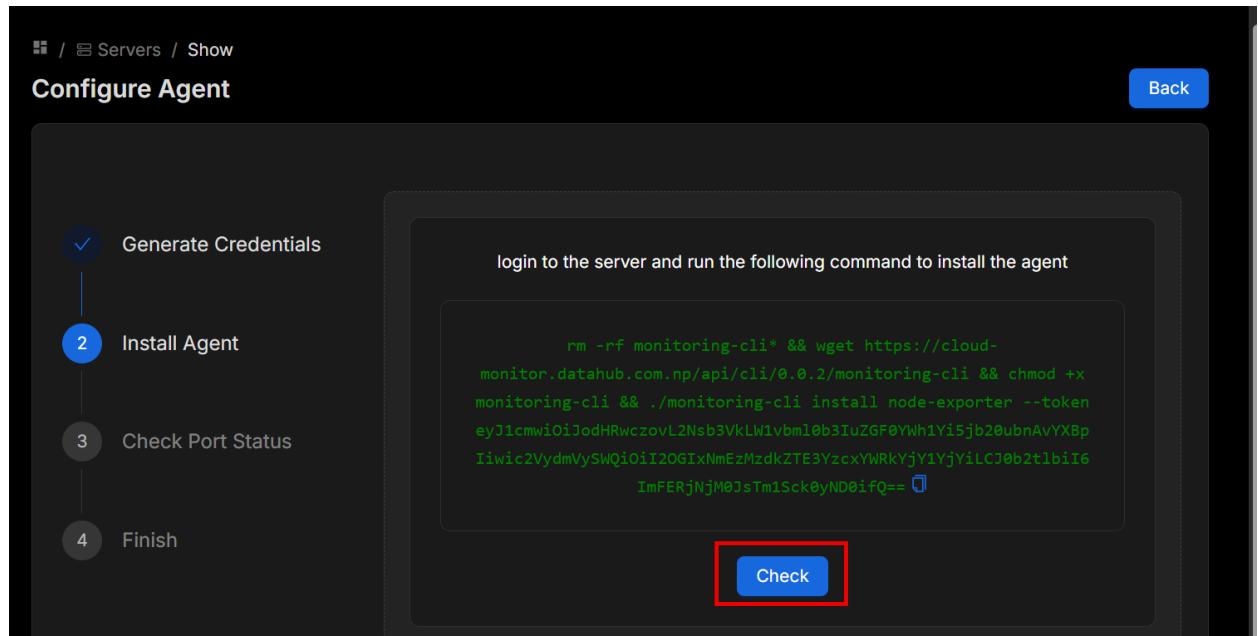
monitoring-cli          100%[=====]    7.25M  25.8MB/s   in 0.3s
2025-08-29 05:34:15 (25.8 MB/s) - 'monitoring-cli' saved [7606424/7606424]

Internal IP Addresses: [10.1.1.52]
Installing Node Exporter on SAURAV-POSTGRES-DR-CV...
::Installing Node Exporter...
User node_exporter created successfully.
Group node_exporter already exists.
User node_exporter added to group node_exporter successfully.
Creating directory /etc/node_exporter...
::Installing Node Exporter...
Node Exporter installed successfully.
Please make sure to open port 9100 in your firewall.
Node Exporter installed successfully.
