SUSE

SUSE Linux Enterprise Server code stream 15

支付卡行业数据安全标准 (PCI DSS) 指南

为了保护客户和企业自身，处理信用卡付款的公司必须尽最大努力确保数据安全无虞。遵循支付卡行业数据安全标准有助于保护与付款流程相关的所有方面，以及实施安全相关的措施来确保数据和计算环境的安全。

出版日期：2024 年 9 月 29 日

目录

本文档旨在帮助您基本了解如何配置 SUSE Linux Enterprise Server，以符合支付卡行业数据安全标准。

请务必注意，保护系统的工作不仅涉及到配置，还要考虑到相关的整个环境和所有人员。

实施 PCI DSS 的一个重要组成部分是各种操作的组合：

1. 创建安全配置。
2. 跟踪并审查对配置进行的所有更改：谁在哪个时间点更改了什么配置。

重要：PCI DSS 免责声明

SUSE 力求为我们的客户提供快速简便的指南，以帮助他们保持安全合规性。如果未事先在非操作环境中进行测试，则强烈建议您实施本指南中包含的设置。这些配置文件和文档的开发人员已做出合理的努力来确保整体合规性。这些开发人员对其他方的使用不承担任何责任，也不对其质量、可靠性或任何其他特性做出任何明示或暗示的保证。

1 什么是 PCI DSS?

支付卡行业数据安全标准 (PCI DSS) 是指导商家保护持卡人数据的一套要求。该标准涵盖当前涉及 12 个要求主题的六个主要类别，规定如何实施、保护、维护和监控在信用卡持卡人数据处理中所涉及的系统。

PCI DSS 由 PCI 安全标准理事会 (SSC) 制定和维护，该理事会由 Visa、MasterCard、American Express、Discover 和 JCB 五大信用卡机构创立。2004 年 12 月发布了 PCI DSS 1.0，目的是解决日益猖獗的在线信用卡欺诈威胁。最新版本 PCI DSS 4.0 发布于 2022 年 3 月。

构建和维护安全网络与系统

1. 第 3.1 节 “要求 1：安装并维护防火墙配置以保护持卡人数据”
2. 第 3.2 节 “要求 2：不要使用供应商为系统口令和其他安全参数提供的默认值”

保护持卡人数据

3. 第 3.3 节 “要求 3：保护存储的持卡人数据”
4. 第 3.4 节 “要求 4：对在开放的公共网络上传输的持卡人数据进行加密”

维护漏洞管理程序

5. 第 3.5 节 “要求 5：保护所有系统免遭恶意软件的攻击，并定期更新防病毒软件或程序”
6. 第 3.6 节 “要求 6：开发并维护安全系统和应用程序”

实施严格的访问控制措施

7. 第 3.7 节 “要求 7：限制企业仅可访问其需要知道的持卡人数据”
8. 第 3.8 节 “要求 8：识别并验证对系统组件的访问”
9. 第 3.9 节 “要求 9：限制对持卡人数据的物理访问”

定期监控和测试网络

10. 第 3.10 节 “要求 10：跟踪并监控对网络资源和持卡人数据的所有访问”
11. 第 3.11 节 “要求 11：定期测试安全系统和流程”

维护信息安全策略

12. 第 3.12 节 “要求 12：维护用于处理所有个人信息安全性的策略”

PCI DSS 的大多数要求都是针对组织的指导原则，可帮助确保涉及持卡人数据的方方面面的安全性。对于技术方面，通常不会使用具体的措辞。

这意味着，需要由审计人员确定哪些安全性设置符合要求，哪些不符合要求。因此，本文档中的建议只能为实施 PCI DSS 提供着手点，需要进一步探讨。

2 本文档的重点：与操作系统相关的方面

PCI DSS 中的许多方面都与持卡人数据相关。其中并非所有方面都与操作系统相关，本文档不会着重说明这些不相关的方面，而是重点介绍影响操作系统配置的方面，包括：

- 系统安全性
- 访问控制
- 旨在防范已知漏洞的系统维护

以下主题不在本文档的范畴内：数据处理应用程序、数据库设计，以及不属于操作系统范围的正式流程。具体而言，本文档不会详细讨论要求 9（限制物理访问）和要求 12（维护策略）。

