SUSE

SUSE Linux Enterprise Server code stream 15

Payment Card Industry Data Security Standard (PCI DSS) Guide

To protect customers and the business itself, companies that handle credit card payments must keep data as safe and secure as possible. Following the Payment Card Industry Data Security Standard helps to secure all areas that are connected to payment processes, and to implement security-relevant actions to keep the data and the computing environment safe.

Publication Date: December 05, 2024

Contents

This document aims to provide a basic understanding of how SUSE Linux Enterprise Server can be configured to comply with the Payment Card Industry Data Security Standard.

It is important to understand that protecting systems includes more than configuration. The entire environment and people involved must be taken into account.

An essential part of implementing PCI DSS is the combination of actions:

1. Create a secure configuration.
2. Track and review all changes made to the configuration: who changed what at which point in time.

Important: PCI DSS Disclaimer

SUSE seeks to provide our customers with quick and easy guides that can assist them in maintaining security compliance. Implementation of the settings contained within this guide without its prior testing in a non-operational environment is highly discouraged. The developers of these profiles and documentation have made reasonable efforts to ensure overall compliance. They assume no responsibility for its use by other parties, and make no guarantee, expressed or implied, about its quality, reliability, or any other characteristic.

1 What is the PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements to guide a merchant to protect cardholder data. The standard covers six main categories with currently 12 requirement topics on how to implement, protect, maintain and monitor systems that are involved in credit cardholder data processing.

PCI DSS was created and is maintained by the PCI Security Standards Council (SSC), which was founded by the five major credit card brands, Visa, MasterCard, American Express, Discover, and JCB. In December 2004, PCI DSS 1.0 was released to address the growing threat of online credit card fraud. The current version, PCI DSS version 4.0, has been available since March 2022.

BUILD AND MAINTAIN A SECURE NETWORK AND SYSTEMS

1. *Section 3.1, "Requirement 1: Install and maintain a firewall configuration to protect cardholder data"*
2. *Section 3.2, "Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters"*

PROTECT CARDHOLDER DATA

3. *Section 3.3, "Requirement 3: Protect stored cardholder data"*
4. *Section 3.4, "Requirement 4: Encrypt transmission of cardholder data across open, public networks"*

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

5. *Section 3.5, "Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs"*
6. *Section 3.6, "Requirement 6: Develop and maintain secure systems and applications"*

IMPLEMENT STRONG ACCESS CONTROL MEASURES

7. *Section 3.7, "Requirement 7: Restrict access to cardholder data by business need to know"*
8. *Section 3.8, "Requirement 8: Identify and authenticate access to system components"*
9. *Section 3.9, "Requirement 9: Restrict physical access to cardholder data"*

REGULARLY MONITOR AND TEST NETWORKS

10. *Section 3.10, "Requirement 10: Track and monitor all access to network resources and cardholder data"*
11. *Section 3.11, "Requirement 11: Regularly test security systems and processes"*

MAINTAIN AN INFORMATION SECURITY POLICY

12. *Section 3.12, "Requirement 12: Maintain a policy that addresses information security for all personnel"*

Most requirements of PCI DSS are organizational guidelines that help ensure the security of all areas involved with cardholder data. There is usually no specific wording of the technical aspects.

This means that it is up to auditors to decide which security settings are valid for a requirement and which are not. Therefore, the recommendations in this document can only provide a starting point for implementing the PCI DSS and are necessarily subject to discussion.

2 Focus of this document: areas relevant to the operating system

The PCI DSS covers a wide range of aspects related to cardholder data. Not all of these aspects concern the operating system and this document will not focus on these. Instead, this document focuses on aspects that affect OS configuration, including:

- System security
- Access control
- System maintenance to protect against known vulnerabilities

Topics beyond the scope of this document include data processing applications, database design, and formal processes outside of the OS scope. In particular, requirement 9 (restrict physical access) and requirement 12 (maintain a policy) are not discussed extensively in this document.

3 Requirements in detail

The following section provides an overview of the relevant parts of the PCI DSS, following the ordering of the standard itself.