[root@SAURAV-POSTGRES-DR-CV ~]#
```

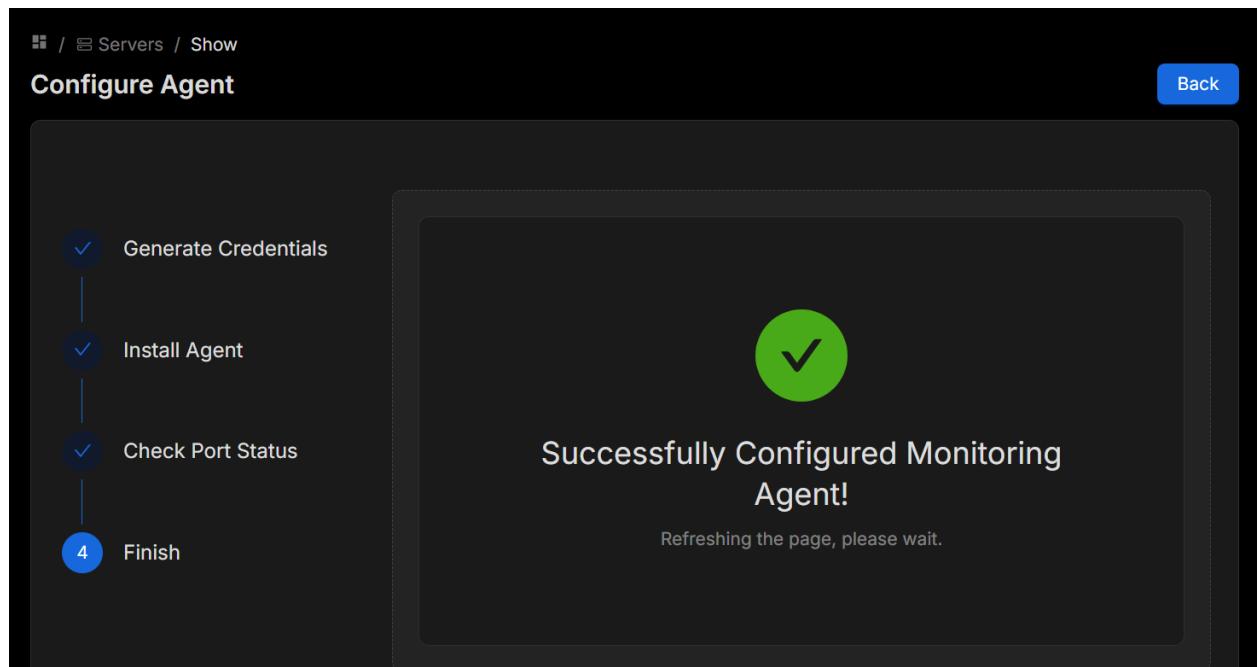
- Return to the portal and click the **Check** button.

The system will automatically verify that:

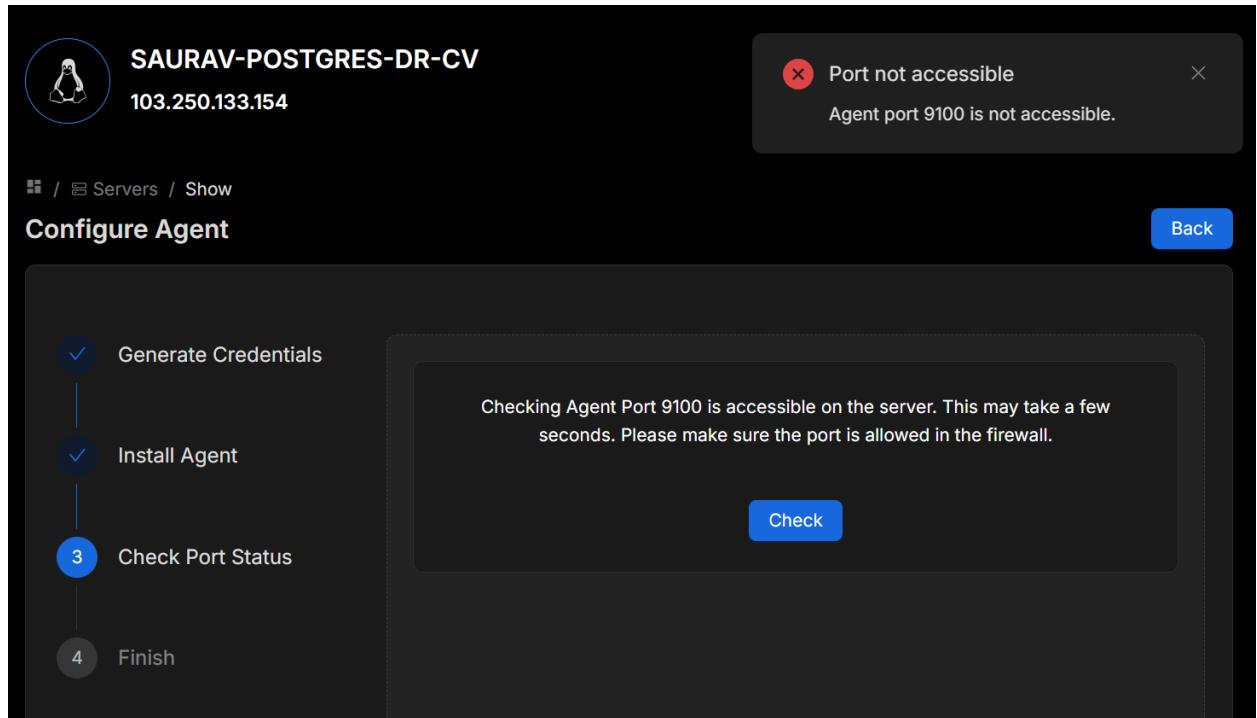
- The required port is correctly configured.