3 要求详细说明

下面的章节按照标准本身的顺序对 PCI DSS 的相关部分进行了概述。

3.1 要求 1：安装并维护防火墙配置以保护持卡人数据

本节列出的条款主要是设计、文档和正式流程方面的要求。对防火墙和路由器进行的所有更改均需经过审批、书面记录和校验，并且需要知会所有利益相关者。网络设计包括 DMZ 环境、互联网访问、受保护的数据库服务器网络、网段之间的流量过滤规则以及其他相关考虑因素。

除了专用的防火墙和路由器以外，SUSE Linux Enterprise Server 还随附了基于 iptables 的主机防火墙。可以将系统配置为仅允许特定入站端口上的连接通过。使用 YaST 防火墙模块，还可以定义更复杂的规则，例如拒绝来自特定地址的连接。这样便可以将本地系统防火墙整合到一个能够最大限度提高网络安全性的总体防火墙设计中。

概括而言，要求 1 中的技术要点如下：

- 识别不安全的服务和协议。
- 限制出入系统的流量，以便阻止不需要的流量。

1.1.6.b 识别允许的不安全服务、协议和端口；校验是否书面记录了每项服务的安全功能

此任务蕴含在有关识别、记录系统上运行的所有服务和协议并证明其合理性的要求中。需要特殊关注可能导致安全风险的服务和协议。如果使用不安全的服务或协议，必须对其进行评估，以了解它的潜在安全影响。应该禁用或去除业务运营中不必要的服务或协议。

1.2.1.b 校验入站和出站流量是否限制为持卡人数据环境中所必需的流量。

应该仅在具体指明的情形中允许出站流量。创建针对允许的出站流量的规则。

在可能的情况下，将 SSH 守护程序限制为只能通过单独的管理接口访问，而不能通过一般的网络接口访问。定义服务允许的流量来源地址。

例如，要仅允许出站 DNS 请求通过接口 `eth0` 发往服务器 `10.0.0.1`，请使用：

```
> 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
```

要阻止所有其他出站流量，请参见 1.2.1.c 校验是否明确拒绝所有其他入站和出站流量。

1.2.1.c 校验是否明确拒绝所有其他入站和出站流量。

拒绝未根据上一节中所述定义其例外情况的所有出站和入站流量。转发通常已通过某个内核参数完全禁用，且不应对端点服务器启用。

中的 `firewalld` 默认会阻止所有入站流量。

要阻止所有出站流量，请手动添加以下规则：

```
> 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
```

此外，还可以通过 TCP 封装程序配置文件 `/etc/hosts.deny` 为特定的服务配置入站流量。

下面的大多数任务涉及到如下事项：检查并校验定义的入站和出站规则是否真正将所有网段（例如 DMZ 和互联网）之间及其内部的流量限制为整个系统能够正常运行所需的最小必要程度。

1.3.3 实施防假冒措施来检测并阻止伪造的源 IP 地址进入网络。

在 SUSE Linux Enterprise Server 中可通过两种方式实施仿假冒措施：

- **使用 `iptables` 规则。这些规则仅允许来自指定接口上特定地址的输入：** 可以在系统设置中明确定义用于通讯的地址空间。任何使用违反这些定义的地址的行为都可能会记录到日志中并触发警报。
- **Linux 内核反向路径过滤：** 此功能会丢弃那些通过不同于初始包的接口的包答复。此功能在 SUSE Linux Enterprise Server 中默认已启用，可使用以下命令检查其启用状态：

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

  如果已启用，此命令会返回 `1`。

1.3.5 仅允许“已建立的”连接进入网络.