3.1 Requirement 1: Install and maintain a firewall configuration to protect cardholder data

The listed terms in this section are mostly design, documentation, and formal process requirements. All changes to the firewalls and routers need to be approved, documented, and verified, and all stakeholders need to be involved. The network design includes a DMZ environment, access to the Internet, a protected network for database servers, traffic filtering rules between network segments, and other relevant considerations.

In addition to a dedicated firewall and router, SUSE Linux Enterprise Server comes with a host firewall based on iptables. The system can be configured to allow only connections on certain inbound ports. With the YaST firewall module it is also possible to define more complex rules, such as refusing connections from specific addresses. This allows integrating the local system firewall into an overall firewall design that maximizes network security.

In generalized terms, the technical points in requirement 1 are the following:

- Identify insecure services and protocols.
- Limit traffic to and from the system so that unwanted traffic is not allowed.

1.1.6.b Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service

This task is embedded in the requirement to identify, document, and justify all services and protocols running on a system. Of special interest are services and protocols that could lead to a security risk. If an insecure service or protocol is used, it must be evaluated to understand its potential security impact. Services or protocols that are not necessary for the business to function should be disabled or removed.

1.2.1.b Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment.

Outbound traffic should only be allowed in specifically defined cases. Create rules for allowed outbound traffic.

Make the SSH daemon only reachable on a separate administration interface, and not on the general network interface if possible. Define the source addresses that a service allows traffic from.

For example, to allow only outbound DNS requests over the interface `eth0` to server `10.0.0.1`, use:

```
> sudo firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 23 \
    -d 10.0.0.1/32 -o eth0 -p udp -m udp --dport 53 -j ACCEPT
> sudo firewall-cmd --reload
```

To block all other outbound traffic, see *1.2.1.c Verify that all other inbound and outbound traffic is specifically denied.* .

1.2.1.c Verify that all other inbound and outbound traffic is specifically denied.

Deny all outbound and inbound traffic for which no exceptions are defined as stated in the previous section. Forwarding is usually completely disabled by a kernel parameter, and should not be enabled for endpoint servers.

`firewalld` in by default blocks all inbound traffic.

To block all outbound traffic, manually add the following rules:

```
> sudo firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -m
 conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
```

```
> sudo firewall-cmd --permanent --direct --add-rule ipv6 filter OUTPUT 0 -m
 conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
> sudo firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 99 -j DROP
> sudo firewall-cmd --permanent --direct --add-rule ipv6 filter OUTPUT 99 -j DROP
> sudo firewall-cmd --reload
```

In addition, inbound traffic can also be configured for specific services via the TCP wrapper configuration file `/etc/hosts.deny`.

Most of the following tasks are about examining and verifying that the defined inbound and outbound rules are really limiting the traffic between and within all network segments, like the DMZ and the Internet, to a necessary minimum for full system operation.

1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.

There are two ways to implement anti-spoofing measurements in SUSE Linux Enterprise Server:

- **`iptables` rules that only allow input from certain addresses on specified interfaces.** The used address space for communications can be clearly defined in the system setup. Any use of addresses that violates these definitions can be logged and trigger an alarm.
- **Linux kernel reverse path filtering.** This feature discards packet replies that do not go through the same interface as the initial packet. This feature is enabled by default in SUSE Linux Enterprise Server and can be checked with the following command:

  ```
  > cat /proc/sys/net/ipv4/conf/all/rp_filter
  ```

  When enabled, this returns `1`.

1.3.5 Permit only “established” connections into the network.

`firewalld` enables connection tracking via `iptables`. Connections to an interface that has been marked as external are dropped by default. Only connections that are associated with an established connection are allowed.

It is possible to define certain services that are allowed to connect to an external interface. However, this must be in compliance with the general security policy.

Keep in mind that the first line of defense against malicious connections from the Internet should be a dedicated firewall system that handles all traffic and acts as a gatekeeper. Unwanted connections should never reach the DMZ network. However, simple firewall rules on SUSE Linux Enterprise Server systems can help avoid misconfigurations and act as another line of defense.

1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.