- The installed service (node-exporter) is running.



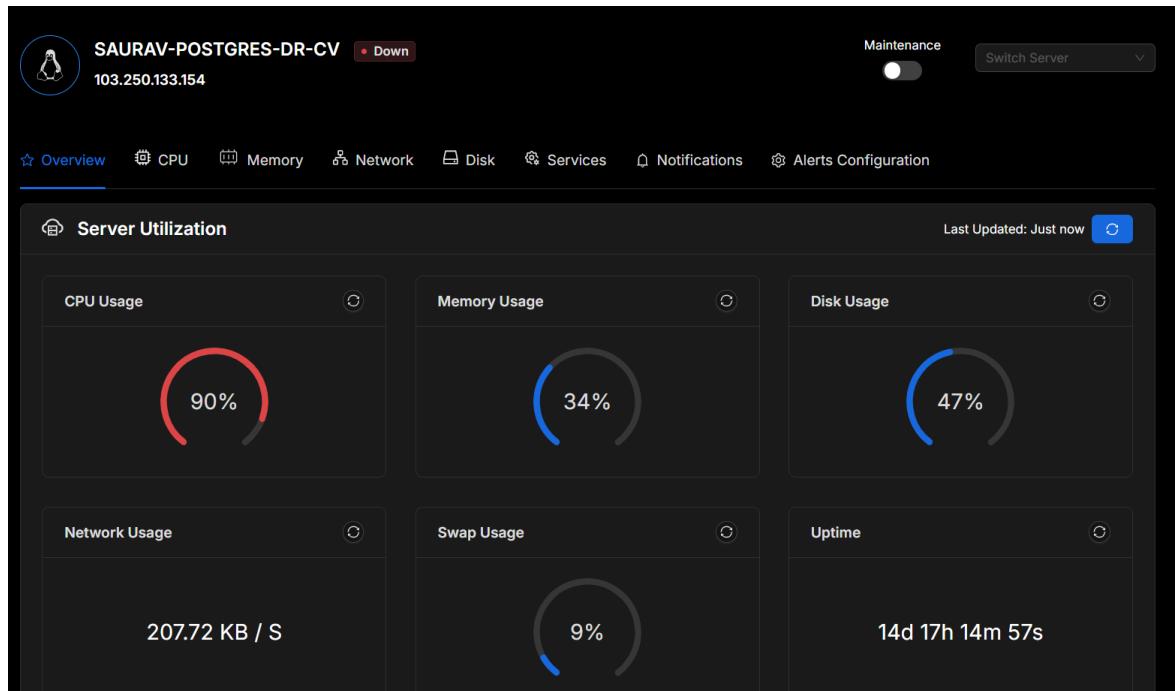
- If all the configuration steps are correct, the monitoring agent is successfully configured.