`firewalld` 通过 `iptables` 启用连接跟踪。默认会丢弃与标记为外部的接口所建立的连接。只允许与已建立的连接相关联的连接。

可以定义允许哪些服务连接到外部接口。但是，这种定义必须符合常规安全策略。

请记住，防御来自互联网的恶意连接的第一道防线应该是将会处理所有流量并充当把关者的专用防火墙系统。不需要的连接应该一律不能进入 DMZ 网络。不过，SUSE Linux Enterprise Server 系统上的简单防火墙规则可帮助避免错误配置，充当另一道防线。

1.3.7 不要向未获授权方透露私用 IP 地址和路由信息。

SUSE Linux Enterprise Server 系统还可充当路由器，将来自一个接口的流量转发到另一个接口上的另一个网络。可以在外部接口上使用网络地址转换 (NAT)，这样便不会真正向外部公开内部 IP 地址。这种做法的目的是减少外部攻击者只需分析网络流量就能收集到的信息。还可以在通过特定接口连接到外部的虚拟化主机或基于容器的环境中使用 NAT。

3.2 要求 2：不要使用供应商为系统口令和其他安全参数提供的默认值

在安装 SUSE Linux Enterprise Server 期间，管理员已设置一般系统口令。该设置还会使用口令检查器 (**`cracklib`**) 根据某个字典来识别输入的弱口令。这意味着，标准配置已包含客户为大多数服务定义的安全选项。

有关操作系统安全性的详细信息，请参见 SUSE Linux Enterprise Server Security Guide。

2.1 在网络中安装系统之前始终先更改供应商提供的默认值，并去除或禁用不必要的默认帐户。

必须评估所有系统服务的配置是否符合所需的安全标准。这包括将所用的协议限制为仅允许当前安全的版本并禁用旧版实现，以及定义访问控制和身份验证。SUSE Linux Enterprise Server 的默认设置已经能够提供良好的总体安全性，但还可以进一步优化。例如，以下安全性设置可能与此相关：

- 默认情况下，SNMP 守护程序仅允许将传入请求发送到 `localhost`。但是，默认的社区字符串命名为 `public`，应在接受常规入站连接之前加以更改。
- 默认情况下，配置文件 `/etc/ssh/sshd_config` 内的 `sshd` 中已列出并注释掉 `sshd` 守护程序的某些不安全上游设置。例如，已禁用不安全的协议版本 1 和空口令 (`PermitEmptyPasswords no`)。

要进一步提高 SSH 安全性，请通过将 `PermitRootLogin` 设置为 `no` 来拒绝直接的 `root` 访问（如果适用）。

可以通过使用 AutoYaST 配置文件自动执行系统安装来自定义默认设置。这样便可以发布新的 SUSE Linux Enterprise Server 实例，并自动启用已经过评估的配置。可以使用 SUSE Manager 实现此设置过程的自动化。有关详细信息，请参见 https://documentation.suse.com/suma/ 上的 SUSE Manager 文档。

默认情况下，SUSE Linux Enterprise Server 不会创建除 `root` 管理用户以外的其他帐户。`/etc/passwd` 中定义了一些系统帐户，但这些帐户未激活，因此不能直接使用。可以通过检查 `/etc/shadow` 文件中的内容来验证这一点。

在 `/etc/shadow` 中，第二列表示定义的口令：

- 星号 (`*`) 表示从未定义某个口令，因此已锁定相应帐户。
- 感叹号 (`!`) 表示已锁定的帐户，可能会独行显示，也可能显示在口令哈希的前面。

2.2 为所有系统组件制定配置标准。确保这些标准能够解决所有已知安全漏洞，并与行业认可的系统强化标准相一致。

如 PCI DSS 文档中所述，行业接受的安全强化标准的可能来源包括：

1. 互联网安全中心 (CIS)
2. 国际标准化组织 (ISO)
3. SysAdmin 审计网络安全 (SANS) 协会
4. 美国国家标准技术研究院 (NIST)

由于未明确规定 PCI DSS 要求，安全强化标准与具体要求之间没有直接的关系。不过，其他安全强化资源也可为符合这些规范提供帮助，其中包括 SUSE Linux Enterprise Server Security Guide。

2.2.1 为每台服务器仅实施一项主要功能，以防止需要不同安全级别的功能在同一台服务器上共存。（例如，应在不同的服务器上实施 Web 服务器、数据库服务器和 DNS。）

要帮助隔离服务，可以使用 SUSE Linux Enterprise Server 随附的各种虚拟化和容器化方法：KVM、Xen、LXC 和 Docker。

还可以在 VMware ESX 或 Microsoft Hyper-V 等第三方虚拟化服务器上运行 SUSE Linux Enterprise Server 来实现服务隔离。

