Monitoring with SUSE Manager 4
Monitoring with SUSE Manager 4

SUSE Manager 4 is a best-in-class, open source infrastructure management solution that lowers costs, enhances availability and reduces complexity for lifecycle management of Linux systems in large, complex and dynamic IT landscapes.

You can use SUSE Manager to configure, deploy and administer thousands of Linux systems running on hypervisors, as containers, on bare metal systems, IoT devices and third-party cloud platforms. SUSE Manager also enables you to easily monitor your entire deployment of systems, across locations.

Why Monitor Your Systems?

One of a system administrator’s most challenging tasks is keeping tabs on every system in the company. When a company’s IT landscape is multi-tenant and multi-region, that task becomes exponentially more difficult. That’s where a monitor becomes a must-have tool. With the right monitor, an administrator will always be on top of their systems.

SUSE Manager 4 includes very powerful monitoring options (which can be added for an additional fee), with the option to install two additional very powerful monitoring and visualization tools: Prometheus (for monitoring) and Grafana (for visualization). These tools add real-time monitoring capability to the SUSE Manager 4 system. In addition, you can monitor a number of other events and system states found within the SUSE Manager 4 framework.

Systems Overview

Some of the most basic monitoring is on the SUSE Manager 4 Overview page (Figure 1). Here you’ll find a dashboard that gives you immediate access to information such as Tasks, Most Critical Systems, Recently Scheduled Actions, Relevant Security Patches, System Groups and Recently Registered Systems.

Figure 1. The SUSE Manager 4 Overview page.

The Overview (or “Start”) page should be one of the first pages that the SUSE Manager 4 administrator looks at. It is also possible to configure what you see on the Overview page. To do this, log into SUSE Manager 4 and go to Home | My Preferences. In this new window (Figure 2), you can enable/disable various options, such as receiving email/taskomatic notifications, Time Zone, CSV file data delineator, and other types of viewable information.

Set the SUSE Manager 4 Overview as your web browser’s home page, and you’ll always be on top of what’s going on with your systems.
Patch and Event Alerts
Alerts are one of the first lines of defense with SUSE Manager 4. You can configure alerts to be sent to a specific email address, so you will always be in the know when patches that are relevant to your systems are released. You will also receive daily emails that summarize a number of events that have occurred on your systems.

Knowing when patches are available is crucial to keeping your systems up to date. This is especially true when security patches are ready. When a vulnerability is discovered, you don't want to hold off on patching affected systems; otherwise, they could be compromised.

The first thing you'll want to do is configure an email address to which those alerts are sent. To do this, log into SUSE Manager 4 and go to Home | User Account | My Account. In the resulting window (Figure 3), configure the email address to be used.

CVE Scans
One form of monitoring that should be at the top of your list is running Common Vulnerability and Exposure (CVE) scans. This will scan all of your servers and images for CVE issues and report whether any of them are affected.

In order for this to be effective, make sure that you are up on your CVE vulnerabilities. You can get the latest vulnerabilities from the Published SUSE Security Advisories or Linux Kernel CVEs. Wherever you get your information about CVEs, you will need to know the CVE number for a particular vulnerability. With that number in hand, log into your SUSE Manager 4 instance and go to Audit | CVE Audit. In the resulting window (Figure 4), select the date of the CVE from the drop-down and then enter the CVE number in the text area to the right. Click the Audit Servers button to scan your systems or click Audit Images to scan the images used to deploy systems.
If any CVE issues are found in any of your deployed servers, they will be listed in the window’s main pane. You’ll see either No action required or a warning to install a specific patch on the affected system. Click the patch number listed, select the affected system (Figure 5) and click Apply Patches.

And that’s all there is to monitoring for and patching specific CVE vulnerabilities.

Prometheus

You can monitor your SUSE Manager 4 environment using Prometheus. SUSE Manager Server and Proxy are able to provide self-health metrics. Server and Proxy can also install and manage a number of Prometheus exporters on Salt clients.

Prometheus is an open source monitoring tool used to record real-time metrics in such a way that allows for higher performance and scalability. Prometheus fetches metrics using a pull mechanism, so the server must be able to establish network communications to monitored clients. Clients must have an open port and be reachable on the network.

