



White Paper

Managing Linux in Distributed Environments

Introduction

Large-scale deployments are infrastructures that contain more than 10,000 clients. And when you have that many clients to manage, automated infrastructure management becomes critical. From performance issues to compliance and security concerns, large-scale deployments pose unique challenges. Are you ready to handle them?

Infrastructure management systems offer many benefits for security, administration, and automation. You can lock down your system to prevent misconfiguration, watch for intruders, deploy new systems, and more. But that management system can only handle so many endpoints before scalability issues catch up with the single-server configuration. Performance starts to waiver, and issues with consistency and patching take a toll on efficiency. And when performance and consistency start to fail, security and compliance are often close behind.

Many organizations with large infrastructures simply deploy multiple independent management servers (Figure 1). This approach addresses the scalability issues by breaking the infrastructure into smaller units. The first thing to notice about the solution depicted in Figure 1, however, is that the infrastructure is no longer centrally managed. That might be fine if the various parts of your infrastructure are managed separately anyway, but keep in mind that

separate management silos increase costs because of the need for duplicating procedures and roles, and, importantly, independent networks tend to drift, leading to a lack of uniformity, which can increase overhead and lead to security problems. Some organizations attempt to address this divergence using scripted controls and other homegrown solutions, but custom tools typically have limited effect and require their own share of overhead.

SUSE has a better idea for large deployments. SUSE Manager is a Linux management solution for managing any Linux, anywhere, at any scale. SUSE Manager keeps the management servers unified and working together, allowing full integration of configuration and security (Figure 2). If you manage a large deployment with more than 10,000 nodes, a well-designed hub configuration will deliver all the benefits of SUSE Manager (see the “Benefits” box) for infrastructures of 90,000 nodes or even larger. Regardless of whether your organization specializes

in retail, business, cloud support, or manufacturing, SUSE Manager can help you configure, administer, and secure your large-scale deployment.

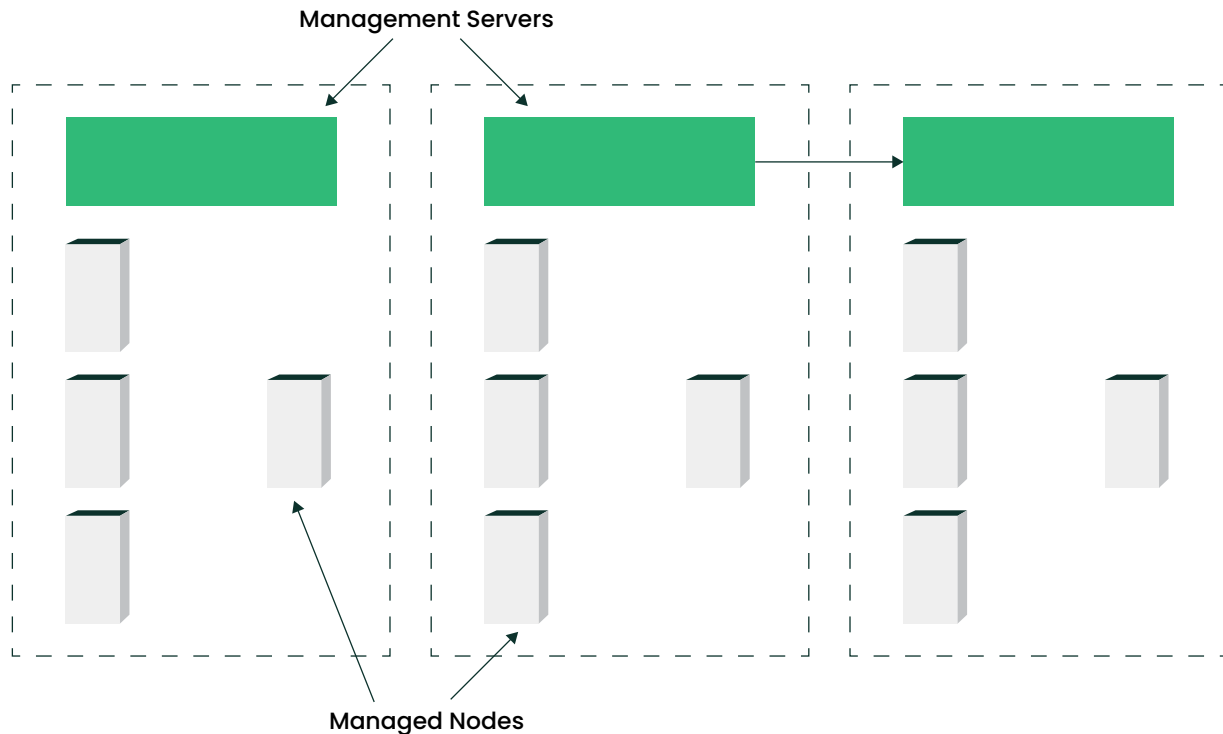


Figure 1. One way to scale a large deployment is to break it into smaller, independently managed parts.

