

# SUSE

## LINUX ENTERPRISE SERVER – OPTION PACK: SERVER GUARD



# SUSE

## LINUX ENTERPRISE SERVER – OPTION PACK: SERVER GUARD

<b>OVERVIEW</b>	.....	3
<b>AIMS</b>	.....	3
<b>VALUE PROPOSITION</b>	.....	4
<b>FUNCTIONS</b>	.....	4
<b>AUTHENTICATION</b>	.....	5
<b>AUTHORIZATION</b>	.....	5
<b>ACCOUNTING/AUDITING</b>	.....	5
<b>ADMINISTRATION</b>	.....	5

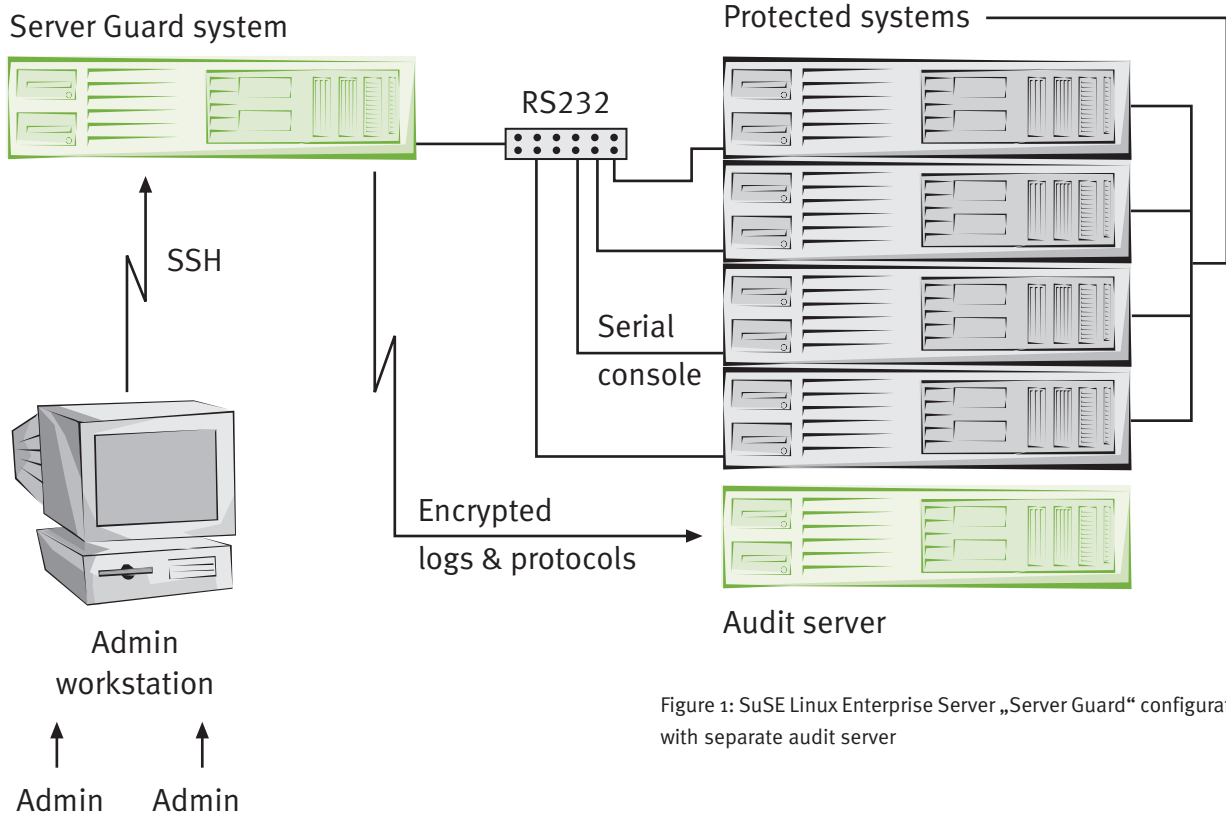


Figure 1: SuSE Linux Enterprise Server „Server Guard“ configuration with separate audit server

## OVERVIEW

The SuSE Linux Enterprise Server option pack “Server Guard” delivers a number of protective mechanisms for the administrative access to highly critical server systems in a controlled environment.

This aim is achieved by means of a specially hardened SuSE Linux Enterprise Server installation on a system placed in front of the servers to be protected. This system features a special software component (the Login Manager) and a number of existing Open Source components for the authentication, authorization, and accounting/auditing. Moreover, configuration guidelines and operating procedures are enclosed for the systems to be protected as well as for the Server Guard system.

## AIMS

The Server Guard system meets the following requirements:

- Single point of access for the systems to be protected
- Logging of all entries of the administrators
- Protection of the log data against unauthorized accessed
- Secure authentication of the administrators
- Authorization procedure for the differentiated access to individual systems
- 4-eyes/n-eyes sign-on
- 4-eyes/n-eyes sign-off
- Encryption of the data connections
- Flexible backend with various methods of access to the systems to be protected

OVERVIEW

## VALUE PROPOSITION

By means of the Server Guard system, the compliance with secure operating procedures for the administration of systems with a need for advanced protection can be ensured without necessitating fundamental changes on the target systems, e.g. for a 4-eyes sign-on procedure. In this way, even heterogeneous environments can be administered securely.