A SUSE Linux Enterprise Server system can also act as a router to forward traffic from one interface to another network on a second interface. It is possible to use Network Address Translation (NAT) on the external interface so that no internal IP address is actually exposed to the outside. This is done to mitigate the information an external attacker can gather by simply analyzing the network traffic. NAT can also be used on virtualization hosts or container-based environments that connect to the outside via a specific interface.

3.2 Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

During the installation of SUSE Linux Enterprise Server, general system passwords are already set by the administrator. The setup also uses a password checker (**`cracklib`**) that identifies weak entries against a dictionary. This means that the standard configuration already includes customer-defined security options for most services.

For more information about OS security, see the *SUSE Linux Enterprise Server Security Guide*.

2.1 Always change vendor-supplied defaults, and remove or disable unnecessary default accounts before installing a system on the network.

The configuration of any system service must be evaluated to meet the needed security standards. This goes from limiting the used protocols to only allow currently secure versions and to disable legacy implementations, to the definition of access controls and authentication. The default settings of SUSE Linux Enterprise Server already provide good overall security, but they can be tweaked further.

For example, the following security settings might be relevant:

- By default, the SNMP daemon only allows incoming requests to `localhost`. However, the default community string is named `public` and should be changed before accepting general inbound connections.

- By default, certain insecure upstream settings of the `sshd` daemon are listed and commented out inside the `sshd` configuration file `/etc/ssh/sshd_config`. For example, the insecure protocol version 1 and empty passwords (`PermitEmptyPasswords no`) are already disabled.

  To further increase SSH security, if applicable, deny direct `root` access by setting `PermitRootLogin` to `no`.

Default settings can be customized by automating system installation with an AutoYaST profile. This allows rolling out new instances of SUSE Linux Enterprise Server and automatically enabling an evaluated configuration. This setup procedure can also be automated with the SUSE Manager. For more information, see the SUSE Manager documentation at https://documentation.suse.com/suma/.

By default, SUSE Linux Enterprise Server does not create additional accounts apart from the `root` administrative user. There are system accounts defined in `/etc/passwd`, but they are not activated and therefore not directly reachable. This can be validated by checking the lines inside the `/etc/shadow` file.

In `/etc/shadow`, the second column represents the defined password:

- An asterisk (`*`) means that a password was never defined and the account is therefore locked.
- An exclamation mark (`!`) stands for a locked account and can appear either alone or in front of a password hash.

2.2 Develop configuration standards for all system components. Ensure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

As mentioned in the PCI DSS document, possible sources for industry-accepted hardening standards are:

1. Center for Internet Security (CIS)
2. International Organization for Standardization (ISO)
3. SysAdmin Audit Network Security (SANS) Institute
4. National Institute of Standards Technology (NIST)

As the PCI DSS requirements are not specified precisely, there is no direct relationship between hardening standards and specific requirements. However, other hardening resources can also help in complying with these specifications, including the *SUSE Linux Enterprise Server Security Guide*.

2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)

To help separate services, use the variety of virtualization and containerization methods included with SUSE Linux Enterprise Server: KVM, Xen, LXC, and Docker.

You can also run SUSE Linux Enterprise Server on third-party virtualization servers like VMware ESX or Microsoft Hyper-V to achieve service separation.
When using the options built in to SUSE Linux Enterprise Server, see:

- For information about virtualization, see *SUSE Linux Enterprise Server Virtualization Guide*.
- For information about containerization, see *SUSE Linux Enterprise Server Docker Open Source Engine Guide*.

2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.

This is directly related to an item of requirement 1: To allow only services that are really needed and are using secure protocols and settings (*1.1.6.b Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service*). All parties involved must be aware of the dangers of using insecure communication. Research, clearly document, and communicate the risk of using insecure protocols and services.
Enable and disable system services using the following **`systemctl`** commands:

- `> systemctl status SERVICE`
- `> sudo systemctl enable SERVICE`
- `> sudo systemctl disable SERVICE`

To list all available services that are installed on the system and see their status, use the following command:

```
> systemctl list-unit-files --type=service
```

2.2.3.a Inspect configuration settings to verify that security features are documented and implemented for all insecure services, daemons, or protocols.

To add an additional layer of security to insecure services, use VPN tunnels (for example, IPsec). With a VPN tunnel, network traffic of such services can be isolated and all data is protected against eavesdropping, both internally and externally. However, note that the communication is still insecure at the endpoints of the VPN tunnel and that this is only a workaround.