In order to take advantage of Prometheus, you must first install it. Prometheus can be installed on any SLES instances with the command:

```
zypper in golang-github-prometheus-prometheus
```

Prometheus can also be installed via the SUSE Manager 4 GUI (Figure 6).

By installing Prometheus via the SUSE Manager GUI, you are able to create a formula to deploy a particular Prometheus package to any system.

Once installed, you must enable the service with the command:

```
systemctl enable --now prometheus
```
Once installed and enabled, you are ready to configure and enable Prometheus-based self-monitoring within SUSE Manager 4. Log into SUSE Manager and go to Admin | Manager Configuration | Monitoring. Click Enable services (Figure 7) and wait for the services to be enabled.

After you have monitoring enabled, you can then configure monitoring formulas by following these steps:

1. Log into SUSE Manager 4 Web UI and locate/open the details page of the system to be monitored.
2. Navigate to the Formulas tab.
3. Select the Monitoring checkbox to enable all monitoring formulas (Figure 8) and activate the Prometheus exporters if this is a client system.
4. Continue filling in the formula and then apply the highstate.

Next, you must configure the exporters with the following steps:

1. In the SUSE Manager Web UI, open the details page of the system to be monitored and navigate to the Formulas | Prometheus Exporters tab.
2. Check the Enabled checkbox for both Node and Postgres Exporter (Figure 9). Make sure to only activate the exporters that you need. (For example, if there is no Postgres database, you won’t need to activate the Postgres exporter.)
3. In the Postgres Exporter section, in the Data Source Name field, enter the path to your data source (for example, postgresql://user:passwd@localhost:5432/database?sslmode=disable).
4. Click Save Formula.
5. Apply the highstate.
Finally, open the Prometheus static configuration file `/etc/prometheus/prometheus.yml` and add or update the following section.

Where `SERVER` is the IP address or domain of your SUSE Manager server and `APIUSER` and `PASSWORD` match your authentication information. Save and close the file and then restart Prometheus with the command:

```bash
systemctl restart prometheus
```

Prometheus metrics exporters can also be used on Salt clients. The packages are available from the SUSE Manager 4 client tools channels and can be enabled and configured directly in the SUSE Manager 4 Web UI. Currently, two exporters are supported:

- **Node exporter**: [golang-github-prometheus-node_exporter](https://github.com/prometheus/node_exporter).
- **PostgreSQL exporter**: [golang-github-wrouesnel-postgres_exporter](https://github.com/wrouesnel/postgres_exporter).

Installing and configuring exporters is done using a Salt formula. When you have the exporters installed and configured, you can begin using Prometheus to scrape metrics from monitored systems. Service discovery instructs Prometheus to automatically scrape metrics from systems as they are enabled.

### Grafana

One thing that hasn’t been mentioned yet is monitoring the SUSE Manager 4 server itself. Fortunately, Grafana has an application for that. Grafana is an open source tool that enables you to visualize data from a number of services (such as Graphite, MySQL, InfluxDB, Prometheus, Elasticsearch and CloudWatch). With this tool, you can customize your dashboard to keep tabs on your SUSE Manager 4 server.

Grafana must first be installed. On smaller setups, Grafana can be installed on the same server as Prometheus. On larger rollouts, it should be deployed to its own server. It is possible to install Grafana with the command:

```bash
zypper in grafana
```

The best practice, however, is to install Grafana via the SUSE Manager GUI.
Once installed, start and enable the service with the command:

```
systemctl enable --now grafana-server
```

You can then reach Grafana at http://SERVER:3000 (where SERVER is either the domain or IP address of the hosting server). During the creation of the Grafana formula, a new data source will be automatically configured (which will point to the Prometheus server at port 9090). With this configuration complete, you should start seeing real-time data for your SUSE Manager 4 server (Figure 10).

With everything in place, you now have the means to monitor all of the servers and patches deployed by SUSE Manager 4, as well as the SUSE Manager 4 server itself—all from within your web browser. That’s power. That’s the SUSE way.

Figure 10. Grafana monitoring SUSE Manager 4 by way of Prometheus.