使用 SUSE Linux Enterprise Server 内置的选项时，请参见：

- 有关虚拟化的信息，请参见SUSE Linux Enterprise Server Virtualization Guide。
- 有关容器化的信息，请参见 SUSE Linux Enterprise Server Docker Open Source Engine Guide。

2.2.2 仅启用正常运行系统所必需的服务、协议、守护程序等。

此规定与要求 1 中的某条规定直接相关：仅允许真正需要且在使用安全协议和设置的服务（1.1.6.b 识别允许的不安全服务、协议和端口；校验是否书面记录了每项服务的安全功能）。所有相关方必须清楚使用不安全通讯存在的风险。研究、明确书面记录并传达使用不安全协议和服务所带来的风险。

使用以下 **`systemctl`** 命令启用和禁用系统服务：

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

要列出系统上安装的所有可用服务及其状态，请使用以下命令：

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

2.2.3.a 检查配置设置，以校验是否书面记录并实施了针对所有不安全服务、守护程序或协议的安全功能。

要对不安全的服务添加额外的安全层，请使用 VPN 隧道（例如 IPsec）。使用 VPN 隧道可以隔离此类服务的网络流量，并防范所有数据遭到内部和外部窃听。但请注意，VPN 隧道端点上的通讯仍不安全，隧道只能作为一种因应措施。

要在 SUSE Linux Enterprise Server 内部提高安全性，请使用 SELinux 或 AppArmor。不过，这些框架的设置不在本文档的范畴内。

- 有关 SELinux 的信息，请参见 SUSE Linux Enterprise Server Security Guide, Chapter Configuring SELinux。
- 有关 AppArmor 的信息，请参见 SUSE Linux Enterprise Server Security Guide, Part Confining Privileges with AppArmor。

2.2.5.a 选择系统组件的样本并检查配置，以校验所有不需要的功能（例如脚本、驱动程序、功能、子系统、文件系统等）是否已去除。

Linux 内核是主要系统组件。它包括一个核心映像，根据硬件和系统设计加载的内核模块会对该映像进行扩展。例如：会根据系统的网卡自动加载网卡驱动程序。可以启用文件系统模块来扩展 Linux 内核的文件系统支持。

加载的内核模块的列表通常很长，其中包含偶尔才使用的模块。内核模块框架允许将模块加入黑名单，以及限制要加载的功能。

要阻止加载模块，请通过 `/etc/modprobe.d` 目录配置这些模块。例如，只有配备软盘驱动器的系统才需要内核模块 `floppy`。在没有软盘驱动器的系统上，可以阻止加载该模块：创建包含以下内容的配置文件 `/etc/modprobe.d/00-disable-modules.conf`：

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

`floppy` 模块通常是在初始 RAM 磁盘执行期间加载的。因此，请使用 **`dracut`** 将此项配置更改传播到 `initrd` 文件（将 `NAME` 替换为当前 initrd 的名称，将 `KERNELVERSION` 替换为当前运行的内核）。

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

去除或限制应用程序功能会更困难，因为大多数情况下，功能已编译到应用程序或库本身之中。甚至通过删除文件也不一定能够干净地去除功能：如果该文件是从某个 RPM 软件包安装的，更新该软件包后就会重新安装该文件。

2.3 使用强加密来加密所有非控制台管理访问。使用 SSH、VPN 或 TLS 等技术进行具有管理权限的 Web 访问及其他非控制台访问。

加密所有管理网络访问：选择的手段应该是 SSH 以及符合安全理念的适当配置设置。

管理访问权限也可以通过网站授予。在这种情况下，必须对浏览器与服务器系统之间的完整连接链进行加密。可以通过 TLS 和 X.509 证书实现此目的。

3.3 要求 3：保护存储的持卡人数据

本节说明如何安全处理持卡人和身份验证数据。以下定义适用：

- 持卡人数据包括持卡人姓名和主帐号 (PAN) 等信息。
- 身份验证数据包括个人识别号 (PIN) 和卡验证码 (CVC2)。

持卡人数据和身份验证数据之间的主要差别在于，绝对不允许存储身份验证数据。相比之下，PAN 等数据是可以存储的，但必须经过加密且不可读，以防攻击者访问这些存储的数据。