For additional security within SUSE Linux Enterprise Server, use SELinux or AppArmor. However, the setup of these frameworks is beyond the scope of this document:

- For information about SELinux, see *SUSE Linux Enterprise Server Security Guide, Chapter Configuring SELinux*.
- For information about AppArmor, see *SUSE Linux Enterprise Server Security Guide, Part Confining Privileges with AppArmor*.

2.2.5.a Select a sample of system components and inspect the configurations to verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.

The Linux kernel is the main system component. It consists of a core image that is extended by kernel modules which are loaded depending on the hardware and system design. For example: Network card drivers are automatically loaded depending on the system's network card. File system modules can be enabled to extend the Linux kernel's file system support.

The list of loaded kernel modules is usually quite long and includes modules that are only used occasionally. The kernel module framework allows blacklisting modules and limiting which functionalities are loaded.

To block modules from being loaded, configure them via the directory `/etc/modprobe.d`. For example, the kernel module `floppy` is only necessary for systems that have a floppy drive. On systems that do not have a floppy drive, prevent the module from loading: Create a configuration file `/etc/modprobe.d/00-disable-modules.conf` with the following content:

```
install floppy /bin/true
```

The `floppy` module is usually loaded during the execution of the initial RAM disk. Therefore, propagate this configuration change to the `initrd` file using **`dracut`** (replace *`NAME`* with the name of the current initrd and *`KERNELVERSION`* with the currently running kernel).

```
> sudo /usr/bin/dracut --logfile /var/log/YaST2/mkinitrd.log --force /boot/
$initrd-NAME $KERNELVERSION
```

It is harder to remove or restrict application functionality, as functionality is in most cases compiled into the application or library itself. Even cases where deleting a file cleanly removes a functionality are problematic: If the file was installed from an RPM package, it will be reinstalled when the package is updated.

2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.

Encrypt all administrative network access: SSH with appropriate configuration settings that fit into the security concept should be the tool of choice.

Administrative access can also be granted via a Web site. In this case, the complete connection chain between the browser and the server system must be encrypted. This is done via TLS and X.509 certificates.

3.3 Requirement 3: Protect stored cardholder data

This section explains how to handle cardholder and authentication data securely. The following definitions apply:

- *Cardholder data* includes information such as the cardholder name and the Primary Account Number (PAN).
- *Authentication data* includes the Personal Identification Number (PIN) and the Card Validation Code (CVC2).

The main difference between cardholder data and authentication data is that storing authentication is never allowed. In contrast, data such as the PAN can be stored, but must be encrypted and unreadable in case an attacker gains access to the stored data.

The database design for storing cardholder data is beyond the scope of this document. However, data can be encrypted in different ways:

- The DBMS can use column-level encryption inside the database scheme.
- Alternatively, the database files can be encrypted.
- SUSE Linux Enterprise Server supports full-disk encryption, so that the whole database storage is always encrypted. However, access to an encrypted disk works the same way as to a non-encrypted disk. This is discussed in more detail in requirement 3.4.1.

3.4.1.a If disk encryption is used, inspect the configuration and observe the authentication process to verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating system's authentication mechanism (for example, not using local user account databases or general network login credentials).

The guidance description of the PCI DSS document says the following about this requirement: "Full disk encryption helps to protect data in the event of physical loss of a disk and therefore may be appropriate for portable devices that store cardholder data."

From an administrator's point of view, a block device encryption with the Linux Unified Key Setup (LUKS)/dm-crypt offers an abstraction layer that allows the usage of encrypted disks in the same way as unencrypted disks.

Therefore, access control can only be limited with the general ACL permissions that the file system offers. To comply with this requirement, the decryption key used must not be associated with any general login credentials or authentication methods.

When using LUKS, this is usually fulfilled: The password needs to be entered separately when booting, inserting portable devices or manually mounting disks.

LUKS is fully integrated into SUSE Linux Enterprise Server and can be used via YaST to create new partitions.

3.4.1.c Examine the configurations and observe the processes to verify that cardholder data on removable media is encrypted wherever stored.