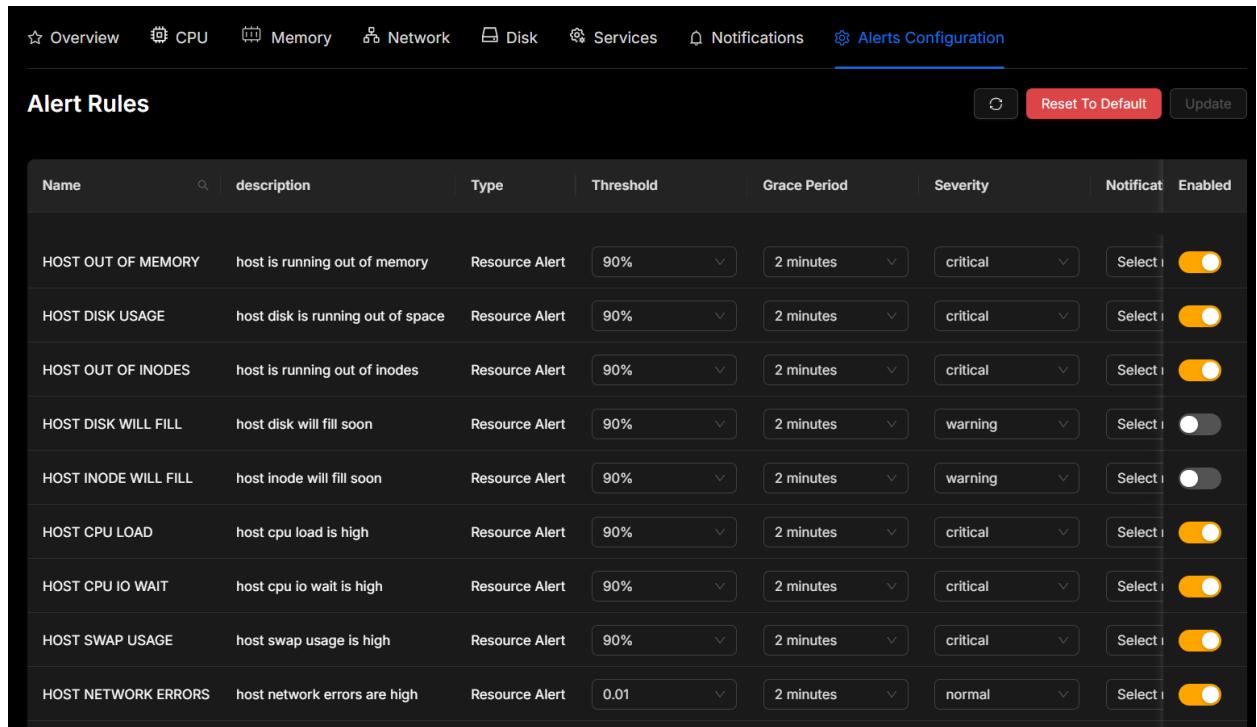
- If SELinux isn't disabled for the RedHat distribution OS, the following error occurs even though the port is configured.



- Once the agent is successfully configured, you will gain access to the monitoring dashboard.



- From the **Alert Configuration** section, you can set up and enable alerts for different types of issues to ensure timely notifications.



The screenshot shows a user interface for managing alert rules. At the top, there are navigation tabs: Overview, CPU, Memory, Network, Disk, Services, Notifications, and Alerts Configuration. The Alerts Configuration tab is selected, indicated by a blue underline. Below the tabs, the title "Alert Rules" is displayed. On the right side of the header are three buttons: a refresh icon, a red "Reset To Default" button, and a grey "Update" button. The main area is a table titled "Alert Rules" with the following columns: Name, description, Type, Threshold, Grace Period, Severity, Notifications, and Enabled. There are two search/filter icons on the left of the table header. The table contains nine rows of data:

Name	description	Type	Threshold	Grace Period	Severity	Notifications	Enabled
HOST OUT OF MEMORY	host is running out of memory	Resource Alert	90%	2 minutes	critical	Select...	<input checked="" type="checkbox"/>
HOST DISK USAGE	host disk is running out of space	Resource Alert	90%	2 minutes	critical	Select...	<input checked="" type="checkbox"/>
HOST OUT OF INODES	host is running out of inodes	Resource Alert	90%	2 minutes	critical	Select...	<input checked="" type="checkbox"/>
HOST DISK WILL FILL	host disk will fill soon	Resource Alert	90%	2 minutes	warning	Select...	<input type="checkbox"/>
HOST INODE WILL FILL	host inode will fill soon	Resource Alert	90%	2 minutes	warning	Select...	<input type="checkbox"/>
HOST CPU LOAD	host cpu load is high	Resource Alert	90%	2 minutes	critical	Select...	<input checked="" type="checkbox"/>
HOST CPU IO WAIT	host cpu io wait is high	Resource Alert	90%	2 minutes	critical	Select...	<input checked="" type="checkbox"/>
HOST SWAP USAGE	host swap usage is high	Resource Alert	90%	2 minutes	critical	Select...	<input checked="" type="checkbox"/>
HOST NETWORK ERRORS	host network errors are high	Resource Alert	0.01	2 minutes	normal	Select...	<input checked="" type="checkbox"/>