Benefits

Why use SUSE Manager for large deployments? The same reason you would want to use SUSE Manager in other contexts. SUSE Manager benefits include:

- Cross-platform management for all enterprise Linux distributions
- Automated infrastructure security and compliance
- Automated patch management
- Centralized control and reporting
- Centralized and automated configuration management

For more on the benefits of SUSE Manager, see suse.com/products/suse-manager.

Hub architecture

In the configuration depicted in Figure 2, the single server at the top of the chart is known as the *hub*, and the bank of servers below it are called *peripherals*. The first thing to understand is that a peripheral is not like a proxy. A proxy is a local content cache that SUSE Manager uses to minimize network traffic with the central server while performing updates and other configuration changes. Proxies can improve performance by spreading out the I/O and reducing network load, but they will not solve the scalability issues for networks with more than 10,000 nodes.

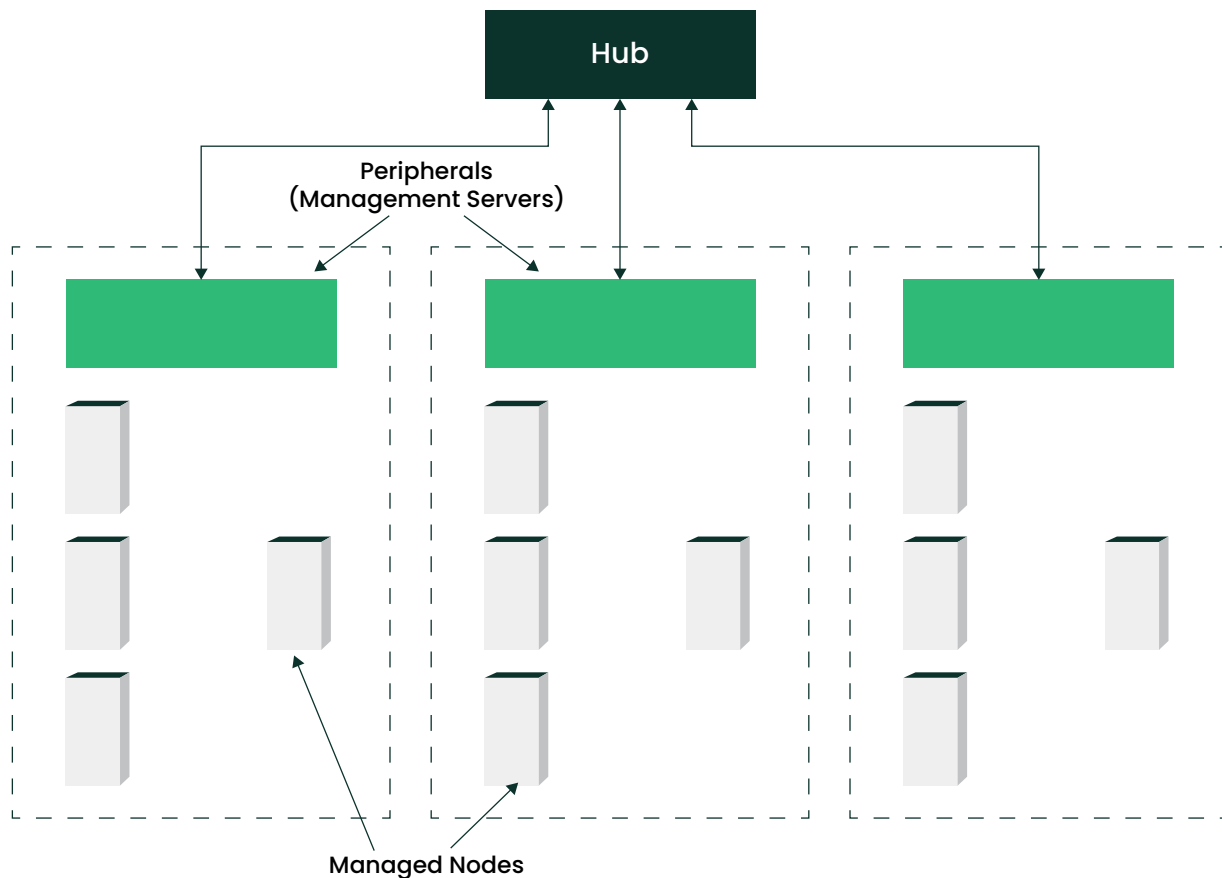


Figure 2. Centralized management can improve security and reduce the cost of ownership.

In a hub configuration, the peripherals act more like the independent servers shown in Figure 1, except that they are capable of receiving content from the hub server and federating reporting data to the hub. A fuller view of the hub configuration is shown in Figure 3.