As described in *3.4.1.a If disk encryption is used, inspect the configuration and observe the authentication process to verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating system's authentication mechanism (for example, not using local user account databases or general network login credentials).* , LUKS/dm-crypt provides full-disk encryption that fulfills this requirement. Access to the stored data is only possible via a decryption password that must be entered when the disk is mounted.

3.4 Requirement 4: Encrypt transmission of cardholder data across open, public networks

Cardholder data must be encrypted during transmissions over insecure networks. Ideally, encrypt all traffic, externally and internally. This makes it hard for attackers to gain inside information and privileged access to the cardholder data environment.

4.1 Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: (1) Only trusted keys and certificates are accepted, (2) The protocol in use only supports secure versions or configurations, (3) The encryption strength is appropriate for the encryption methodology in use.

Any connection that transmits sensitive information must be protected against eavesdropping and tampering.

For incoming client requests, use the HTTPS protocol with a secure TLS connection. The authentication is done with a public X.509 certificate that proves to a certain level that the server is the right endpoint the customer is looking for.

SUSE Linux Enterprise Server comes with a set of services and tools that allow protected HTTPS connections. For example, this can be done directly with the Apache HTTP Server or via `stunnel`, which functions as a proxy to offer TLS encryption functionality.

IPsec or other VPN technologies can be used for securing the connection between network segments that are connected via a public network. Such connections can also be secured with a public X.509 certificate. For internal usage, it is possible to use a private Certificate Authority (CA) to sign X.509 certificates and to keep track of trusted keys.

In SUSE Linux Enterprise Server, this can be established directly with strongSwan, which is a IPsec-based VPN solution, or with OpenVPN, which uses a custom security protocol.

To administrate the OS, use SSH. For information about configuring SSH to provide better security, see *Section 3.1, "Requirement 1: Install and maintain a firewall configuration to protect cardholder data"* and *Section 3.2, "Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters"*.

3.5 Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

For PCI DSS compliance, it is necessary to protect against malicious software. Third-party anti-virus software is available from the major anti-virus software vendors and can be integrated into the Linux environment. SUSE Linux Enterprise Server comes with the open source anti-virus engine ClamAV.

ClamAV has a limited set of scanning capabilities and limited performance compared to third-party products. Hence, expect ClamAV to only provide basic protection.

On the other hand, ClamAV is shipped with SUSE Linux Enterprise Server and it can be included during server installation. This makes it easy to fulfill this requirement, but the drawbacks compared to third-party products need to be clearly understood.

3.6 Requirement 6: Develop and maintain secure systems and applications

The major part of this requirement concerns in-house software development, documentation, and design questions that are beyond the scope of this document. However, SUSE Linux Enterprise Server provides tools that help keep your systems safe:

- The software package manager Zypper is a powerful instrument of SUSE Linux Enterprise Server. Among other things, it resolves dependencies of packages, products, patterns, and patches, has a locking mechanism to prevent package installation, and provides a complete update stack to keep the system up-to-date and protected against known security issues.
  `zypper` is part of any SUSE Linux Enterprise Server installation and has direct access to the update repositories after system registration.
  For information about Zypper, see *SUSE Linux Enterprise Server Administration Guide, Chapter Managing Software with Command Line Tools, Section Using Zypper*.

- For system management, SUSE provides SUSE Manager, which provides an efficient way to keep systems up-to-date. It offers seamless management of both SUSE Linux Enterprise Server and Red Hat Enterprise Linux client systems. This is particularly useful in larger system environments, when you need to check the current update status of each system and to react to known security risks.
  For information about SUSE Manager, see the SUSE Manager documentation page (https://documentation.suse.com/suma/).

6.2.a Examine policies and procedures related to security patch installation to verify processes are defined for: (1) Installation of applicable critical vendor-supplied security patches within one month of release, (2) Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months).