用于存储持卡人数据的数据库设计不在本文档的范畴内。不过，您可通过不同的方式加密数据：

- DBMS 可以在数据库模式中使用列级加密。
- 或者，可以加密数据库文件。
- SUSE Linux Enterprise Server 支持全盘加密，因此始终会加密整个数据库存储区。不过，访问加密磁盘的方式与访问非加密磁盘的方式相同。要求 3.4.1 中对此进行了详细介绍。

3.4.1.a 如果使用磁盘加密，请检查配置并观察身份验证流程，以校验对加密文件系统的逻辑访问是否是通过一种与本机操作系统身份验证机制不同的机制（例如，不使用本地用户帐户数据库或一般的网络登录身份凭证）实现的。

PCI DSS 文档中的准则说明对此项要求的规定如下：“全盘加密有助于在磁盘实物丢失时保护数据，因此可能适合用于存储持卡人数据的便携式设备。”

从管理员的角度而言，使用 Linux 统一密钥设置 (LUKS)/dm-crypt 实现的块设备加密可提供一个抽象层，通过该抽象层可以像使用未加密磁盘那样使用加密磁盘。

因此，只能使用文件系统提供的一般 ACL 权限来限制访问控制。要符合此要求，所用的解密密钥不得与任何一般登录身份凭证或身份验证方法相关联。

使用 LUKS 通常可以满足此要求：引导、插入便携式设备或手动挂载磁盘时需要单独输入口令。

LUKS 已完全集成到 SUSE Linux Enterprise Server 中，可以通过 YaST 使用它来创建新分区。

3.4.1.c 检查配置并观察流程，以校验可移动媒体上的持卡人数据是否无论存储在何处都会加密。

如 3.4.1.a 如果使用磁盘加密，请检查配置并观察身份验证流程，以校验对加密文件系统的逻辑访问是否是通过一种与本机操作系统身份验证机制不同的机制（例如，不使用本地用户帐户数据库或一般的网络登录身份凭证）实现的。 中所述，LUKS/dm-crypt 提供的全盘加密可以满足此项要求。用户只能通过挂载磁盘时必须输入的解密口令来访问存储的数据。

3.4 要求 4：对在开放的公共网络上传输的持卡人数据进行加密

在通过不安全的网络传输持卡人数据时必须对这些数据进行加密。理想情况下，应在外部和内部加密所有流量。这样，攻击者便很难获取内部信息以及对持卡人数据环境的特权访问权限。

4.1 通过开放的公共网络传输敏感的持卡人数据期间，使用强加密和安全协议（例如 TLS、IPSEC、SSH 等）保护这些数据，具体措施包括：(1) 仅接受可信的密钥和证书；(2) 使用的协议仅支持安全版本或配置；(3) 加密强度适合所用的加密方法。

必须防范传输敏感信息的连接遭到窃听和篡改。

对于传入的客户端请求，请结合使用 HTTPS 协议与安全的 TLS 连接。使用 X.509 公共证书进行身份验证，该证书在一定程度上能够证实服务器正是客户要访问的那个端点。

SUSE Linux Enterprise Server 随附了一组可让 HTTPS 连接受到保护的服务和工具。例如，可以直接使用 Apache HTTP Server 或通过 **`stunnel`**（充当代理来提供 TLS 加密功能）提供这种保护。

可以使用 IPsec 或其他 VPN 技术来保护通过公共网络连接的网段之间的连接。还可以使用 X.509 公共证书保护此类连接。对于内部用途，可以使用私用证书颁发机构 (CA) 来为 X.509 证书签名以及跟踪可信密钥。

在 SUSE Linux Enterprise Server 中，可以直接通过 strongSwan（一个基于 IPsec 的 VPN 解决方案）或通过 OpenVPN（使用自定义安全协议）来确保做到这一点。