As you can see in Figure 3, the hub initially provides the Salt modules and formulas needed to configure the peripheral servers (including users, system groups, and activation keys).

Once the peripherals are set up and a channel to the hub is established, the hub serves as a central source for passing images, software packages, and configuration changes to the peripherals. The peripherals also report logging data back to the hub. The hub aggregates data from the peripherals into a PostgreSQL database, which serves as a unified source of information on the complete infrastructure. (Each peripheral server also keeps its own database with a local source of information on the systems the server manages.)

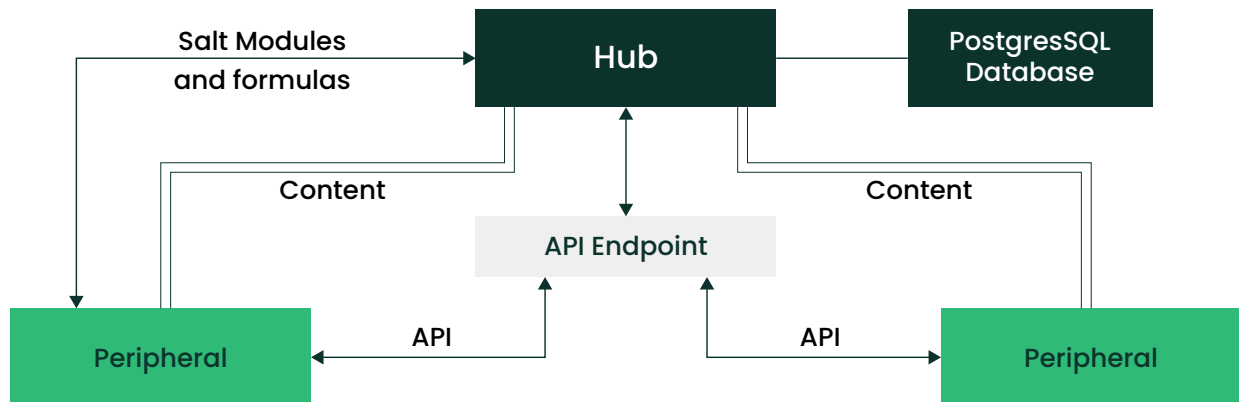


Figure 3. Peripherals receive content and API calls from the hub.

In hub deployment scenarios the communication is API driven. The hub serves as a central API endpoint, broadcasting API calls to the peripherals. The single “point of control” for the infrastructure is API only, meaning it doesn’t provide a single web UI where user can have a integrated view of all machines registered across all the peripherals.

The principal components of the hub are:

- Uyuni-configuration-modules — Salt modules and formulas for deploying and configuring the peripherals.
- HUB-XMLRPC-API — the central endpoint that broadcasts API calls to peripherals.
- Inter-server-sync — a service that synchronizes content to SUSE Manager peripherals through software and configuration channels.

The hub also provides a federation mechanism for reporting by aggregating all peripheral reporting data in a single database.

When to use the hub architecture

The hub architecture is a very efficient and practical solution for large deployments, but keep in mind that it adds a layer of complication that isn't necessary for smaller installations. If your infrastructure has fewer than 10,000 clients, and you don't expect it will grow beyond the 10,000 limit at a later date, you're better off with a single SUSE Manager server configuration, possibly with proxies to add efficiency and speed up package delivery.

If your infrastructure has more than 10,000 managed nodes, the next question is whether your organization will benefit from centralized management. If the organization consists of several different locations that are each managed by separate teams, you are better off maintaining separate servers (as shown in Figure 1). On the other hand, you should use a hub architecture if you have a large deployment of more than 10,000 clients and you stand to benefit from the advantages of centralized management, including:

- Lower staffing overhead (less duplication of effort)
- Uniform configuration
- Uniform security, and
- Secure package delivery across the enterprise

Hub scenarios

When should you use hub architecture? Here are a few common scenarios:

Managed service providers. Typically, the hub architecture is used to manage more than 10,000 endpoints. However, there is an exception. If you are a managed service provider and you need to support a collection of customer networks, the hub architecture should be considered. In this scenario, you can allow each customer a measure of independent control, yet still impose a uniformity for matters that are of concern, such as package updates and configuration management.

Retail environment. The hub configuration is popular for the retail environment because it supports peripherals with proxies serving many locations. This could be an environment with more than 10,000 managed nodes, including a custom combination of peripherals, proxies, Salt minions, and other infrastructure elements.

Large disparate organizations. The hub configuration is a perfect option for any large corporate network spread out across many locations. Introducing hub and peripherals in this scenario will not only maintain consistency but also help to speed up the performance.