## FUNCTIONS

In order to sign on to a protected system, the administrator first uses SSH<sup>1</sup> (Secure Shell) to establish a connection to one of the technical users on the Server Guard system that is unequivocally associated with the respective system. This procedure guarantees a cryptographically protected communication channel that can be checked on the network level and by means of the deposited key.

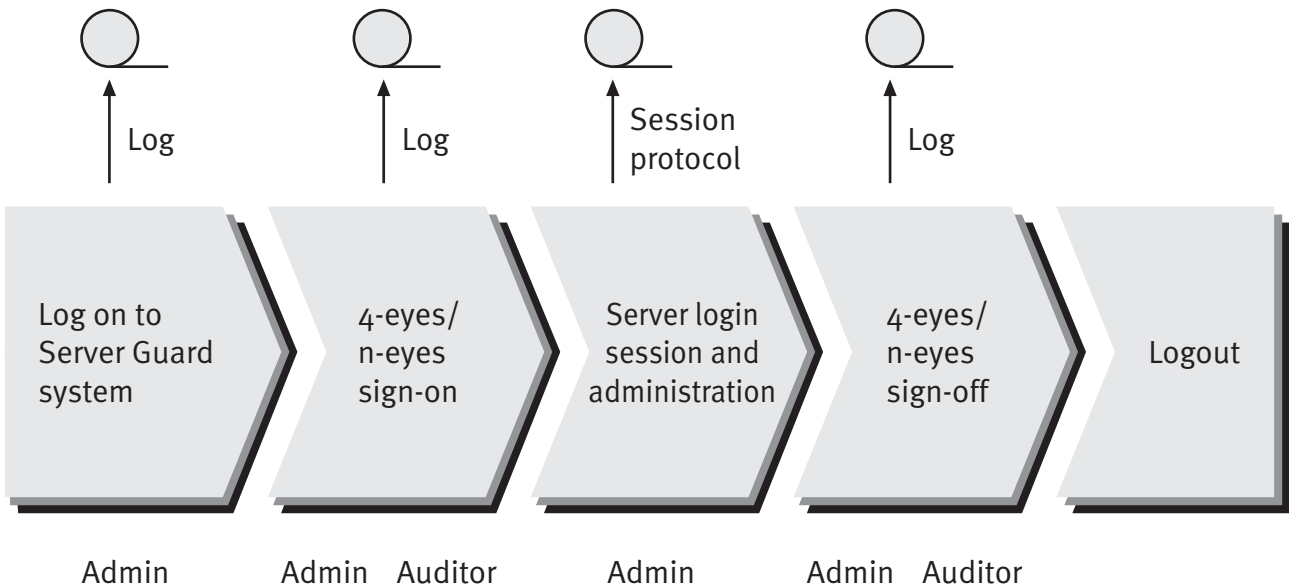


Figure 2: Workflow of the administration supported with SuSE Linux Enterprise Server „Server Guard“

Powerful logging mechanisms support the analysis of errors and security-relevant incidents and help to relieve the administration personnel.

Depending on the measure of protection required by the system, the Login Manager now queries a one or several (for an n-eyes procedure) valid administrator login(s) and password(s). The authorization of the access to the system for this combination of administrators is checked.

Then a connection to the target system is established automatically, usually over the serial line to the system console or optionally by way of an SSH connection. All entries to the target system are logged. A key combination can be pressed to switch to a separate log for the entry of passwords. In this way, the disclosure of server passwords can be prevented.

As soon as the connection to the target system is terminated, the passwords of the involved administrators can be queried once more for the purpose of verifying the presence and control during the entire session.

<sup>1</sup> Secure Shell

The session logs are saved in encrypted form. Additionally, individual connection and authentication attempts are logged with the standard syslog mechanism.

## AUTHENTICATION

Administrators are authenticated by means of the PAM<sup>2</sup> (Pluggable Authentication Modules) interface, a modular authentication mechanism integrated in Linux. Normal user passwords or separate administration passwords can be used. The authentication can be based on the standard Linux system files or on mechanisms such as Kerberos or UserDB.

## AUTHORIZATION

The authorization for the access to certain protected servers can be configured for the individual administrators. The necessity of a 4-eyes or n-eyes authorization can also be set for the individual administrators within a group concept. For example, the sign-on can be configured for two administrators from a specific group or from two different groups.

In order to make sure that the multilateral control continued throughout the entire session, the authentication of the administrators who signed on when the connection was established can be checked anew.

## ACCOUNTING/AUDITING

Every login attempt is logged in detail by the syslog system. The session logs are saved in their entirety and encrypted with a public key procedure for which the private key is not deposited on the Server Guard system. In this way, unauthorized access to the logs is prevented even if the system is breached.

The evaluation of the logs can be performed by means of the enclosed tools which merely need to be customized by the auditor. Thus, reports and protocols can be prepared in a flexible way according to local requirements.

Manipulation of the logs can be prevented even more reliably by immediately forwarding the encrypted data to another system.

## ADMINISTRATION

The use of PAM enables the management of the administrators with standard procedures. The Login Manager is adapted to the local operating procedures and security regulations by means of a separate configuration file.

The configuration file is a simple XML file that can be marked with a cryptographic signature which is checked and logged at every sign-on.

<sup>2</sup> Pluggable Authentication Modules

© SuSE Linux AG 2003

Linux is a registered trademark of Linus Torvalds.

UNIX is a registered trademark of The Open Group.

All other company, product, and service names or designations may be trademarks or service marks or registered trademarks or service marks of other companies around the world and shall be treated as such.