要管理操作系统，请使用 SSH。有关配置 SSH 以提供更高安全性的信息，请参见第 3.1 节 “要求 1：安装并维护防火墙配置以保护持卡人数据”和第 3.2 节 “要求 2：不要使用供应商为系统口令和其他安全参数提供的默认值”。

3.5 要求 5：保护所有系统免遭恶意软件的攻击，并定期更新防病毒软件或程序

要符合 PCI DSS 规范，需要防御恶意软件的攻击。可以使用主流防病毒软件供应商提供的第三方防病毒软件，并将其集成到 Linux 环境中。SUSE Linux Enterprise Server 随附了开源的防病毒引擎 ClamAV。

ClamAV 可提供一组有限的扫描功能，与第三方产品相比性能有限。因此，ClamAV 预期只能提供基本保护。

另一方面，由于 ClamAV 是 SUSE Linux Enterprise Server 随附的，在安装服务器期间可将其一并安装。这样就可以轻松满足此要求，但也需要清楚地知道它与第三方产品相比存在的缺点。

3.6 要求 6：开发并维护安全系统和应用程序

此项要求的主要部分涉及到内部软件开发、文档和设计问题，超出了本文档的范畴。不过，SUSE Linux Enterprise Server 提供了帮助确保系统安全的工具：

- 软件包管理器 Zypper 是 SUSE Linux Enterprise Server 的一个强大工具。除其他众多功能外，它还能解析软件包、产品、软件集和补丁的依赖关系，具有一项锁定机制用于防止安装软件包，并提供了一个完整的更新堆栈，用于确保系统处于最新状态并使其能够防范已知安全问题。

  `zypper` 是所有 SUSE Linux Enterprise Server 安装的组成部分，当系统注册之后便可直接访问更新储存库。

  有关 Zypper 的信息，请参见 SUSE Linux Enterprise Server Administration Guide, Chapter Managing Software with Command Line Tools, Section Using Zypper。

- SUSE 提供了 SUSE Manager 用于进行系统管理，该程序提供了有效的方法确保系统处于最新状态。它提供 SUSE Linux Enterprise Server 和 Red Hat Enterprise Linux 客户端系统的无缝管理。在大型系统环境中，当您需要检查每个系统的当前更新状态以及需要应对已知安全问题时，这一点极为有用。

  有关 SUSE Manager 的信息，请参见 SUSE Manager documentation page (https://documentation.suse.com/suma/)。

6.2.a 检查与安全补丁安装相关的策略和过程，以校验是否定义了以下操作的流程：(1) 在供应商发布适用关键安全补丁后的一个月内安装这些补丁；(2) 在适当时间范围内（例如三个月内）安装供应商提供的所有适用安全补丁。

要识别需要安装以保护系统安全的补丁，请执行以下操作：

首先刷新所有储存库，以获得最新信息：

```
> sudo zypper refresh
```

然后使用 Zypper 的补丁相关命令：

- 搜索尚未安装的重要安全修复程序：

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

- 也可以搜索 CVE 或 SUSE Bugzilla 编号。默认情况下，此命令只会列出必要的补丁。要同时显示已安装的补丁，请使用参数 `--all`：

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

- 要列出单个补丁的细节，请使用 **`patch-info`** 子命令：

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

- 要仅安装重要的安全补丁，请使用 **`patch`** 子命令：

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

要自动执行更新，可以使用所有 Zypper 子命令都支持的 `--non-interactive` 参数。有关 Zypper 的详细信息，请参见 SUSE Linux Enterprise Server Administration Guide, Chapter Managing Software with Command Line Tools, Section Using Zypper。

3.7 要求 7：限制企业仅可访问其需要知道的持卡人数据

操作系统访问控制是个复杂的主题。同样，此项 PCI DSS 要求并无明确规定，也未具体指出需要实施哪种程度的限制。SUSE Linux Enterprise Server 随附了用于限制对特定系统区域和组件的访问的所有常规 Linux 工具：

- 可以使用传统的 Unix 权限设置通过特定的用户和用户组来控制访问。

有关管理权限的信息，请参见 SUSE Linux Enterprise Server Security Guide, Chapter Access Control Lists in Linux。