To identify patches that need to be installed to secure your system, do the following:
First, refresh all software repositories, so you have up-to-date information:

```
> sudo zypper refresh
```

Then use the patch-related commands of Zypper:

- Search for important security fixes that have not yet been installed:

```
> zypper list-patches --category security --severity important
```

- It is also possible to search for CVE or SUSE Bugzilla numbers. By default, only necessary patches are listed by this command. To also show patches that have already been installed, use the parameter `--all`:

```
> zypper list-patches --all --cve=CVE-2016-4957
```

- To list details of individual patches, use the **`patch-info`** subcommand:

```
> zypper patch-info SUSE-SLE-Product-SLES-15-SP3-2021-2126
```

- To install only important security patches, use the **`patch`** subcommand:

```
> sudo zypper patch --category security --severity important
```

To perform updates automatically, the parameter `--non-interactive`, which is supported by all Zypper subcommands, is helpful.
For more information about Zypper, see *SUSE Linux Enterprise Server Administration Guide, Chapter Managing Software with Command Line Tools, Section Using Zypper*.

3.7 Requirement 7: Restrict access to cardholder data by business need to know

OS access control is a complex topic. Again, this PCI DSS requirement is not specified precisely and does not specifically state to what degree the restrictions need to be implemented. SUSE Linux Enterprise Server comes with all general Linux tools to limit and restrict access to certain system areas and components:

- Access can be controlled via specific users and groups of users by using the traditional Unix permission settings.

For information about managing permissions, see *SUSE Linux Enterprise Server Security Guide, Chapter Access Control Lists in Linux*.

- A more flexible mechanism for file systems are Access Control Lists (ACLs), which offer a more granular approach. SELinux can be used for maximum system separation and to prevent processes from gaining more resources and access than allowed. SELinux and AppArmor are beyond the scope of this document but should be employed to protect critical systems that are likely to be targeted.

  - For information about SELinux, see *SUSE Linux Enterprise Server Security Guide, Chapter Configuring SELinux*.
  - For information about AppArmor, see *SUSE Linux Enterprise Server Security Guide, Part Confining Privileges with AppArmor*.

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

The standard Unix permissions allow setting Read, Write, and Execution flags for user and group IDs. A general group called `others` or `world` defines the access for users that do not fit into the first two groups. This provides a straightforward way to grant or deny access to file system resources.

ACLs provide an extra level of restrictions. It is possible to set read-write access for one user ID and only read access for a second one. The same goes for group IDs.

The commands **`getfacl`** and **`setfacl`** (on SUSE Linux Enterprise Server shipped with the package `acl`) allow direct modification of file system resources. For example, to check and set ACL restrictions of the file `/tmp/test.txt` for the user `wilber`:

```
> getfacl /tmp/test.txt
# file: /tmp/test.txt
# owner: tux
# group: users
user::r--
group::r--
other::r--

> setfacl -m "u:wilber:rw" /tmp/test.txt

> getfacl /tmp/test.txt
# file: /tmp/test.txt
# owner: tux
# group: users
user::rw-
```

```
user:wilber:r--
group::r--
mask::r--
other::r--
```

Standard Unix permissions include the so-called Sticky Bit. This allows the execution of certain programs with higher privileges than the user who is executing those programs. The best example of this is the **`passwd`** tool, which needs to modify `/etc/shadow` to change the user password.

For a more gradual approach to explicitly allowing certain operations or behaviors to binaries, use extended capabilities. As an example of a command that uses extended capabilities by default, consider **`ping`** (from the package `iputils`).

`ping` sends ICMP IP packets over the network card. To do so, it needs the `CAP_NET_RAW` capability to be Effective and Permitted (`+ep`):

```
> sudo getcap /usr/bin/ping
/usr/bin/ping = cap_net_raw+ep
```

Login access control to the system can be managed using Pluggable Authentication Modules (PAM). There are several modules available in SUSE Linux Enterprise Server that allow setups such as logging the login time, multiple authentication mechanisms, and central databases like NIS, LDAP, or Active Directory.

For more information about managing permissions, see *SUSE Linux Enterprise Server Security Guide, Chapter Access Control Lists in Linux*.

3.8 Requirement 8: Identify and authenticate access to system components

Ideally, use a central database with user information and a unique identifier (UID) to grant or deny access to certain system components. This makes it easy to give administrators special access to a group of servers or a database engineer permission for a certain DBMS system.

