腾讯云默认合规镜像

技术手册

2020-03-24

腾讯云计算北京有限责任公司

文档控制

文档名称	腾讯云默认合规镜像技术手册
保密级别	公开
拟制	腾讯云计算（北京）有限责任公司
审核	腾讯云计算（北京）有限责任公司
标准化	腾讯云计算（北京）有限责任公司

目 录

1 概述

腾讯云合规镜像是基于腾讯云官方公共镜像，根据《GB/T22239-2019 信息安全技术网络安全等级保护基本要求》进行安全加固的镜像，用户使用本镜像无需额外配置即可满足等保合规要求。

2 安全特性

合规镜像依据国家最新等保 2.0 标准进行适配研发，其具备等保合规技术要求中的大部分可落地功能，如下为等保合规部分技术要求参考：

2.1 身份鉴别

（1）对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。

（2）具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

（3）进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；

（4）采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

2.2 访问控制

（1）对登录的用户分配账户和权限；

（2）重命名或删除默认账户，修改默认账户的默认口令；

（3）及时删除或停用多余的、过期的账户，避免共享账户的存在；

（4）授予管理用户所需的最小权限，实现管理用户的权限分离；

（5）由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；

（6）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；

2.3 安全审计

（1）启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

（2）审计记录应包括事件的日期和时间、事件类型、主体标识、客体标识和结果等；

（3）对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

（4）对审计进程进行保护，防止未经授权的中断。

2.4 入侵防范

（1）遵循最小安装的原则，仅安装需要的组件和应用程序；

（2）关闭不需要的系统服务、默认共享和高危端口；

（3）通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

（4）提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

（5）能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；

（6）能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

2.5 恶意代码防范

采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。

2.6 可信验证

基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

3 产品使用

3.1 用户登录

按照《GB/T22239-2019 信息安全技术网络安全等级保护基本要求》中“身份鉴别”相关要求，“应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换”。 因此，根据业务需要，创建用户组与相应的用户。建议创建管理组、审计组与相应的用户，若服务器为数据库服务器，同时建议创建数据库管理组与数据库管理员。

为了避免影响用户使用，在初始化合规镜像中并没有做此项限制，用户可以通过 root 用户登录系统后执行 /root/user_init.sh 来实现此项加固。

执行之后，系统将创建三个用户：

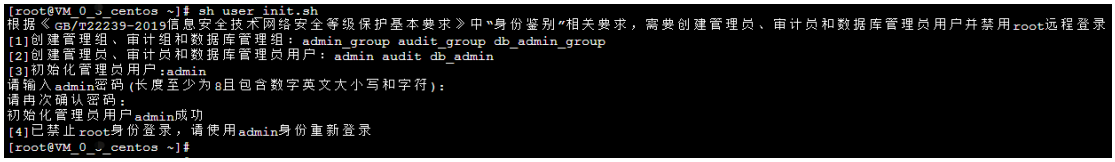
用户名	角色	备注
admin	管理员	常用于应用部署、日常运维操作管理
audit	审计员	常用于查看和审计系统操作日志等
db_admin	数据库管理员	常用于数据库日常操作管理

三个用户将分别加入相应的用户组中：

admin_group	管理组
audit_group	审计组
db_admin_group	数据库管理组

同时将会设置禁止 root 用户远程登录系统，请使用 admin 用户登录系统。

执行效果：



3.2 访问控制

按照《GB/T22239-2019 信息安全技术网络安全等级保护基本要求》中“入侵防范”部分的合规要求，需要限制操作系统重要服务对外开放。当前合规镜像仅仅允许外部访问本地 ssh 服务，其他服务默认禁止访问。如果需要对外开放服务，请手工放开 iptables 限制。

举例：如果需要将本地 80 端口的 http 服务开放外部访问，可以切换到 root 用户执行命令：

```
su root
iptables -I INPUT -p tcp --dport 80 -j ACCEPT
service iptables save
service iptables restart
```