- 一种适用于文件系统的更灵活的机制是访问控制列表 (ACL)，它可提供更精细的控制方式。SELinux 能够实现最高的系统隔离性，并可防止进程获得超出允许范围的资源和访问权限。SELinux 和 AppArmor 不在本文档的范畴内，但应该利用它们来保护可能会被攻击者针对的关键系统。
  - 有关 SELinux 的信息，请参见 SUSE Linux Enterprise Server Security Guide, Chapter Configuring SELinux。
  - 有关 AppArmor 的信息，请参见 SUSE Linux Enterprise Server Security Guide, Part Confining Privileges with AppArmor。

7.1.2 将特权用户 ID 的访问权限限制为履行职责所必需的最低特权。

标准 Unix 权限允许为用户和组 ID 设置 Read、Write 和 Execution 标志。名为 `others` 或 `world` 的常规组定义了不适合加入前两个组的用户的访问权限。这提供了一种简单直接的方法来授予或拒绝对文件系统资源的访问权限。

ACL 提供了额外的限制级别。使用它可为一个用户 ID 设置读写访问权限，并为另一个用户 ID 仅设置读取访问权限。对于组 ID 也可以采用这样的设置。

使用 **`getfacl`** 和 **`setfacl`** 命令（随附在 SUSE Linux Enterprise Server 的 `acl` 软件包中）可以直接修改文件系统资源。例如，要针对用户 `wilber` 检查和设置 `/tmp/test.txt` 文件的 ACL 限制，请执行以下命令：

```
> 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--
```

标准 Unix 权限包括所谓的粘滞位。这允许使用比正在执行特定程序的用户更高的特权来执行这些程序。此功能最典型的示例是 **passwd** 工具，它需要修改 /etc/shadow 才能更改用户口令。

要以更循序渐进的方式明确允许对二进制文件的特定操作或行为，请使用扩展功能。一个默认使用扩展功能的示例命令是 **ping**（包含在软件包 iputils 中）。

ping 通过网卡发送 ICMP IP 包。为此，它需要将 CAP_NET_RAW 功能设置为“有效且允许”（+ep）：

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

可以使用可插入身份验证模块 (PAM) 来管理系统的登录访问控制。SUSE Linux Enterprise Server 中提供了多个模块，允许记录登录时间、多个身份验证机制以及中心数据库（例如 NIS、LDAP 或 Active Directory）等设置。

有关管理权限的详细信息，请参见 SUSE Linux Enterprise Server Security Guide, Chapter Access Control Lists in Linux。

3.8 要求 8：识别并验证对系统组件的访问

理想情况下，应使用包含用户信息的中心数据库以及唯一标识符 (UID) 来授予或拒绝对特定系统组件的访问权限。这样就可以轻松为管理员授予对一组服务器的特殊访问权限，或者为数据库工程师授予对特定 DBMS 系统的权限。

在独立服务器上，唯一标识符通过标准 Linux 用户和组 ID 来管理。这些 ID 列在 /etc/passwd 和 /etc/group 中。

8.1.4 去除/禁用在 90 天内处于非活动状态的用户帐户。

在此环境中，对用户帐户使用集中式基础架构（例如 NIS、LDAP 或 Active Directory）会带来许多优势：

- 可轻松识别并自动禁用非活动的帐户。
- 只需在一个位置禁用用户帐户。撤消用户的访问权限后，他们将无法使用任何依赖于集中式帐户基础架构的服务。

不过，如果您使用的是本地帐户，可以在用户登录时检查它们是否为非活动帐户。此模块会检查 `/var/log/lastlog` 中记录的上次登录时间，并计算该时间距离此时的天数。默认情况下，当非活动天数达到 90 天时，将会拒绝访问。
要列出本地帐户的上次登录时间，请使用 **`lastlog`** 命令。

8.1.6 通过在用户 ID 尝试访问最多六次后锁定该 ID 来限制重复的访问尝试。

如 8.1.4 去除/禁用在 90 天内处于非活动状态的用户帐户。 中所述，集中式帐户基础架构可提供此功能。在 SUSE Linux Enterprise Server 系统上，可以使用 `pam_tally2` PAM 模块检查和限制访问尝试。该模块将在登录时执行，会检查自上次成功登录以来所记录的失败尝试。要检查和重置帐户状态，请使用 **`pam_tally2`** 工具。