On a stand-alone server, unique identifiers are managed via the standard Linux user and group IDs. These are listed in `/etc/passwd` and `/etc/group`.

8.1.4 Remove/disable inactive user accounts within 90 days.

In this context, there are many advantages to using a centralized infrastructure for user accounts like NIS, LDAP, or Active Directory:

- It is easy to identify and automatically disable inactive accounts.
- User accounts only need to be disabled in one place. After their access is revoked, the user cannot use any service that relies on the centralized account infrastructure.

However, if you are using local accounts, these can be checked for inactivity when a user is logging in. This module checks the last login time recorded in `/var/log/lastlog` and calculates the number of days since. By default, access is denied when the inactivity reaches 90 days.
To list the local account's last login time use the command **`lastlog`**.

8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.

As stated in *8.1.4 Remove/disable inactive user accounts within 90 days.*, a centralized account infrastructure will have this capability. On SUSE Linux Enterprise Server systems, access attempts can be checked and limited with the `pam_tally2` PAM module. The module is executed during login time and checks the recorded failed attempts since the last successful login. To check and reset the account status, use the tool **`pam_tally2`**.

8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

The PAM module `pam_tally2` described in *8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.* can be used to lock an account for a given time after a failed login attempt. The parameter `unlock_time=1800` must be specified in the PAM configuration. By default, only the administrator can reactivate a locked account.

8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.

To authenticate users for administrative access with multiple factors, use the following methods:

- Use Pluggable Authentication Modules (PAM): This increases flexibility when adding new methods to the authentication process and when adjusting it.
  For third-party one-time password (OTP) products, there is usually also a Linux PAM module available.

For information about PAM, see *SUSE Linux Enterprise Server Security Guide, Chapter Authentication with PAM*.

- To add multi-factor authentication for SSH connections, mandate use of public keys in addition to passwords.

  To connect to a system, it is then necessary to prove possession of an appropriate private key. At the second stage, you then enter a password. This means attackers need to acquire a private key before they can even try to brute-force a password prompt.

8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.

For details, see *8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.* .

3.9 Requirement 9: Restrict physical access to cardholder data

Physical access to systems that are involved in processing cardholder data are not within the scope of general operating system security. Appropriate facility entry controls must be in place to allow on-site personnel and visitors to access systems directly.

3.10 Requirement 10: Track and monitor all access to network resources and cardholder data

To track user activities, it is important to have a synchronized time reference. This is done via the NTP protocol, which allows servers to keep their local time in synchronization with a central system. The central NTP server inside the cardholder data environment (CDE) should not rely on external connections to the Internet to update the system time. Alternatively, system time can be updated using DCF77 radio transmissions or a GPS receiver.

A synchronized time reference makes it easier to correlate events inside recorded log files. This reference can include general system log entries collected by a central system log server or kernel audit messages by the daemon `audit`.

For information about auditing, see *SUSE Linux Enterprise Server, Security Guide, Part The Linux Audit Framework*.

All auditing requirements from this section can be fulfilled by defining centrally stored auditing rules.

3.11 Requirement 11: Regularly test security systems and processes

Testing the discussed security mechanisms is also a key requirement for PCI DSS. Evaluating the configurations and testing logging mechanisms can protect against known security risks and ensure that essential information is available to identify possible security breaches. Testing capabilities should be considered during system design, before installation and deployment.

To keep track of system integrity, SUSE Linux Enterprise Server comes with the Advanced Intrusion Detection Environment (AIDE). AIDE creates a hash value database of all relevant OS files. After initialization, it can be used to verify the integrity of all previously saved files. To employ AIDE, it is best to regularly create database snapshots and save them to a central system on which you can evaluate possible modifications.

For more information about AIDE, see *SUSE Linux Enterprise Server Security Guide, Chapter Intrusion Detection with AIDE*.

3.12 Requirement 12: Maintain a policy that addresses information security for all personnel

Any organization that handles valuable information should have a general security policy. All relevant aspects should be included to make it clear for employees and stakeholders what the possible risks are and how to avoid them.

All security policies should also be evaluated regularly and adjusted to keep the protection level as high as possible.

4 Legal notice

GNU Free Documentation License

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See https://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.