See the box entitled “Hub Scenarios” for examples of use cases that commonly employ a hub configuration. Figure 4 shows some of the most common hub topologies at a glance. Peripherals 1 and 2 support a collection of proxies and Salt minions managing client systems across an internal network. Peripheral 3 manages a point-of-service network with multiple retail locations. Interactions of the hub with the peripherals do not require a fast Internet connection. Keep in mind that the hub architecture performs well even in scenarios of slow or bad connectivity.

Peripheral 4 supports a remote network, which could be part of an environment that includes several remote networks all receiving updates and configuration changes through the hub. Remember that there must be a network connection between the hub, peripherals, and endpoints. If the Hub or peripherals cannot communicate with the endpoints, there is no way to apply patches or configuration changes.

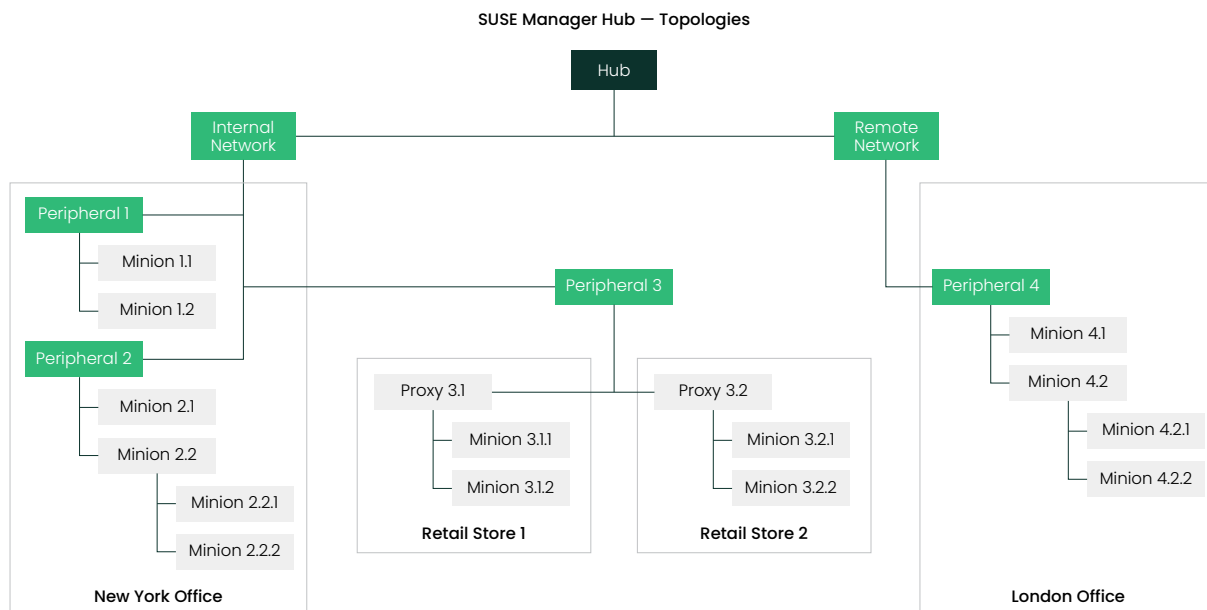


Figure 4: Some common topologies for deploying SUSE Manager in a hub configuration.

Why SUSE Manager?

SUSE Manager comes with a variety of powerful tools for configuration, software channels, auditing, and lifecycle management. SUSE Manager's integration with the Salt automated configuration environment is another important benefit, especially in large deployment scenarios where automation is essential.

You can use SUSE Manager to manage SUSE, RHEL (and its variations), Ubuntu, and many other popular Linux variants. SUSE Manager for Retail supports management of retail point-of-sale devices. A flexible pricing model means that you pay per managed system — users can deploy an additional SUSE Manager server on a managed network without incurring additional software licensing costs.

Conclusion

SUSE Manager is a powerful solution for managing any Linux, anywhere, and at any scale. You can use SUSE Manager to enforce policies, automate configurations, and manage the lifecycle of Linux systems from the server room to the edge and cloud. SUSE is committed to open source solutions that maximize choice, save money, and help you avoid vendor lock-in. If you have a large deployment of more than 10,000 managed nodes and are looking for a centralized and versatile solution with minimal overhead, consider the SUSE Manager hub architecture.

It is a good idea to include SUSE in the planning stages as you begin to envision your large deployment to ensure the most efficient use of available tools and resources. For more on SUSE Manager and the hub architecture for large deployments, visit <https://www.suse.com/products/suse-manager> or talk to your account executive.



SUSE

Maxfeldstrasse 5

90409 Nuremberg

www.suse.com

For more information, contact SUSE at:

+1 800 796 3700 (U.S./Canada)

+49 (0)911-740 53-0 (Worldwide)

Innovate Everywhere

© 2023 SUSE LLC. All Rights Reserved. SUSE and the SUSE logo are registered trademarks of SUSE LLC in the United States and other countries. All third-party trademarks are the property of their respective owners.