8.1.7 将锁定持续时间设置为最少 30 分钟或直到管理员启用了该用户 ID。

8.1.6 通过在用户 ID 尝试访问最多六次后锁定该 ID 来限制重复的访问尝试。 中所述的 PAM 模块 `pam_tally2` 可用于在登录尝试失败后，将帐户锁定一段指定的时间。必须在 PAM 配置中指定 `unlock_time=1800` 参数。默认情况下，只有管理员能够重新激活锁定的帐户。

8.3.1 针对进行管理访问的人员，将用于所有非控制台访问的多重身份验证纳入 CDE 中。

要使用多重验证机制验证进行管理访问的用户的身份，请使用以下方法：

- 使用可插入身份验证模块 (PAM)：这可以提高将新方法添加到身份验证流程以及调整该流程时的灵活性。
  第三方一次性口令 (OTP) 产品通常也有一个 Linux PAM 模块。
  有关 PAM 的信息，请参见 SUSE Linux Enterprise Server Security Guide, Chapter Authentication with PAM。
- 要为 SSH 连接添加多重身份验证，除了使用口令外，还必须使用公共密钥。
  要连接到某个系统，您必须证明自己拥有相应的私用密钥，然后在第二阶段输入口令。这意味着，攻击者需要先获取私用密钥才能尝试强行突破口令提示。

8.3.2 针对源自实体网络外部的所有远程网络访问（用户和管理员的访问，包括为了支持或维护目的而进行的第三方访问）纳入多重身份验证。

有关详细信息，请参见 8.3.1 针对进行管理访问的人员，将用于所有非控制台访问的多重身份验证纳入 CDE 中。

3.9 要求 9：限制对持卡人数据的物理访问

对用于处理持卡人数据的系统的物理访问不属于一般操作系统安全性的范围。如要允许现场人员和访客直接访问系统，必须实施适当的机构出入管控措施。

3.10 要求 10：跟踪并监控对网络资源和持卡人数据的所有访问

要跟踪用户活动，必须提供一个同步的时间参考。可以通过 NTP 协议实现此目的。NTP 允许服务器将其本地时间与中心系统保持同步。持卡人数据环境 (CDE) 内部的中心 NTP 服务器不应依赖于通过连接外部互联网来更新系统时间。作为替代方法，可以使用 DCF77 无线电传输或 GPS 接收器更新系统时间。

使用同步时间参考可以更轻松地关联所记录的日志文件中的事件。此参考可以包括中心系统日志服务器收集的一般系统日志项，或 `audit` 守护程序生成的内核审计消息。

有关审计的信息，请参见 SUSE Linux Enterprise Server, Security Guide, Part The Linux Audit Framework。

可以通过定义集中存储的审计规则来满足本节中所述的所有审计要求。

3.11 要求 11：定期测试安全系统和流程

测试所述安全机制也是 PCI DSS 的一项关键要求。评估配置并测试日志记录机制可以防范已知安全风险，并确保能够提供必要的信息来识别可能的安全违规。在进行系统设计期间，应考虑在安装和部署前对各项功能进行测试。

SUSE Linux Enterprise Server 随附了高级入侵检测环境 (AIDE)，用于跟踪系统完整性。AIDE 会创建所有相关操作系统文件的哈希值数据库。初始化后，可以使用它来校验以前保存的所有文件的完整性。要采用 AIDE，最好定期创建数据库快照并将其保存到一个中心系统，以便在此系统上评估可能发生的修改。

有关 AIDE 的详细信息，请参见 SUSE Linux Enterprise Server Security Guide, Chapter Intrusion Detection with AIDE。

3.12 要求 12：维护用于处理所有个人信息安全性的策略

需要处理宝贵信息的任何组织都应实施一项常规安全策略。策略应包括所有相关方面，使员工和利益相关者能够清楚地知道存在哪些可能的风险，以及如何避免这些风险。

此外，应定期评估所有安全策略并做出调整，以尽量保持最高的保护级别。

4 法律声明

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.